Documentation StorageGRID 11.7

StorageGRID

NetApp
December 04, 2025

This PDF was generated from https://docs.netapp.com/fr-fr/storagegrid-117/index.html on December 04, 2025. Always check docs.netapp.com for the latest.

Sommaire

Documentation StorageGRID 11.7 . . . 1
Notes de mise à jour . . . 2
Commencez . . . 3
Découvrez StorageGRID . . . 3
Qu'est-ce que StorageGRID ? . . . 3
Clouds hybrides avec StorageGRID . . . 6
Architecture StorageGRID et topologie réseau . . . 7
La gestion des données par StorageGRID . . . 16
Découvrez StorageGRID . . . 29
Instructions de mise en réseau . . . 41
Directives de mise en réseau : présentation . . . 41
Types de réseau StorageGRID . . . 42
Exemples de topologie réseau . . . 46
Configuration réseau requise . . . 54
Exigences spécifiques au réseau . . . 55
Considérations relatives au réseau propres au déploiement . . . 57
Installation et provisionnement réseau . . . 60
Instructions de post-installation . . . 61
Référence du port réseau . . . 61
Démarrage rapide pour StorageGRID . . . 72
Installation et mise à niveau . . . 75
Installez le matériel de l'appliance . . . 75
Démarrage rapide pour l'installation du matériel . . . 75
Présentation du matériel . . . 76
Avant l'installation . . . 104
Automatisez l'installation et la configuration de l'appliance . . . 150
Automatisez la configuration de StorageGRID . . . 156
Présentation de l'installation des API REST . . . 157
Installer le matériel de fixation . . . 159
Configurer le matériel . . . 199
Déployez le nœud de l'appliance . . . 249
Installez Red Hat Enterprise Linux ou CentOS . . . 286
Installez Red Hat Enterprise Linux ou CentOS: Présentation . . . 286
Planifiez et préparez-vous pour l'installation de Red Hat ou CentOS . . . 287
Déploiement de nœuds de grid virtuel (Red Hat ou CentOS) . . . 311
Configurer le grid et l'installation complète (Red Hat ou CentOS) . . . 331
Automatisation de l'installation (Red Hat Enterprise Linux ou CentOS) . . . 345
Présentation de l'API REST d'installation . . . 348
Par où aller plus loin . . . 349
Résoudre les problèmes d'installation . . . 350
Exemple /etc/sysconfig/network-scripts . . . 350
Installez Ubuntu ou Debian . . . 352
Installer Ubuntu ou Debian: Présentation . . . 352

Planifier et préparer l'installation d'Ubuntu ou de Debian . . . 353
Déploiement de nœuds de grid virtuel (Ubuntu ou Debian) . . . 377
Configurer la grille et l'installation complète (Ubuntu ou Debian) . . . 397
Automatisation de l'installation (Ubuntu ou Debian) . . . 411
Présentation de l'API REST d'installation . . . 414
Par où aller plus loin . . . 415
Résoudre les problèmes d'installation . . . 416
Exemple /etc/network/interfaces . . . 416
Installez VMware . . . 418
Installer VMware : présentation . . . 418
Planification et préparation de l'installation VMware . . . 419
Déploiement de nœuds grid de machine virtuelle (VMware) . . . 427
Configuration du grid et installation complète (VMware) . . . 436
Automatisation de l'installation (VMware) . . . 450
Présentation de l'API REST d'installation . . . 464
Par où aller plus loin . . . 465
Résoudre les problèmes d'installation . . . 466
Mettez à niveau le logiciel StorageGRID . . . 467
Mettre à niveau le logiciel StorageGRID : présentation . . . 467
Nouveautés d'StorageGRID 11.7 . . . 467
Fonctions supprimées ou obsolètes . . . 472
Modifications apportées à l'API de gestion du grid . . . 474
Modifications apportées à l'API de gestion des locataires . . . 474
Planifiez et préparez la mise à niveau . . . 475
Mise à niveau du logiciel . . . 483
Résoudre les problèmes de mise à niveau . . . 491
Configurez et gérez . . . 494
Administrer StorageGRID . . . 494
StorageGRID d'administration : présentation . . . 494
Lancez-vous avec Grid Manager . . . 494
Contrôle de l'accès à StorageGRID . . . 526
Utiliser la fédération de grille . . . 575
Gérer la sécurité . . . 613
Gérer les locataires . . . 688
Configurer les connexions client . . . 708
Gestion des réseaux et des connexions . . . 750
Utiliser AutoSupport . . . 767
Gérer des nœuds de stockage . . . 782
Gérer les nœuds d'administration . . . 806
Gérer les nœuds d'archivage . . . 816
Migrer les données vers StorageGRID . . . 838
Gestion des objets avec ILM . . . 841
Gérez les objets avec ILM : présentation . . . 841
ILM et cycle de vie des objets . . . 842
Créer et attribuer des notes de stockage . . . 863

Utiliser des pools de stockage . . . 865
Utilisation des pools de stockage cloud . . . 874
Gestion des profils de code d'effacement . . . 895
Configuration des régions (facultatif et S3 uniquement) . . . 899
Création d'une règle ILM . . . 901
Création de la règle ILM . . . 918
Utilisation des règles ILM et ILM . . . 934
Utilisez le verrouillage d'objet S3 . . . 938
Exemples de règles et de règles ILM . . . 948
Durcissement du système . . . 968
Durcissement du système : vue d'ensemble . . . 968
Directives de renforcement des mises à niveau logicielles . . . 968
Instructions de renforcement des réseaux StorageGRID . . . 969
Instructions de renforcement pour les nœuds StorageGRID . . . 970
Instructions de renforcement pour TLS et SSH . . . 973
Autres directives de durcissement . . . 974
Configuration de StorageGRID pour FabricPool . . . 975
Configurer StorageGRID pour FabricPool : présentation . . . 975
Informations nécessaires pour rattacher StorageGRID à un niveau cloud . . . 977
Utilisez l'assistant d'installation FabricPool . . . 978
Configurez StorageGRID manuellement . . . 993
Configuration de ONTAP System Manager . . . 1004
Configurer le serveur DNS . . . 1006
Meilleures pratiques StorageGRID pour FabricPool . . . 1006
Supprimez les données FabricPool de StorageGRID . . . 1011
Utiliser StorageGRID . . . 1012
Utilisez un compte de locataire . . . 1012
Utilisez un compte de locataire : présentation . . . 1012
Comment se connecter et se déconnecter . . . 1013
Présentation du tableau de bord du gestionnaire de locataires . . . 1018
API de gestion des locataires . . . 1021
Utiliser les connexions de fédération de grille . . . 1026
Gestion des groupes et des utilisateurs . . . 1039
Gestion des clés d'accès S3 . . . 1058
Gestion des compartiments S3 . . . 1064
Gérez les services de la plateforme S3 . . . 1085
UTILISEZ L'API REST S3 . . . 1128
Versions et mises à jour prises en charge par l'API REST S3 . . . 1128
Référence rapide : demandes d'API S3 prises en charge . . . 1131
Configurez les comptes et les connexions des locataires . . . 1149
La prise en charge des services de plateforme StorageGRID . . . 1152
Implémentation de l'API REST S3 par StorageGRID . . . 1153
Prise en charge de l'API REST Amazon S3 . . . 1171
Requêtes StorageGRID S3 . . . 1221
Règles d'accès au compartiment et au groupe . . . 1242

Configuration de la sécurité pour l'API REST . . . 1268
Surveiller et auditer les opérations . . . 1270
Avantages des connexions HTTP actives, inactives et simultanées . . . 1273
Utiliser l'API REST de Swift (obsolète) . . . 1276
Utilisez l'API REST de Swift : présentation . . . 1276
Configurez les comptes et les connexions des locataires . . . 1279
Opérations prises en charge par l'API REST Swift . . . 1283
Opérations de l'API REST StorageGRID Swift . . . 1296
Configuration de la sécurité pour l'API REST . . . 1299
Surveiller et auditer les opérations . . . 1301
Surveiller et résoudre les problèmes . . . 1306
Surveiller le système StorageGRID . . . 1306
Surveillance d'un système StorageGRID : présentation . . . 1306
Affichez et gérez le tableau de bord . . . 1306
Afficher la page nœuds . . . 1309
Informations à surveiller régulièrement . . . 1345
Alertes et alarmes . . . 1374
Référence des fichiers journaux . . . 1468
Configurez les messages d'audit et les destinations des journaux . . . 1487
Utiliser un serveur syslog externe . . . 1491
Utiliser la surveillance SNMP . . . 1504
Collecte de données StorageGRID supplémentaires . . . 1520
Dépanner le système StorageGRID . . . 1555
Dépannage d'un système StorageGRID : présentation . . . 1555
Résoudre les problèmes liés au stockage et aux objets . . . 1564
Diagnostiquez les problèmes liés aux métadonnées . . . 1601
Résoudre les erreurs de certificat . . . 1608
Résolution des problèmes liés au nœud d'administration et à l'interface utilisateur . . . 1609
Résolution des problèmes de réseau, de matériel et de plateforme . . . 1614
Dépanner un serveur syslog externe . . . 1623
Examiner les journaux d'audit . . . 1626
Examiner les journaux d'audit : présentation . . . 1626
Flux et conservation des messages d'audit . . . 1627
Accéder au fichier journal d'audit . . . 1629
Rotation du fichier journal d'audit . . . 1630
Format du fichier journal d'audit . . . 1631
Format du message d'audit . . . 1644
Messages d'audit et cycle de vie de l'objet . . . 1648
Messages d'audit . . . 1656
Maintenance . . . 1711
Développez votre grille . . . 1711
Développez votre grille : présentation . . . 1711
Planifiez l'extension de StorageGRID . . . 1712
Rassembler les matériaux nécessaires . . . 1722
Ajout de volumes de stockage . . . 1730

Ajout de nœuds grid ou d'un site . . . 1738
Configuration du système faisant l'objet de l'extension . . . 1753
Contactez l'assistance technique . . . 1763
Restaurez les nœuds et gérez votre grid . . . 1764
Restauration et maintenance : vue d'ensemble . . . 1764
Téléchargez le progiciel de restauration . . . 1765
Procédure de correctif StorageGRID . . . 1765
Procédures de restauration des nœuds de la grille . . . 1773
Comment la reprise sur site est effectuée par le support technique . . . 1893
Procédure de mise hors service . . . 1895
Renommez la grille, les sites et les nœuds . . . 1948
Procédures de maintenance du réseau . . . 1958
Procédures au niveau de l'hôte et du middleware . . . 1986
Procédures des nœuds de la grille . . . 1994
Maintenance de la configuration de l'appliance . . . 2018
Procédures courantes de maintenance des nœuds : présentation . . . 2018
Mettez l'appareil en mode maintenance . . . 2019
Modifier le paramètre MTU . . . 2021
Vérifiez la configuration du serveur DNS . . . 2023
Mettre à jour les références d'adresse MAC . . . 2026
Surveillez le chiffrement des nœuds en mode de maintenance . . . 2027
Clonage de nœuds d'appliance . . . 2032
Maintenance du matériel SGF6112 . . . 2039
Maintenance de l'appliance SGF6112 . . . 2039
Procédures de maintenance de la configuration . . . 2040
Procédures de maintenance du matériel . . . 2046
Maintenance du matériel SG6000 . . . 2079
Entretenir l'appareil SG6000 . . . 2079
Procédures de configuration de la maintenance . . . 2080
Procédures matérielles . . . 2105
Maintenance du matériel SG5700 . . . 2137
Conservez l'appliance SG5700 . . . 2137
Procédures de configuration de la maintenance . . . 2137
Procédures matérielles . . . 2157
Conservez l'appliance SG5600 . . . 2173
Maintenance du matériel SG100 et SG1000 . . . 2173
Maintenance des appliances SG100 et SG1000 . . . 2173
Procédures de configuration de la maintenance . . . 2173
Procédures matérielles . . . 2178
Activation de StorageGRID dans votre environnement . . . 2188
Mentions légales . . . 2189
Droits d'auteur . . . 2189
Marques déposées . . . 2189
Brevets . . . 2189
Politique de confidentialité . . . 2189

Source ouverte 2189

Documentation StorageGRID 11.7

Notes de mise à jour

Obtention d’informations spécifiques à la version sur les nouvelles fonctionnalités, les fonctions supprimées ou obsolètes, les problèmes résolus et les problèmes connus.

Connectez-vous au site de support NetApp à "Afficher ou télécharger un fichier PDF" Contenant les notes de version de StorageGRID 11.7.

Commencez

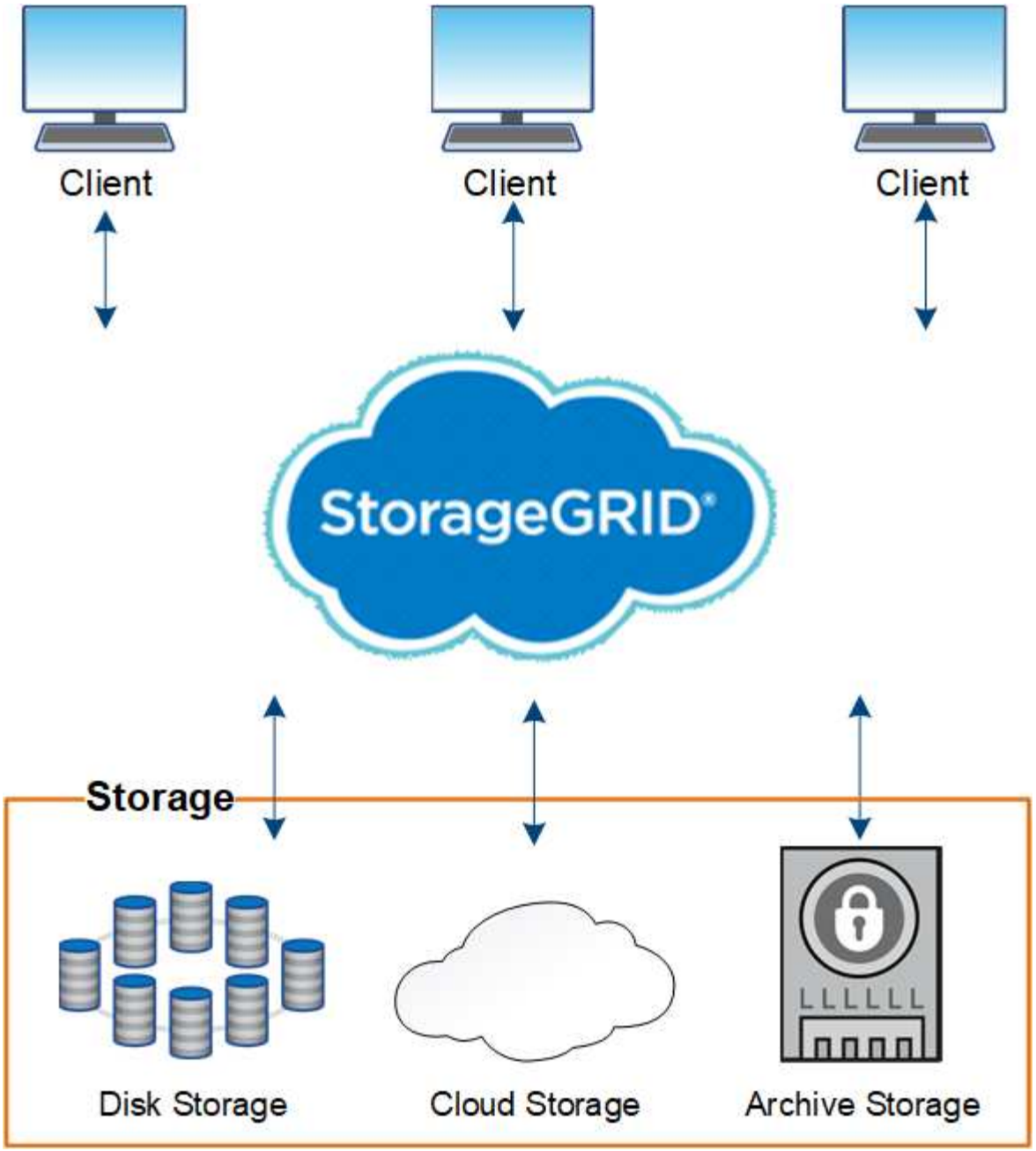
Découvrez StorageGRID

Qu’est-ce que StorageGRID ?

NetApp® StorageGRID® est une suite de stockage objet Software-defined qui prend en charge un large éventail d’utilisations dans les environnements multiclouds publics, privés et hybrides. StorageGRID offre une prise en charge native de l’API Amazon S3 et propose des innovations de pointe, telles que la gestion automatisée du cycle de vie, pour stocker, sécuriser, protéger et conserver les données non structurées de manière économique sur de longues périodes.

StorageGRID offre un stockage sécurisé et durable pour les données non structurées à grande échelle. Des règles intégrées de gestion du cycle de vie basées sur des métadonnées optimisent l’emplacement des données tout au long de leur vie. Les contenus sont placés au bon endroit, au bon moment et sur le Tier de stockage adéquat pour réduire les coûts.

StorageGRID se compose de nœuds hétérogènes, redondants et répartis géographiquement, qui peuvent être intégrés aux applications client existantes et nouvelle génération.



La prise en charge des nœuds d'archivage (pour l'archivage dans le cloud à l'aide de l'API S3 et l'archivage sur bande à l'aide du middleware TSM) est obsolète et sera supprimée dans une prochaine version. Le déplacement d'objets d'un nœud d'archivage vers un système de stockage d'archives externe a été remplacé par les pools de stockage cloud ILM pour offrir davantage de fonctionnalités.

Avantages de StorageGRID

La baie StorageGRID présente plusieurs avantages :

- Référentiel de données distribué géographiquement extrêmement évolutif et facile à utiliser pour les données non structurées.
- Protocoles de stockage objet standard :
  - Amazon Web Services simple Storage Service (S3)

- OpenStack Swift

> La prise en charge des applications du client Swift a été obsolète et sera supprimée dans une prochaine version.

- Compatibilité avec le cloud hybride. La gestion du cycle de vie des informations basée sur des règles stocke les objets dans des clouds publics, notamment Amazon Web Services (AWS) et Microsoft Azure. Les services de plateforme StorageGRID permettent la réplication de contenu, la notification d'événements et la recherche de métadonnées d'objets stockés dans les clouds publics.
- Protection flexible des données pour assurer la durabilité et la disponibilité. Les données peuvent être protégées au moyen de la réplication et du code d'effacement à plusieurs couches. La vérification des données au repos et à la volée garantit l'intégrité des données conservées à long terme.
- Gestion dynamique du cycle de vie des données pour vous aider à gérer les coûts de stockage. Vous pouvez créer des règles ILM pour gérer le cycle de vie des données au niveau de l'objet, et personnaliser la localisation, la durabilité, les performances, les coûts et la durée de conservation des données.
- Haute disponibilité du stockage de données et certaines fonctions de gestion, avec équilibrage de la charge intégré pour optimiser la charge de données sur les ressources StorageGRID.
- Prise en charge de plusieurs comptes de locataires de stockage pour isoler les objets stockés sur votre système par des entités différentes.
- De nombreux outils de contrôle de l'état de santé de votre système StorageGRID, notamment un système d'alertes complet, un tableau de bord graphique et des États détaillés pour tous les nœuds et sites.
- Prise en charge des déploiements logiciels ou matériels. Vous pouvez déployer StorageGRID sur l'un des éléments suivants :
  - Ordinateurs virtuels exécutés dans VMware.
  - Moteurs de mise en conteneurs sur hôtes Linux.
  - Appliances StorageGRID spécialisées.
    - Les appliances de stockage fournissent le stockage objet.
    - Les appliances de services proposent des services d'administration du grid et d'équilibrage de la charge.
- Conformité avec les exigences pertinentes de ces réglementations en matière de stockage :
  - Securities and Exchange Commission (SEC), in 17 CFR § 240.17a-4(f), qui réglemente les membres, courtiers ou courtiers en bourse.
  - Autorité de réglementation du secteur financier (FINRA) règle 4511(c) qui diffère du format et des exigences médias de la règle SEC 17a-4(f).
  - La Commodity futures Trading Commission (CFTC) dans le règlement 17 CFR § 1.31(c)-(d), qui réglemente la négociation des marchandises à terme.
- Les opérations de mise à niveau et de maintenance sans interruption. Maintenez l'accès au contenu lors des procédures de mise à niveau, d'extension, de déclassement et de maintenance.
- Gestion fédérée des identités. S'intègre à Active Directory, OpenLDAP ou Oracle Directory Service pour l'authentification des utilisateurs. Prise en charge de l'authentification unique (SSO) à l'aide de la norme SAML 2.0 (Security assertion Markup Language 2.0) pour échanger les données d'authentification et d'autorisation entre StorageGRID et Active Directory Federation Services (AD FS).

Clouds hybrides avec StorageGRID

Utilisez StorageGRID dans une configuration de cloud hybride en implémentant la gestion des données pilotée par des règles pour stocker les objets dans les pools de stockage cloud, en exploitant les services de plateforme StorageGRID et en transférant les données de ONTAP vers StorageGRID avec NetApp FabricPool.

Pools de stockage cloud

Vous pouvez stocker des objets en dehors du système StorageGRID grâce aux pools de stockage cloud. Par exemple, vous pouvez déplacer les objets rarement consultés vers un stockage cloud moins coûteux, comme Amazon S3 Glacier, S3 Glacier Deep Archive, Google Cloud ou le Tier d'accès Archive dans le stockage Microsoft Azure Blob. Vous pouvez également conserver une sauvegarde dans le cloud d'objets StorageGRID qui peuvent être utilisés pour restaurer des données perdues en raison d'un volume de stockage ou d'une défaillance du nœud de stockage.

Le stockage de partenaires tiers est également pris en charge, y compris le stockage sur disque et sur bande.

> ⓘ L'utilisation de pools de stockage cloud avec FabricPool n'est pas prise en charge en raison de la latence ajoutée pour extraire un objet de la cible du pool de stockage cloud.

Services de plateforme S3

Les services de plateforme S3 vous permettent d'utiliser des services distants comme terminaux pour la réplication d'objets, les notifications d'événements ou l'intégration de la recherche. Les services de plateforme fonctionnent indépendamment des règles ILM du grid et sont activés pour les compartiments S3 individuels. Les services suivants sont pris en charge :

- Le service de réplication CloudMirror met automatiquement en miroir les objets spécifiés dans un compartiment S3 cible, qui peut se trouver sur Amazon S3 ou sur un second système StorageGRID.
- Le service de notification d'événements envoie des messages concernant des actions spécifiées à un terminal externe qui prend en charge la réception d'événements Amazon SNS (simple notification Service).
- Le service d'intégration de recherche envoie les métadonnées d'objet à un service Elasticsearch externe, ce qui permet de rechercher, de visualiser et d'analyser les métadonnées à l'aide d'outils tiers.

Vous pouvez, par exemple, utiliser la réplication CloudMirror pour mettre en miroir des enregistrements client spécifiques dans Amazon S3, puis exploiter les services AWS pour analyser vos données.

Tiering des données ONTAP avec FabricPool

Vous pouvez réduire le coût du stockage ONTAP grâce au Tiering des données vers StorageGRID à l'aide de FabricPool. FabricPool permet le Tiering automatisé des données vers des tiers de stockage objet à faible coût, sur site ou hors site.

Contrairement aux solutions de hiérarchisation manuelle, FabricPool réduit le TCO en automatisant la hiérarchisation des données pour réduire le coût de stockage. Et offre les avantages du modèle économique du cloud grâce à son Tiering dans les clouds publics et privés y compris StorageGRID.

Informations associées

- "Qu'est-ce que le pool de stockage cloud ?"
- "Qu'est-ce que les services de plateforme ?"

- "Configuration de StorageGRID pour FabricPool"

Architecture StorageGRID et topologie réseau

Un système StorageGRID se compose de plusieurs types de nœuds grid sur un ou plusieurs sites de data Center.

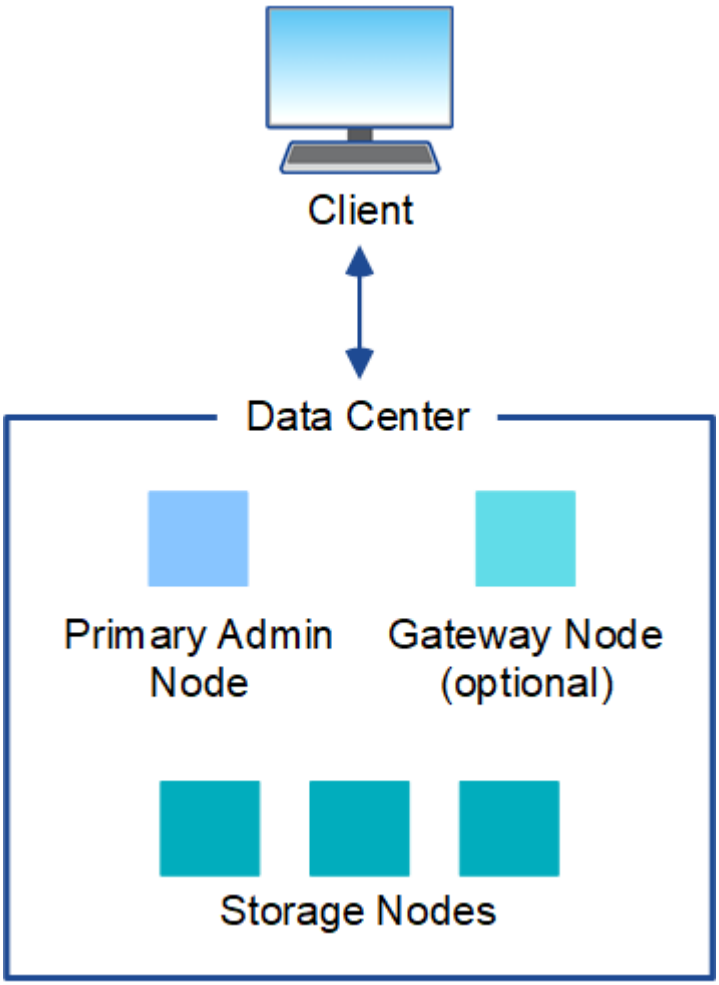
Pour plus d'informations sur la topologie réseau StorageGRID, les exigences et les communications de grille, consultez le "Instructions de mise en réseau".

Topologies de déploiement

Le système StorageGRID peut être déployé sur un seul data Center ou sur plusieurs sites de data Center.

Sur un seul site

Dans un déploiement avec un site unique, l'infrastructure et les opérations du système StorageGRID sont centralisées.

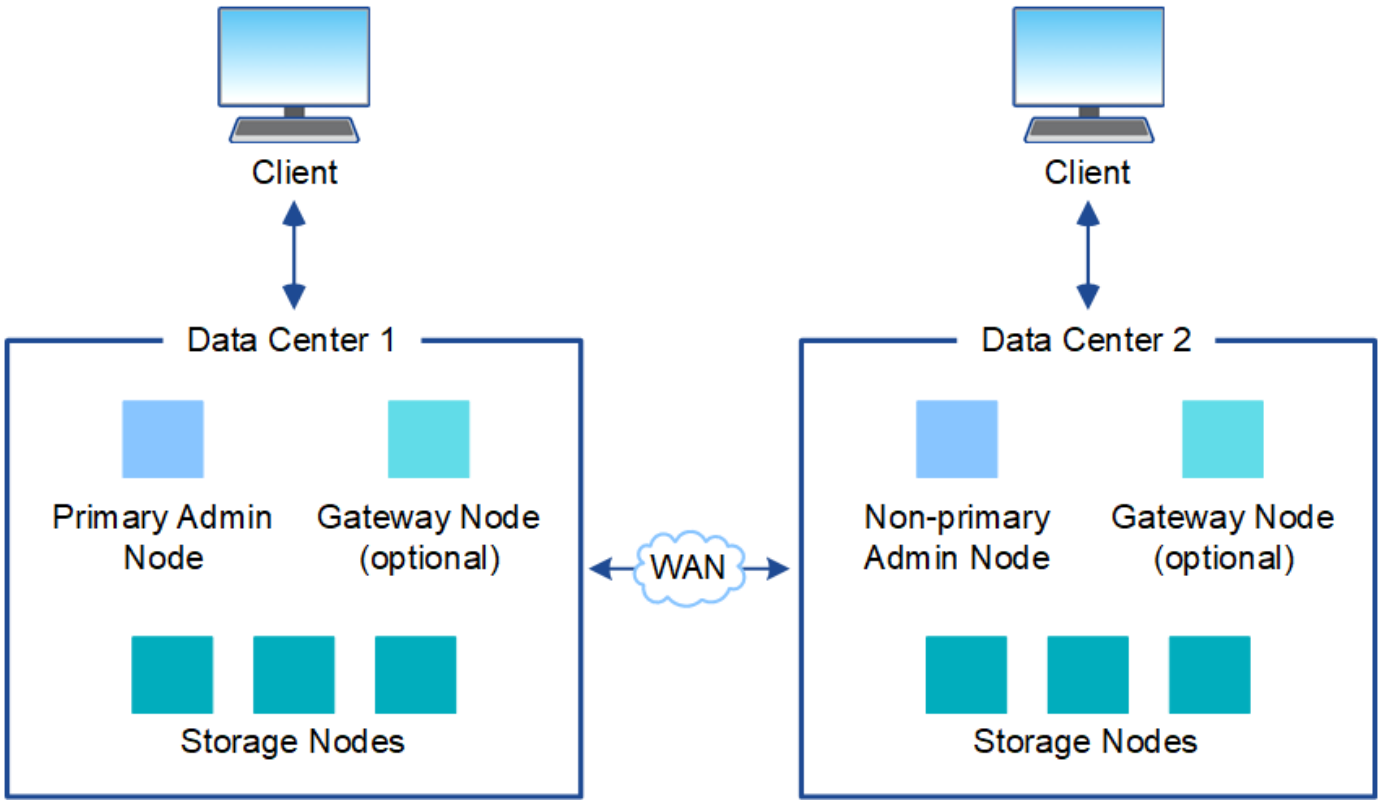


Sites multiples

Dans un déploiement sur plusieurs sites, il est possible d'installer différents types et quantités de ressources StorageGRID sur chaque site. Par exemple, un data Center peut nécessiter plus de stockage qu'un autre.

Différents sites sont souvent situés dans des emplacements géographiques différents dans différents

domaines de défaillance, tels qu'une ligne de défaut sismique ou une inondation. Le partage des données et la reprise après incident sont réalisés par la distribution automatisée des données vers d'autres sites.



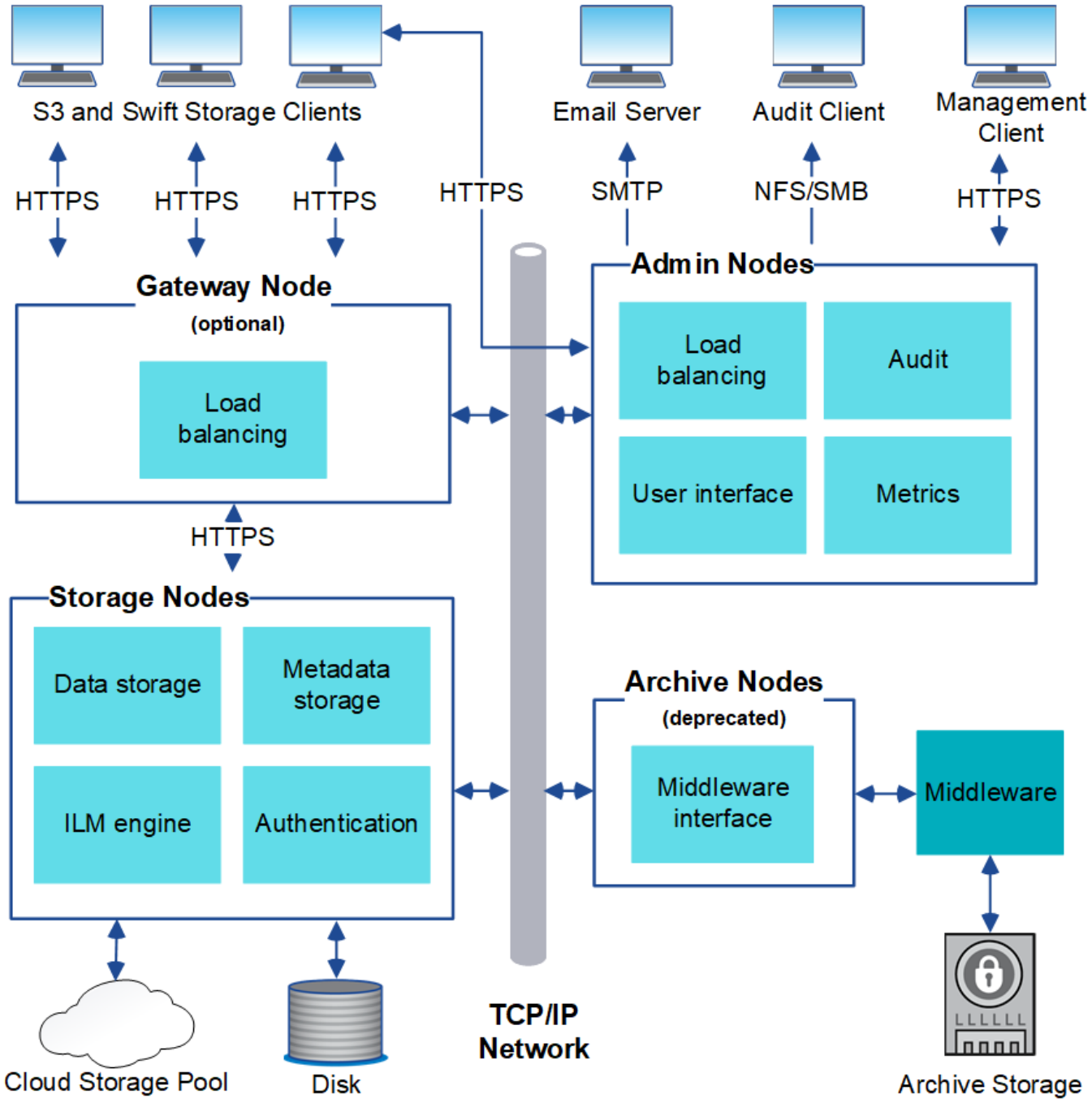
Plusieurs sites logiques peuvent également exister au sein d'un même data Center, afin de permettre l'utilisation de la réplication distribuée et du codage d'effacement pour améliorer la disponibilité et la résilience.

Redondance des nœuds du grid

Dans un déploiement sur un ou plusieurs sites, vous pouvez éventuellement inclure plusieurs nœuds d'administration ou nœuds de passerelle afin d'assurer la redondance. Par exemple, vous pouvez installer plusieurs nœuds d'administration sur un seul site ou sur plusieurs sites. Cependant, chaque système StorageGRID ne peut avoir qu'un seul nœud d'administration principal.

Architecture du système

Ce schéma montre comment les nœuds grid sont organisés dans un système StorageGRID.



Les clients S3 et Swift stockent et récupèrent des objets dans StorageGRID. D'autres clients sont utilisés pour envoyer des notifications par e-mail, pour accéder à l'interface de gestion StorageGRID et éventuellement pour accéder au partage d'audit.

Les clients S3 et Swift peuvent se connecter à un nœud de passerelle ou à un nœud d'administration pour utiliser l'interface d'équilibrage de la charge sur les nœuds de stockage. Les clients S3 et Swift peuvent également se connecter directement aux nœuds de stockage via HTTPS.

Les objets peuvent être stockés dans StorageGRID sur des nœuds de stockage logiciels ou matériels, ou dans des pools de stockage cloud, composés de compartiments S3 externes ou de conteneurs de stockage Azure Blob.

Grid, nœuds et services

L'élément de base d'un système StorageGRID est le nœud grid. Les nœuds contiennent des services, qui sont des modules logiciels qui fournissent un ensemble de capacités à un nœud grid.

Le système StorageGRID utilise quatre types de nœuds grid :

- **Admin Nodes** fournit des services de gestion tels que la configuration du système, la surveillance et la journalisation. Lorsque vous vous connectez à Grid Manager, vous vous connectez à un noeud d'administration. Chaque grid doit posséder un nœud d'administration principal et des nœuds d'administration non primaires supplémentaires pour assurer la redondance. Vous pouvez vous connecter à n'importe quel nœud d'administration et chaque nœud d'administration affiche une vue similaire du système StorageGRID. Cependant, les procédures de maintenance doivent être effectuées à l'aide du nœud d'administration principal.

  Les nœuds d'administration peuvent également être utilisés pour équilibrer la charge du trafic des clients S3 et Swift.

- **Storage Nodes** gère et stocke les données et les métadonnées des objets. Chaque système StorageGRID doit disposer d'au moins trois nœuds de stockage. Si vous avez plusieurs sites, chaque site de votre système StorageGRID doit également disposer de trois nœuds de stockage.
- **Les nœuds de passerelle (facultatifs)** fournissent une interface d'équilibrage de charge que les applications clientes peuvent utiliser pour se connecter à StorageGRID. Un équilibreur de charge dirige de manière transparente les clients vers un nœud de stockage optimal, de sorte que la défaillance de nœuds ou même d'un site entier soit transparente. Vous pouvez utiliser une combinaison de nœuds de passerelle et de nœuds d'administration pour équilibrer la charge, ou implémenter un équilibreur de charge HTTP tiers.
- **Les nœuds d'archivage (obsolètes)** fournissent une interface facultative par laquelle les données d'objet peuvent être archivées sur bande.

Pour en savoir plus, voir "Administrer StorageGRID".

Nœuds basés sur logiciel

Les nœuds grid logiciels peuvent être déployés de plusieurs manières :

- En tant que machines virtuelles dans VMware vSphere
- Dans les moteurs de mise en conteneurs sur les hôtes Linux. Les systèmes d'exploitation suivants sont pris en charge :
  - Red Hat Enterprise Linux
  - CentOS
  - Ubuntu
  - Debian

Pour plus d'informations, reportez-vous aux sections suivantes :

- "Installez VMware"
- "Installez Red Hat Enterprise Linux ou CentOS"
- "Installez Ubuntu ou Debian"

Utilisez le "Matrice d'interopérabilité NetApp (IMT)" pour obtenir une liste des versions prises en charge.

Nœuds d'appliance StorageGRID

Les appliances matérielles StorageGRID sont spécialement conçues pour une utilisation dans un système StorageGRID. Certaines appliances peuvent être utilisées comme nœuds de stockage. Les autres appliances peuvent être utilisées comme nœuds d'administration ou nœuds de passerelle. Vous pouvez combiner des nœuds d'appliance avec des nœuds basés sur des logiciels ou déployer des grilles 100 % appliance entièrement conçues sans dépendance vis-à-vis d'hyperviseurs, de systèmes de stockage ou de matériel de calcul externes.

Les types d'appliances StorageGRID suivants sont disponibles :

- Le **SGF6112 Storage Appliance** est un serveur 1U 100 % Flash doté de 12 disques SSD NVMe (Nonvolatile Memory Express) avec contrôleurs de stockage et de calcul intégrés.
- Les appliances de services **SG100 et SG1000** sont des serveurs à 1 unité de rack (1U) qui peuvent chacun fonctionner comme un nœud d'administration principal, un nœud d'administration non primaire ou un nœud de passerelle. Les deux appliances peuvent fonctionner en tant que nœuds de passerelle et de nœud d'administration (primaire et non primaire) à la fois.
- Le **SG6000 Storage Appliance** fonctionne comme un nœud de stockage et combine le contrôleur de calcul 1U SG6000-CN avec un tiroir de contrôleur de stockage 2U ou 4U. Le SG6000 est disponible en deux modèles :
  - **SGF6024** : associe le contrôleur de calcul SG6000-CN à un tiroir de contrôleur de stockage 2U incluant 24 disques SSD (Solid State Drives) et des contrôleurs de stockage redondants.
  - **SG6060** : associe le contrôleur de calcul SG6000-CN à un boîtier 4U qui comprend 58 disques NL-SAS, 2 disques SSD et des contrôleurs de stockage redondants. Chaque appliance SG6060 prend en charge un ou deux tiroirs d'extension de 60 disques, offrant jusqu'à 178 disques dédiés au stockage objet.
- **SG5700 Storage Appliance** est une plateforme de calcul et de stockage intégrée qui fonctionne comme un nœud de stockage. Deux modèles de SG5700 sont disponibles :
  - **SG5712** : un boîtier 2U qui comprend 12 disques NL-SAS et des contrôleurs de calcul et de stockage intégrés.
  - **SG5760** : un boîtier 4U qui comprend 60 disques NL-SAS et des contrôleurs de calcul et de stockage intégrés.

Pour plus d'informations, reportez-vous aux sections suivantes :

- "NetApp Hardware Universe"
- "Appliance de stockage SGF6112"
- "Appareils de services SG100 et SG1000"
- "Dispositifs de stockage SG6000"
- "Appliances de stockage SG5700"

Services primaires pour les nœuds d'administration

Le tableau ci-dessous présente les services principaux pour les nœuds d'administration, mais ce tableau ne répertorie pas tous les services de nœud.

Service	Fonction de touche
Système de gestion des audits (AMS)	Suit l'activité et les événements du système.
Nœud de gestion de la configuration (CMN)	Gestion de la configuration à l'échelle du système. Nœud d'administration principal uniquement.
Interface de gestion du programme d'applications de gestion (api)	Traite les requêtes à partir de l'API de gestion Grid et de l'API de gestion des locataires.
Haute disponibilité	Gère les adresses IP virtuelles haute disponibilité pour les groupes de nœuds d'administration et de nœuds de passerelle. **Remarque :** ce service se trouve également sur les nœuds de passerelle.
Équilibreur de charge	Équilibrage de la charge du trafic S3 et Swift entre les clients et les nœuds de stockage. **Remarque :** ce service se trouve également sur les nœuds de passerelle.
Système de gestion de réseau (NMS)	Fournit des fonctionnalités pour le gestionnaire de grille.
Prometheus	Collecte et stocke les mesures de séries chronologiques des services sur tous les nœuds.
Moniteur d'état du serveur (SSM)	Surveille le système d'exploitation et le matériel sous-jacent.

Services primaires des nœuds de stockage

Le tableau ci-dessous présente les services principaux pour les nœuds de stockage, mais ce tableau ne répertorie pas tous les services de nœuds.

Certains services, tels que le service ADC et le service RSM, n'existent généralement que sur trois nœuds de stockage de chaque site.

Service	Fonction de touche
Compte (compte)	Gestion des comptes de locataire.
Contrôleur de domaine administratif (ADC)	Maintien de la topologie et de la configuration dans l'ensemble du grid.
Cassandra	Stocke et protège les métadonnées d'objet.

Service	Fonction de touche
Cône Cassandra	Répare automatiquement les métadonnées d'objet.
Bloc	Gestion des données avec code d'effacement et des fragments de parité.
Data Mover (dmv)	Déplacement des données vers des pools de stockage cloud.
Stockage de données distribué (DDS)	Surveille le stockage des métadonnées d'objet.
Identité (idnt)	Fédération des identités d'utilisateur à partir de LDAP et d'Active Directory.
Routeur de distribution local (LDR)	Traite les demandes de protocole de stockage objet et gère les données d'objet sur le disque.
RSM (Replicated State machine)	Envoi des demandes de services de la plateforme S3 à leurs terminaux respectifs
Moniteur d'état du serveur (SSM)	Surveille le système d'exploitation et le matériel sous-jacent.

Services primaires pour les nœuds de passerelle

Le tableau ci-dessous présente les services principaux pour les nœuds de passerelle ; toutefois, ce tableau ne répertorie pas tous les services de nœud.

Service	Fonction de touche
Haute disponibilité	Gère les adresses IP virtuelles haute disponibilité pour les groupes de nœuds d'administration et de nœuds de passerelle. **Remarque :** ce service se trouve également sur les noeuds d'administration.
Équilibreur de charge	Équilibrage de la charge de couche 7 du trafic S3 et Swift à partir des clients vers les nœuds de stockage. Il s'agit du mécanisme d'équilibrage de charge recommandé. **Remarque :** ce service se trouve également sur les noeuds d'administration.
Moniteur d'état du serveur (SSM)	Surveille le système d'exploitation et le matériel sous-jacent.

Services primaires pour les nœuds d'archivage

Le tableau suivant présente les services primaires pour les nœuds d'archivage (maintenant obsolètes) ; cependant, ce tableau ne répertorie pas tous les services de nœuds.

La prise en charge des nœuds d'archivage est obsolète et sera supprimée dans une version ultérieure.

Service	Fonction de touche
Archivage (ARC)	Communique avec un système de stockage sur bande externe Tivoli Storage Manager (TSM).
Moniteur d'état du serveur (SSM)	Surveille le système d'exploitation et le matériel sous-jacent.

Des services StorageGRID

Voici la liste complète des services StorageGRID.

- **Transitaire de service de compte**

  Fournit une interface permettant au service Load Balancer d'interroger le service Account Service sur des hôtes distants et fournit des notifications sur les modifications de configuration de point de terminaison Load Balancer au service Load Balancer. Le service Load Balancer est présent sur les nœuds d'administration et les nœuds de passerelle.

- **Service ADC (contrôleur de domaine administratif)**

  Gère les informations de topologie, fournit des services d'authentification et répond aux requêtes des services LDR et CMN. Le service ADC est présent sur chacun des trois premiers nœuds de stockage installés sur un site.

- **Service AMS (système de gestion de la vérification)**

  Surveille et consigne tous les événements et transactions système audités dans un fichier journal texte. Le service AMS est présent sur les nœuds Admin.

- **Service ARC (Archive)**

  Offre l'interface de gestion avec laquelle vous configurez les connexions au système de stockage d'archivage externe, tel que le cloud via une interface S3 ou une bande via le middleware TSM. Le service ARC est présent sur les nœuds d'archivage.

- **Service de re-couches Cassandra**

  Répare automatiquement les métadonnées d'objet. Le service Cassandra Reaper est présent sur tous les nœuds de stockage.

- **Service de bloc**

  Gestion des données avec code d'effacement et des fragments de parité. Le service de bloc est présent sur les nœuds de stockage.

- **Service CMN (nœud de gestion de la configuration)**

  Gestion des configurations et des tâches de grid à l'échelle du système. Chaque grid dispose d'un service CMN présent sur le nœud d'administration principal.

- **Service DDS (Distributed Data Store)**

  Interfaces avec la base de données Cassandra pour gérer les métadonnées d'objet. Le service DDS est présent sur les nœuds de stockage.

- **Service DMV (Data Mover)**

  Déplacement des données vers les terminaux cloud Le service DMV est présent sur les nœuds de stockage.

- **Service IP dynamique**

  Surveille la grille pour détecter les changements d'adresse IP dynamiques et met à jour les configurations locales. Le service IP dynamique (dynap) est présent sur tous les nœuds.

- **Service Grafana**

  Utilisé pour la visualisation des metrics dans Grid Manager. Le service Grafana est présent sur les nœuds Admin.

- **Service haute disponibilité**

  Gère les adresses IP virtuelles haute disponibilité sur les nœuds configurés sur la page groupes haute disponibilité. Le service haute disponibilité est présent sur les nœuds d'administration et les nœuds de passerelle. Ce service est également connu sous le nom de service keepalspé.

- **Service identité (idnt)**

  Fédération des identités d'utilisateur à partir de LDAP et d'Active Directory. Le service d'identité (idnt) est présent sur trois nœuds de stockage de chaque site.

- **Service d'arbitre Lambda**

  Gère les demandes S3 Select SelectObjectContent.

- **Service Load Balancer**

  Équilibrage de la charge du trafic S3 et Swift entre les clients et les nœuds de stockage. Le service Load Balancer peut être configuré via la page de configuration des noeuds finaux Load Balancer. Le service Load Balancer est présent sur les nœuds d'administration et les nœuds de passerelle. Ce service est également connu sous le nom de service nginx-gw.

- **Service LDR (routeur de distribution local)**

  Gestion du stockage et du transfert de contenu au sein de la grille. Le service LDR est présent sur les nœuds de stockage.

- **Service d'information MISCd Service Daemon service**

  Fournit une interface pour interroger et gérer les services sur d'autres noeuds et pour gérer les configurations environnementales sur le noeud, telles que interroger l'état des services exécutés sur d'autres noeuds. Le service MISCd est présent sur tous les nœuds.

- **nginx service**

  Agit comme un mécanisme d'authentification et de communication sécurisée pour divers services de grid

(Prometheus et IP dynamique, par exemple), afin de pouvoir communiquer avec les services sur d'autres nœuds via des API HTTPS. Le service nginx est présent sur tous les nœuds.

- **nginx-gw service**

  Alimente le service Load Balancer. Le service nginx-gw est présent sur les nœuds d'administration et les nœuds de passerelle.

- **Service NMS (système de gestion de réseau)**

  Alimente les options de surveillance, de rapport et de configuration qui sont affichées via le gestionnaire de grille. Le service NMS est présent sur les nœuds d'administration.

- **Service de persistance**

  Gère les fichiers sur le disque racine qui doivent persister au cours d'un redémarrage. Le service de persistance est présent sur tous les nœuds.

- **Service Prometheus**

  Collecte des metrics de séries chronologiques à partir des services sur tous les nœuds. Le service Prometheus est présent sur les nœuds d'administration.

- **Service RSM (Replicated State machine Service)**

  S'assure que les demandes de service de la plate-forme sont envoyées à leurs terminaux respectifs. Le service RSM est présent sur les nœuds de stockage qui utilisent le service ADC.

- **Service SSM (moniteur d'état du serveur)**

  Surveille l'état du matériel et communique des rapports au service NMS. Une instance du service SSM est présente sur chaque nœud de la grille.

- **Service collecteur trace**

  Effectue la collecte des traces afin de recueillir des informations à utiliser par le support technique. Le service trace Collector utilise le logiciel Jaeger open source et est présent sur les nœuds d'administration.

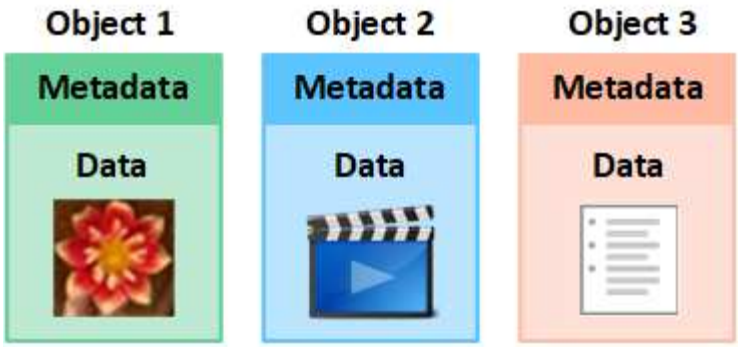
La gestion des données par StorageGRID

Qu'est-ce qu'un objet

Avec le stockage objet, l'unité de stockage est un objet, et non un fichier ou un bloc. Contrairement à la hiérarchie de type arborescence d'un système de fichiers ou stockage en blocs, le stockage objet organise les données dans une disposition plate et non structurée.

Le stockage objet dissocie l'emplacement physique des données de la méthode de stockage et de récupération utilisée.

Chaque objet d'un système de stockage basé sur les objets comporte deux parties : les données d'objet et les métadonnées d'objet.



Qu'est-ce que les données d'objet ?

Les données d'objet peuvent être quoi que ce soit ; par exemple, une photographie, un film ou un dossier médical.

Qu'est-ce que les métadonnées d'objet ?

Les métadonnées d'objet constituent toutes les informations qui décrivent un objet. StorageGRID utilise les métadonnées d'objet pour suivre l'emplacement de tous les objets de la grille, et pour gérer le cycle de vie de chaque objet au fil du temps.

Les métadonnées de l'objet incluent les informations suivantes :

- Les métadonnées du système, y compris un ID unique pour chaque objet (UUID), le nom de l'objet, le nom du compartiment S3 ou du conteneur Swift, le nom ou l'ID du compte du locataire, la taille logique de l'objet, la date et l'heure de la première création de l'objet, et la date et l'heure de la dernière modification de l'objet.
- Emplacement de stockage actuel de chaque copie d'objet ou fragment codé d'effacement.
- Toutes les métadonnées utilisateur associées à l'objet.

Les métadonnées de l'objet sont personnalisables et extensibles, ce qui rend la possibilité d'utiliser les applications.

Pour plus d'informations sur la façon et l'emplacement StorageGRID de stockage des métadonnées d'objet, accédez à "Gérer le stockage des métadonnées d'objet".

Comment les données d'objet sont-elles protégées ?

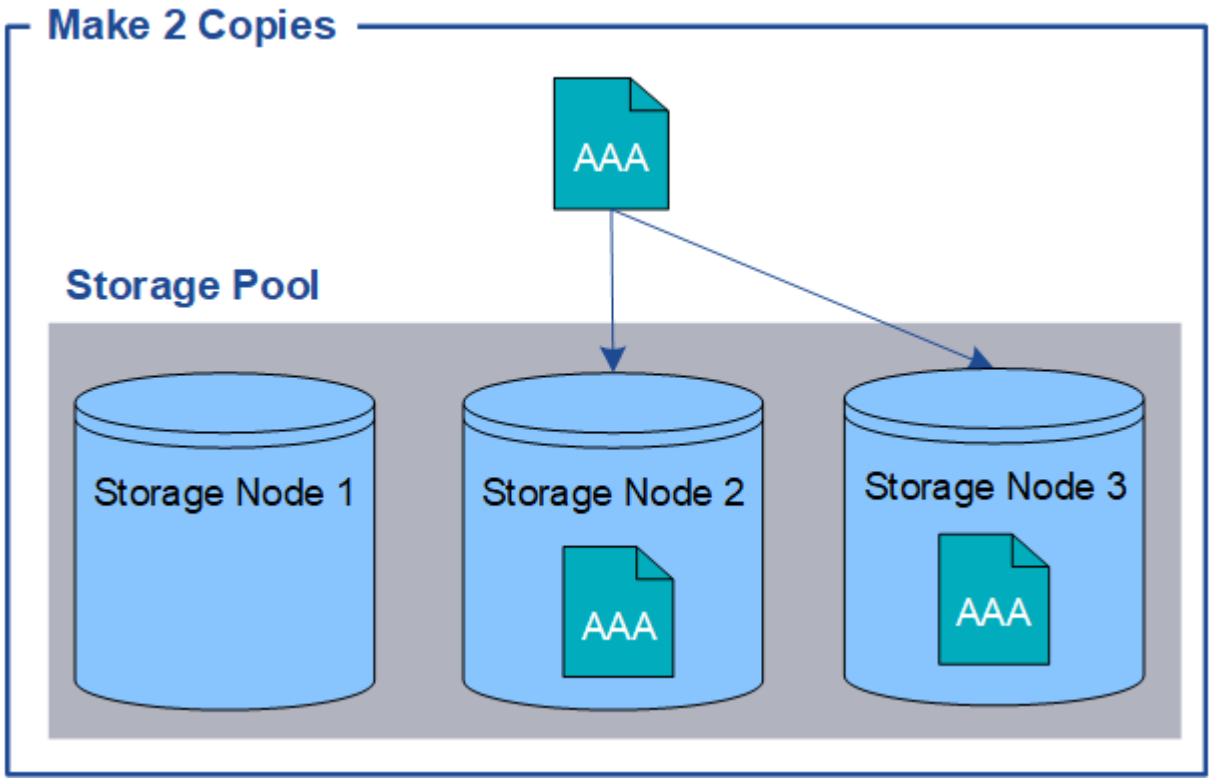
Le système StorageGRID propose deux mécanismes de protection des données d'objet contre la perte : la réplication et le codage d'effacement.

La réplication

Lorsque StorageGRID mappe les objets sur une règle de gestion du cycle de vie des informations (ILM) configurée pour créer des copies répliquées, le système crée des copies exactes des données d'objet et les stocke sur des nœuds de stockage, des nœuds d'archivage ou des pools de stockage cloud. Les règles ILM déterminent le nombre de copies effectuées, l'emplacement de stockage de ces copies et la durée pendant laquelle elles sont conservées par le système. Par exemple, en cas de perte d'une copie suite à la perte d'un nœud de stockage, l'objet est toujours disponible si une copie de celui-ci existe ailleurs dans le système StorageGRID.

Dans l'exemple suivant, la règle Make 2 copies spécifie que deux copies répliquées de chaque objet sont

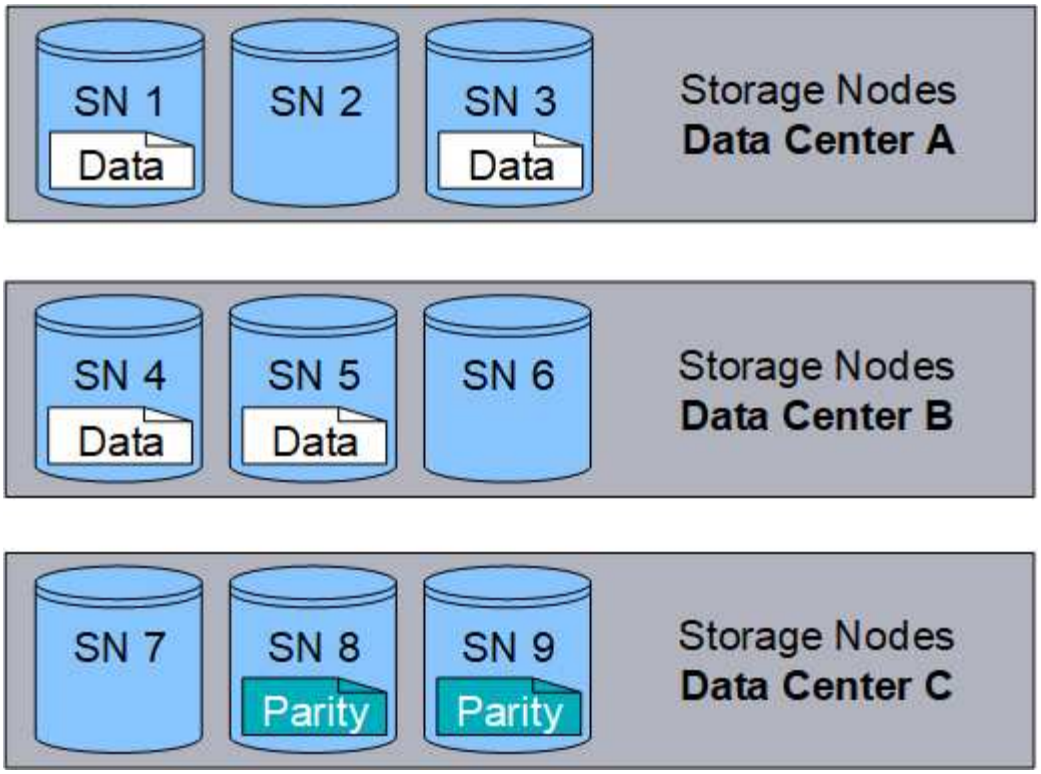
placées dans un pool de stockage contenant trois nœuds de stockage.



Le code d'effacement

Lorsque StorageGRID mappe les objets sur une règle ILM configurée pour créer des copies avec code d'effacement, elle coupe les données d'objet en fragments de données, calcule des fragments de parité supplémentaires et stocke chaque fragment sur un autre nœud de stockage. Lorsqu'un objet est accédé, il est réassemblé à l'aide des fragments stockés. En cas de corruption ou de perte d'un fragment de parité, l'algorithme de codage d'effacement peut recréer ce fragment à l'aide d'un sous-ensemble des données restantes et des fragments de parité. Les règles ILM et les profils de code d'effacement déterminent le schéma de code d'effacement utilisé.

L'exemple suivant illustre l'utilisation du code d'effacement sur les données d'un objet. Dans cet exemple, la règle ILM utilise un schéma de code d'effacement 4+2. Chaque objet est tranché en quatre fragments de données égaux et deux fragments de parité sont calculés à partir des données d'objet. Chacun des six fragments est stocké sur un nœud de stockage différent dans trois data centers pour assurer la protection des données en cas de défaillance d'un nœud ou de perte d'un site.



Informations associées

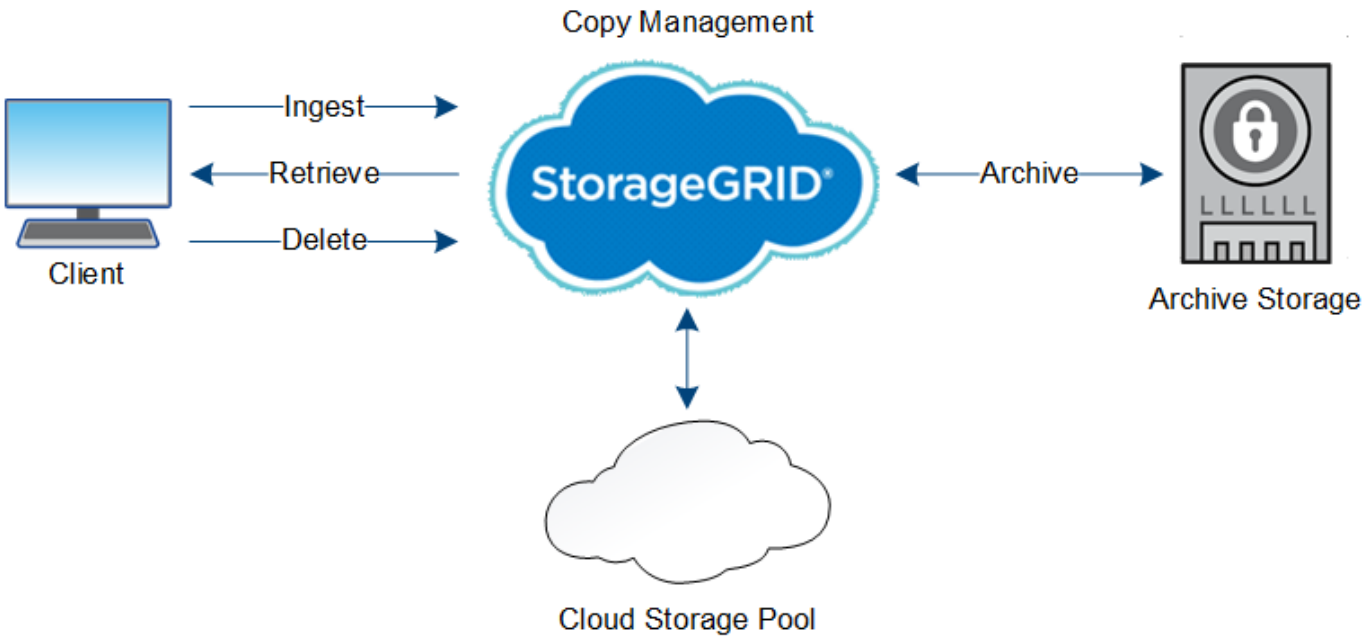
- "Gestion des objets avec ILM"
- "Utilisation de la gestion du cycle de vie des informations"

La vie d'un objet

La vie d'un objet se compose de plusieurs étapes. Chaque étape représente les opérations qui se produisent avec l'objet.

Tout au long de la durée de vie d'un objet comprend les opérations d'ingestion, de gestion des copies, de récupération et de suppression.

- **Ingest** : processus d'enregistrement d'un objet sur HTTP dans le système StorageGRID par une application client S3 ou Swift. À ce stade, le système StorageGRID commence à gérer l'objet.
- **Gestion des copies** : processus de gestion des copies répliquées et codées en fonction de l'effacement dans StorageGRID, comme décrit dans les règles ILM de la politique ILM active. Pendant la phase de gestion des copies, StorageGRID protège les données d'objet de la perte en créant et en conservant le nombre et le type spécifiés de copies d'objet sur les nœuds de stockage, dans un pool de stockage cloud ou sur un nœud d'archivage.
- **Retrieve** : processus d'accès d'une application client à un objet stocké par le système StorageGRID. Le client lit l'objet, qui est extrait d'un nœud de stockage, d'un pool de stockage cloud ou d'un nœud d'archivage.
- **Supprimer** : processus de suppression de toutes les copies d'objet de la grille. Ces objets peuvent être supprimés suite à l'envoi d'une requête de suppression au système StorageGRID ou à un processus automatique exécuté par StorageGRID au moment où sa durée de vie arrive à expiration.



Informations associées

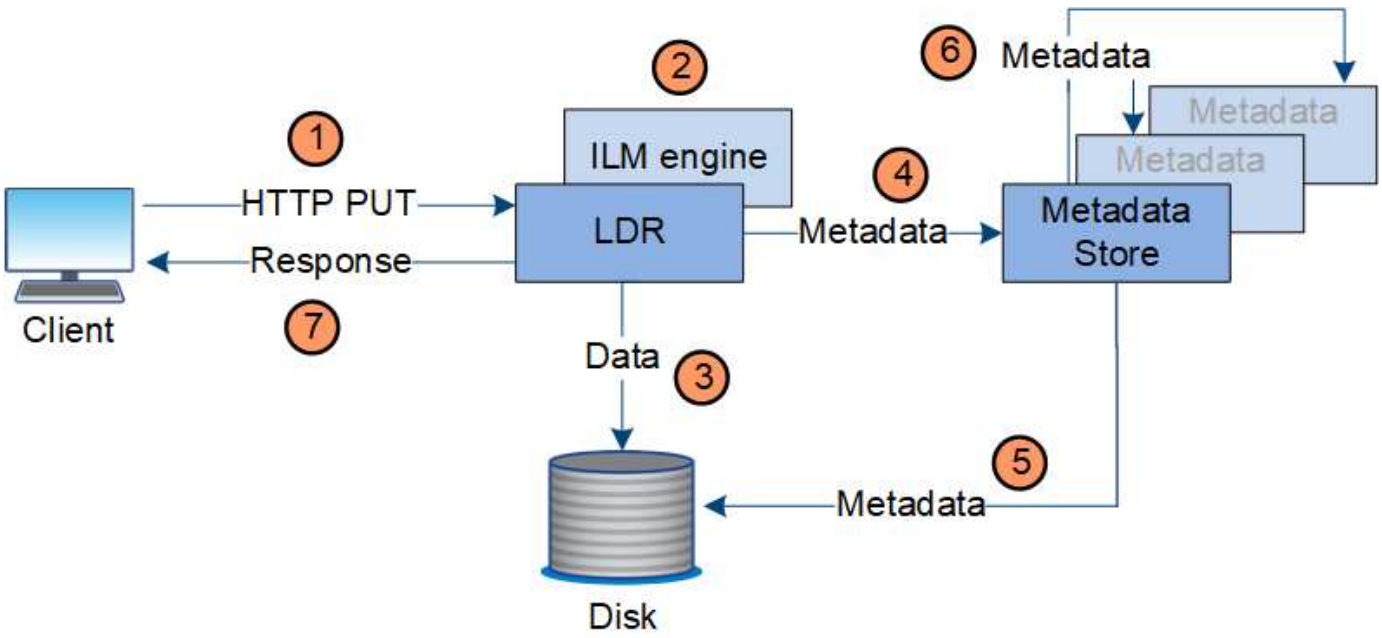
- "Gestion des objets avec ILM"
- "Utilisation de la gestion du cycle de vie des informations"

Ingestion des données

Une opération d'acquisition ou de sauvegarde se compose d'un flux de données défini entre le client et le système StorageGRID.

Flux de données

Lorsqu'un client ingère un objet dans le système StorageGRID, le service LDR sur des nœuds de stockage traite la requête et stocke les métadonnées et les données sur disque.



1. L’application client crée l’objet et l’envoie au système StorageGRID via une requête PUT HTTP.
2. L’objet est évalué par rapport à la politique ILM du système.
3. Le service LDR enregistre les données objet sous forme de copie répliquée ou de copie avec codage d’effacement. (Le schéma représente une version simplifiée du stockage d’une copie répliquée sur disque.)
4. Le service LDR envoie les métadonnées objet au magasin de métadonnées.
5. Le magasin de métadonnées enregistre les métadonnées d’objet sur le disque.
6. Le magasin de métadonnées propage les copies de métadonnées d’objet à d’autres nœuds de stockage. Ces copies sont également enregistrées sur le disque.
7. Le service LDR renvoie une réponse HTTP 200 OK au client pour reconnaître que l’objet a été ingéré.

Gestion des copies

Les données d’objet sont gérées par la règle ILM active et ses règles ILM. Les règles ILM créent des copies répliquées ou codées d’effacement pour protéger les données d’objet contre la perte.

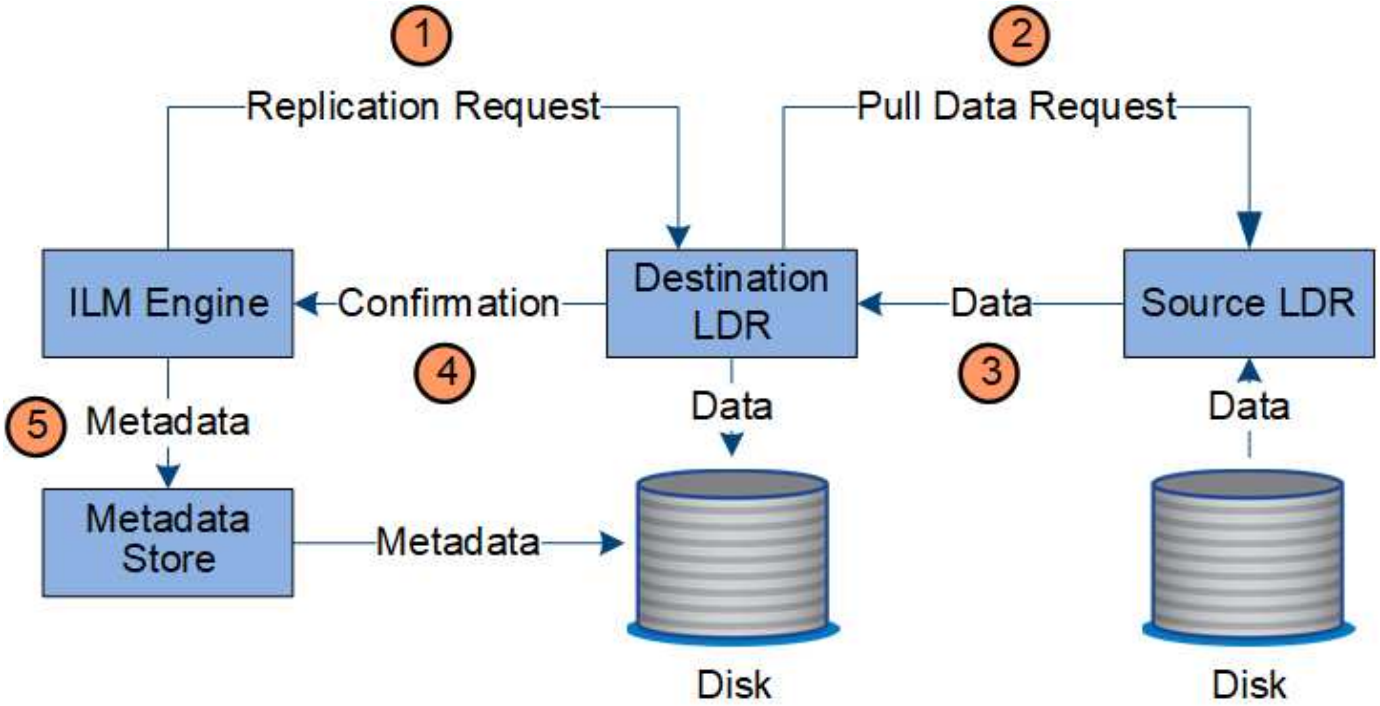
Différents types ou emplacements de copies d’objets peuvent être requis à différents moments de la vie de l’objet. Les règles ILM sont régulièrement évaluées afin de s’assurer que les objets sont placés en fonction des besoins.

Les données d’objet sont gérées par le service LDR.

Protection du contenu : réplication

Si les instructions de placement de contenu d’une règle ILM nécessitent des copies répliquées des données d’objet, des copies sont créées et stockées sur le disque par les nœuds de stockage qui constituent le pool de stockage configuré.

Le moteur ILM du service LDR contrôle la réplication et garantit le stockage du nombre adéquat de copies aux emplacements corrects et pour le laps de temps correct.

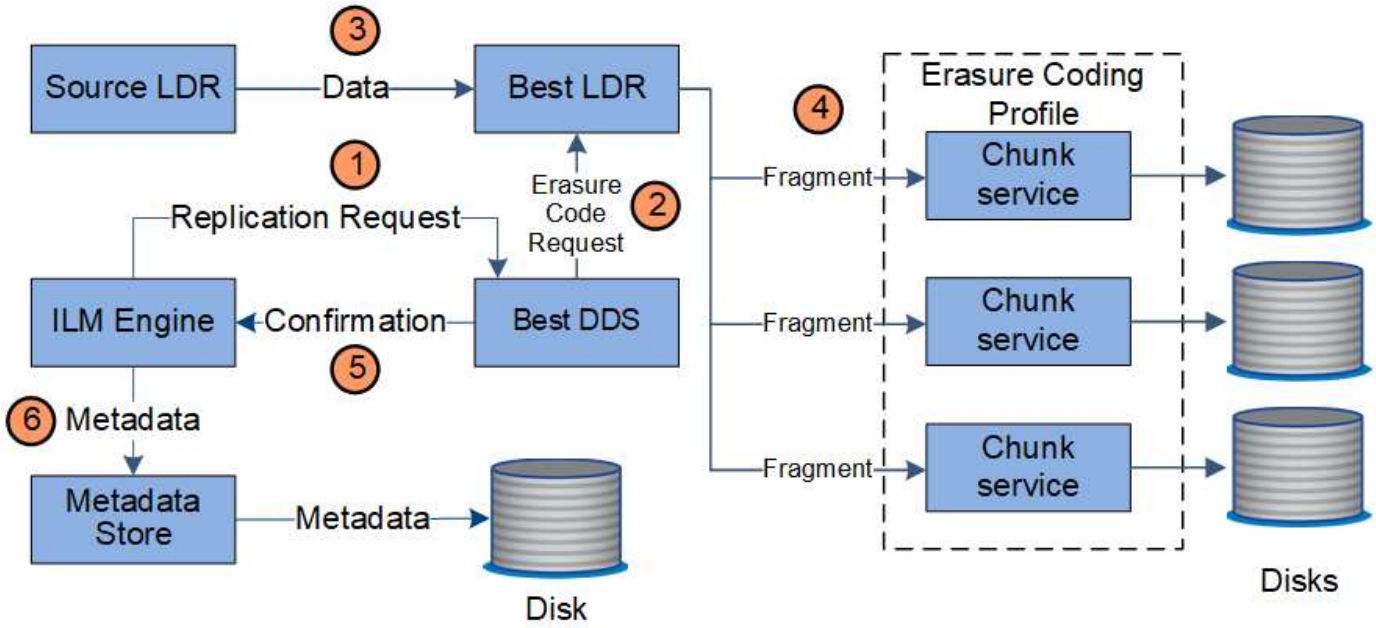


1. Le moteur ILM interroge le service ADC afin de déterminer le meilleur service LDR de destination au sein du pool de stockage spécifié par la règle ILM. Il envoie ensuite une commande au service LDR pour lancer la réplication.
2. Le service LDR de destination interroge le service ADC pour obtenir le meilleur emplacement de la source. Il envoie ensuite une requête de réplication au service LDR source.
3. Le service LDR source envoie une copie au service LDR destination.
4. Le service LDR de destination informe le moteur ILM que les données objet ont été stockées.
5. Le moteur ILM met à jour le magasin de métadonnées avec les métadonnées d'emplacement d'objet.

Protection du contenu : code d'effacement

Si une règle ILM contient des instructions pour effectuer des copies avec code d'effacement des données d'objet, le schéma de code d'effacement applicable répartit les données d'objet en fragments de données et de parité, et distribue ces fragments entre les nœuds de stockage configurés dans le profil de code d'effacement.

Le moteur ILM, qui est un composant du service LDR, contrôle le code d'effacement et veille à ce que le profil de code d'effacement soit appliqué aux données d'objet.

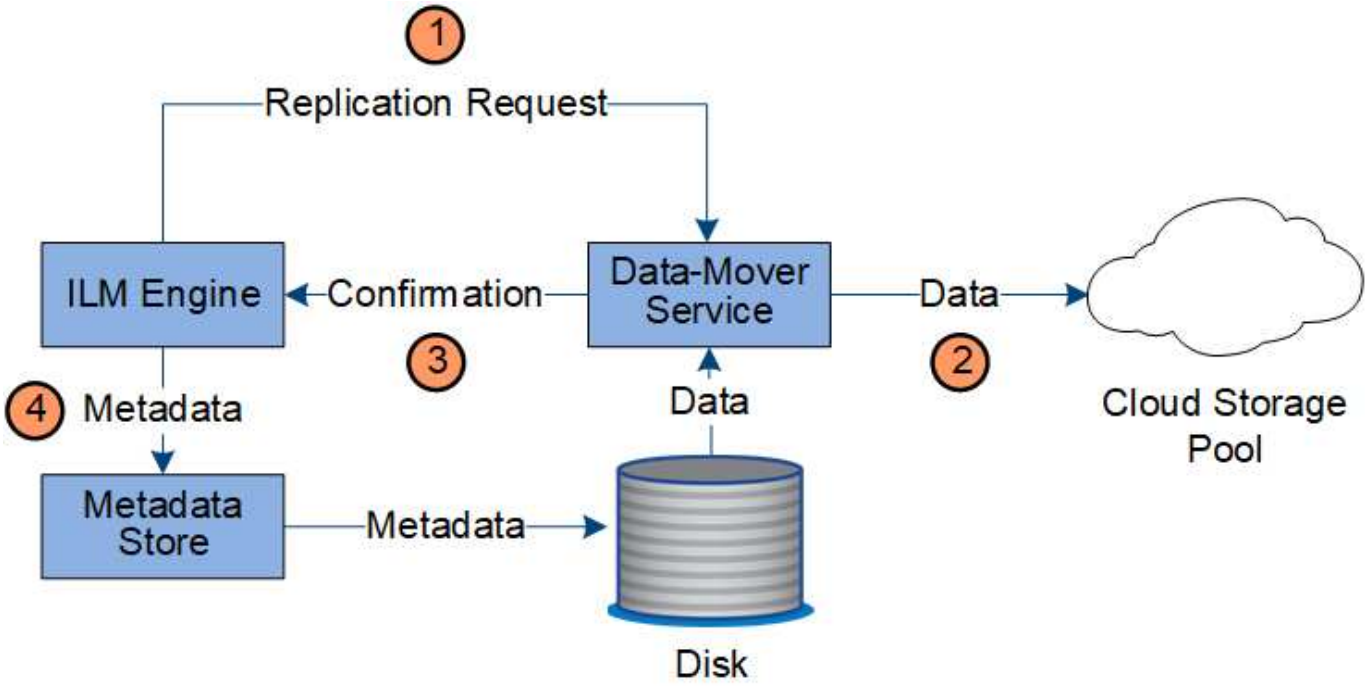


1. Le moteur ILM interroge le service ADC afin de déterminer quel service DDS peut le mieux effectuer l'opération de codage d'effacement. Une fois déterminé, le moteur ILM envoie une demande de lancement à ce service.
2. Le service DDS demande à un LDR de coder les données de l'objet.
3. Le service source LDR envoie une copie au service LDR sélectionné pour le codage d'effacement.
4. Une fois décomposé en nombre approprié de fragments de parité et de données, le service LDR distribue ces fragments entre les nœuds de stockage (services de blocs) qui composent le pool de stockage du profil de code d'effacement.
5. Le service LDR informe le moteur ILM pour confirmer la distribution réussie des données d'objet.
6. Le moteur ILM met à jour le magasin de métadonnées avec les métadonnées d'emplacement d'objet.

Protection du contenu : pool de stockage cloud

Si les instructions de placement de contenu d'une règle ILM requièrent qu'une copie répliquée des données d'objet soit stockée dans un pool de stockage cloud, les données d'objet sont dupliquées dans le compartiment S3 externe ou dans le conteneur de stockage Azure Blob spécifié pour le pool de stockage cloud.

Le moteur ILM, composant du service LDR, et le service Data Mover contrôlent le déplacement des objets vers le Cloud Storage Pool.



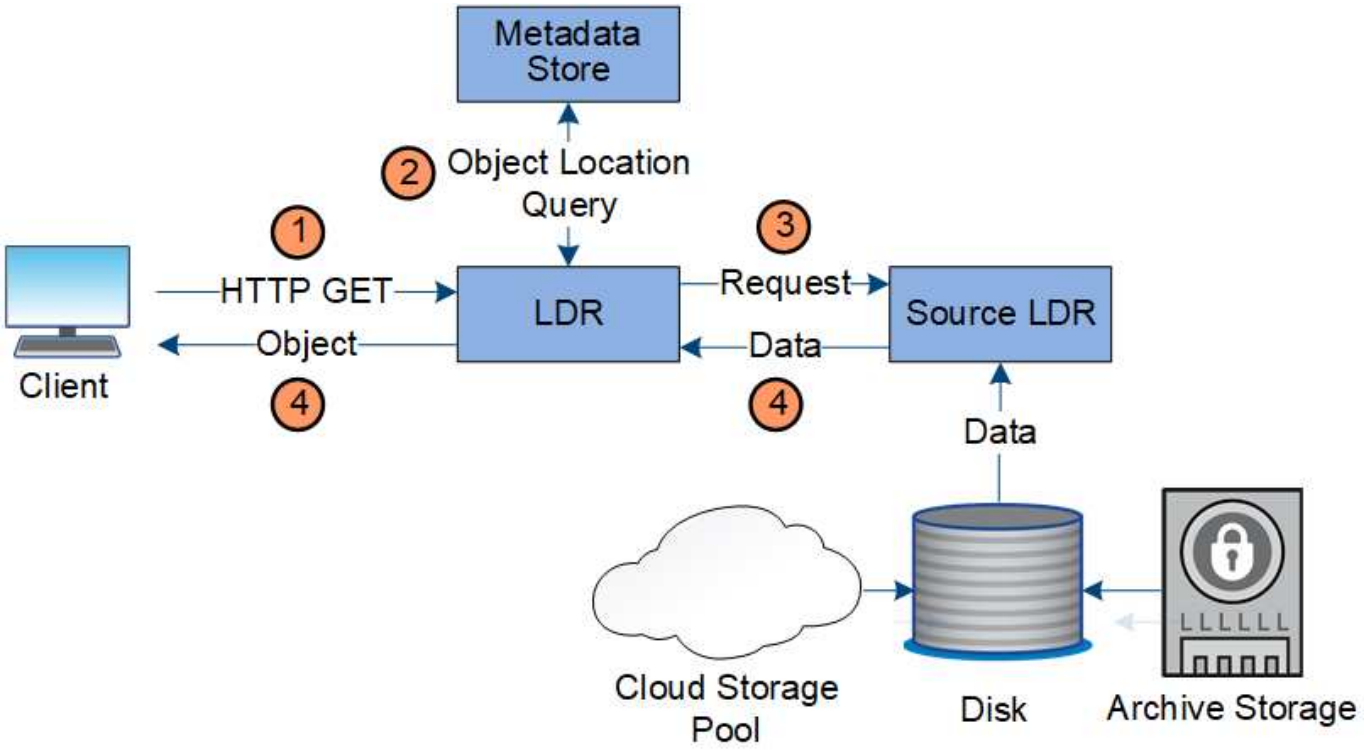
1. Le moteur ILM sélectionne un service de Data Mover à répliquer sur le Cloud Storage Pool.
2. Le service Data Mover envoie les données d'objet au Cloud Storage Pool.
3. Le service Data Mover informe le moteur ILM que les données de l'objet ont été stockées.
4. Le moteur ILM met à jour le magasin de métadonnées avec les métadonnées d'emplacement d'objet.

Récupérer le flux de données

Une opération de récupération se compose d'un flux de données défini entre le système StorageGRID et le client. Le système utilise des attributs pour suivre la récupération de l'objet à partir d'un nœud de stockage ou, si nécessaire, d'un pool de stockage cloud ou d'un nœud d'archivage.

Le service LDR du nœud de stockage interroge le magasin de métadonnées afin d'obtenir l'emplacement des données d'objet et les récupère à partir du service LDR source. De préférence, la récupération se fait à partir d'un nœud de stockage. Si l'objet n'est pas disponible sur un nœud de stockage, la demande de récupération est dirigée vers un pool de stockage cloud ou vers un nœud d'archivage.

Si la seule copie d'objet se trouve sur le stockage AWS Glacier ou sur le niveau Azure Archive, l'application client doit émettre une demande de restauration APRÈS objet S3 pour restaurer une copie récupérable dans le pool de stockage cloud.



1. Le service LDR reçoit une requête de récupération de l'application cliente.
2. Le service LDR interroge le magasin de métadonnées afin d'obtenir l'emplacement des données et des métadonnées d'objet.
3. Le service LDR transmet la requête de récupération au service LDR source.
4. Le service LDR source renvoie les données d'objet du service LDR interrogé et le système renvoie l'objet à l'application client.

Supprimer le flux de données

Toutes les copies d'objet sont supprimées du système StorageGRID lorsqu'un client effectue une opération de suppression ou lorsque sa durée de vie expire, ce qui entraîne sa suppression automatique. Il existe un flux de données défini pour la suppression d'objet.

Hiérarchie de suppression

StorageGRID propose plusieurs méthodes de contrôle du moment où les objets sont conservés ou supprimés. Les objets peuvent être supprimés à la demande du client ou automatiquement. StorageGRID hiérarchise toujours les paramètres de verrouillage d'objet S3 sur les demandes de suppression du client, lesquelles sont prioritaires sur le cycle de vie du compartiment S3 et les instructions de placement de la solution ILM.

- **Verrouillage d'objet S3** : si le paramètre de verrouillage d'objet S3 global est activé pour la grille, les clients S3 peuvent créer des compartiments avec le verrouillage d'objet S3 activé, puis utiliser l'API REST S3 pour spécifier les paramètres de conservation à jour et de conservation légale pour chaque version d'objet ajoutée à ce compartiment.
  - Aucune méthode ne permet de supprimer une version d'objet faisant l'objet d'une conservation légale.
  - Avant que la date de conservation d'une version d'objet ne soit atteinte, cette version ne peut pas être supprimée par aucune méthode.

- Les objets des compartiments où le verrouillage d'objet S3 est activé sont conservés par ILM « toujours ». Une fois la date de conservation atteinte, une version d'objet peut être supprimée par une demande client ou l'expiration du cycle de vie du compartiment.
- Si les clients S3 appliquent une date de conservation jusqu'au compartiment par défaut, ils n'ont pas besoin de spécifier une date de conservation jusqu'à pour chaque objet.

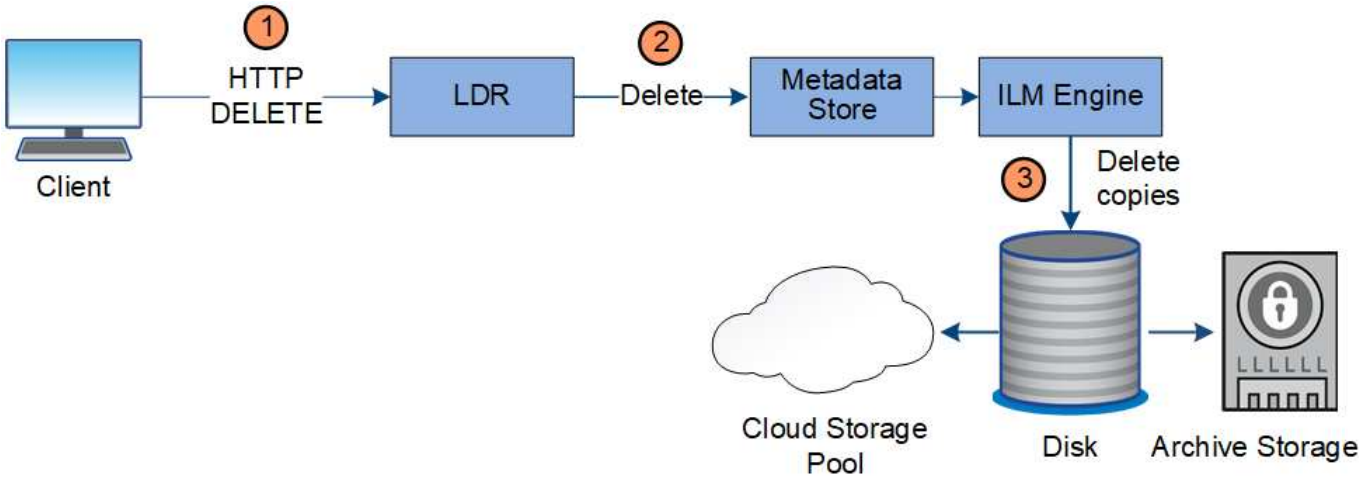
- **Demande de suppression de client** : un client S3 ou Swift peut émettre une requête de suppression d'objet. Lorsqu'un client supprime un objet, toutes les copies de cet objet sont supprimées du système StorageGRID.
- **Supprimer les objets dans le compartiment** : les utilisateurs du gestionnaire de locataires peuvent utiliser cette option pour supprimer définitivement toutes les copies des objets et des versions d'objet dans les compartiments sélectionnés du système StorageGRID.
- **Cycle de vie des compartiments S3** : les clients S3 peuvent ajouter une configuration de cycle de vie à leurs compartiments qui spécifie une action d'expiration. Lorsqu'il existe un cycle de vie de compartiment, StorageGRID supprime automatiquement toutes les copies d'un objet lorsque la date ou le nombre de jours spécifiés dans l'action d'expiration sont atteints, à moins que le client n'ait supprimé l'objet en premier.
- **Instructions de placement ILM** : en supposant que le verrouillage objet S3 n'est pas activé dans le compartiment et qu'il n'y a pas de cycle de vie de compartiment, StorageGRID supprime automatiquement un objet lorsque la dernière période de la règle ILM se termine et qu'aucun autre placement n'est spécifié pour l'objet.

> L'action d'expiration dans un cycle de vie des compartiments S3 remplace toujours les paramètres ILM. Par conséquent, un objet peut être conservé dans la grille même après l'expiration des instructions ILM de placement de l'objet.

Suppression des marqueurs de suppression S3

Lorsqu'un objet versionné est supprimé, StorageGRID crée un marqueur de suppression en tant que version actuelle de l'objet. Pour supprimer le marqueur de suppression de zéro octet du compartiment, le client S3 doit supprimer explicitement la version de l'objet. Les marqueurs de suppression ne sont pas supprimés par ILM, les règles de cycle de vie des compartiments ou la suppression d'objets dans les opérations de compartiment.

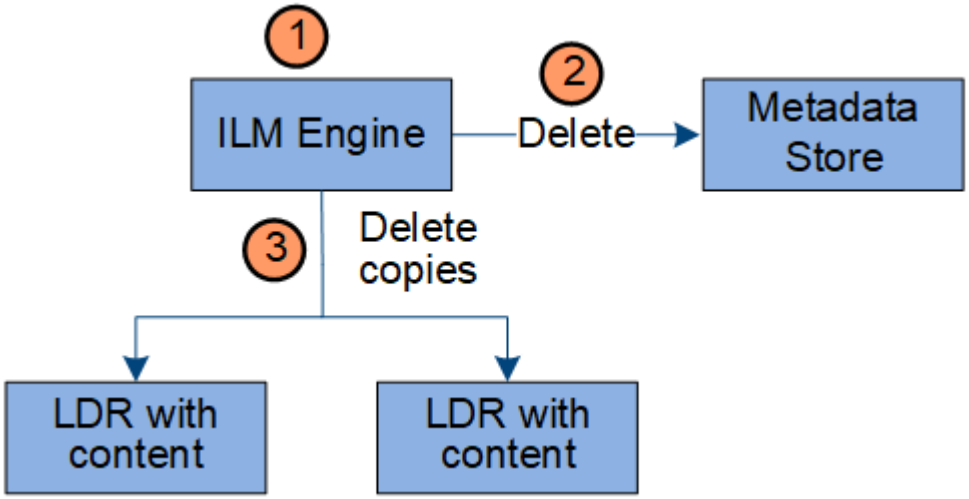
Flux de données pour les suppressions client



1. Le service LDR reçoit une requête de suppression de l'application cliente.

2. Le service LDR met à jour le magasin de métadonnées afin que l'objet soit supprimé des requêtes client et demande au moteur ILM de supprimer toutes les copies des données d'objet.
3. L'objet est supprimé du système. Le magasin de métadonnées est mis à jour pour supprimer les métadonnées d'objet.

Flux de données pour les suppressions ILM



1. Le moteur ILM détermine que l'objet doit être supprimé.
2. Le moteur ILM informe le magasin de métadonnées. Le magasin de métadonnées met à jour les métadonnées d'objet afin que l'objet soit supprimé des requêtes client.
3. Le moteur ILM supprime toutes les copies de l'objet. Le magasin de métadonnées est mis à jour pour supprimer les métadonnées d'objet.

Utilisation de la gestion du cycle de vie des informations

La gestion du cycle de vie des informations (ILM) permet de contrôler le placement, la durée et le comportement d'ingestion de tous les objets de votre système StorageGRID. Les règles ILM déterminent la façon dont StorageGRID stocke les objets au fil du temps. Vous configurez une ou plusieurs règles ILM, puis les ajoutez à une règle ILM.

Une grille n'a qu'une seule règle active à la fois. Une politique peut contenir plusieurs règles.

Les règles ILM définissent :

- Les objets à stocker. Une règle peut s'appliquer à tous les objets ou vous pouvez spécifier des filtres pour identifier les objets auxquels une règle s'applique. Par exemple, une règle ne peut s'appliquer qu'aux objets associés à certains comptes de locataire, à des compartiments S3 spécifiques, à des conteneurs Swift ou à des valeurs de métadonnées spécifiques.
- Type et emplacement de stockage. Les objets peuvent être stockés sur des nœuds de stockage, dans des pools de stockage cloud ou sur des nœuds d'archivage.
- Le type de copie d'objet effectuée. Les copies peuvent être répliquées ou codées en fonction de l'effacement.
- Pour les copies répliquées, le nombre de copies effectuées.
- Pour les copies avec code d'effacement, le schéma de code d'effacement utilisé.

- Évolution au fil du temps vers l'emplacement de stockage et le type de copies d'un objet
- La protection des données objet lors de l'ingestion des objets dans la grille (placement synchrone ou double allocation).

Les métadonnées d'objet ne sont pas gérées par les règles ILM. Les métadonnées d'objet sont stockées dans la base de données Cassandra, dans ce qu'on appelle un magasin de métadonnées. Trois copies des métadonnées des objets sont automatiquement conservées sur chaque site afin de protéger les données contre les pertes.

Exemple de règle ILM

À titre d'exemple, une règle ILM peut spécifier les éléments suivants :

- Appliquer uniquement aux objets appartenant au locataire A.
- Faites deux copies répliquées de ces objets et stockez chaque copie sur un site différent.
- Conservez les deux copies « pour toujours », ce qui signifie que StorageGRID ne les supprimera pas automatiquement. À la place, StorageGRID les conserve jusqu'à leur suppression par une demande de suppression de client ou avant l'expiration d'un cycle de vie de compartiment.
- Utilisez l'option équilibrée pour le comportement d'ingestion : l'instruction de placement sur deux sites est appliquée dès que le locataire A enregistre un objet dans StorageGRID, à moins qu'il ne soit pas possible d'effectuer immédiatement les deux copies requises.

  Par exemple, si le site 2 est injoignable lorsque le locataire A enregistre un objet, StorageGRID effectue deux copies provisoires sur les nœuds de stockage du site 1. Dès que le site 2 sera disponible, StorageGRID effectuera la copie requise sur ce site.

Évaluation des objets par une règle ILM

La règle ILM active de votre système StorageGRID contrôle le placement, la durée et le comportement d'ingestion de tous les objets.

Lorsque des clients enregistrent des objets dans StorageGRID, les objets sont évalués en fonction du jeu ordonné de règles ILM de la politique active, comme suit :

1. Si les filtres de la première règle de la règle correspondent à un objet, celui-ci est ingéré conformément au comportement d'ingestion de cette règle et stocké conformément aux instructions de placement de cette règle.
2. Si les filtres de la première règle ne correspondent pas à l'objet, l'objet est évalué par rapport à chaque règle ultérieure de la règle jusqu'à ce qu'une correspondance soit établie.
3. Si aucune règle ne correspond à un objet, les instructions de comportement d'ingestion et de placement de la règle par défaut de cette règle sont appliquées. La règle par défaut est la dernière règle d'une stratégie et ne peut pas utiliser de filtres. Elle doit s'appliquer à tous les locataires, à tous les compartiments et à toutes les versions d'objet.

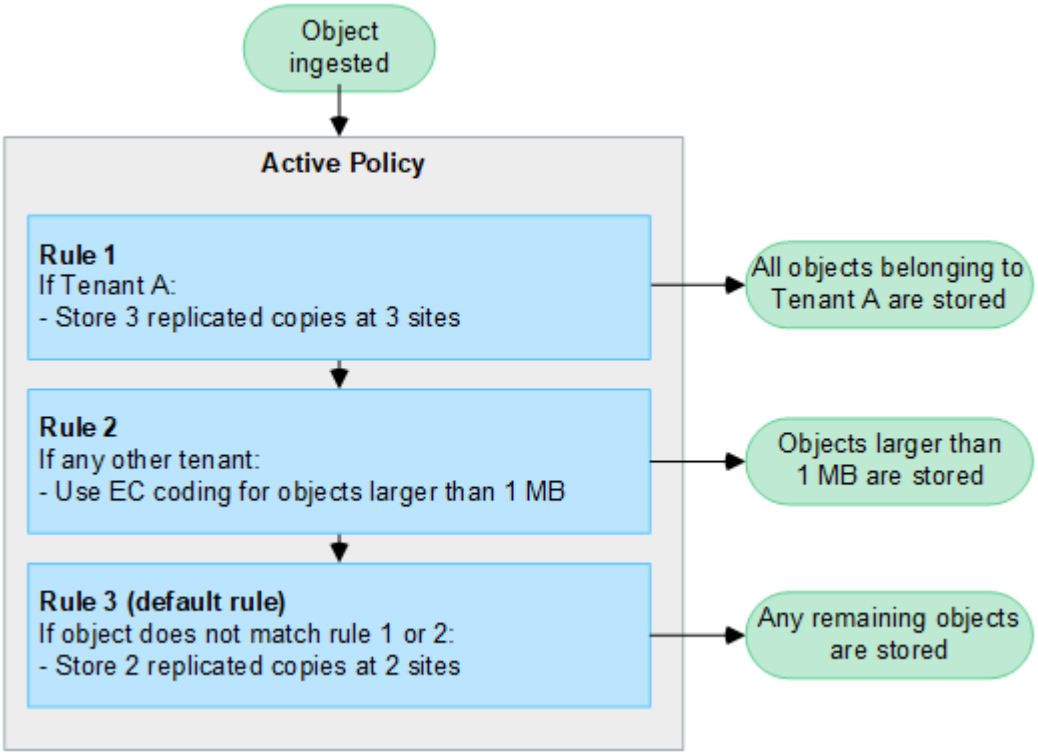
Exemple de règle ILM

À titre d'exemple, une politique ILM peut contenir trois règles ILM pour spécifier :

- **Règle 1 : copies répliquées pour le locataire A**
  - Faites correspondre tous les objets appartenant au locataire A.
  - Stockez ces objets sous forme de trois copies répliquées sur trois sites.

- Les objets appartenant à d'autres locataires ne correspondent pas à la règle 1, ils sont donc évalués par rapport à la règle 2.

- **Règle 2 : code d'effacement pour les objets supérieurs à 1 Mo**
  - Faites correspondre tous les objets d'autres locataires, mais uniquement s'ils sont supérieurs à 1 Mo. Ces objets plus volumineux sont stockés au moyen d'un code d'effacement de 6+3 sur trois sites.
  - Ne correspond pas aux objets de 1 Mo ou moins, ces objets sont donc évalués par rapport à la règle 3.
- **Règle 3 : 2 copies 2 centres de données** (par défaut)
  - Est la dernière règle et la règle par défaut de la règle. N'utilise pas de filtres.
  - Faites deux copies répliquées de tous les objets qui ne correspondent pas à la règle 1 ou à la règle 2 (objets qui n'appartiennent pas au locataire A de 1 Mo ou moins).



Informations associées

- "Gestion des objets avec ILM"

Découvrez StorageGRID

Explorez le Grid Manager

L'interface graphique Web du gestionnaire de grid permet de configurer, de gérer et de surveiller votre système StorageGRID.

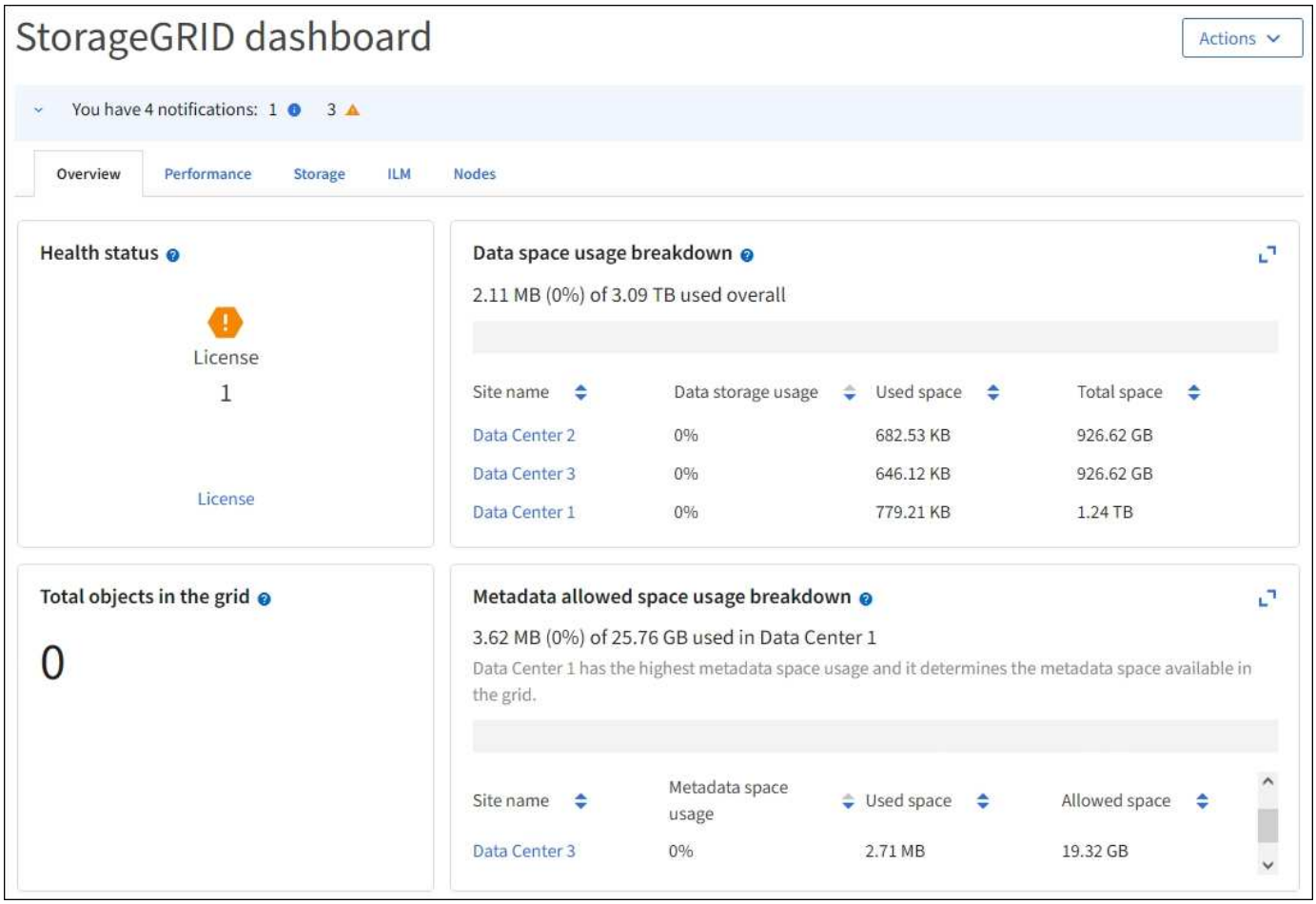
Lorsque vous vous connectez à Grid Manager, vous vous connectez à un noeud d'administration. Chaque système StorageGRID comprend un nœud d'administration principal et un nombre quelconque de nœuds d'administration non primaires. Vous pouvez vous connecter à n'importe quel nœud d'administration et chaque nœud d'administration affiche une vue similaire du système StorageGRID.

Vous pouvez accéder au Gestionnaire de grille à l'aide d'un "navigateur web pris en charge".

Tableau de bord de Grid Manager

Lorsque vous vous connectez pour la première fois au Gestionnaire de grille, vous pouvez utiliser le tableau de bord pour surveiller les activités du système en un coup d'œil.

Le tableau de bord contient des informations sur l'état et les performances du système, l'utilisation du stockage, les processus ILM, les opérations S3 et Swift, ainsi que les nœuds de la grille. Vous pouvez configurer le tableau de bord en le sélectionnant dans un ensemble de cartes contenant les informations dont vous avez besoin pour surveiller efficacement votre système.



Pour une explication des informations affichées sur chaque carte, sélectionnez l'icône d'aide pour cette carte.

En savoir plus >>

- "Afficher et configurer le tableau de bord"

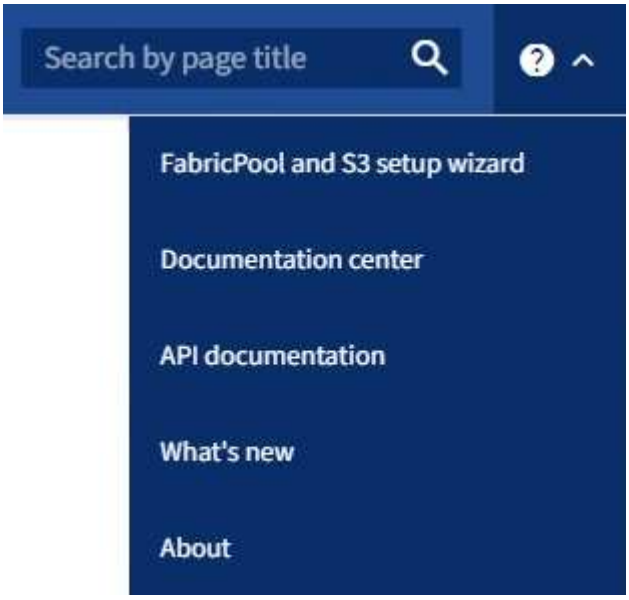
Champ de recherche

Le champ **Search** de la barre d'en-tête vous permet de naviguer rapidement vers une page spécifique dans Grid Manager. Par exemple, vous pouvez entrer **km** pour accéder à la page serveur de gestion des clés (KMS). Vous pouvez utiliser **Search** pour rechercher des entrées dans la barre latérale du Gestionnaire de grille et dans les menus Configuration, Maintenance et support.

Menu aide

Le menu d'aide Permet d'accéder aux assistants d'installation FabricPool et S3, au centre de documentation StorageGRID de la version actuelle et à la documentation de l'API. Vous pouvez également

déterminer la version de StorageGRID actuellement installée.

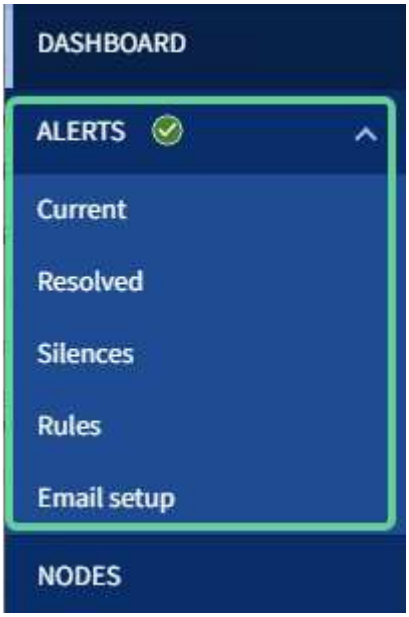


En savoir plus >>

- "Utilisez l'assistant d'installation FabricPool"
- "Utilisation de l'assistant d'installation S3"
- "Utilisez l'API de gestion du grid"

Menu alertes

Le menu alertes offre une interface facile à utiliser pour détecter, évaluer et résoudre les problèmes susceptibles de se produire lors du fonctionnement de StorageGRID.



Dans le menu alertes, vous pouvez effectuer les opérations suivantes :

- Examiner les alertes en cours
- Examiner les alertes résolues

- Configurez les silences pour supprimer les notifications d'alerte
- Définissez des règles d'alerte pour les conditions qui déclenchent des alertes
- Configurez le serveur de messagerie pour les notifications d'alerte

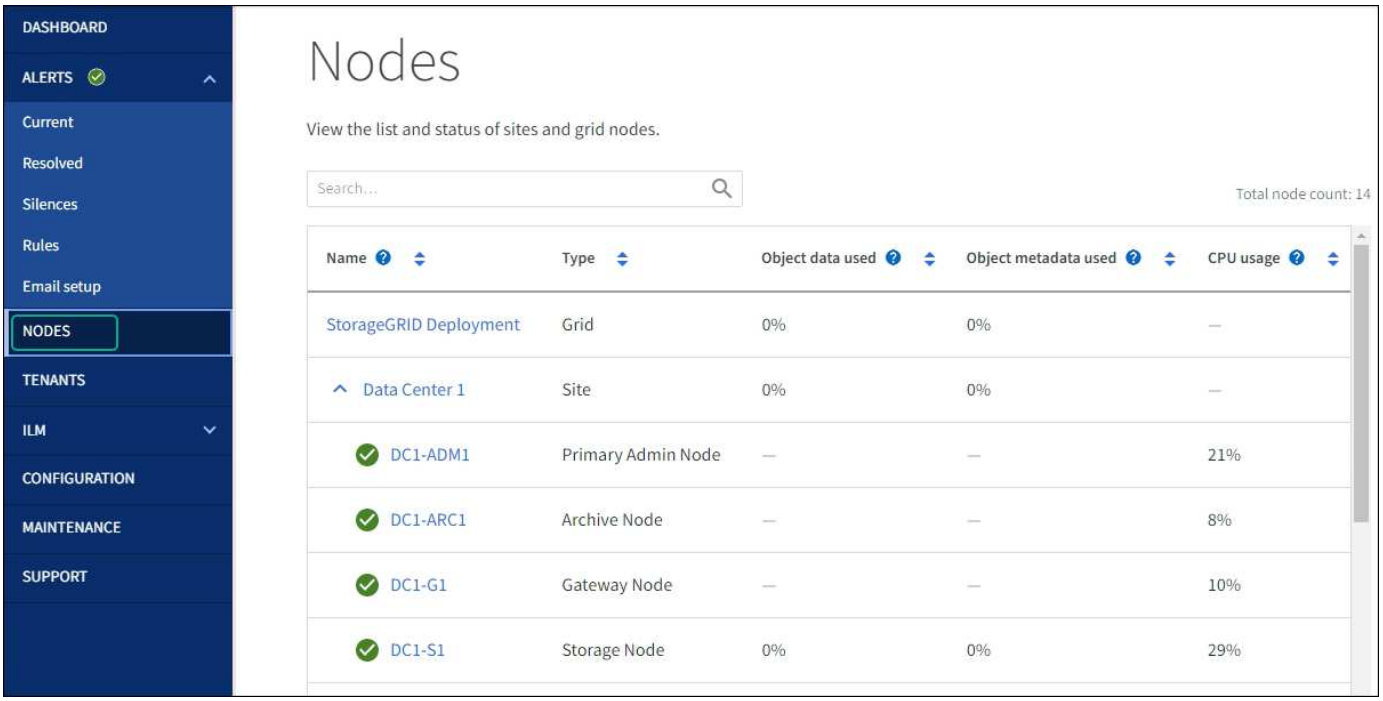
En savoir plus >>

- "Gérer les alertes"

Page nœuds

La page nœuds affiche des informations sur l'ensemble de la grille, sur chaque site de la grille et sur chaque nœud d'un site.

La page d'accueil nœuds affiche des mesures combinées pour l'ensemble de la grille. Pour afficher les informations d'un site ou nœud particulier, sélectionnez le site ou le nœud.



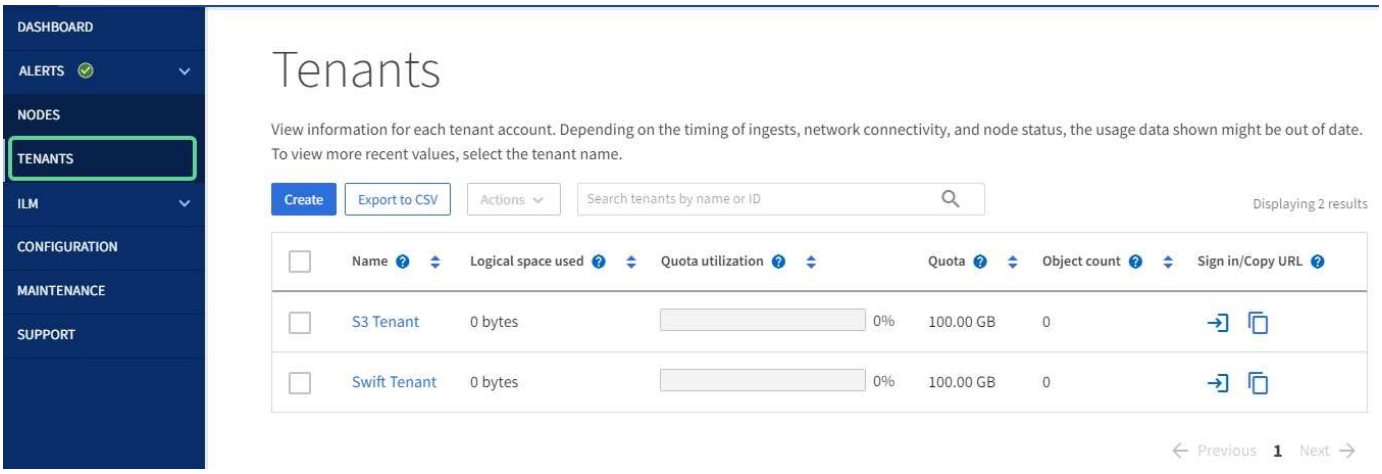
En savoir plus >>

- "Afficher la page nœuds"

Page locataires

La page des locataires vous permet de créer et de surveiller les comptes de locataires pour votre système StorageGRID. Vous devez créer au moins un compte de tenant pour spécifier qui peut stocker et récupérer des objets et la fonctionnalité qui leur est disponible.

La page locataires fournit également des détails sur l'utilisation pour chaque locataire, y compris la quantité de stockage utilisée et le nombre d'objets. Si vous définissez un quota lors de la création du locataire, vous pouvez voir la part utilisée de ce quota.



En savoir plus >>

- "Gérer les locataires"
- "Utilisez un compte de locataire"

Menu ILM

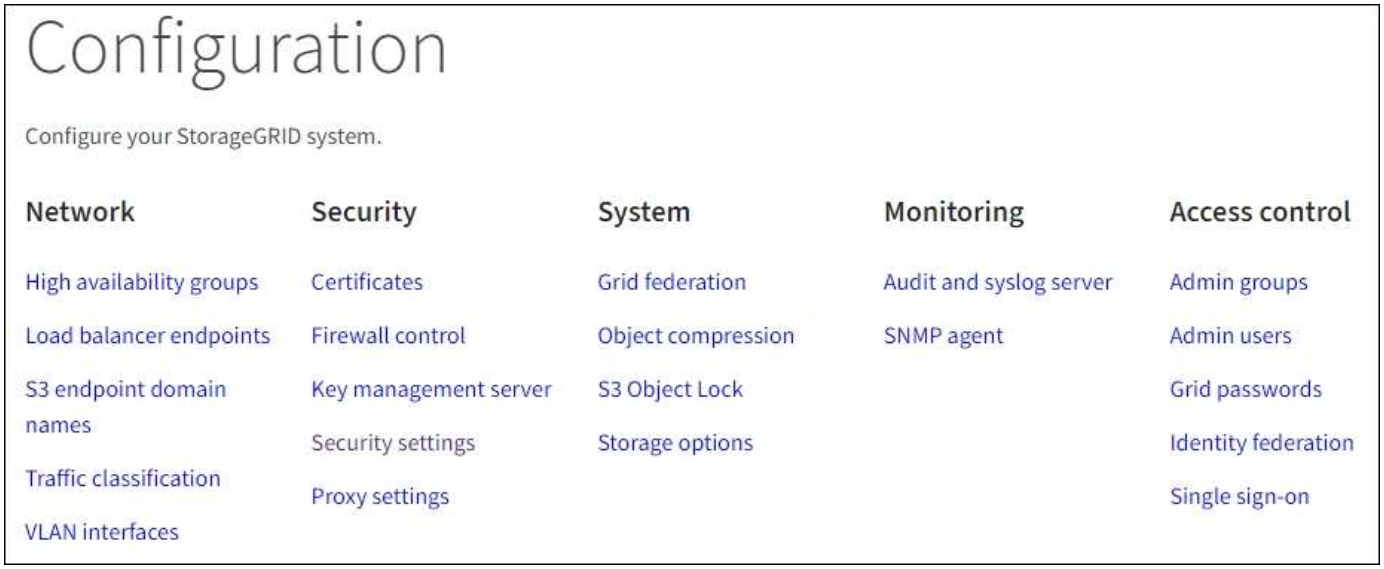
Le menu ILM vous permet de configurer les règles et règles de gestion du cycle de vie des informations (ILM) qui régissent la durabilité et la disponibilité des données. Vous pouvez également saisir un identifiant d'objet pour afficher les métadonnées de cet objet.

En savoir plus >>

- "Utilisation de la gestion du cycle de vie des informations"
- "Gestion des objets avec ILM"

Menu Configuration

Le menu Configuration vous permet de spécifier les paramètres réseau, les paramètres de sécurité, les paramètres système, les options de surveillance et les options de contrôle d'accès.



Tâches réseau

Les tâches réseau incluent :

- "Gestion des groupes haute disponibilité"
- "Gestion des terminaux d'équilibrage de la charge"
- "Configuration des noms de domaine de terminaux S3"
- "Gestion des stratégies de classification du trafic"
- "Configuration des interfaces VLAN"

Tâches de sécurité

Les tâches de sécurité comprennent :

- "Gestion des certificats de sécurité"
- "Gestion des contrôles de pare-feu internes"
- "Configuration des serveurs de gestion des clés"
- Configuration des paramètres de sécurité, y compris "Règles TLS et SSH", "options de sécurité du réseau et des objets", et le "délai d'inactivité du navigateur dépassé".
- Configuration des paramètres d'un "Proxy de stockage" ou un "Proxy d'administration"

Tâches système

Les tâches système incluent :

- À l'aide de "fédération des grilles" Pour cloner les informations de compte de locataire et répliquer les données d'objet entre deux systèmes StorageGRID.
- Vous pouvez également activer le "Compresser les objets stockés" option.
- "Gestion du verrouillage d'objet S3"
- Présentation des options de stockage telles que "segmentation d'objet" et "filigranes de volume de stockage".

Tâches de surveillance

Les tâches de surveillance incluent :

- "Configuration des messages d'audit et des destinations des journaux"
- "Utilisation de la surveillance SNMP"

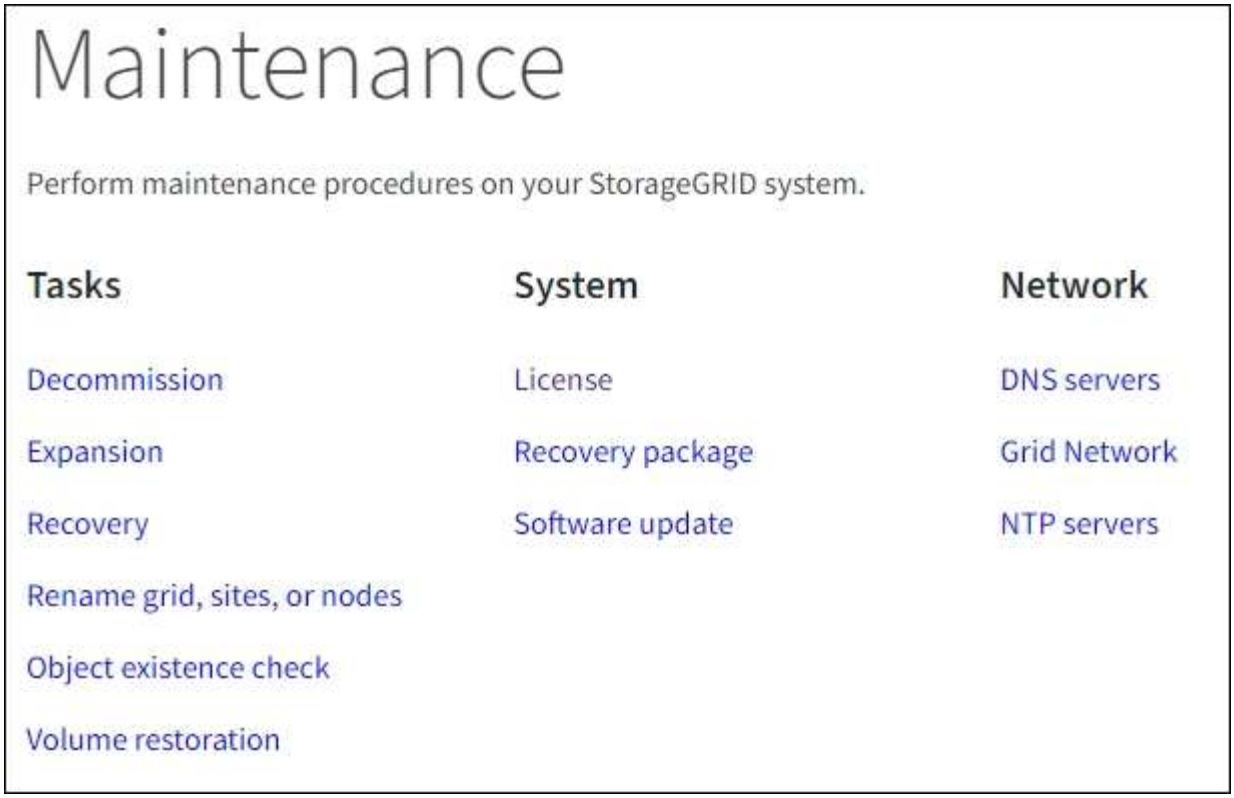
Tâches de contrôle d'accès

Les tâches de contrôle d'accès comprennent :

- "Gestion des groupes d'administration"
- "Gestion des utilisateurs admin"
- Remplacement du "phrase secrète de provisionnement" ou "mots de passe de la console de nœuds"
- "Utilisation de la fédération des identités"
- "Configuration de SSO"

Menu Maintenance

Le menu Maintenance vous permet d'effectuer des tâches de maintenance, de maintenance du système et de maintenance du réseau.



Tâches

Les tâches de maintenance sont les suivantes :

- "Désaffectation des opérations" pour supprimer les sites et les nœuds de grille inutilisés
- "Opérations d'extension" pour ajouter de nouveaux nœuds et sites de grille
- "Procédures de restauration des nœuds de la grille" pour remplacer un nœud défaillant et restaurer les données
- "Renommer les procédures" pour modifier les noms d'affichage de votre grille, de vos sites et de vos nœuds
- "Opérations de vérification de l'existence des objets" pour vérifier l'existence (bien que ce ne soit pas l'exactitude) des données d'objet
- "Opérations de restauration de volumes"

Système

Les tâches de maintenance du système que vous pouvez effectuer sont les suivantes :

- "Affichage des informations de licence StorageGRID" ou "mise à jour des informations de licence"
- Génération et téléchargement du "Package de restauration"
- Effectuer des mises à jour logicielles StorageGRID, y compris des mises à niveau logicielles, des correctifs et des mises à jour du logiciel SANtricity OS sur des appliances sélectionnées
  - "Procédure de mise à jour"
  - "Procédure de correctif"
  - "Mettez à niveau le système d'exploitation SANtricity sur des contrôleurs de stockage SG6000 à l'aide de Grid Manager"

- "Mettez à niveau le système d'exploitation SANtricity sur les contrôleurs de stockage SG5700 à l'aide de Grid Manager"

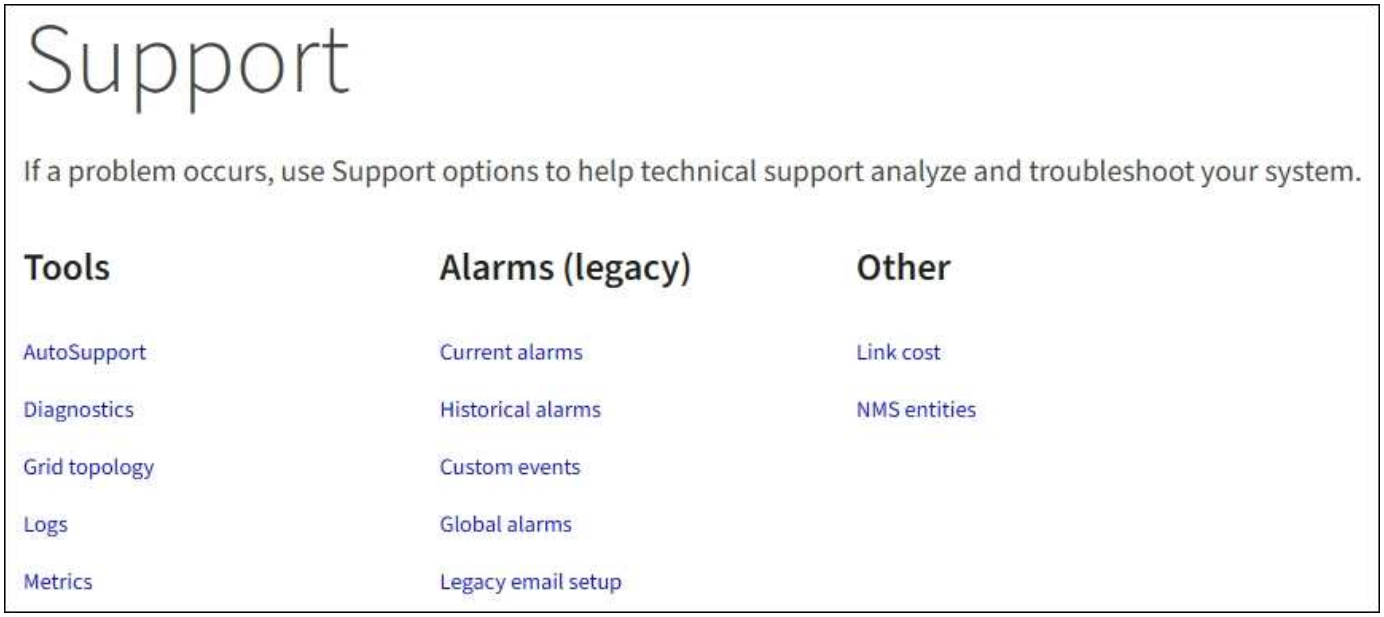
Le réseau

Les tâches de maintenance réseau que vous pouvez effectuer sont les suivantes :

- "Configuration des serveurs DNS"
- "Mise à jour des sous-réseaux réseau de la grille"
- "Gestion des serveurs NTP"

Menu support

Le menu support fournit des options qui vous aident à analyser et à dépanner votre système. Le menu support comporte trois parties : Outils, alarmes (héritées) et autres.



Outils

À partir de la section Outils du menu support, vous pouvez :

- "Configurez AutoSupport"
- "Exécuter les diagnostics" sur l'état actuel de la grille
- "Accédez à l'arborescence topologie de la grille" pour afficher des informations détaillées sur les nœuds de grille, les services et les attributs
- "Collecte de fichiers journaux et de données système"
- "Examinez les metrics de support"

> Les outils disponibles dans l'option **Metrics** sont destinés à être utilisés par le support technique. Certaines fonctions et options de menu de ces outils ne sont intentionnellement pas fonctionnelles.

Alarmes (existantes)

Dans la section alarmes (héritage) du menu support, vous pouvez consulter les alarmes actuelles, historiques et globales, configurer des événements personnalisés et configurer des notifications par e-mail pour les alarmes héritées. Voir "Gestion des alarmes (système hérité)".

> Bien que le système d'alarme existant continue d'être pris en charge, le système d'alerte offre des avantages significatifs et est plus facile à utiliser.

Explorez le Gestionnaire de locataires

Le gestionnaire de locataires est une interface graphique basée sur un navigateur qui permet aux utilisateurs locataires d'accéder pour configurer, gérer et surveiller leurs comptes de stockage.

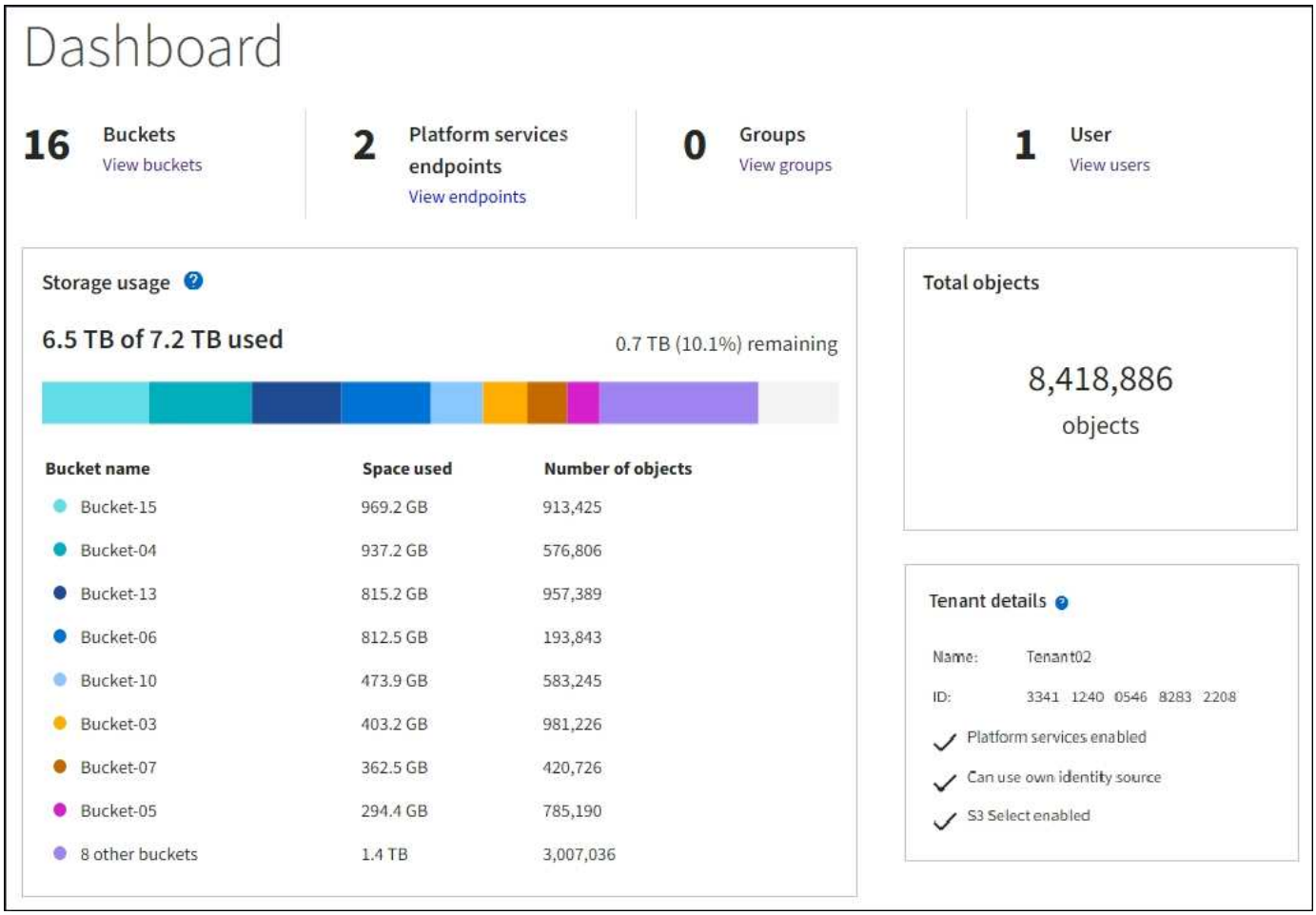
Lorsque les utilisateurs locataires se connectent au Gestionnaire de locataires, ils se connectent à un noeud d'administration.

Tableau de bord du gestionnaire des locataires

Une fois qu'un administrateur du grid a créé un compte de locataire à l'aide de Grid Manager ou de l'API Grid Management, les locataires peuvent se connecter au Gestionnaire de locataires.

Le tableau de bord du gestionnaire de locataires permet aux utilisateurs locataires de surveiller l'utilisation du stockage en un coup d'œil. Le panneau Storage usage contient la liste des compartiments (S3) ou conteneurs (Swift) les plus grands du locataire. La valeur espace utilisé correspond à la quantité totale de données d'objet dans le compartiment ou le conteneur. Le graphique à barres représente les tailles relatives de ces compartiments ou conteneurs.

La valeur affichée au-dessus du graphique à barres est une somme de l'espace utilisé pour tous les compartiments ou conteneurs du locataire. Si le nombre maximal de gigaoctets, de téraoctets ou de pétaoctets disponibles pour le locataire a été spécifié lors de la création du compte, le volume de quota utilisé et restant est également affiché.



Menu stockage (S3)

Le menu stockage est disponible uniquement pour les comptes de tenant S3. Ce menu permet aux utilisateurs de S3 de gérer les clés d'accès, de créer, de gérer et de supprimer des compartiments, de gérer les terminaux des services de plateforme et d'afficher toutes les connexions de fédération de grille qu'ils sont autorisés à utiliser.

Mes clés d'accès

Les locataires S3 peuvent gérer les clés d'accès comme suit :

- Les utilisateurs disposant de l'autorisation gérer vos propres identifiants S3 peuvent créer ou supprimer leurs propres clés d'accès S3.
- Les utilisateurs disposant de l'autorisation d'accès racine peuvent gérer les clés d'accès du compte racine S3, de leur propre compte et de tous les autres utilisateurs. Les clés d'accès racine offrent également un accès complet aux compartiments et objets du locataire, sauf si une règle de compartiment est explicitement désactivée.

> La gestion des clés d'accès pour les autres utilisateurs s'effectue à partir du menu gestion des accès.

Seaux

Les utilisateurs de locataires S3 disposant des autorisations appropriées peuvent effectuer les tâches suivantes pour leurs compartiments :

- Créer des compartiments
- Activer le verrouillage des objets S3 pour un nouveau compartiment (le verrouillage des objets S3 est activé pour le système StorageGRID)
- Mettez à jour les paramètres de niveau de cohérence
- Activer et désactiver les mises à jour de l'heure du dernier accès
- Activer ou suspendre la gestion des versions d'objets
- Mettre à jour la conservation par défaut du verrouillage d'objet S3
- Configurer le partage de ressources inter-sources (CORS)
- Supprime tous les objets d'un compartiment
- Supprimer les compartiments vides
- Utilisez le "Console S3 expérimentale" pour gérer les objets de compartiment

Si un administrateur du grid a activé l'utilisation de services de plateforme pour le compte du locataire, un utilisateur locataire S3 avec les autorisations appropriées peut également effectuer les tâches suivantes :

- Configurez les notifications d'événements S3, qui peuvent être envoyées à un service de destination prenant en charge Amazon simple notification Service™ (Amazon SNS).
- Configurez la réplication CloudMirror, qui permet au locataire de répliquer automatiquement les objets dans un compartiment S3 externe.
- Configurer l'intégration de la recherche, qui envoie des métadonnées d'objet à un index de recherche de destination lors de la création ou de la suppression d'un objet ou de ses métadonnées ou balises.

Terminaux des services de plateforme

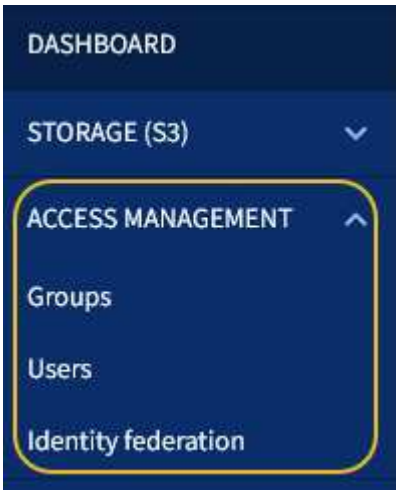
Si un administrateur du grid a activé l'utilisation des services de plateforme pour le compte de locataire, un utilisateur locataire S3 disposant de l'autorisation gérer les terminaux peut configurer un terminal de destination pour chaque service de plateforme.

Connexions de fédération de grille

Si un administrateur du grid a activé l'utilisation d'une connexion de fédération grid pour le compte de locataire, un utilisateur de locataire S3 disposant de l'autorisation d'accès racine peut afficher le nom de la connexion et accéder à la page d'informations sur le compartiment pour chaque compartiment pour lequel la réplication inter-grid est activée, et afficher l'erreur la plus récente à se produire lorsque les données de compartiment étaient répliquées sur l'autre grille de la connexion. Voir "Afficher les connexions de fédération de grille".

Accès au menu gestion

Le menu gestion des accès permet aux locataires StorageGRID d'importer des groupes d'utilisateurs à partir d'un référentiel d'identité fédéré et d'attribuer des autorisations de gestion. Les locataires peuvent également gérer des groupes et des utilisateurs de locataires locaux, sauf si la connexion unique (SSO) est appliquée à l'ensemble du système StorageGRID.



Informations associées

- "Utilisez un compte de locataire"

Instructions de mise en réseau

Directives de mise en réseau : présentation

Utilisez ces instructions pour en savoir plus sur l'architecture StorageGRID et les topologies réseau, ainsi que sur les exigences de configuration et de provisionnement réseau.

À propos de ces instructions

Ces instructions fournissent des informations permettant de créer l'infrastructure réseau StorageGRID avant de déployer et de configurer des nœuds StorageGRID. Utilisez ces directives pour vous assurer que la communication peut se produire entre tous les nœuds de la grille et entre la grille et les clients et services externes.

Les clients externes et les services externes doivent se connecter aux réseaux StorageGRID pour exécuter les fonctions suivantes :

- Le stockage et la récupération des données d'objet

- Recevoir des notifications par e-mail
- Accès à l'interface de gestion StorageGRID (Grid Manager et tenant Manager)
- Accéder au partage d'audit (facultatif)
- Fournir des services tels que :
  - NTP (Network Time Protocol)
  - Système de noms de domaine (DNS)
  - Serveur de gestion des clés (KMS)

Le réseau StorageGRID doit être configuré de manière appropriée pour gérer le trafic pour ces fonctions, et bien plus encore.

Avant de commencer

La configuration de la mise en réseau d'un système StorageGRID nécessite un haut niveau d'expérience en matière de commutation Ethernet, de mise en réseau TCP/IP, de sous-réseaux, de routage réseau et de pare-feu.

Avant de configurer la mise en réseau, familiarisez-vous avec l'architecture StorageGRID, comme décrit dans "Découvrez StorageGRID".

Après avoir déterminé les réseaux StorageGRID que vous souhaitez utiliser et la façon dont ces réseaux seront configurés, vous pouvez installer et configurer les nœuds StorageGRID en suivant les instructions appropriées.

Installation des nœuds basés sur logiciel

- "Installez Red Hat Enterprise Linux ou CentOS"
- "Installez Ubuntu ou Debian"
- "Installez VMware"

Installez les nœuds d'appliance

- "Installez le matériel de l'appliance"

Configuration et administration du logiciel StorageGRID

- "Administrer StorageGRID"
- "Notes de mise à jour"

Types de réseau StorageGRID

Les nœuds de grille d'un système StorageGRID traitent *le trafic de grille*, *le trafic admin* et *le trafic client*. Vous devez configurer le réseau de façon appropriée pour gérer ces trois types de trafic et pour assurer le contrôle et la sécurité.

Types de trafic

Type de trafic	Description	Type de réseau
Trafic grid	Trafic StorageGRID interne qui circule entre tous les nœuds de la grille. Tous les nœuds de la grille doivent pouvoir communiquer avec tous les autres nœuds de la grille sur ce réseau.	Réseau Grid (requis)
Trafic administratif	Trafic utilisé pour l'administration et la maintenance du système.	Réseau d'administration (facultatif), Réseau VLAN (facultatif)
Trafic client	Le trafic qui circule entre les applications client externes et la grille, y compris toutes les demandes de stockage objet des clients S3 et Swift.	Réseau client (facultatif), Réseau VLAN (facultatif)

Vous pouvez configurer la mise en réseau de l'une des manières suivantes :

- Réseau Grid uniquement
- Réseaux Grid et d'administration
- Réseaux Grid et clients
- Grid, Admin et réseaux client

Le Grid Network est obligatoire et peut gérer l'ensemble du trafic de la grille. Les réseaux d'administration et de client peuvent être inclus au moment de l'installation ou ajoutés ultérieurement pour s'adapter aux modifications des exigences. Bien que le réseau Admin et le réseau client soient facultatifs, lorsque vous utilisez ces réseaux pour gérer le trafic administratif et client, le réseau Grid peut être isolé et sécurisé.

Les ports internes ne sont accessibles que sur le réseau Grid. Les ports externes sont accessibles à partir de tous les types de réseaux. Cette flexibilité offre de nombreuses options pour la conception d'un déploiement StorageGRID et la configuration du filtrage externe des adresses IP et des ports dans les commutateurs et les pare-feu. Voir "communications internes sur les nœuds de la grille" et "communications externes".

Interfaces réseau

Des nœuds StorageGRID sont connectés à chaque réseau au moyen des interfaces spécifiques suivantes :

Le réseau	Nom de l'interface
Réseau Grid (requis)	eth0
Réseau d'administration (facultatif)	eth1
Réseau client (facultatif)	eth2

Pour plus de détails sur le mappage de ports virtuels ou physiques aux interfaces réseau de nœuds, reportez-vous aux instructions d'installation :

Nœuds basés sur logiciel

- "Installez Red Hat Enterprise Linux ou CentOS"

- "Installez Ubuntu ou Debian"
- "Installez VMware"

Nœuds d'appliance

- "Appliance de stockage SGF6112"
- "Dispositif de stockage SG6000"
- "Appliance de stockage SG5700"
- "Appareils de services SG100 et SG1000"

Informations réseau pour chaque nœud

Vous devez configurer ce qui suit pour chaque réseau activé sur un nœud :

- Adresse IP
- Masque de sous-réseau
- Adresse IP de la passerelle

Vous ne pouvez configurer qu'une seule combinaison adresse IP/masque/passerelle pour chacun des trois réseaux de chaque nœud de la grille. Si vous ne souhaitez pas configurer de passerelle pour un réseau, vous devez utiliser l'adresse IP comme adresse de passerelle.

Groupes haute disponibilité

Les groupes haute disponibilité (HA) permettent d'ajouter des adresses IP virtuelles (VIP) à l'interface Grid ou client Network. Pour plus d'informations, voir "Gérez les groupes haute disponibilité".

Réseau Grid

Le réseau Grid est requis. Il est utilisé pour tout le trafic StorageGRID interne. Le réseau Grid assure la connectivité entre tous les nœuds de la grille, sur tous les sites et sous-réseaux. Tous les nœuds du réseau Grid doivent pouvoir communiquer avec tous les autres nœuds. Le réseau Grid peut être composé de plusieurs sous-réseaux. Les réseaux contenant des services de grille critiques, tels que NTP, peuvent également être ajoutés en tant que sous-réseaux de grille.

StorageGRID ne prend pas en charge la traduction d'adresses réseau (NAT) entre les nœuds.

Le réseau Grid Network peut être utilisé pour tout le trafic administrateur et tout le trafic client, même si le réseau Admin et le réseau client sont configurés. La passerelle réseau Grid est la passerelle par défaut du nœud, sauf si le réseau client est configuré sur le nœud.

Lors de la configuration du réseau Grid, vous devez vous assurer que le réseau est sécurisé par des clients non approuvés, tels que ceux sur Internet ouvert.

Notez les exigences et détails suivants pour la passerelle Grid Network :

- La passerelle Grid Network doit être configurée s'il existe plusieurs sous-réseaux de grille.
- La passerelle Grid Network est la passerelle par défaut du nœud jusqu'à la fin de la configuration du grid.
- Les routes statiques sont générées automatiquement pour tous les nœuds de tous les sous-réseaux configurés dans la liste de sous-réseaux du réseau Grid global.

- Si un réseau client est ajouté, la passerelle par défaut passe de la passerelle réseau Grid à la passerelle réseau client lorsque la configuration de la grille est terminée.

Réseau d'administration

Le réseau d'administration est facultatif. Une fois configuré, il peut être utilisé pour l'administration du système et le trafic de maintenance. Le réseau Admin est généralement un réseau privé et n'a pas besoin d'être routable entre les nœuds.

Vous pouvez choisir les nœuds de la grille sur lesquels le réseau Admin doit être activé.

Lorsque vous utilisez le réseau d'administration, le trafic d'administration et de maintenance n'a pas besoin de se déplacer à travers le réseau Grid. Les utilisations courantes du réseau d'administration sont les suivantes :

- Accès aux interfaces utilisateur Grid Manager et tenant Manager.
- Accès aux services critiques tels que les serveurs NTP, les serveurs DNS, les serveurs de gestion externe des clés (KMS) et les serveurs LDAP (Lightweight Directory Access Protocol).
- Accès aux journaux d'audit sur les nœuds d'administration.
- Accès SSH (Secure Shell Protocol) pour la maintenance et le support.

Le réseau Admin n'est jamais utilisé pour le trafic interne du grid. Une passerelle réseau Admin est fournie et permet au réseau Admin de communiquer avec plusieurs sous-réseaux externes. Cependant, la passerelle réseau Admin n'est jamais utilisée comme passerelle par défaut du nœud.

Notez la configuration requise et les détails suivants pour la passerelle réseau d'administration :

- La passerelle réseau d'administration est requise si des connexions sont effectuées en dehors du sous-réseau du réseau d'administration ou si plusieurs sous-réseaux du réseau d'administration sont configurés.
- Des routes statiques sont créées pour chaque sous-réseau configuré dans la liste de sous-réseaux du réseau Admin du nœud.

Réseau client

Le réseau client est facultatif. Lorsqu'elle est configurée, elle permet d'offrir l'accès à des services de grid pour les applications client telles que S3 et Swift. Si vous prévoyez d'accéder aux données StorageGRID à une ressource externe (par exemple, un pool de stockage cloud ou le service de réplication StorageGRID CloudMirror), la ressource externe peut également utiliser le réseau client. Les nœuds de la grille peuvent communiquer avec tout sous-réseau accessible via la passerelle réseau client.

Vous pouvez choisir les nœuds de la grille sur lesquels le réseau client doit être activé. Tous les nœuds n'ont pas besoin d'être sur le même réseau client et les nœuds ne communiquent jamais entre eux sur le réseau client. Le réseau client ne fonctionne pas tant que l'installation de la grille n'est pas terminée.

Pour plus de sécurité, vous pouvez spécifier que l'interface client Network d'un nœud n'est pas fiable afin que le réseau client soit plus restrictif que les connexions autorisées. Si l'interface réseau client d'un nœud n'est pas fiable, l'interface accepte les connexions sortantes telles que celles utilisées par la réplication CloudMirror, mais accepte uniquement les connexions entrantes sur les ports qui ont été explicitement configurés comme des noeuds finaux d'équilibreur de charge. Voir "Gérer les contrôles de pare-feu" et "Configurer les terminaux de l'équilibreur de charge".

Lorsque vous utilisez un réseau client, le trafic client n'a pas besoin de circuler sur le réseau Grid. Le trafic réseau de la grille peut être séparé sur un réseau sécurisé et non routable. Les types de nœud suivants sont souvent configurés avec un réseau client :

- Nœuds de passerelle, car ces nœuds fournissent l'accès au service StorageGRID Load Balancer et aux clients S3 et Swift à la grille.
- Nœuds de stockage, car ces nœuds donnent accès aux protocoles S3 et Swift, ainsi qu'aux pools de stockage cloud et au service de réplication CloudMirror.
- Nœuds d'administration, pour s'assurer que les utilisateurs locataires peuvent se connecter au Gestionnaire de locataires sans avoir à utiliser le réseau Admin.

Notez les éléments suivants pour la passerelle réseau client :

- La passerelle réseau client est requise si le réseau client est configuré.
- Lorsque la configuration de la grille est terminée, la passerelle réseau client devient la route par défaut pour le nœud de la grille.

Réseaux VLAN facultatifs

Si nécessaire, vous pouvez éventuellement utiliser des réseaux LAN virtuels (VLAN) pour le trafic client et pour certains types de trafic d'administration. Cependant, le trafic du grid ne peut pas utiliser d'interface VLAN. Le trafic StorageGRID interne entre les nœuds doit toujours utiliser le réseau Grid sur eth0.

Pour prendre en charge l'utilisation des VLAN, vous devez configurer une ou plusieurs interfaces sur un nœud en tant qu'interfaces de jonction au niveau du commutateur. Vous pouvez configurer l'interface réseau Grid (eth0) ou l'interface réseau client (eth2) en tant que ligne réseau, ou vous pouvez ajouter des interfaces de ligne réseau au nœud.

Si eth0 est configuré en tant que ligne réseau, le trafic réseau Grid passe par l'interface native de la ligne de réseau, comme configuré sur le commutateur. De même, si eth2 est configuré en tant que jonction et que le réseau client est également configuré sur le même nœud, le réseau client utilise le VLAN natif du port de jonction, tel qu'il est configuré sur le switch.

Seul le trafic administratif entrant, tel qu'utilisé pour le trafic SSH, Grid Manager ou tenant Manager, est pris en charge sur les réseaux VLAN. Le trafic sortant, tel qu'utilisé pour les réseaux NTP, DNS, LDAP, KMS et Cloud Storage pools, n'est pas pris en charge sur les réseaux VLAN.

> ⓘ Les interfaces VLAN peuvent être ajoutées aux nœuds d'administration et aux nœuds de passerelle uniquement. Vous ne pouvez pas utiliser d'interface VLAN pour l'accès des clients ou des administrateurs aux nœuds de stockage ou aux nœuds d'archivage.

Voir "Configurez les interfaces VLAN" pour instructions et instructions.

Les interfaces VLAN sont utilisées uniquement dans les groupes haute disponibilité et des adresses VIP sont attribuées sur le nœud actif. Voir "Gérez les groupes haute disponibilité" pour instructions et instructions.

Exemples de topologie réseau

Topologie du réseau grid

La topologie réseau la plus simple est créée en configurant le réseau Grid uniquement.

Lorsque vous configurez le réseau Grid, vous définissez l'adresse IP de l'hôte, le masque de sous-réseau et l'adresse IP de la passerelle pour l'interface eth0 de chaque nœud de la grille.

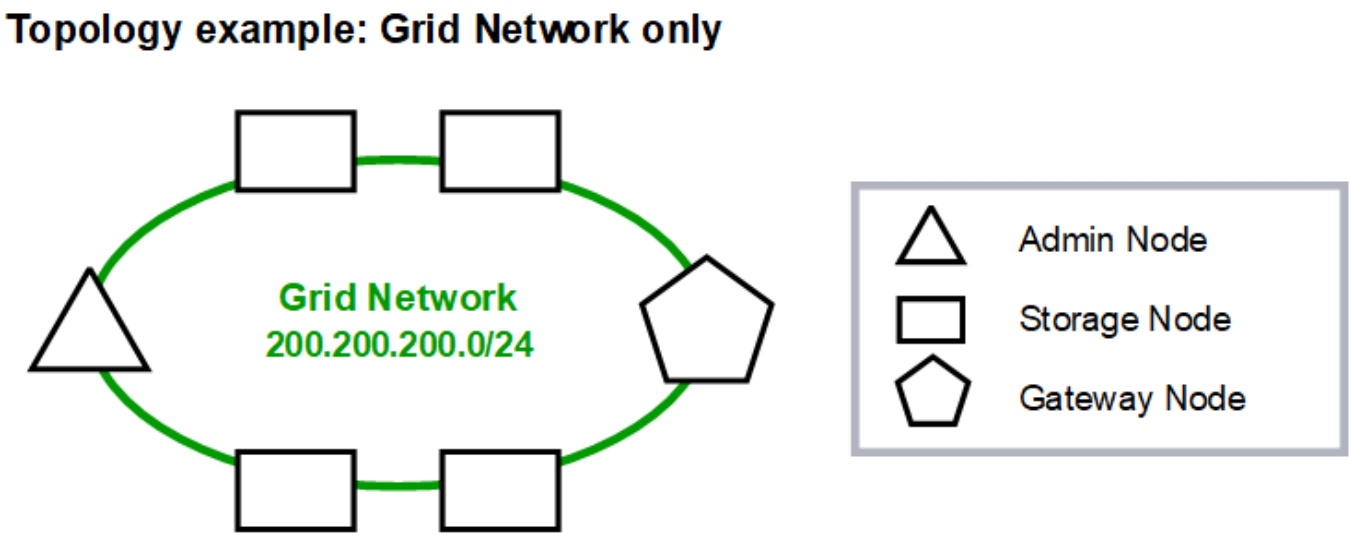
Lors de la configuration, vous devez ajouter tous les sous-réseaux du réseau Grid à la liste de sous-réseaux

du réseau Grid (GNSL). Cette liste inclut tous les sous-réseaux de tous les sites, et peut également inclure des sous-réseaux externes permettant l'accès à des services critiques tels que NTP, DNS ou LDAP.

Lors de l'installation, l'interface réseau de grille applique des routes statiques pour tous les sous-réseaux du GNSL et définit la route par défaut du nœud vers la passerelle réseau de grille si elle est configurée. Le GNSL n'est pas nécessaire s'il n'y a pas de réseau client et que la passerelle réseau Grid est la route par défaut du nœud. Des routes hôte vers tous les autres nœuds de la grille sont également générées.

Dans cet exemple, tout le trafic partage le même réseau, y compris le trafic lié aux demandes des clients S3 et Swift et aux fonctions d'administration et de maintenance.

Cette topologie est adaptée aux déploiements sur un seul site qui ne sont pas disponibles en externe, aux démonstrations de faisabilité ou aux déploiements de test, ou lorsqu'un équilibreur de charge tiers agit comme limite d'accès client. Lorsque cela est possible, le réseau Grid doit être utilisé exclusivement pour le trafic interne. Le réseau d'administration et le réseau client disposent d'autres restrictions de pare-feu qui bloquent le trafic externe vers les services internes. L'utilisation du réseau Grid pour le trafic client externe est prise en charge, mais cette utilisation offre moins de couches de protection.



Provisioned

GNSL → 200.200.200.0/24		
	Grid Network	
Nodes	**IP/mask**	**Gateway**
Admin	200.200.200.32/24	200.200.200.1
Storage	200.200.200.33/24	200.200.200.1
Storage	200.200.200.34/24	200.200.200.1
Storage	200.200.200.35/24	200.200.200.1
Storage	200.200.200.36/24	200.200.200.1
Gateway	200.200.200.37/24	200.200.200.1

System Generated

Nodes	Routes			Type	From
All	0.0.0.0/0	→	200.200.200.1	Default	Grid Network gateway
	200.200.200.0/24	→	eth0	Link	Interface IP/mask

Topologie du réseau d'administration

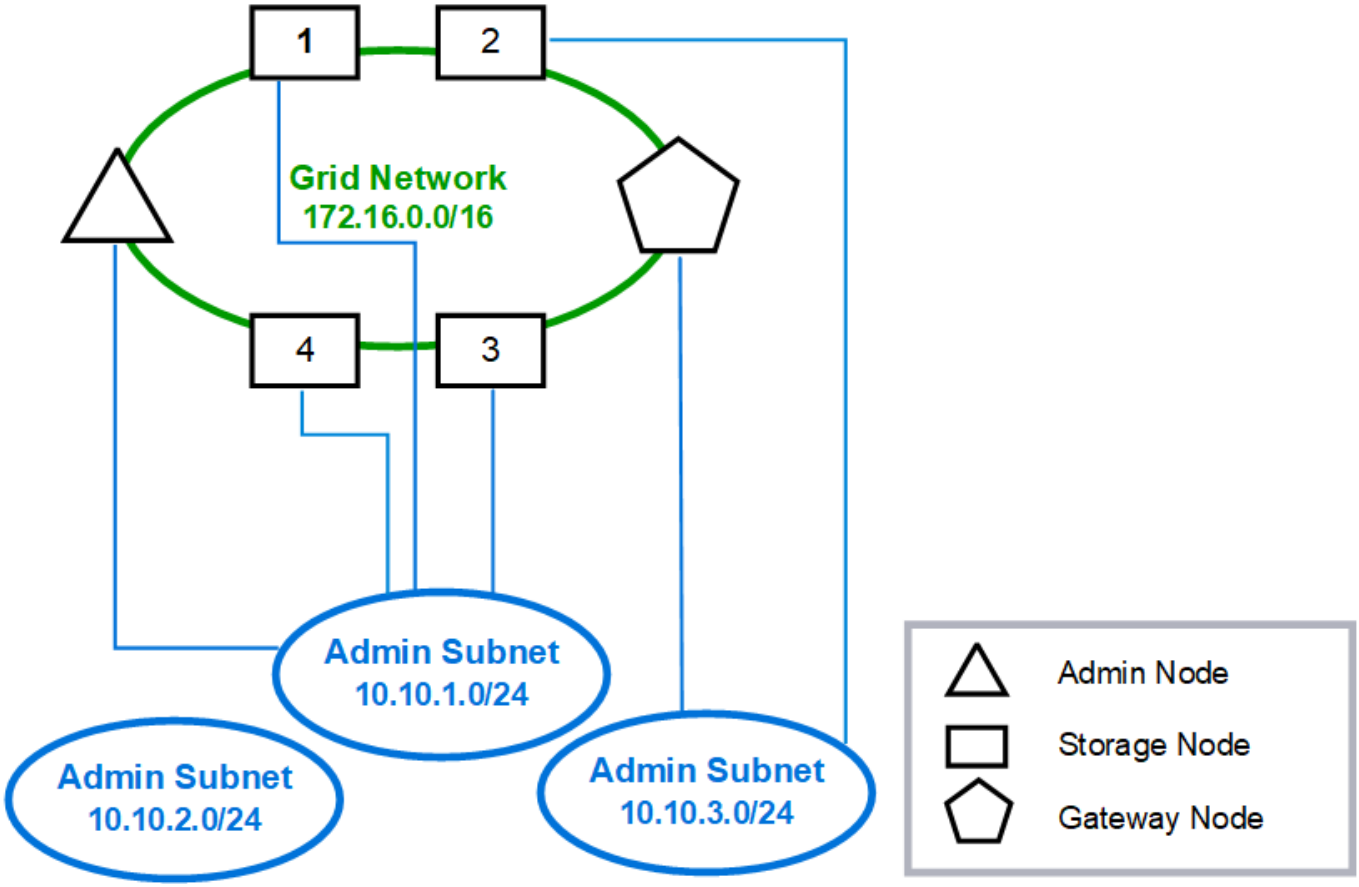
L'utilisation d'un réseau d'administration est facultative. L'une des façons de pouvoir utiliser un réseau d'administration et un réseau de grille consiste à configurer un réseau de grille routable et un réseau d'administration limité pour chaque nœud.

Lorsque vous configurez le réseau Admin, vous définissez l'adresse IP de l'hôte, le masque de sous-réseau et l'adresse IP de la passerelle pour l'interface eth1 de chaque nœud de la grille.

Le réseau d'administration peut être unique à chaque nœud et peut être composé de plusieurs sous-réseaux. Chaque nœud peut être configuré avec une liste de sous-réseau externe (AESL, Admin External Subnet List). L'AESL répertorie les sous-réseaux accessibles sur le réseau Admin pour chaque nœud. L'AESL doit également inclure les sous-réseaux de tous les services que la grille aura accès via le réseau d'administration, tels que NTP, DNS, KMS et LDAP. Des routes statiques sont appliquées pour chaque sous-réseau dans l'AESL.

Dans cet exemple, le réseau Grid est utilisé pour le trafic lié aux demandes des clients S3 et Swift et à la gestion des objets. Pendant que le réseau Admin est utilisé pour les fonctions administratives.

Topology example: Grid and Admin Networks



Provisioned

GNSL → 172.16.0.0/16
AESL (all) → 10.10.1.0/24 10.10.2.0/24 10.10.3.0/24

	Grid Network		Admin Network	
Nodes	**IP/mask**	**Gateway**	**IP/mask**	**Gateway**
Admin	172.16.200.32/24	172.16.200.1	10.10.1.10/24	10.10.1.1
Storage 1	172.16.200.33/24	172.16.200.1	10.10.1.11/24	10.10.1.1
Storage 2	172.16.200.34/24	172.16.200.1	10.10.3.65/24	10.10.3.1
Storage 3	172.16.200.35/24	172.16.200.1	10.10.1.12/24	10.10.1.1
Storage 4	172.16.200.36/24	172.16.200.1	10.10.1.13/24	10.10.1.1
Gateway	172.16.200.37/24	172.16.200.1	10.10.3.66/24	10.10.3.1

System Generated

Nodes	**Routes**			**Type**	**From**
All	0.0.0.0/0	→	172.16.200.1	Default	Grid Network gateway
Admin, Storage 1, 3, and 4	172.16.0.0/16	→	eth0	Static	GNSL
	10.10.1.0/24	→	eth1	Link	Interface IP/mask
	10.10.2.0/24	→	10.10.1.1	Static	AESL
	10.10.3.0/24	→	10.10.1.1	Static	AESL
Storage 2, Gateway	172.16.0.0/16	→	eth0	Static	GNSL
	10.10.1.0/24	→	10.10.3.1	Static	AESL
	10.10.2.0/24	→	10.10.3.1	Static	AESL
	10.10.3.0/24	→	eth1	Link	Interface IP/mask

Topologie du réseau client

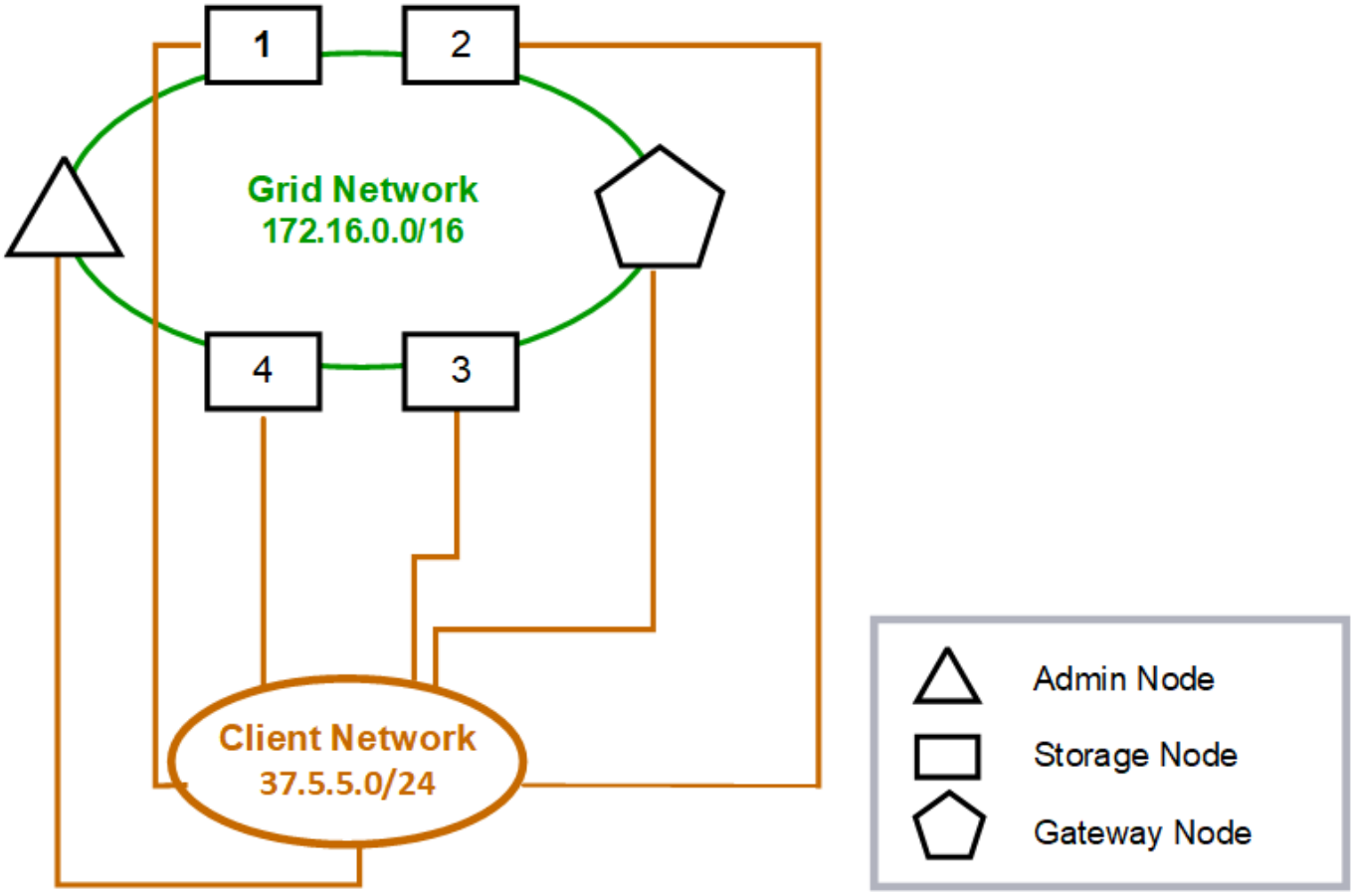
L'utilisation d'un réseau client est facultative. L'utilisation d'un réseau client permet de séparer le trafic réseau client (S3 et Swift, par exemple) du trafic interne du grid, ce qui améliore la sécurité du réseau grid. Le trafic administratif peut être géré par le client ou le réseau de grille lorsque le réseau d'administration n'est pas configuré.

Lorsque vous configurez le réseau client, vous définissez l'adresse IP de l'hôte, le masque de sous-réseau et l'adresse IP de la passerelle pour l'interface eth2 du nœud configuré. Le réseau client de chaque nœud peut être indépendant du réseau client sur n'importe quel autre nœud.

Si vous configurez un réseau client pour un nœud au cours de l'installation, la passerelle par défaut du nœud passe de la passerelle réseau Grid à la passerelle réseau client une fois l'installation terminée. Si un réseau client est ajouté ultérieurement, la passerelle par défaut du nœud change de la même manière.

Dans cet exemple, le réseau client est utilisé pour les demandes de clients S3 et Swift ainsi que pour les fonctions d'administration, tandis que le réseau Grid est dédié aux opérations de gestion d'objets internes.

Topology example: Grid and Client Networks



Provisioned

GNSL → 172.16.0.0/16			
	Grid Network	Client Network	
Nodes	IP/mask	IP/mask	Gateway
Admin	172.16.200.32/24	37.5.5.10/24	37.5.5.1
Storage	172.16.200.33/24	37.5.5.11/24	37.5.5.1
Storage	172.16.200.34/24	37.5.5.12/24	37.5.5.1
Storage	172.16.200.35/24	37.5.5.13/24	37.5.5.1
Storage	172.16.200.36/24	37.5.5.14/24	37.5.5.1
Gateway	172.16.200.37/24	37.5.5.15/24	37.5.5.1

System Generated

Nodes	Routes			Type	From
All	0.0.0.0/0	→	37.5.5.1	Default	Client Network gateway
	172.16.0.0/16	→	eth0	Link	Interface IP/mask
	37.5.5.0/24	→	eth2	Link	Interface IP/mask

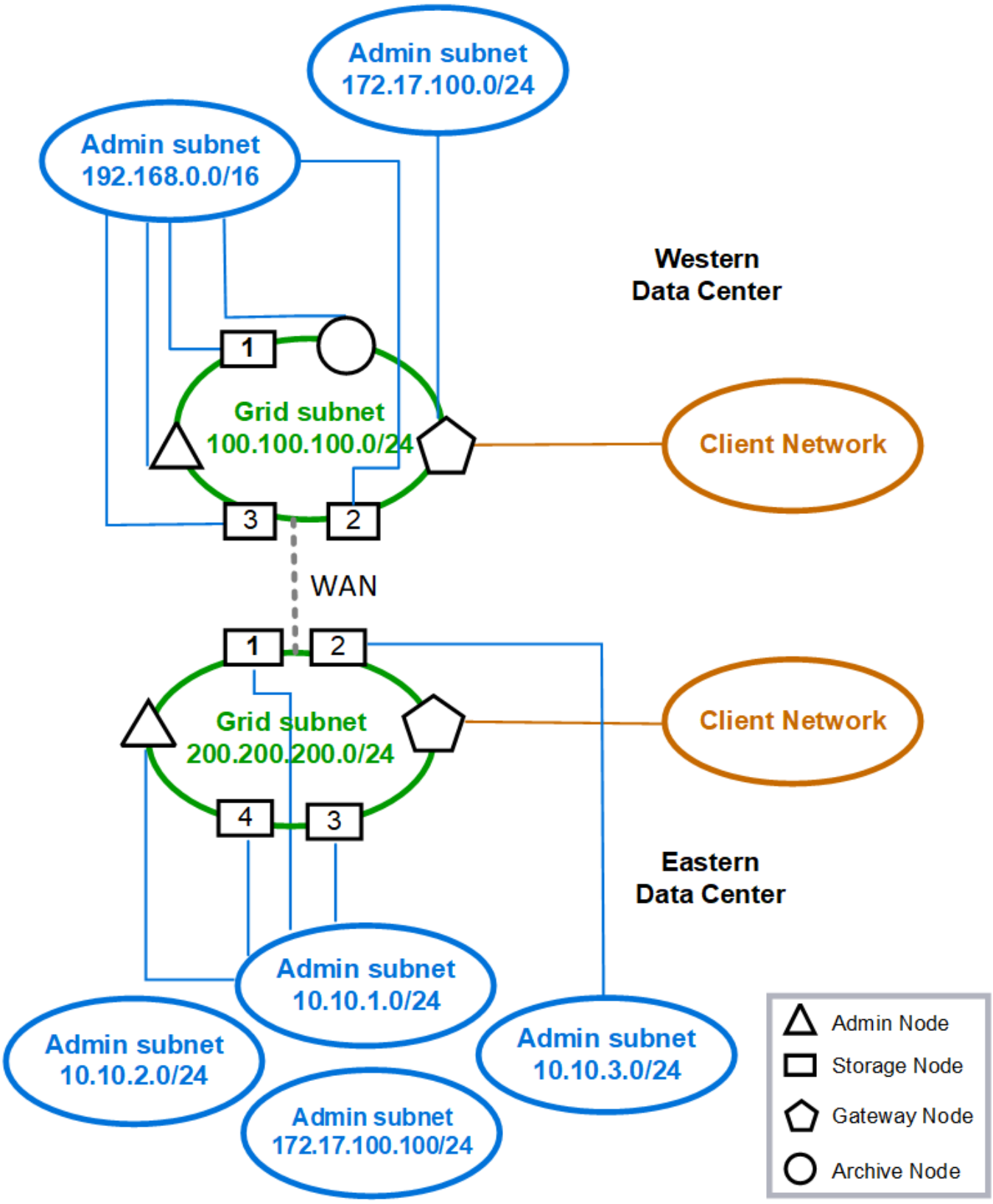
Topologie des trois réseaux

Vous pouvez configurer les trois réseaux en une topologie de réseau composée d'un réseau Grid privé, de réseaux d'administration spécifiques à un site délimité et de réseaux clients ouverts. L'utilisation de terminaux d'équilibrage de charge et de réseaux clients non fiables peut fournir une sécurité supplémentaire si nécessaire.

Dans cet exemple :

- Le réseau Grid est utilisé pour le trafic réseau lié aux opérations de gestion d'objets internes.
- Le réseau Admin est utilisé pour le trafic lié aux fonctions administratives.
- Le réseau client est utilisé pour le trafic lié aux demandes des clients S3 et Swift.

Topology example: Grid, Admin, and Client Networks



Configuration réseau requise

Vous devez vérifier que l'infrastructure réseau et la configuration actuelles peuvent prendre en charge la conception de réseau StorageGRID planifiée.

Exigences générales de mise en réseau

Tous les déploiements StorageGRID doivent être capables de prendre en charge les connexions suivantes.

Ces connexions peuvent se produire via la grille, les réseaux d'administration ou les réseaux clients, ou les combinaisons de ces réseaux comme illustré dans les exemples de topologie réseau.

- **Connexions de gestion** : connexions entrantes d'un administrateur au nœud, généralement via SSH. Accès par navigateur Web au gestionnaire de grille, au gestionnaire de locataires et au programme d'installation de l'appliance StorageGRID.
- **Connexions serveur NTP** : connexion UDP sortante qui reçoit une réponse UDP entrante.

  Au moins un serveur NTP doit être accessible par le nœud d'administration principal.

- **Connexions serveur DNS** : connexion UDP sortante qui reçoit une réponse UDP entrante.
- **Connexions serveur LDAP/Active Directory** : connexion TCP sortante à partir du service identité sur les nœuds de stockage.
- **AutoSupport** : connexion TCP sortante des nœuds d'administration vers l'un ou l'autre `support.netapp.com` ou un proxy configuré par le client.
- **Serveur de gestion de clés externe** : connexion TCP sortante à partir de chaque nœud d'appliance avec cryptage de nœud activé.
- Connexions TCP entrantes des clients S3 et Swift.
- Des demandes sortantes provenant de services de plateforme StorageGRID, tels que la réplication CloudMirror ou depuis Cloud Storage pools.

Si StorageGRID ne parvient pas à contacter l'un des serveurs NTP ou DNS provisionnés à l'aide des règles de routage par défaut, il tente automatiquement de contacter tous les réseaux (grille, administrateur et client) tant que les adresses IP des serveurs DNS et NTP sont spécifiées. Si les serveurs NTP ou DNS peuvent être atteints sur n'importe quel réseau, StorageGRID crée automatiquement des règles de routage supplémentaires afin de s'assurer que le réseau est utilisé pour toutes les tentatives de connexion futures.

Bien que vous puissiez utiliser ces routes hôtes automatiquement découvertes, en général, vous devez configurer manuellement les routes DNS et NTP pour garantir la connectivité en cas d'échec de la détection automatique.

Si vous n'êtes pas prêt à configurer les réseaux optionnels Admin et client pendant le déploiement, vous pouvez configurer ces réseaux lorsque vous approuvez les nœuds de grille pendant les étapes de configuration. En outre, vous pouvez configurer ces réseaux après l'installation, à l'aide de l'outil Modifier IP (voir "Configurez les adresses IP").

Seules les connexions des clients S3 et Swift, ainsi que les connexions d'administration SSH, Grid Manager et tenant Manager sont prises en charge via les interfaces VLAN. Connexions sortantes, telles que les serveurs NTP, DNS, LDAP, AutoSupport et KMS Doit passer directement sur les interfaces client, Admin ou Grid Network. Si l'interface est configurée comme une jonction pour prendre en charge les interfaces VLAN, ce trafic transite par le VLAN natif de l'interface, comme configuré au niveau du commutateur.

Réseaux étendus (WAN) pour plusieurs sites

Lors de la configuration d'un système StorageGRID avec plusieurs sites, la connexion WAN entre sites doit avoir une bande passante minimale de 25 Mbit/s dans chaque direction avant de prendre en compte le trafic client. La réplication des données ou le code d'effacement entre les sites, l'extension de nœud ou de site, la restauration de nœuds et les autres opérations ou configurations nécessitent une bande passante supplémentaire.

Les besoins réels minimaux en bande passante WAN dépendent de l'activité du client et du schéma de protection ILM. Pour obtenir de l'aide sur l'estimation des besoins minimaux en bande passante WAN, contactez votre consultant en services professionnels NetApp.

Connexions pour les nœuds d'administration et les nœuds de passerelle

Les nœuds d'administration doivent toujours être sécurisés par des clients non fiables, comme ceux sur Internet ouvert. Vous devez vous assurer qu'aucun client non approuvé ne peut accéder à un nœud d'administration sur le réseau Grid, le réseau Admin ou le réseau client.

Les nœuds d'administration et les nœuds de passerelle que vous prévoyez d'ajouter aux groupes haute disponibilité doivent être configurés avec une adresse IP statique. Pour plus d'informations, voir "Gérez les groupes haute disponibilité".

Utilisation de la traduction d'adresses réseau (NAT)

N'utilisez pas la traduction d'adresses réseau (NAT) sur le réseau de grille entre les nœuds de grille ou entre les sites StorageGRID. Lorsque vous utilisez des adresses IPv4 privées pour le réseau Grid, ces adresses doivent être directement routables à partir de chaque nœud de la grille sur chaque site. Toutefois, vous pouvez utiliser NAT entre des clients externes et des nœuds de grille, par exemple pour fournir une adresse IP publique pour un nœud de passerelle. L'utilisation de la fonction NAT pour relier un segment de réseau public n'est prise en charge que lorsque vous utilisez une application de tunneling transparente pour tous les nœuds de la grille, ce qui signifie que les nœuds de la grille ne nécessitent aucune connaissance des adresses IP publiques.

Exigences spécifiques au réseau

Respectez les exigences spécifiques à chaque type de réseau StorageGRID.

Passerelles et routeurs réseau

- Si elle est définie, la passerelle d'un réseau donné doit se trouver dans le sous-réseau du réseau spécifique.
- Si vous configurez une interface à l'aide d'un adressage statique, vous devez spécifier une adresse de passerelle autre que 0.0.0.0.
- Si vous ne disposez pas d'une passerelle, il est recommandé de définir l'adresse de la passerelle comme adresse IP de l'interface réseau.

Sous-réseaux

> Chaque réseau doit être connecté à son propre sous-réseau qui ne se chevauchent pas avec un autre réseau du nœud.

Les restrictions suivantes sont appliquées par le Grid Manager pendant le déploiement. Ils sont fournis ici pour vous aider dans la planification du réseau de pré-déploiement.

- Le masque de sous-réseau d'une adresse IP réseau ne peut pas être 255.255.255.254 ou 255.255.255.255 (/31 ou /32 en notation CIDR).
- Le sous-réseau défini par une adresse IP d'interface réseau et un masque de sous-réseau (CIDR) ne peut pas chevaucher le sous-réseau d'une autre interface configurée sur le même nœud.
- Le sous-réseau du réseau Grid pour chaque nœud doit être inclus dans le GNSL.
- Le sous-réseau Admin Network ne peut pas chevaucher le sous-réseau Grid Network, le sous-réseau client Network ou tout sous-réseau dans le GNSL.
- Les sous-réseaux de l'AESL ne peuvent pas se chevaucher avec les sous-réseaux de la GNSL.
- Le sous-réseau du réseau client ne peut pas chevaucher le sous-réseau du réseau Grid, le sous-réseau du réseau Admin, tout sous-réseau du réseau GNSL ou tout sous-réseau de l'AESL.

Réseau Grid

- Au moment du déploiement, chaque nœud de la grille doit être relié au réseau de la grille et doit pouvoir communiquer avec le nœud d'administration principal à l'aide de la configuration réseau que vous spécifiez lors du déploiement du nœud.
- Au cours des opérations normales de la grille, chaque nœud de la grille doit pouvoir communiquer avec tous les autres nœuds de la grille sur le réseau.

> Le réseau Grid doit être routable directement entre chaque nœud. La traduction d'adresses réseau (NAT) entre nœuds n'est pas prise en charge.

- Si le réseau Grid est composé de plusieurs sous-réseaux, ajoutez-les à la liste de sous-réseaux du réseau Grid (GNSL). Des routes statiques sont créées sur tous les nœuds pour chaque sous-réseau du GNSL.
- Si l'interface réseau Grid est configurée comme une jonction pour prendre en charge les interfaces VLAN, le VLAN natif de la jonction doit être le VLAN utilisé pour le trafic réseau Grid. Tous les nœuds grid doivent être accessibles via le VLAN natif du trunk.

Réseau d'administration

Le réseau d'administration est facultatif. Si vous envisagez de configurer un réseau d'administration, suivez les exigences et les instructions ci-dessous.

Les utilisations typiques du réseau d'administration incluent les connexions de gestion, AutoSupport, KMS et les connexions aux serveurs critiques tels que NTP, DNS et LDAP si ces connexions ne sont pas fournies via le réseau Grid ou le réseau client.

> Le réseau Admin et l'AESL peuvent être uniques à chaque nœud, tant que les services réseau et les clients souhaités sont accessibles.

> Vous devez définir au moins un sous-réseau sur le réseau d'administration pour activer les connexions entrantes à partir de sous-réseaux externes. Des routes statiques sont générées automatiquement sur chaque nœud pour chaque sous-réseau de l'AESL.

Réseau client

Le réseau client est facultatif. Si vous avez l'intention de configurer un réseau client, prenez en compte les considérations suivantes.

- Le réseau client est conçu pour prendre en charge le trafic des clients S3 et Swift. S'il est configuré, la passerelle réseau client devient la passerelle par défaut du nœud.
- Si vous utilisez un réseau client, vous pouvez protéger StorageGRID des attaques hostiles en acceptant le trafic client entrant uniquement sur les noeuds finaux de l'équilibreur de charge configurés explicitement. Voir "Configurer les terminaux de l'équilibreur de charge".
- Si l'interface réseau client est configurée comme une jonction pour prendre en charge les interfaces VLAN, déterminez si la configuration de l'interface réseau client (eth2) est nécessaire. S'il est configuré, le trafic réseau client transite par le VLAN natif du trunk, tel qu'il est configuré dans le commutateur.

Considérations relatives au réseau propres au déploiement

Déploiements Linux

Garantissant efficacité, fiabilité et sécurité, le système StorageGRID s'exécute sous Linux comme un ensemble de moteurs de mise en conteneurs. La configuration réseau liée au moteur de mise en conteneurs n'est pas requise dans un système StorageGRID.

Utilisez un périphérique sans lien, tel qu'une paire VLAN ou Ethernet virtuel (veth), pour l'interface réseau du conteneur. Spécifiez ce périphérique comme interface réseau dans le fichier de configuration de nœud.

> N'utilisez pas de périphérique de liaison ou de pont directement comme interface réseau du conteneur. Cela pourrait empêcher le démarrage du nœud en raison d'un problème de noyau lié à l'utilisation de macvlan avec des périphériques de liaison et de pont dans l'espace de noms de conteneur.

Reportez-vous aux instructions d'installation pour "Red Hat Enterprise Linux ou CentOS" ou "Ubuntu ou Debian" de nombreux déploiements.

Configuration réseau de l'hôte pour les déploiements de moteurs de conteneurs

Avant de démarrer votre déploiement StorageGRID sur une plateforme de moteur de conteneurs, déterminez les réseaux (Grid, Admin, client) que chaque nœud utilisera. Vous devez vous assurer que l'interface réseau de chaque nœud est configurée sur l'interface hôte physique ou virtuelle appropriée, et que chaque réseau dispose de suffisamment de bande passante.

Hôtes physiques

Si vous utilisez des hôtes physiques pour prendre en charge les nœuds grid :

- Vérifiez que tous les hôtes utilisent la même interface hôte pour chaque interface de nœud. Cette stratégie simplifie la configuration de l'hôte et permet la migration de nœuds à venir.
- Obtenir une adresse IP pour l'hôte physique lui-même.

> Une interface physique sur l'hôte peut être utilisée par l'hôte lui-même et un ou plusieurs nœuds exécutés sur l'hôte. Toutes les adresses IP attribuées à l'hôte ou aux nœuds utilisant cette interface doivent être uniques. L'hôte et le nœud ne peuvent pas partager d'adresses IP.

- Ouvrez les ports requis vers l'hôte.
- Si vous prévoyez d'utiliser des interfaces VLAN dans StorageGRID, l'hôte doit disposer d'une ou plusieurs interfaces de jonction qui fournissent l'accès aux VLAN souhaités. Ces interfaces peuvent être transmises

au conteneur de nœud comme eth0, eth2, ou comme interfaces supplémentaires. Pour ajouter une jonction ou des interfaces d'accès, consultez les éléments suivants :

- **RHEL ou CentOS (avant d'installer le nœud)** : "Créez des fichiers de configuration de nœud"
- **Ubuntu ou Debian (avant d'installer le nœud)** : "Créez des fichiers de configuration de nœud"
- **RHEL, CentOS, Ubuntu ou Debian (après l'installation du nœud)** : "Linux : ajoutez une jonction ou des interfaces d'accès à un nœud"

Recommandations minimales sur la bande passante

Le tableau suivant présente les recommandations minimales de bande passante pour chaque type de nœud StorageGRID et chaque type de réseau. Vous devez provisionner chaque hôte physique ou virtuel avec une bande passante réseau suffisante pour répondre aux besoins de bande passante minimale de l'agrégat pour le nombre et le type de nœuds StorageGRID que vous prévoyez d'exécuter sur cet hôte.

Type de nœud	Type de réseau		
	Grille	Admin	Client
	Bande passante LAN minimale	Admin	10 Gbits/s.
1 Gbit/s.	1 Gbit/s.	Passerelle	10 Gbits/s.
1 Gbit/s.	10 Gbits/s.	Stockage	10 Gbits/s.
1 Gbit/s.	10 Gbits/s.	Archivage	10 Gbits/s.

Ce tableau n'inclut pas la bande passante SAN, requise pour l'accès au stockage partagé. Si vous utilisez un stockage partagé accessible via Ethernet (iSCSI ou FCoE), vous devez provisionner des interfaces physiques distinctes sur chaque hôte pour fournir suffisamment de bande passante SAN. Pour éviter tout goulet d'étranglement, la bande passante SAN d'un hôte donné doit correspondre à peu près à la bande passante réseau du nœud de stockage de l'agrégat pour tous les nœuds de stockage exécutant cet hôte.

Utilisez le tableau pour déterminer le nombre minimal d'interfaces réseau à provisionner sur chaque hôte, en fonction du nombre et du type de nœuds StorageGRID que vous prévoyez d'exécuter sur cet hôte.

Par exemple, pour exécuter un nœud d'administration, un nœud de passerelle et un nœud de stockage sur un même hôte :

- Connecter les réseaux Grid et Admin sur le nœud d'administration (10 + 1 = 11 Gbit/s requis)
- Connecter les réseaux Grid et client sur le nœud passerelle (10 + 10 = 20 Gbit/s requis)
- Connexion du réseau Grid sur le nœud de stockage (10 Gbit/s requis)

Dans ce scénario, vous devez fournir un minimum de 11 + 20 + 10 = 41 Gbit/s de bande passante réseau, Qui peut être remplie par deux interfaces 40 Gbits/s ou cinq interfaces 10 Gbits/s, potentiellement agrégées dans les lignes réseau, puis partagées par les trois VLAN ou plus transportant les sous-réseaux Grid, Admin et client locaux au centre de données physique contenant l'hôte.

Pour connaître les méthodes recommandées de configuration des ressources physiques et réseau sur les

hôtes de votre cluster StorageGRID afin de préparer le déploiement StorageGRID, consultez les éléments suivants :

- "Configuration du réseau hôte (Red Hat Enterprise Linux ou CentOS)"
- "Configurer le réseau hôte (Ubuntu ou Debian)"

Mise en réseau et ports pour les services de plateforme et les pools de stockage cloud

Si vous prévoyez d'utiliser les services de plateforme StorageGRID ou les pools de stockage cloud, vous devez configurer la mise en réseau et les pare-feu des grilles pour vous assurer que les terminaux de destination peuvent être atteints.

Mise en réseau pour les services de plate-forme

Comme décrit dans "Gestion des services de plateforme pour les locataires" et "Qu'est-ce que les services de plateforme ?", Les services de plate-forme comprennent des services externes qui fournissent l'intégration de la recherche, la notification d'événements et la réplication CloudMirror.

Les services de plateforme requièrent l'accès depuis des nœuds de stockage qui hébergent le service ADC StorageGRID vers les terminaux de service externes. Voici quelques exemples d'accès à ce service :

- Sur les nœuds de stockage avec services ADC, configurez des réseaux d'administration uniques avec des entrées AESL qui roulent vers les terminaux cibles.
- Utilisez la route par défaut fournie par un réseau client. Si vous utilisez l'itinéraire par défaut, vous pouvez utiliser le "Fonction réseau client non fiable" pour limiter les connexions entrantes.

Mise en réseau pour les pools de stockage cloud

Les pools de stockage cloud nécessitent également l'accès des nœuds de stockage aux terminaux fournis par le service externe utilisé, comme Amazon S3 Glacier ou Microsoft Azure Blob Storage. Pour plus d'informations, reportez-vous à la section "Qu'est-ce qu'un pool de stockage cloud ?".

Ports pour les services de plateforme et les pools de stockage cloud

Par défaut, les services de plateforme et les communications de pool de stockage cloud utilisent les ports suivants :

- **80**: Pour les URI de point final qui commencent par `http`
- **443**: Pour les URI de point final qui commencent par `https`

Un port différent peut être spécifié lors de la création ou de la modification du noeud final. Voir "Référence du port réseau".

Si vous utilisez un serveur proxy non transparent, vous devez également "configurez les paramètres du proxy de stockage" pour permettre l'envoi de messages vers des points de terminaison externes, tels qu'un point de terminaison sur internet.

VLAN, services de plateforme et pools de stockage cloud

Vous ne pouvez pas utiliser de réseaux VLAN pour des services de plateforme ou des pools de stockage cloud. Les terminaux de destination doivent être accessibles via la grille, l'administrateur ou le réseau client.

Nœuds d'appliance

Vous pouvez configurer les ports réseau sur les appliances StorageGRID de sorte à utiliser les modes de liaison de ports qui répondent à vos exigences en matière de débit, de redondance et de basculement.

Les ports 10/25 GbE des appliances StorageGRID peuvent être configurés en mode de liaison fixe ou agrégée pour les connexions au réseau Grid et au réseau client.

Les ports réseau d'administration 1 GbE peuvent être configurés en mode indépendant ou en mode sauvegarde active pour les connexions au réseau d'administration.

Pour plus d'informations sur les modes de port de votre appareil, consultez :

- "Modes de liaison de port (SGF6112)"
- "Modes de liaison du port (contrôleur SG6000-CN)"
- "Modes de liaison des ports (contrôleur E5700SG)"
- "Modes de liaison de port (SG100 et SG1000)"

Installation et provisionnement réseau

Vous devez comprendre comment le réseau Grid et les réseaux d'administration et de client facultatifs sont utilisés pendant le déploiement des nœuds et la configuration de la grille.

Déploiement initial d'un nœud

Lorsque vous déployez un nœud pour la première fois, vous devez le connecter au réseau Grid et vous assurer qu'il a accès au nœud d'administration principal. Si le réseau de grille est isolé, vous pouvez configurer le réseau d'administration sur le nœud d'administration principal pour l'accès à la configuration et à l'installation depuis l'extérieur du réseau de grille.

Un réseau Grid avec une passerelle configurée devient la passerelle par défaut d'un nœud pendant le déploiement. La passerelle par défaut permet aux nœuds de grille sur des sous-réseaux séparés de communiquer avec le nœud d'administration principal avant la configuration de la grille.

Si nécessaire, les sous-réseaux contenant des serveurs NTP ou nécessitant un accès à Grid Manager ou à l'API peuvent également être configurés en tant que sous-réseaux de grille.

Enregistrement automatique des nœuds avec le nœud d'administration principal

Une fois les nœuds déployés, ils s'enregistrent eux-mêmes avec le nœud d'administration principal à l'aide du réseau Grid Network. Vous pouvez ensuite utiliser le Gestionnaire de grille, le `configure-storagegrid.py` Script Python ou API d'installation pour configurer la grille et approuver les nœuds enregistrés. Lors de la configuration de la grille, vous pouvez configurer plusieurs sous-réseaux de la grille. Les routes statiques vers ces sous-réseaux via la passerelle réseau grille sont créées sur chaque nœud lorsque vous terminez la configuration de la grille.

Désactivation du réseau Admin ou du réseau client

Si vous souhaitez désactiver le réseau d'administration ou le réseau client, vous pouvez supprimer la configuration d'eux pendant le processus d'approbation du nœud, ou vous pouvez utiliser l'outil Modifier IP une

fois l'installation terminée (voir "Configurez les adresses IP").

Instructions de post-installation

Une fois le déploiement et la configuration des nœuds de la grille effectués, suivez ces instructions pour l'adressage DHCP et les modifications de configuration réseau.

- Si DHCP était utilisé pour attribuer des adresses IP, configurez une réservation DHCP pour chaque adresse IP sur les réseaux utilisés.

  Vous ne pouvez configurer DHCP que pendant la phase de déploiement. Vous ne pouvez pas configurer DHCP pendant la configuration.

  > Les nœuds redémarrent lors de la modification de leurs adresses IP, ce qui peut entraîner des pannes si une modification d'adresse DHCP affecte plusieurs nœuds simultanément.

- Vous devez utiliser les procédures Modifier IP pour modifier les adresses IP, les masques de sous-réseau et les passerelles par défaut pour un noeud de grille. Voir "Configurez les adresses IP".
- Si vous modifiez la configuration réseau, y compris le routage et les modifications de passerelle, la connectivité client au nœud d'administration principal et à d'autres nœuds de la grille risque d'être perdue. En fonction des modifications de réseau appliquées, vous devrez peut-être rétablir ces connexions.

Référence du port réseau

Vous devez vous assurer que l'infrastructure réseau peut assurer une communication interne et externe entre les nœuds de la grille et les clients et services externes. Il se peut que vous ayez besoin d'accéder à des pare-feu internes et externes, à des systèmes de commutation et à des systèmes de routage.

Utilisez les informations fournies pour "Communications internes sur les nœuds de la grille" et "Communications externes" pour déterminer comment configurer chaque port requis.

Communications internes sur les nœuds de la grille

Le pare-feu interne StorageGRID permet les connexions entrantes à des ports spécifiques du réseau de la grille. Les connexions sont également acceptées sur les ports définis par les terminaux d'équilibreur de charge.

> NetApp vous recommande d'activer le trafic ICMP (Internet Control message Protocol) entre les nœuds de la grille. L'autorisation du trafic ICMP peut améliorer les performances de basculement lorsqu'un nœud de grille ne peut pas être atteint.

Outre ICMP et les ports répertoriés dans le tableau, StorageGRID utilise le protocole VRRP (Virtual Router Redundancy Protocol). VRRP est un protocole Internet qui utilise le protocole IP numéro 112. StorageGRID utilise le protocole VRRP en mode monodiffusion uniquement. VRRP n'est nécessaire que si "groupes haute disponibilité" sont configurés.

Instructions pour les nœuds basés sur Linux

Si les stratégies de réseau d'entreprise limitent l'accès à l'un de ces ports, vous pouvez remappage les ports au moment du déploiement à l'aide d'un paramètre de configuration de déploiement. Pour plus d'informations

sur le remappage des ports et les paramètres de configuration de déploiement, reportez-vous à la section :

- "Installez Red Hat Enterprise Linux ou CentOS"
- "Installez Ubuntu ou Debian"

Instructions pour les nœuds VMware

Configurez les ports suivants uniquement si vous devez définir des restrictions de pare-feu externes à la mise en réseau VMware.

Si les stratégies de mise en réseau d'entreprise limitent l'accès à l'un de ces ports, vous pouvez remappage les ports lors du déploiement des nœuds à l'aide du client Web VMware vSphere, ou à l'aide d'un paramètre de fichier de configuration lors de l'automatisation du déploiement des nœuds de la grille. Pour plus d'informations sur le remappage des ports et les paramètres de configuration de déploiement, reportez-vous à la section"Installez VMware".

Consignes pour les nœuds d'appliance

Si les stratégies de réseau d'entreprise limitent l'accès à l'un de ces ports, vous pouvez remappage les ports à l'aide du programme d'installation de l'appliance StorageGRID. Voir "Facultatif : remappage des ports réseau pour l'appliance".

Ports internes StorageGRID

Port	TCP ou UDP	De	À	Détails
22	TCP	Nœud d'administration principal	Tous les nœuds	Pour les procédures de maintenance, le nœud d'administration principal doit pouvoir communiquer avec tous les autres nœuds via SSH sur le port 22. L'autorisation du trafic SSH depuis d'autres nœuds est facultative.
80	TCP	Appliances	Nœud d'administration principal	Utilisé par les appliances StorageGRID pour communiquer avec le nœud d'administration principal afin de démarrer l'installation.
123	UDP	Tous les nœuds	Tous les nœuds	Service de protocole de temps de réseau. Chaque nœud synchronise son heure avec chaque autre nœud à l'aide du protocole NTP.
443	TCP	Tous les nœuds	Nœud d'administration principal	Utilisé pour communiquer l'état au nœud d'administration principal lors de l'installation et d'autres procédures de maintenance.
1055	TCP	Tous les nœuds	Nœud d'administration principal	Trafic interne pour l'installation, l'extension, la récupération et d'autres procédures de maintenance.

Port	TCP ou UDP	De	À	Détails
1139	TCP	Nœuds de stockage	Nœuds de stockage	Trafic interne entre les nœuds de stockage.
1501	TCP	Tous les nœuds	Nœuds de stockage avec ADC	Création de rapports, audit et configuration trafic interne.
1502	TCP	Tous les nœuds	Nœuds de stockage	Trafic interne lié aux protocoles S3 et Swift.
1504	TCP	Tous les nœuds	Nœuds d'administration	Rapports de service NMS et trafic interne de configuration.
1505	TCP	Tous les nœuds	Nœuds d'administration	Trafic interne du service AMS.
1506	TCP	Tous les nœuds	Tous les nœuds	Trafic interne de l'état du serveur.
1507	TCP	Tous les nœuds	Nœuds de passerelle	Trafic interne de l'équilibreur de charge.
1508	TCP	Tous les nœuds	Nœud d'administration principal	Trafic interne de gestion de la configuration.
1509	TCP	Tous les nœuds	Nœuds d'archivage	Trafic interne du nœud d'archivage.
1511	TCP	Tous les nœuds	Nœuds de stockage	Trafic interne de métadonnées.
5353	UDP	Tous les nœuds	Tous les nœuds	Fournit le service DNS multicast (mDNS) utilisé pour les changements d'adresse IP sur l'ensemble du réseau et pour la découverte du nœud d'administration principal lors de l'installation, de l'extension et de la récupération. **Remarque** : La configuration de ce port est facultative.
7001	TCP	Nœuds de stockage	Nœuds de stockage	Communication inter-nœud Cassandra TLS avec cluster.

Port	TCP ou UDP	De	À	Détails
7443	TCP	Tous les nœuds	Nœud d'administration principal	Trafic interne pour l'installation, l'extension, la récupération, les autres procédures de maintenance et le signalement des erreurs.
8011	TCP	Tous les nœuds	Nœud d'administration principal	Trafic interne pour l'installation, l'extension, la récupération et d'autres procédures de maintenance.
8443	TCP	Nœud d'administration principal	Nœuds d'appliance	Trafic interne lié à la procédure de mode de maintenance.
9042	TCP	Nœuds de stockage	Nœuds de stockage	Port client Cassandra.
9999	TCP	Tous les nœuds	Tous les nœuds	Trafic interne pour plusieurs services. Inclut les procédures de maintenance, les mesures et les mises à jour réseau.
10226	TCP	Nœuds de stockage	Nœud d'administration principal	Utilisé par les appliances StorageGRID pour le transfert des messages AutoSupport depuis E-Series SANtricity System Manager vers le nœud d'administration principal.
10342	TCP	Tous les nœuds	Nœud d'administration principal	Trafic interne pour l'installation, l'extension, la récupération et d'autres procédures de maintenance.
11139	TCP	Nœuds d'archivage/stockage	Nœuds d'archivage/stockage	Trafic interne entre les nœuds de stockage et les nœuds d'archivage.
18000	TCP	Nœuds d'administration/de stockage	Nœuds de stockage avec ADC	Trafic interne du service de compte.
18001	TCP	Nœuds d'administration/de stockage	Nœuds de stockage avec ADC	Trafic interne de la fédération des identités.

Port	TCP ou UDP	De	À	Détails
18002	TCP	Nœuds d'administration/de stockage	Nœuds de stockage	Trafic API interne lié aux protocoles objet
18003	TCP	Nœuds d'administration/de stockage	Nœuds de stockage avec ADC	Trafic interne des services de plate-forme.
18017	TCP	Nœuds d'administration/de stockage	Nœuds de stockage	Trafic interne du service Data Mover pour les pools de stockage cloud.
18019	TCP	Nœuds de stockage	Nœuds de stockage	Trafic interne de service de bloc pour le code d'effacement.
18082	TCP	Nœuds d'administration/de stockage	Nœuds de stockage	Trafic interne lié à S3.
18083	TCP	Tous les nœuds	Nœuds de stockage	Trafic interne lié à Swift.
18086	TCP	Tous les nœuds grid	Tous les nœuds de stockage	Trafic interne lié au service LDR.
18200	TCP	Nœuds d'administration/de stockage	Nœuds de stockage	Statistiques supplémentaires sur les demandes client.
19000	TCP	Nœuds d'administration/de stockage	Nœuds de stockage avec ADC	Trafic interne du service Keystone.

Informations associées

"Communications externes"

Communications externes

Les clients doivent communiquer avec les nœuds du grid pour ingérer et récupérer le contenu. Les ports utilisés dépendent des protocoles de stockage objet choisis. Ces ports

doivent être accessibles au client.

Accès restreint aux ports

Si les stratégies de réseau d'entreprise limitent l'accès à l'un des ports, vous pouvez utiliser "terminaux d'équilibrage de charge" pour autoriser l'accès sur les ports définis par l'utilisateur. Vous pouvez ensuite utiliser "Réseaux clients non fiables" pour autoriser l'accès uniquement sur les ports de point de terminaison de l'équilibreur de charge.

Remappage du port

Pour utiliser des systèmes et des protocoles tels que SMTP, DNS, SSH ou DHCP, vous devez remappage les ports lors du déploiement des nœuds. Toutefois, vous ne devez pas remapper les terminaux de l'équilibreur de charge. Pour plus d'informations sur le remappage des ports, reportez-vous aux instructions d'installation :

- "Installez Red Hat Enterprise Linux ou CentOS"
- "Installez Ubuntu ou Debian"
- "Installez VMware"
- "Facultatif : remappage des ports réseau pour l'appliance"

Ports utilisés pour les communications externes

Le tableau suivant indique les ports utilisés pour le trafic dans les nœuds.

Cette liste ne comprend pas les ports pouvant être configurés comme "terminaux d'équilibrage de charge" ou utilisé pour "serveurs syslog".

Port	TCP ou UDP	Protocole	De	À	Détails
22	TCP	SSH	L'ordinateur portable de service	Tous les nœuds	Un accès SSH ou via la console est requis pour les procédures liées aux étapes de la console. Vous pouvez également utiliser le port 2022 au lieu de 22.
25	TCP	SMTP	Nœuds d'administration	Serveur de messagerie	Utilisé pour les alertes et l'adresse AutoSupport basée sur des e-mails. Vous pouvez remplacer le paramètre de port par défaut de 25 à l'aide de la page serveurs de messagerie.
53	TCP/UDP	DNS	Tous les nœuds	Serveurs DNS	Utilisé pour DNS.
67	UDP	DHCP	Tous les nœuds	Service DHCP	Permet de prendre en charge la configuration réseau basée sur DHCP. Le service dhclient ne fonctionne pas pour les grilles configurées de façon statique.

Port	TCP ou UDP	Protocole	De	À	Détails
68	UDP	DHCP	Service DHCP	Tous les nœuds	Permet de prendre en charge la configuration réseau basée sur DHCP. Le service dhclient ne s'exécute pas pour les grilles qui utilisent des adresses IP statiques.
80	TCP	HTTP	Navigateur	Nœuds d'administration	Le port 80 redirige vers le port 443 pour l'interface utilisateur du nœud d'administration.
80	TCP	HTTP	Navigateur	Appliances	Le port 80 redirige vers le port 8443 du programme d'installation de l'appliance StorageGRID.
80	TCP	HTTP	Nœuds de stockage avec ADC	AWS	Utilisé pour les messages de services de plateforme envoyés à AWS ou à d'autres services externes utilisant HTTP. Les locataires peuvent remplacer le paramètre de port HTTP par défaut de 80 lors de la création d'un noeud final.
80	TCP	HTTP	Nœuds de stockage	AWS	Demandes de pools de stockage cloud envoyées aux cibles AWS utilisant HTTP. Les administrateurs du grid peuvent remplacer le paramètre de port HTTP par défaut de 80 lors de la configuration d'un pool de stockage cloud.
111	TCP/UDP	Rpcbind	Client NFS	Nœuds d'administration	Utilisé par l'export d'audit basé sur NFS (portmap). **Remarque :** ce port n'est nécessaire que si l'exportation d'audit NFS est activée.
123	UDP	NTP	Nœuds NTP principaux	NTP externe	Service de protocole de temps de réseau. Les nœuds sélectionnés comme sources NTP principales synchronisent également les heures d'horloge avec les sources d'heure NTP externes.
137	UDP	NetBIOS	Client SMB	Nœuds d'administration	Utilisé par l'exportation d'audit SMB pour les clients nécessitant la prise en charge NetBIOS. **Remarque :** ce port n'est requis que si l'exportation d'audit SMB est activée.

Port	TCP ou UDP	Protocole	De	À	Détails
138	UDP	NetBIOS	Client SMB	Nœuds d'administration	Utilisé par l'exportation d'audit SMB pour les clients nécessitant la prise en charge NetBIOS. **Remarque :** ce port n'est requis que si l'exportation d'audit SMB est activée.
139	TCP	PME	Client SMB	Nœuds d'administration	Utilisé par l'exportation d'audit SMB pour les clients nécessitant la prise en charge NetBIOS. **Remarque :** ce port n'est requis que si l'exportation d'audit SMB est activée.
161	TCP/UDP	SNMP	Client SNMP	Tous les nœuds	Utilisé pour l'interrogation SNMP. Tous les nœuds fournissent des informations de base ; les nœuds d'administration fournissent également des données d'alerte et d'alarme. Le port UDP 161 est défini par défaut lorsqu'il est configuré. **Remarque :** ce port n'est nécessaire que, et n'est ouvert que sur le pare-feu de nœud si SNMP est configuré. Si vous prévoyez d'utiliser SNMP, vous pouvez configurer d'autres ports. **Remarque :** pour plus d'informations sur l'utilisation de SNMP avec StorageGRID, contactez votre ingénieur commercial NetApp.
162	TCP/UDP	Notifications SNMP	Tous les nœuds	Destinations de notification	Notifications et interruptions SNMP sortantes par défaut au port UDP 162. **Remarque :** ce port n'est requis que si SNMP est activé et que les destinations de notification sont configurées. Si vous prévoyez d'utiliser SNMP, vous pouvez configurer d'autres ports. **Remarque :** pour plus d'informations sur l'utilisation de SNMP avec StorageGRID, contactez votre ingénieur commercial NetApp.
389	TCP/UDP	LDAP	Nœuds de stockage avec ADC	Active Directory/LDAP	Utilisé pour la connexion à un serveur Active Directory ou LDAP pour la fédération des identités.

Port	TCP ou UDP	Protocole	De	À	Détails
443	TCP	HTTPS	Navigateur	Nœuds d'administration	Utilisé par les navigateurs Web et les clients API de gestion pour accéder à Grid Manager et tenant Manager. **Remarque** : si vous fermez les ports Grid Manager 443 ou 8443, tous les utilisateurs actuellement connectés sur un port bloqué, y compris vous, perdront l'accès à Grid Manager à moins que leur adresse IP n'ait été ajoutée à la liste d'adresses privilégiées. Voir "Configurer les contrôles de pare-feu" Pour configurer des adresses IP privilégiées.
443	TCP	HTTPS	Nœuds d'administration	Active Directory	Utilisé par les nœuds d'administration se connectant à Active Directory si l'authentification unique (SSO) est activée.
443	TCP	HTTPS	Nœuds d'archivage	Amazon S3	Utilisé pour accéder à Amazon S3 à partir des nœuds d'archivage.
443	TCP	HTTPS	Nœuds de stockage avec ADC	AWS	Utilisé pour les messages de services de plateforme envoyés à AWS ou à d'autres services externes utilisant HTTPS. Les locataires peuvent remplacer le paramètre de port HTTP par défaut de 443 lors de la création d'un noeud final.
443	TCP	HTTPS	Nœuds de stockage	AWS	Les demandes de pools de stockage cloud sont envoyées aux cibles AWS qui utilisent HTTPS. Les administrateurs du grid peuvent remplacer le paramètre de port HTTPS par défaut de 443 lors de la configuration d'un pool de stockage cloud.
445	TCP	PME	Client SMB	Nœuds d'administration	Utilisé par l'exportation d'audit basée sur SMB. **Remarque :** ce port n'est requis que si l'exportation d'audit SMB est activée.
903	TCP	NFS	Client NFS	Nœuds d'administration	Utilisé par l'exportation d'audit basée sur NFS (`rpc.mountd`). **Remarque :** ce port n'est nécessaire que si l'exportation d'audit NFS est activée.

Port	TCP ou UDP	Protocole	De	À	Détails
2022	TCP	SSH	L'ordinateur portable de service	Tous les nœuds	Un accès SSH ou via la console est requis pour les procédures liées aux étapes de la console. Vous pouvez également utiliser le port 22 au lieu de 2022.
2049	TCP	NFS	Client NFS	Nœuds d'administration	Utilisé par l'export d'audit basé sur NFS (nfs). **Remarque :** ce port n'est nécessaire que si l'exportation d'audit NFS est activée.
5353	UDP	MDNS	Tous les nœuds	Tous les nœuds	Fournit le service DNS multicast (mDNS) utilisé pour les changements d'adresse IP sur l'ensemble du réseau et pour la découverte du nœud d'administration principal lors de l'installation, de l'extension et de la récupération. **Remarque** : La configuration de ce port est facultative.
5696	TCP	KMIP	Appliance	KM	Trafic externe KMIP (Key Management Interoperability Protocol) depuis les appliances configurées pour le chiffrement des nœuds vers le serveur de gestion des clés (KMS), sauf si un autre port est spécifié sur la page de configuration KMS du programme d'installation de l'appliance StorageGRID.
8022	TCP	SSH	L'ordinateur portable de service	Tous les nœuds	SSH sur le port 8022 permet d'accéder au système d'exploitation de base sur l'appliance et les plateformes de nœuds virtuels pour le support et le dépannage. Ce port n'est pas utilisé pour les nœuds Linux (bare Metal) et n'est pas requis pour être accessible entre les nœuds de la grille ou pendant les opérations normales.

Port	TCP ou UDP	Protocole	De	À	Détails
8443	TCP	HTTPS	Navigateur	Nœuds d'administration	Facultatif. Utilisé par les navigateurs Web et les clients API de gestion pour accéder à Grid Manager. Peut être utilisé pour séparer les communications Grid Manager et tenant Manager. **Remarque** : si vous fermez les ports Grid Manager 443 ou 8443, tous les utilisateurs actuellement connectés sur un port bloqué, y compris vous, perdront l'accès à Grid Manager à moins que leur adresse IP n'ait été ajoutée à la liste d'adresses privilégiées. Voir "Configurer les contrôles de pare-feu" Pour configurer des adresses IP privilégiées.
9022	TCP	SSH	L'ordinateur portable de service	Appliances	Permet d'accéder aux appliances StorageGRID en mode préconfiguration pour le support et le dépannage. Ce port n'est pas nécessaire pour être accessible entre des nœuds grid ou pendant les opérations normales.
9091	TCP	HTTPS	Service externe Grafana	Nœuds d'administration	Utilisés par les services Grafana externes pour sécuriser l'accès au service StorageGRID Prometheus. **Remarque :** ce port n'est nécessaire que si l'accès Prometheus basé sur un certificat est activé.
9443	TCP	HTTPS	Navigateur	Nœuds d'administration	Facultatif. Utilisé par les navigateurs Web et les clients API de gestion pour accéder au Gestionnaire de locataires. Peut être utilisé pour séparer les communications Grid Manager et tenant Manager.
18082	TCP	HTTPS	Clients S3	Nœuds de stockage	Trafic des clients S3 directement vers les nœuds de stockage (HTTPS).
18083	TCP	HTTPS	Clients Swift	Nœuds de stockage	Trafic des clients Swift directement vers les nœuds de stockage (HTTPS).
18084	TCP	HTTP	Clients S3	Nœuds de stockage	Trafic client S3 directement vers les nœuds de stockage (HTTP).
18085	TCP	HTTP	Clients Swift	Nœuds de stockage	Trafic des clients Swift directement vers les nœuds de stockage (HTTP).

Port	TCP ou UDP	Protocole	De	À	Détails
23000-23999	TCP	HTTPS	Tous les nœuds du grid source pour la réplication inter-grid	Nœuds d'administration et nœuds de passerelle sur le grid de destination pour la réplication inter-grid	Cette plage de ports est réservée aux connexions de fédération de grille. Les deux grilles d'une connexion donnée utilisent le même port.

Démarrage rapide pour StorageGRID

Suivez ces étapes générales pour configurer et utiliser n'importe quel système StorageGRID.

Apprenez, planifiez et collectez des données

Contactez votre ingénieur commercial NetApp pour en savoir plus sur les options et planifier votre nouveau système StorageGRID. Prenez en compte les types de questions suivants :

- Quelle quantité de données d'objet prévoyez-vous de stocker au départ et au fil du temps ?
- De combien de sites avez-vous besoin ?
- De combien de nœuds et de quels types de nœuds avez-vous besoin sur chaque site ?
- Quels réseaux StorageGRID utiliserez-vous ?
- Qui va utiliser votre grille pour stocker des objets ? Quelles applications utiliseront-ils ?
- Avez-vous des exigences spéciales en matière de sécurité ou de stockage ?
- Devez-vous vous conformer à des exigences légales ou réglementaires ?

Vous pouvez également consulter votre consultant en services professionnels NetApp pour accéder à l'outil NetApp ConfigBuilder et remplir un manuel de configuration à utiliser lors de l'installation et du déploiement de votre nouveau système. Vous pouvez également l'utiliser pour automatiser la configuration de n'importe quelle appliance StorageGRID. Voir "Automatisez l'installation et la configuration de l'appliance".

Révision "Découvrez StorageGRID" et le "Instructions de mise en réseau".

Installez les nœuds

Un système StorageGRID se compose de nœuds matériels et logiciels individuels. Vous devez d'abord installer le matériel pour chaque nœud d'appliance et configurer chaque hôte Linux ou VMware.

Pour terminer l'installation, vous devez installer le logiciel StorageGRID sur chaque appliance ou hôte logiciel et connecter les nœuds à un grid. Au cours de cette étape, vous fournissez les noms de site et de nœud, les détails de sous-réseau et les adresses IP de vos serveurs NTP et DNS.

Découvrez comment :

- "Installez le matériel de l'appliance"
- "Installez Red Hat Enterprise Linux ou CentOS"
- "Installez Ubuntu ou Debian"
- "Installez VMware"

3 Connectez-vous et vérifiez l'état du système

Dès que vous installez le nœud d'administration principal, vous pouvez vous connecter à Grid Manager. Ensuite, vous pouvez vérifier l'état de santé général de votre nouveau système, activer AutoSupport et les e-mails d'alerte, et configurer les noms de domaine de terminaux S3.

Découvrez comment :

- "Connectez-vous au Grid Manager"
- "Contrôle de l'état des systèmes"
- "Configurez AutoSupport"
- "Configurez les notifications par e-mail pour les alertes"
- "Configuration des noms de domaine de terminaux S3"

4 Configurez et gérez

Les tâches de configuration que vous devez effectuer pour un nouveau système StorageGRID dépendent de la manière dont vous utiliserez votre grille. Vous configurez au moins l'accès au système, utilisez les assistants FabricPool et S3 et gérez les divers paramètres de stockage et de sécurité.

Découvrez comment :

- "Contrôlez l'accès au StorageGRID"
- "Utilisation de l'assistant d'installation S3"
- "Utilisez l'assistant d'installation FabricPool"
- "Gérer la sécurité"
- "Durcissement du système"

5 Configuration d'ILM

Vous contrôlez le placement et la durée de chaque objet de votre système StorageGRID en configurant une règle de gestion du cycle de vie des informations (ILM) constituée d'une ou plusieurs règles ILM. Les règles ILM indiquent à StorageGRID comment créer et distribuer des copies de données en mode objet et comment gérer ces copies au fil du temps.

Découvrez comment : "Gestion des objets avec ILM"

6 Utiliser StorageGRID

Une fois la configuration initiale terminée, les comptes de locataires StorageGRID peuvent utiliser les applications client S3 et Swift pour ingérer, récupérer et supprimer des objets.

Découvrez comment :

- "Utilisez un compte de locataire"
- "Utilisez l'API REST S3"
- "Utilisez l'API REST Swift"

7 Surveiller et résoudre les problèmes

Lorsque votre système est opérationnel, vous devez surveiller régulièrement ses activités et résoudre les problèmes éventuels. Vous pouvez également configurer un serveur syslog externe, utiliser la surveillance SNMP ou collecter des données supplémentaires.

Découvrez comment :

- "Surveillez StorageGRID"
- "Dépanner StorageGRID"

8 Développez et entretenez

Vous pouvez ajouter des nœuds ou des sites pour augmenter la capacité ou les fonctionnalités de votre système. Vous pouvez également exécuter diverses procédures de maintenance pour effectuer une reprise après incident ou maintenir votre système StorageGRID à jour et performant.

Découvrez comment :

- "Développez votre grille"
- "Restaurez les nœuds et gérez votre grid"

Installation et mise à niveau

Installez le matériel de l'appliance

Démarrage rapide pour l'installation du matériel

Suivez ces étapes générales pour installer et configurer une appliance StorageGRID et la déployer comme nœud dans votre système StorageGRID.

1 **Avant l'installation**

1. Automatisez l'installation et la configuration avec votre consultant en services professionnels NetApp. Voir "Automatisez l'installation et la configuration de l'appliance".

   Cette étape est facultative. Cependant, la rationalisation et l'automatisation des étapes de configuration peuvent faire gagner du temps et assurer la cohérence de la configuration de plusieurs appliances.

2. "Préparer le site"
3. "Déballez les boîtes"
4. "Procurez-vous des équipements et outils supplémentaires"
5. "Consultez les exigences relatives au navigateur Web"
6. "Vérifiez les connexions réseau de l'appliance"
7. "Rassembler les informations d'installation"

2 **Installer le matériel de fixation**

1. "Enregistrez le matériel"
2. Installez-le dans l'armoire ou sur le rack
   - "SGF6112"
   - "SG6000"
   - "SG5700"
   - "SG100 et SG1000"
3. Appareil câblé
   - "SGF6112"
   - "SG6000"
   - "SG5700"
   - "SG100 et SG1000"
4. Branchez les câbles d'alimentation et mettez le système sous tension
   - "SGF6112"
   - "SG6000"
   - "SG5700"

- "SG100 et SG1000"

5. "Afficher les indicateurs d'état et les codes"

3 Configurer le matériel

Si vous configurez et déployez plusieurs appliances, utilisez l'outil NetApp ConfigBuilder pour automatiser les étapes suivantes de configuration et de déploiement. Pour obtenir de l'aide, contactez votre consultant en services professionnels NetApp. Voir "Automatisez l'installation et la configuration de l'appliance".

1. Configurer les connexions StorageGRID
   - "Accédez au programme d'installation de l'appliance StorageGRID" et vérifiez que vous utilisez la version la plus récente
   - "Configurer les liaisons réseau"
   - "Configurez les adresses IP StorageGRID"
   - "Vérifiez les connexions réseau"
   - "Vérifiez les connexions réseau au niveau des ports"
2. "Accès à SANtricity System Manager et configuration de celui-ci" (SG6000 et SG5700)
3. "Configurez l'interface BMC" (SGF6112, SG6000, SG100 ET SG1000)
4. Effectuez les étapes de configuration facultatives
   - "Activez le chiffrement de nœud"
   - "Changement de mode RAID (SG6000 et SG5700)"
   - "Remappez les ports réseau"

4 Déployez le nœud de l'appliance

Déployez l'appliance comme un nouveau nœud dans votre système StorageGRID.

- "Déployez le nœud de stockage de l'appliance"
- "Déployez le nœud d'appliance des services"

Présentation du matériel

Appliance SGF6112 : présentation

L'appliance StorageGRID SGF6112 fonctionne comme un nœud de stockage dans un système StorageGRID. L'appliance peut être utilisée dans un environnement de grid hybride qui combine des nœuds de stockage d'appliance et des nœuds de stockage virtuels (basés sur logiciel).

L'appliance SGF6112 offre les fonctionnalités suivantes :

- 12 disques SSD NVMe (Nonvolatile Memory Express) avec contrôleurs de stockage et de calcul intégrés.
- Intègre les éléments de calcul et de stockage d'un nœud de stockage StorageGRID.
- Inclut le programme d'installation de l'appliance StorageGRID pour simplifier le déploiement et la configuration des nœuds de stockage.

- Inclut un contrôleur BMC (Baseboard Management Controller) pour la surveillance et le diagnostic du matériel dans le contrôleur de calcul.
- Prend en charge jusqu'à quatre connexions 10 GbE ou 25 GbE au réseau Grid et au réseau client StorageGRID.

Description du matériel du SGF6112

Le système StorageGRID SGF6112 est une appliance 100 % Flash au design compact comprenant un contrôleur de calcul et un contrôleur de stockage intégré dans un châssis 1U. L'appliance prend en charge 12 disques NVMe SSD avec une capacité de stockage allant jusqu'à 15.3 To par disque.

Stockage objet résilient

Le SGF6112 est conçu avec des disques SSD dans une configuration RAID et offre les fonctionnalités de protection des données suivantes :

- Fonctionnement après panne d'un disque SSD unique, sans impact sur la disponibilité des objets.
- Possibilité de fonctionner après plusieurs pannes SSD avec une réduction minimale de la disponibilité des objets (basée sur la conception du schéma RAID sous-jacent).
- Restauration complète, pendant la mise en service, suite à des pannes de disque SSD qui ne provoquent pas d'endommagement extrême du RAID hébergeant le volume racine du nœud (le système d'exploitation StorageGRID).

Composants matériels du SGF6112

L'appliance SGF6112 inclut les composants suivants :

Composant	Description
Des plateformes de calcul et de stockage	Un serveur à une unité de rack (1U) qui comprend : • Deux processeurs 2.1/2.6 GHz 165 W fournissant 48 cœurs • 256 GO DE RAM • 2 ports GBase-T 1/10 • 4 ports Ethernet 10/25 GbE • 1 lecteur de démarrage interne de 256 Go (logiciel StorageGRID inclus) • Le contrôleur de gestion de la carte mère (BMC) simplifie la gestion du matériel • Alimentations et ventilateurs redondants

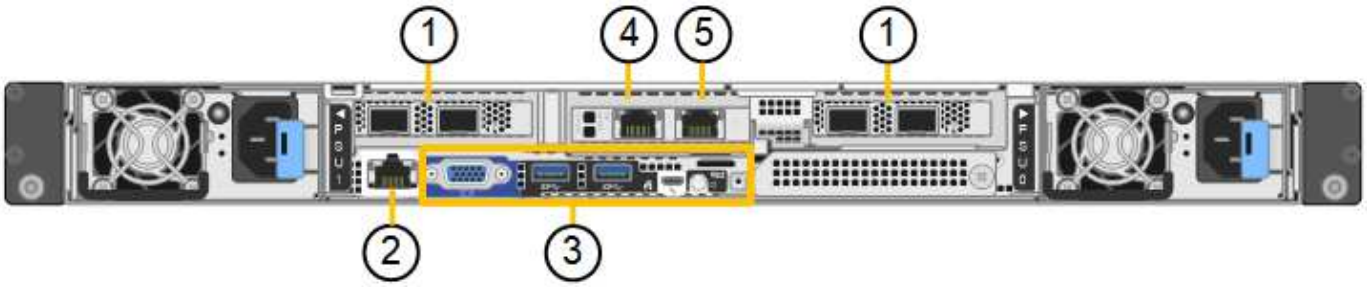
Diagrammes SGF6112

Vue avant du SGF6112

Cette figure illustre l'avant du SGF6112 sans le cadre. L'appliance inclut une plateforme de calcul et de stockage 1U qui contient 12 disques SSD.

Vue arrière du SGF6112

Cette figure illustre l'arrière du SGF6112, y compris les ports, les ventilateurs et les blocs d'alimentation.



Légende	Port	Type	Utiliser
1	Ports réseau 1-4	10/25-GbE, basé sur le type de câble ou d'émetteur-récepteur SFP (les modules SFP28 et SFP+ sont pris en charge), la vitesse du switch et la vitesse de liaison configurée.	Connectez-vous au réseau Grid et au réseau client pour StorageGRID.
2	Port de gestion BMC	1 GbE (RJ-45)	Se connecte au contrôleur de gestion de la carte de base de l'appliance.
3	Ports de diagnostic et de support	• VGA • USB • Port console micro-USB • Module d'emplacement micro-SD	Réservé au support technique.
4	Port réseau d'administration 1	1/10-GbE (RJ-45)	Connectez l'appliance au réseau d'administration pour StorageGRID.

Légende	Port	Type	Utiliser
5	Port réseau d'administration 2	1/10-GbE (RJ-45)	Options : • Liaison avec le port 1 du réseau d'administration pour une connexion redondante au réseau d'administration pour StorageGRID. • Laisser déconnecté et disponible pour l'accès local temporaire (IP 169.254.0.1). • Lors de l'installation, utilisez le port 2 pour la configuration IP si les adresses IP attribuées par DHCP ne sont pas disponibles.

Appliances SG6060 et SG6060X : présentation

Les appliances StorageGRID SG6060 et SG6060X incluent un contrôleur de calcul et un tiroir de contrôleur de stockage contenant deux contrôleurs de stockage et 60 disques.

Des tiroirs d'extension de 60 disques peuvent également être ajoutés aux deux appliances. Il n'existe aucune différence de spécification ou de fonctionnalité entre les SG6060 et SG6060X, à l'exception de l'emplacement des ports d'interconnexion sur le contrôleur de stockage.

SG6060 et SG6060X

Les appliances SG6060 et SG6060X comprennent les composants suivants :

Composant	Description
Contrôleur de calcul	Contrôleur SG6000-CN, serveur à un rack (1U) qui comprend : • 40 cœurs (80 threads) • 192 GO DE RAM • Jusqu'à 4 × 25 Gbit/s de bande passante Ethernet agrégée • 4 interconnexion Fibre Channel (FC) 16 Gbit/s • Le contrôleur de gestion de la carte mère (BMC) simplifie la gestion du matériel • Blocs d'alimentation redondants

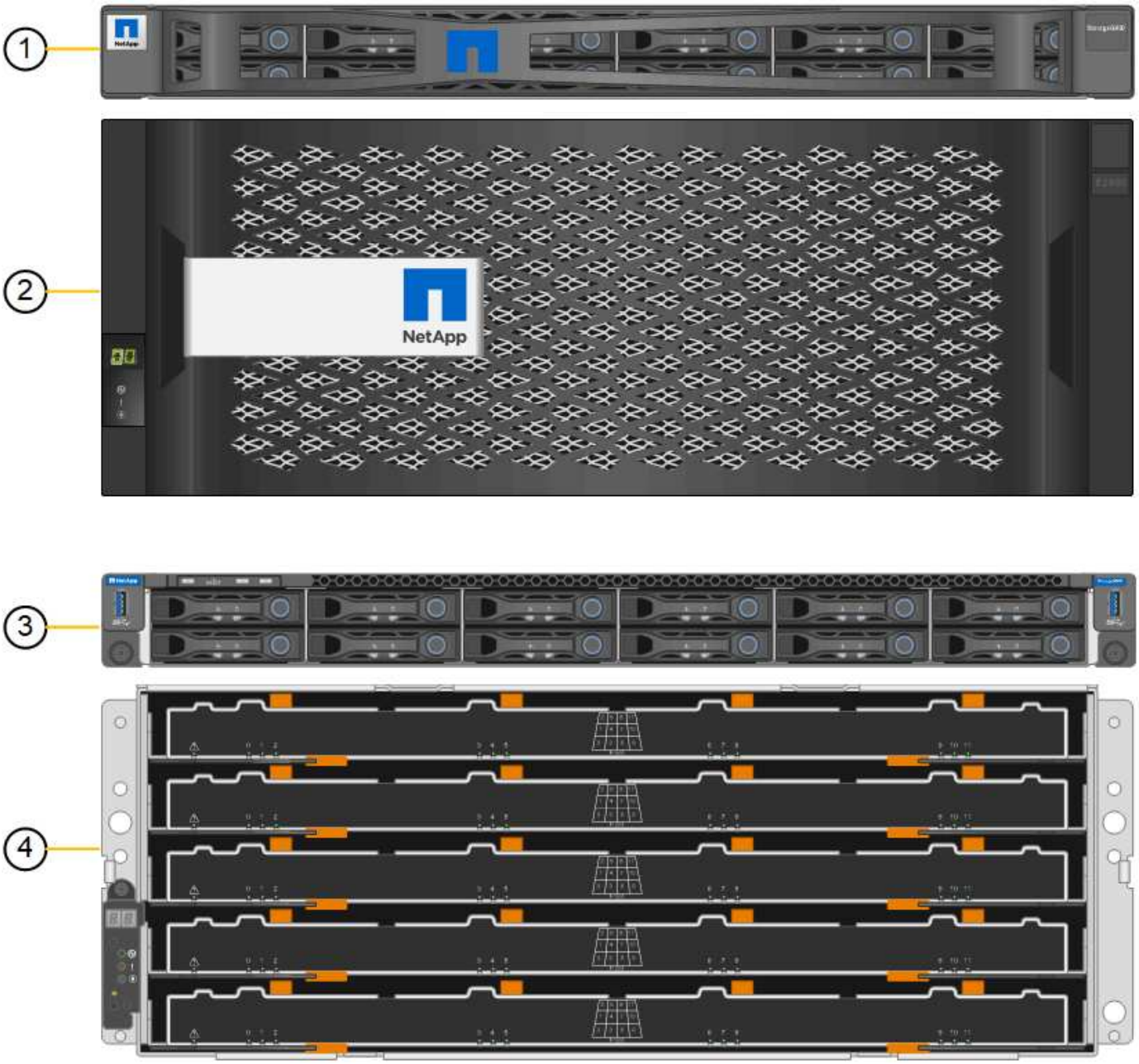
Composant	Description
Tiroir contrôleur de stockage	Tiroir contrôleur E2860 E-Series (baie de stockage), tiroir 4U qui inclut : • Deux contrôleurs E2800 Series (configuration duplex) pour une prise en charge du basculement du contrôleur de stockage ◦ Tandis que le SG6060 contient des contrôleurs de stockage E2800A ◦ Le SG6060X contient des contrôleurs de stockage E2800B • Tiroir à cinq tiroirs pour accueillir soixante disques de 3.5 pouces (2 disques SSD ou SSD et 58 disques NL-SAS) • Alimentations et ventilateurs redondants
Facultatif : tiroirs d'extension de stockage **Remarque :** les tiroirs d'extension peuvent être installés lors du déploiement initial ou ajoutés ultérieurement.	Boîtier E-Series DE460C, tiroir 4U qui inclut : • Deux modules d'entrée/sortie (IOM) • Cinq tiroirs, chacun contenant 12 disques NL-SAS, pour un total de 60 disques • Alimentations et ventilateurs redondants Chaque appliance SG6060 et SG6060X peut disposer d'une ou deux tiroirs d'extension pour un total de 180 disques (deux de ces disques sont réservés pour le cache de lecture E-Series).

Diagrammes SG6060 et SG6060X

Les faces avant des SG6060 et SG6060X sont identiques.

Vue avant SG6060 ou SG6060X

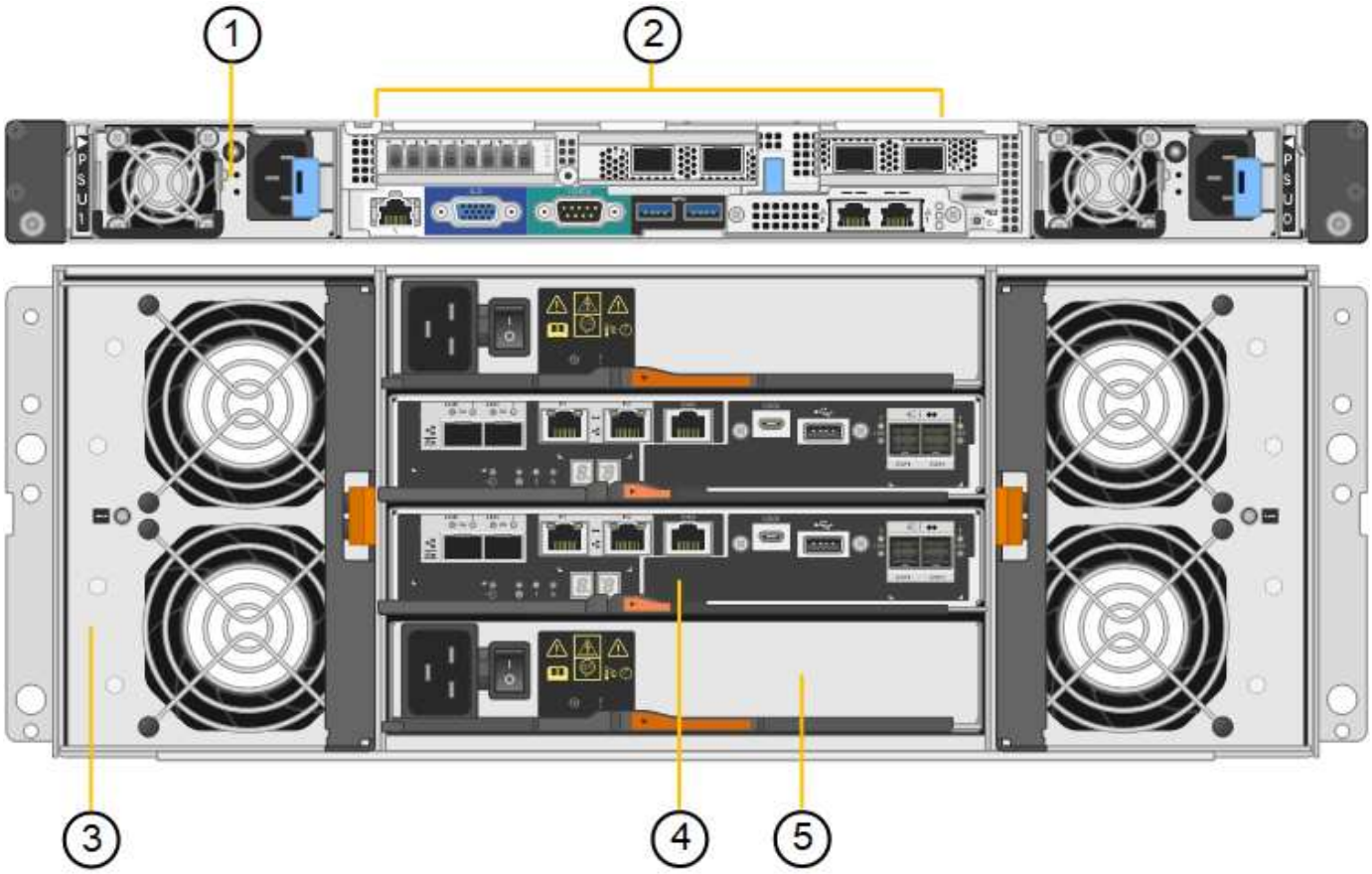
Cette figure présente l'avant du SG6060 ou du SG6060X, qui inclut un contrôleur de calcul 1U et un tiroir 4U contenant deux contrôleurs de stockage et 60 disques dans cinq tiroirs disques.



Légende	Description
1	Contrôleur de calcul SG6000-CN avec cadre avant
2	Tiroir contrôleur E2860 avec panneau avant (le tiroir d'extension en option apparaît identique)
3	Contrôleur de calcul SG6000-CN avec cadre avant retiré
4	Tiroir contrôleur E2860 avec panneau avant retiré (le tiroir d'extension en option apparaît identique)

Vue arrière SG6060

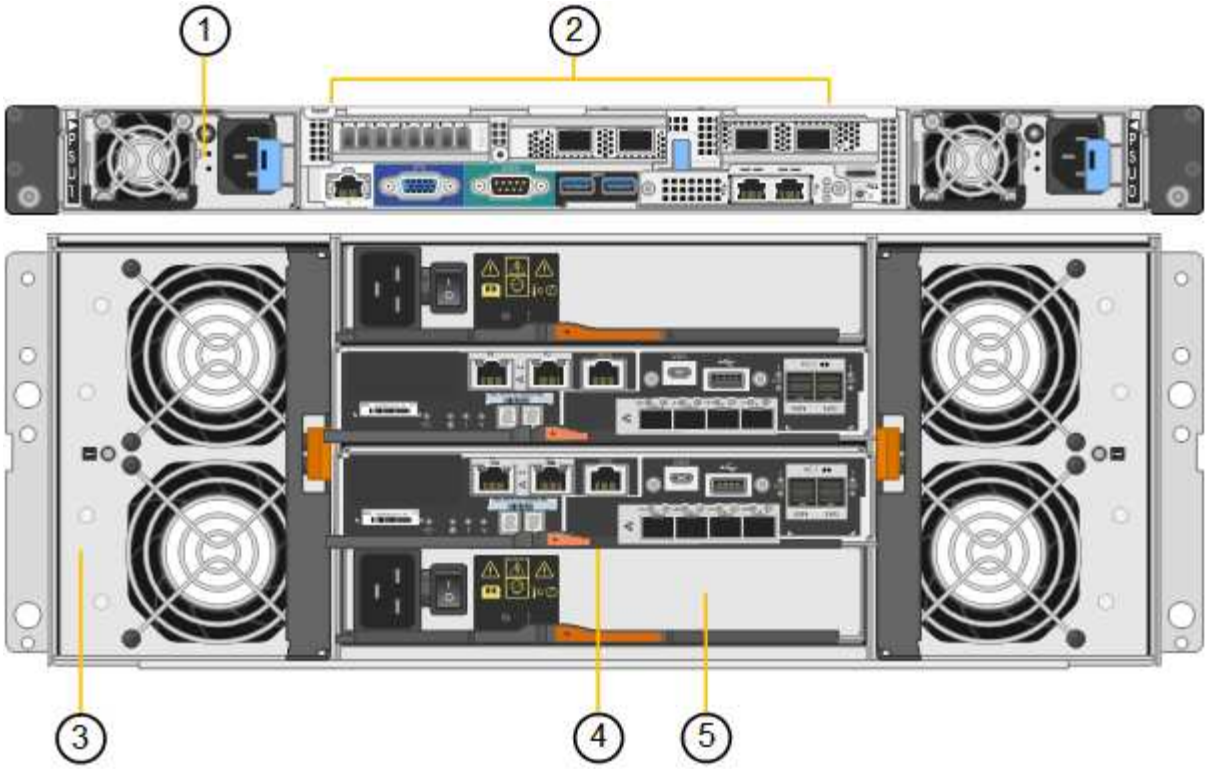
Cette figure illustre la arrière du SG6060, y compris des contrôleurs de calcul et de stockage, des ventilateurs et des blocs d'alimentation.



Légende	Description
1	Alimentation (1 sur 2) pour contrôleur de calcul SG6000-CN
2	Connecteurs pour contrôleur de calcul SG6000-CN
3	Ventilateur (1 sur 2) pour le tiroir contrôleur E2860
4	Contrôleur de stockage E-Series E2800A (1 sur 2) et connecteurs
5	Alimentation (1 sur 2) pour le tiroir contrôleur E2860

Vue arrière du SG6060X

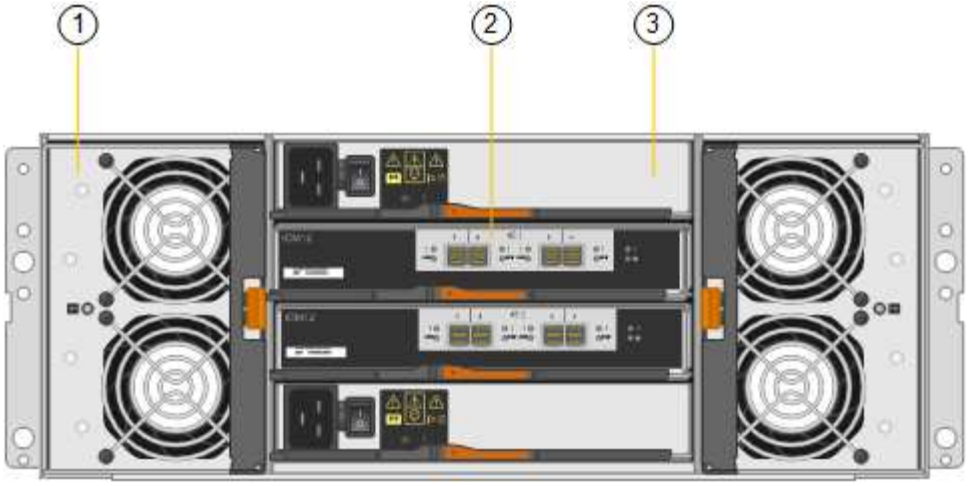
Cette figure illustre l'arrière du SG6060X.



Légende	Description
1	Alimentation (1 sur 2) pour contrôleur de calcul SG6000-CN
2	Connecteurs pour contrôleur de calcul SG6000-CN
3	Ventilateur (1 sur 2) pour le tiroir contrôleur E2860
4	Contrôleur de stockage E-Series E2800B (1 sur 2) et connecteurs
5	Alimentation (1 sur 2) pour le tiroir contrôleur E2860

Tiroir d’extension

Cette figure illustre l’arrière du tiroir d’extension en option pour les SG6060 et SG6060X, notamment des modules d’entrée/sortie (IOM), des ventilateurs et des blocs d’alimentation. Chaque SG6060 peut être installé avec un ou deux tiroirs d’extension, qui peuvent être inclus dans l’installation initiale ou ajoutés ultérieurement.



Légende	Description
1	Ventilateur (1 sur 2) pour le tiroir d'extension
2	Module d'E/S (1 sur 2) pour le tiroir d'extension
3	Bloc d'alimentation (1 sur 2) pour le tiroir d'extension

Contrôleurs SG6000

Chaque modèle de l'appliance StorageGRID SG6000 est doté d'un contrôleur de calcul SG6000-CN dans un boîtier 1U et de contrôleurs de stockage E-Series duplex dans un boîtier 2U ou 4U, selon le modèle. Consultez les schémas pour en savoir plus sur chaque type de contrôleur.

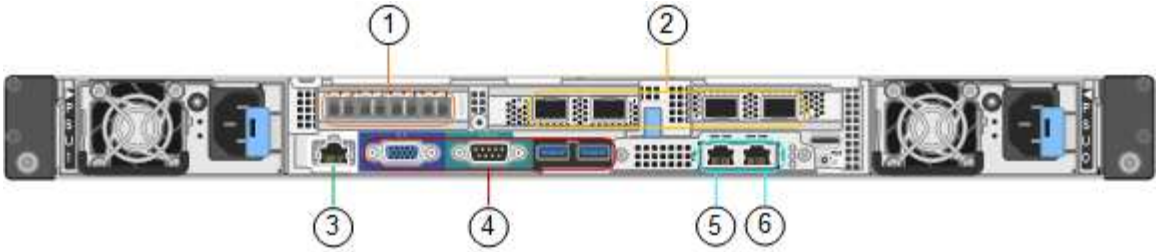
Contrôleur de calcul SG6000-CN

- Fournit des ressources de calcul pour l'appliance.
- Inclut le programme d'installation de l'appliance StorageGRID.

> Le logiciel StorageGRID n'est pas préinstallé sur l'appliance. Ce logiciel est extrait du noeud d'administration lorsque vous déployez l'appliance.

- Peut se connecter aux trois réseaux StorageGRID, y compris le réseau Grid, le réseau d'administration et le réseau client.
- Connexion aux contrôleurs de stockage E-Series et fonctionnement comme initiateur.

Connecteurs SG6000-CN

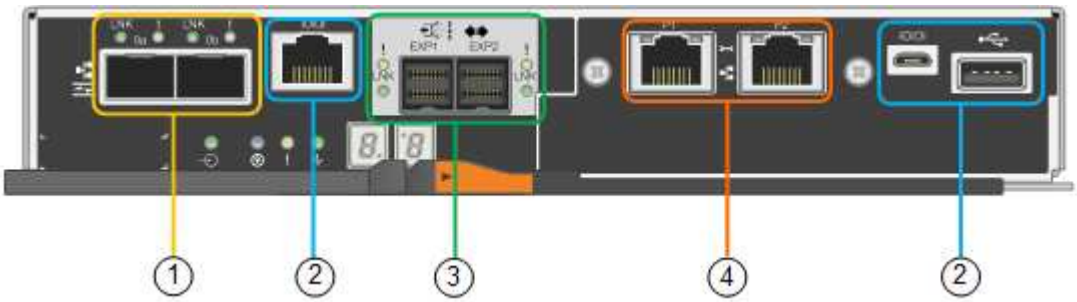


Légende	Port	Type	Utiliser
1	Ports d'interconnexion 1-4	Fibre Channel (FC) 16 Gbit/s avec optique intégrée	Connectez le contrôleur SG6000-CN aux contrôleurs E2800 (deux connexions pour chaque système E2800).
2	Ports réseau 1-4	10 GbE ou 25 GbE, selon le type d'émetteur-récepteur SFP ou câble, la vitesse du commutateur et la vitesse de liaison configurée	Connectez-vous au réseau Grid et au réseau client pour StorageGRID.
3	Port de gestion BMC	1 GbE (RJ-45)	Connectez-vous au contrôleur de gestion de la carte de base SG6000-CN.
4	Ports de diagnostic et de support	• VGA • Série, 115200 8-N-1 • USB	Réservé au support technique.
5	Port réseau d'administration 1	1 GbE (RJ-45)	Connectez le SG6000-CN au réseau Admin pour StorageGRID.
6	Port réseau d'administration 2	1 GbE (RJ-45)	Options : • Lien avec le port de gestion 1 pour une connexion redondante au réseau d'administration pour StorageGRID. • Laissez sans fil et disponible pour l'accès local temporaire (IP 169.254.0.1). • Lors de l'installation, utilisez le port 2 pour la configuration IP si les adresses IP attribuées par DHCP ne sont pas disponibles.

SGF6024 : contrôleurs de stockage EF570

- Deux contrôleurs pour la prise en charge du basculement.
- Gérer le stockage des données sur les disques.
- Fonctionnement en tant que contrôleurs E-Series standard dans une configuration duplex.
- Incluez le logiciel SANtricity OS (firmware du contrôleur).
- Il comprend SANtricity System Manager pour la surveillance du matériel de stockage et la gestion des alertes, la fonction AutoSupport et la sécurité des disques.
- Connectez-vous au contrôleur SG6000-CN et accédez au stockage Flash.

Connecteurs EF570



Légende	Port	Type	Utiliser
1	Ports d'interconnexion 1 et 2	SFP optique FC 16 Gbit/s	Connectez chacun des contrôleurs EF570 au contrôleur SG6000-CN. Le contrôleur SG6000-CN est doté de quatre connexions (deux de chaque EF570).
2	Ports de diagnostic et de support	• Port série RJ-45 • Port série micro USB • Port USB	Réservé au support technique.
3	Ports d'extension de disque	12 Gb/s SAS	Non utilisé. L'appliance SGF6024 ne prend pas en charge les tiroirs disques d'extension.
4	Ports de gestion 1 et 2	Ethernet 1 Gbit (RJ-45)	• Le port 1 se connecte au réseau dans lequel vous accédez à SANtricity System Manager sur un navigateur. • Le port 2 est réservé au support technique.

SG6060 et SG6060X : contrôleurs de stockage E2800

- Deux contrôleurs pour la prise en charge du basculement.

- Gérer le stockage des données sur les disques.
- Fonctionnement en tant que contrôleurs E-Series standard dans une configuration duplex.
- Incluez le logiciel SANtricity OS (firmware du contrôleur).
- Il comprend SANtricity System Manager pour la surveillance du matériel de stockage et la gestion des alertes, la fonction AutoSupport et la sécurité des disques.
- Connectez-vous au contrôleur SG6000-CN et accédez au stockage.

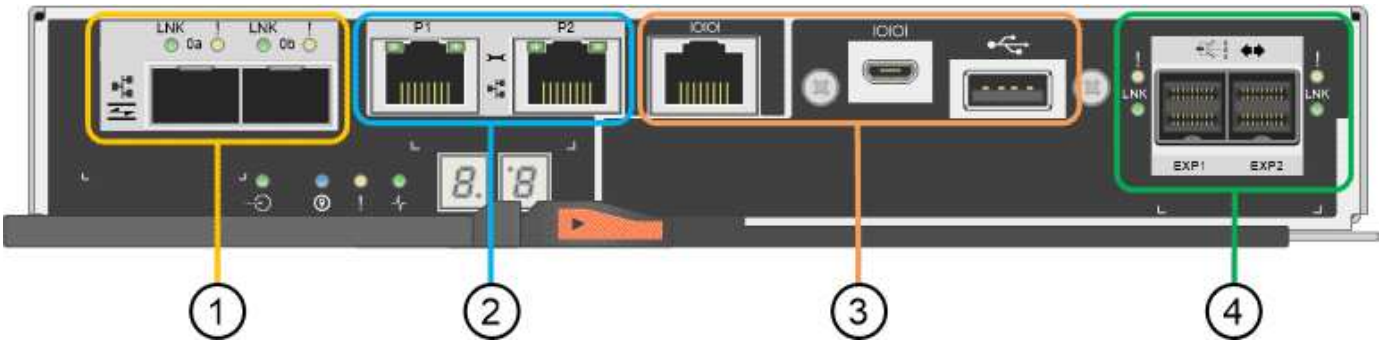
Les SG6060 et SG6060X utilisent les contrôleurs de stockage E2800.

Appliance	Contrôleur	Contrôleur HIC
SG6060	Deux contrôleurs de stockage E2800A	Aucune
SG6060X	Deux contrôleurs de stockage E2800B	Quatre ports HIC

Les contrôleurs de stockage E2800A et E2800B sont identiques en spécifications et en fonction, à l'exception de l'emplacement des ports d'interconnexion.

N'utilisez pas de système E2800A et E2800B dans le même appareil.

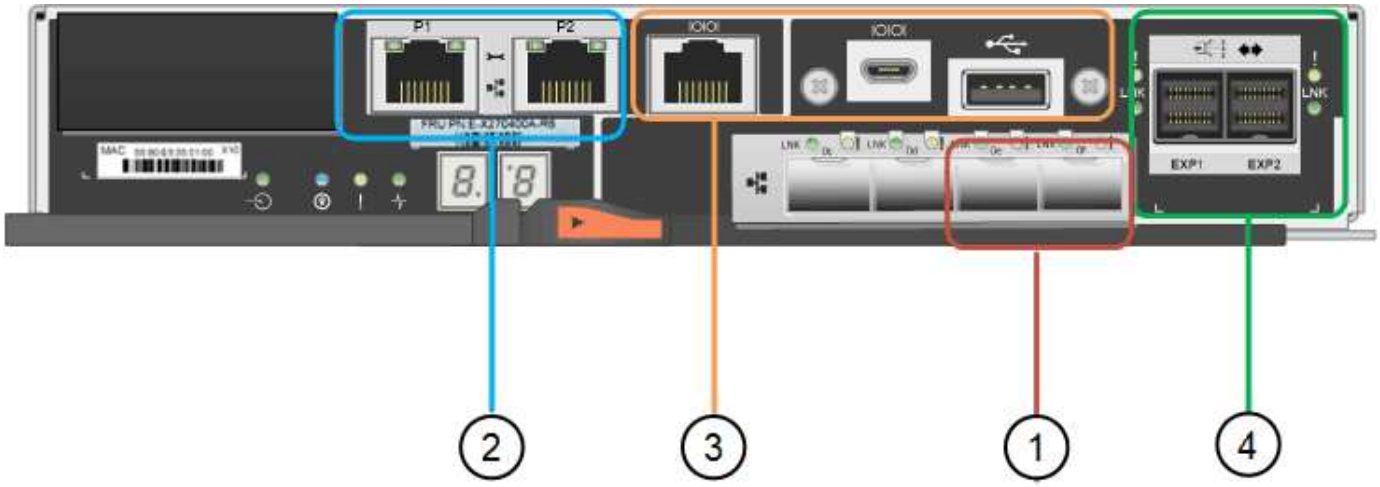
Connecteurs E2800A



Légende	Port	Type	Utiliser
1	Ports d'interconnexion 1 et 2	SFP optique FC 16 Gbit/s	Connectez chacun des contrôleurs E2800A au contrôleur SG6000-CN. Le contrôleur SG6000-CN comporte quatre connexions (deux pour chaque E2800A).

Légende	Port	Type	Utiliser
2	Ports de gestion 1 et 2	Ethernet 1 Gbit (RJ-45)	• Options du port 1 : ◦ Connectez-vous à un réseau de gestion pour activer l'accès TCP/IP direct à SANtricity System Manager ◦ Laissez le câble non câblé pour enregistrer un port de commutateur et une adresse IP. Accédez à SANtricity System Manager à l'aide des interfaces utilisateur Grid Manager ou Storage Grid Appliance installer. **Remarque** : certaines fonctionnalités SANtricity en option, telles que la synchronisation NTP pour des horodatages précis du journal, ne sont pas disponibles lorsque vous choisissez de laisser le port 1 sans fil. **Remarque** : StorageGRID 11.5 ou supérieur et SANtricity 11.70 ou supérieur sont nécessaires lorsque vous quittez le port 1 sans fil. • Le port 2 est réservé au support technique.
3	Ports de diagnostic et de support	• Port série RJ-45 • Port série micro USB • Port USB	Réservé au support technique.
4	Ports d'extension de lecteur 1 et 2	12 Gb/s SAS	Connectez les ports aux ports d'extension de disque sur les IOM du tiroir d'extension.

Connecteurs E2800B



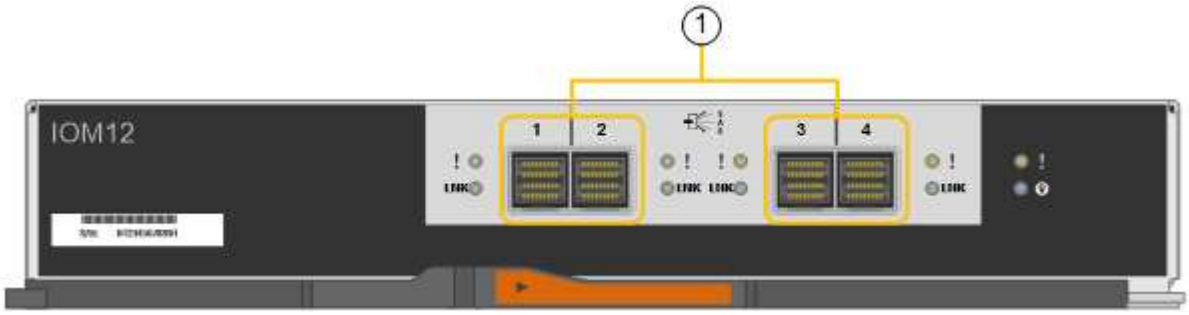
Légende	Port	Type	Utiliser
1	Ports d'interconnexion 1 et 2	SFP optique FC 16 Gbit/s	Connectez chacun des contrôleurs E2800B au contrôleur SG6000-CN. Le contrôleur SG6000-CN comporte quatre connexions (deux pour chaque E2800B).
2	Ports de gestion 1 et 2	Ethernet 1 Gbit (RJ-45)	• Options du port 1 : ◦ Connectez-vous à un réseau de gestion pour activer l'accès TCP/IP direct à SANtricity System Manager ◦ Laissez le câble non câblé pour enregistrer un port de commutateur et une adresse IP. Accédez à SANtricity System Manager à l'aide des interfaces utilisateur Grid Manager ou Storage Grid Appliance installer. **Remarque** : certaines fonctionnalités SANtricity en option, telles que la synchronisation NTP pour des horodatages précis du journal, ne sont pas disponibles lorsque vous choisissez de laisser le port 1 sans fil. **Remarque** : StorageGRID 11.5 ou supérieur et SANtricity 11.70 ou supérieur sont nécessaires lorsque vous quittez le port 1 sans fil. • Le port 2 est réservé au support technique.

Légende	Port	Type	Utiliser
3	Ports de diagnostic et de support	• Port série RJ-45 • Port série micro USB • Port USB	Réservé au support technique.
4	Ports d'extension de lecteur 1 et 2	12 Gb/s SAS	Connectez les ports aux ports d'extension de disque sur les IOM du tiroir d'extension.

SG6060 et SG6060X : modules d'E/S pour tiroirs d'extension en option

Le tiroir d'extension contient deux modules d'entrée/sortie qui se connectent aux contrôleurs de stockage ou à d'autres tiroirs d'extension.

Connecteurs IOM



Légende	Port	Type	Utiliser
1	Ports d'extension de lecteur 1-4	12 Gb/s SAS	Connectez chaque port aux contrôleurs de stockage ou au tiroir d'extension supplémentaire (le cas échéant).

Appliance SG5700 : présentation

L'appliance SG5700 StorageGRID est une plateforme de calcul et de stockage intégrée qui fonctionne comme un nœud de stockage dans un grid StorageGRID. L'appliance peut être utilisée dans un environnement de grid hybride qui combine des nœuds de stockage d'appliance et des nœuds de stockage virtuels (basés sur logiciel).

L'appliance StorageGRID SG5700 Series présente plusieurs caractéristiques :

- Intégrez les éléments de stockage et de calcul d'un nœud de stockage StorageGRID.
- Incluez le programme d'installation de l'appliance StorageGRID pour simplifier le déploiement et la configuration des nœuds de stockage.
- Inclut E-Series SANtricity System Manager pour la gestion et le contrôle du matériel.
- Prenez en charge jusqu'à quatre connexions 10 GbE ou 25 GbE avec le réseau Grid et le réseau client StorageGRID.

- Prise en charge des disques Full Disk Encryption (FDE) ou FIPS Lorsque ces disques sont utilisés avec la fonction de sécurité des disques dans SANtricity System Manager, l'accès non autorisé aux données n'est pas autorisé.

L'appliance SG5700 est disponible en quatre modèles : SG5712 et 101X, SG5760 et 101X. Il n'y a pas de spécifications ni de différences fonctionnelles entre le SG5712 et le 101X, à l'exception de l'emplacement des ports d'interconnexion sur le contrôleur de stockage. De même, il n'existe aucune différence de spécifications ou de fonctionnement entre les modèles SG5760 et SG5760X, sauf pour l'emplacement des ports d'interconnexion sur le contrôleur de stockage.

Composants de SG5700

Les modèles SG5700 comprennent les composants suivants :

Composant	SG5712	LE X112X	SG5760	LE MODÈLE DE LA SÉRIE XCOP60
Contrôleur de calcul	Contrôleur E5700SG	Contrôleur E5700SG	Contrôleur E5700SG	Contrôleur E5700SG
Contrôleur de stockage	Contrôleur E2800A	Contrôleur E2800B	Contrôleur E2800A	Contrôleur E2800B
Châssis	Boîtier E-Series DE212C, boîtier de deux unités de rack (2U)	Boîtier E-Series DE212C, boîtier de deux unités de rack (2U)	Boîtier E-Series DE460C, boîtier 4U	Boîtier E-Series DE460C, boîtier 4U
Disques	12 disques NL-SAS (3.5 pouces)	12 disques NL-SAS (3.5 pouces)	60 disques NL-SAS (3.5 pouces)	60 disques NL-SAS (3.5 pouces)
Alimentations et ventilateurs redondants	Deux blocs d'alimentation	Deux blocs d'alimentation	Deux blocs d'alimentation et deux blocs d'alimentation	Deux blocs d'alimentation et deux blocs d'alimentation

La capacité de stockage brute maximale disponible dans l'appliance StorageGRID est fixe, en fonction du nombre de disques de chaque armoire. Vous ne pouvez pas étendre le stockage disponible en ajoutant un tiroir comportant des disques supplémentaires.

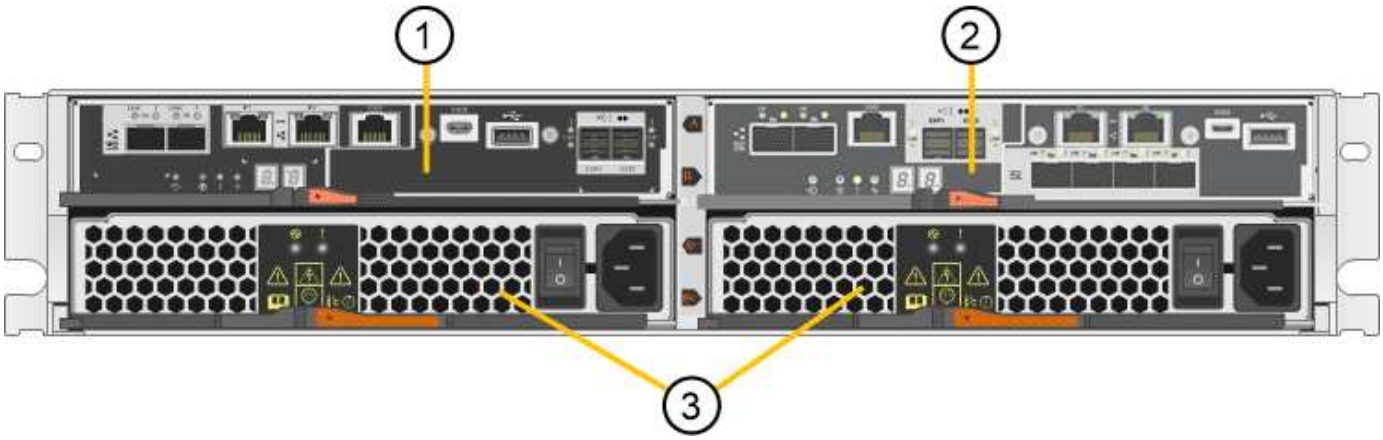
Diagrammes SG5700

SG5712 vues avant et arrière

Les figures illustrent l'avant et l'arrière du SG5712, un boîtier 2U pouvant contenir 12 disques.

Composants SG5712

Le SG5712 comprend deux contrôleurs et deux blocs d'alimentation.



Légende	Description
1	Contrôleur E2800A (contrôleur de stockage)
2	Contrôleur E5700SG (contrôleur de calcul)
3	Blocs d'alimentation

SG5712X, vues avant et arrière

Les figures illustrent l'avant et l'arrière du SG5712X, un boîtier 2U pouvant contenir 12 disques.

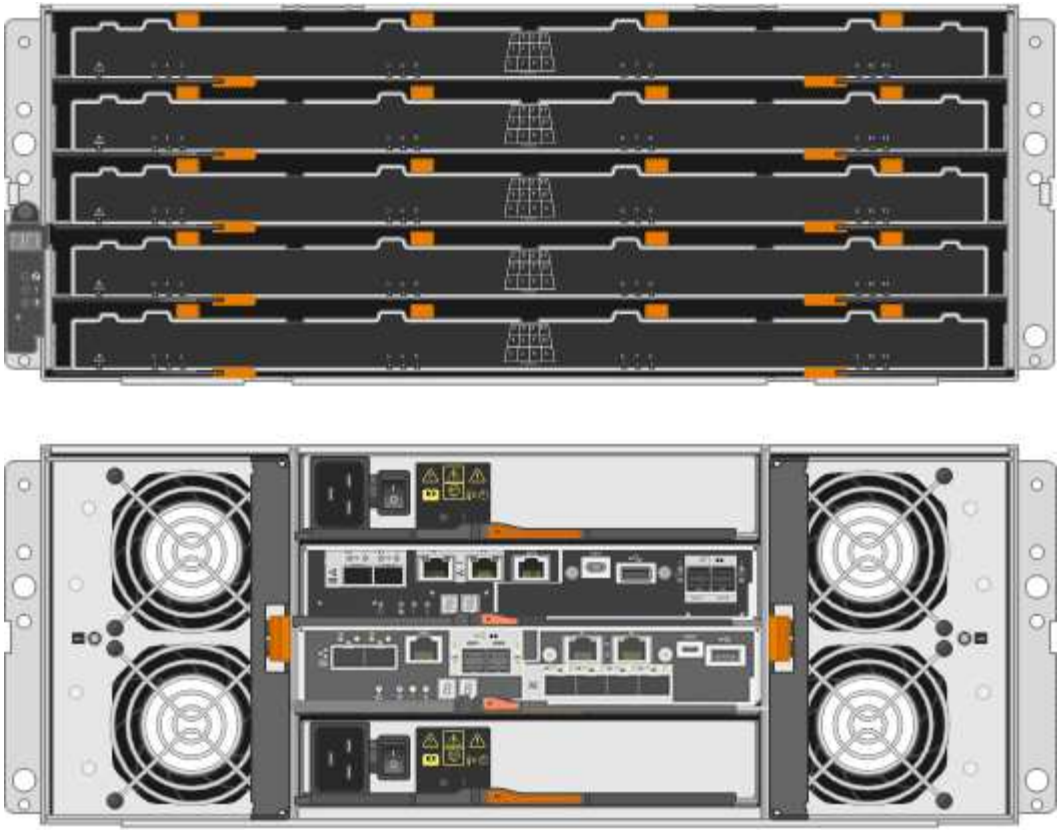
Composants SG5712X

Le modèle X112X est équipé de deux contrôleurs et de deux boîtiers de ventilateur d'alimentation.

Légende	Description
1	Contrôleur E2800B (contrôleur de stockage)
2	Contrôleur E5700SG (contrôleur de calcul)
3	Blocs d'alimentation

SG5760 : vues avant et arrière

La figure présente l'avant et l'arrière du modèle SG5760, un boîtier 4U contenant 60 disques dans 5 tiroirs.



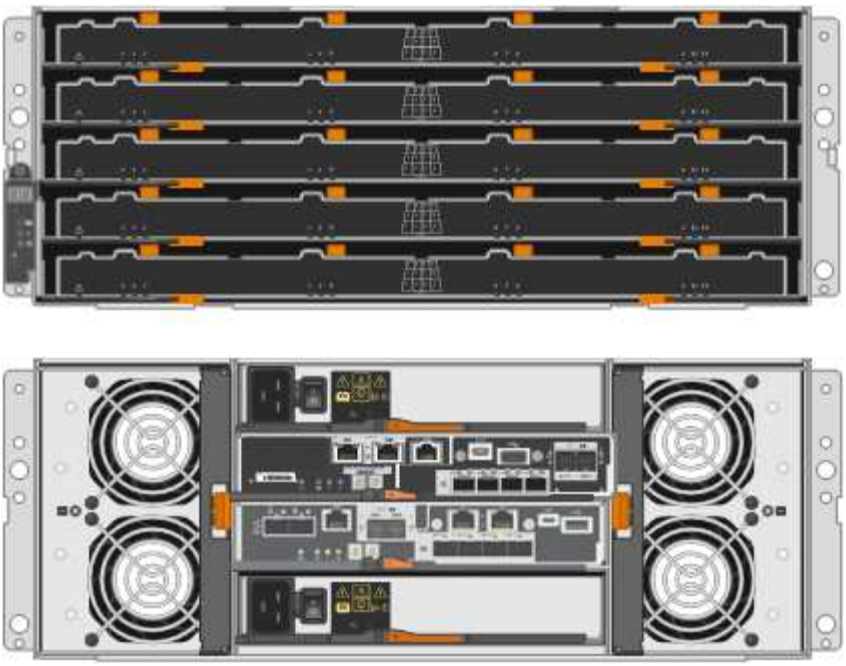
Composants SG5760

Le SG5760 inclut deux contrôleurs, deux blocs de ventilation et deux blocs d'alimentation.

Légende	Description
1	Contrôleur E2800A (contrôleur de stockage)
2	Contrôleur E5700SG (contrôleur de calcul)
3	Cartouche de ventilateur (1 sur 2)
4	Boîtier de puissance (1 sur 2)

SG5760X, vues avant et arrière

Les figures illustrent l'avant et l'arrière du modèle SG5760X, un boîtier 4U contenant 60 disques dans 5 tiroirs.



Composants SG5760X

Le SG5760X comprend deux contrôleurs, deux boîtiers pour ventilateurs et deux blocs d'alimentation.

Légende	Description
1	Contrôleur E2800B (contrôleur de stockage)
2	Contrôleur E5700SG (contrôleur de calcul)
3	Cartouche de ventilateur (1 sur 2)
4	Boîtier de puissance (1 sur 2)

Informations associées

"Site de documentation sur les systèmes NetApp E-Series"

Contrôleurs SG5700

Les modèles SG5712 et SAP12X de 12 disques ainsi que SG5760 et S10X de 60 disques de l'appliance StorageGRID incluent un contrôleur de calcul E5700SG et un contrôleur de stockage E-Series E2800.

- Le SG5712 et SG5760 utilisent un contrôleur E2800A.
- Le modèle U112X et le modèle UB60X utilisent un contrôleur E2800B.

Les contrôleurs E2800A et E2800B sont identiques en termes de spécifications et de fonctions, sauf pour l'emplacement des ports d'interconnexion.

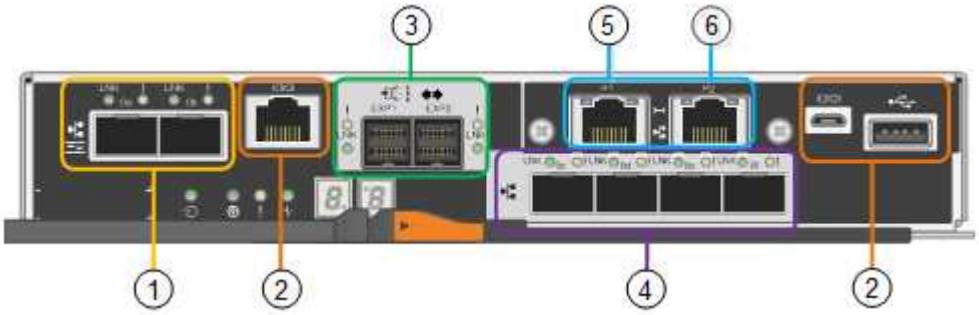
Contrôleur de calcul E5700SG

- Fonctionne comme serveur de calcul pour l'appliance.
- Inclut le programme d'installation de l'appliance StorageGRID.

> Le logiciel StorageGRID n'est pas préinstallé sur l'appliance. Lors du déploiement de l'appliance, il est possible d'accéder à ce logiciel à partir du nœud d'administration.

- Peut se connecter aux trois réseaux StorageGRID, y compris le réseau Grid, le réseau d'administration et le réseau client.
- Connexion au contrôleur E2800 et fonctionne comme initiateur.

Connecteurs E5700SG



Légende	Port	Type	Utiliser
1	Ports d'interconnexion 1 et 2	Fibre Channel (FC) de 16 Gbit/s, SFP optique	Connectez le contrôleur E5700SG au contrôleur E2800.
2	Ports de diagnostic et de support	• Port série RJ-45 • Port série micro USB • Port USB	Réservé au support technique.
3	Ports d'extension de disque	12 Gb/s SAS	Non utilisé. Les appliances StorageGRID ne prennent pas en charge les tiroirs disques d'extension.
4	Ports réseau 1-4	10 GbE ou 25 GbE, selon le type d'émetteur-récepteur SFP, la vitesse du commutateur et la vitesse de liaison configurée	Connectez-vous au réseau Grid et au réseau client pour StorageGRID.
5	Port de gestion 1	Ethernet 1 Gbit (RJ-45)	Connectez-vous au réseau d'administration pour StorageGRID.

Légende	Port	Type	Utiliser
6	Port de gestion 2	Ethernet 1 Gbit (RJ-45)	Options : • Lien avec le port de gestion 1 pour une connexion redondante au réseau d'administration pour StorageGRID. • Laissez sans fil et disponible pour l'accès local temporaire (IP 169.254.0.1). • Lors de l'installation, utilisez le port 2 pour la configuration IP si les adresses IP attribuées par DHCP ne sont pas disponibles.

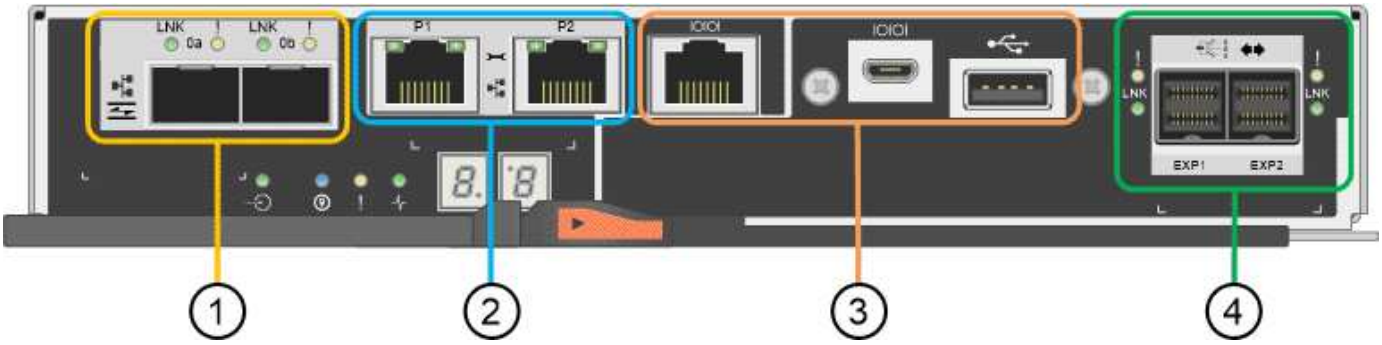
Contrôleur de stockage E2800

Deux versions du contrôleur de stockage E2800 sont utilisées dans les appliances SG5700 : E2800A et E2800B. Le E2800A n'a pas de HIC et le E2800B est équipé d'une HIC à quatre ports. Les deux versions de contrôleur ont des spécifications et des fonctions identiques, à l'exception de l'emplacement des ports d'interconnexion.

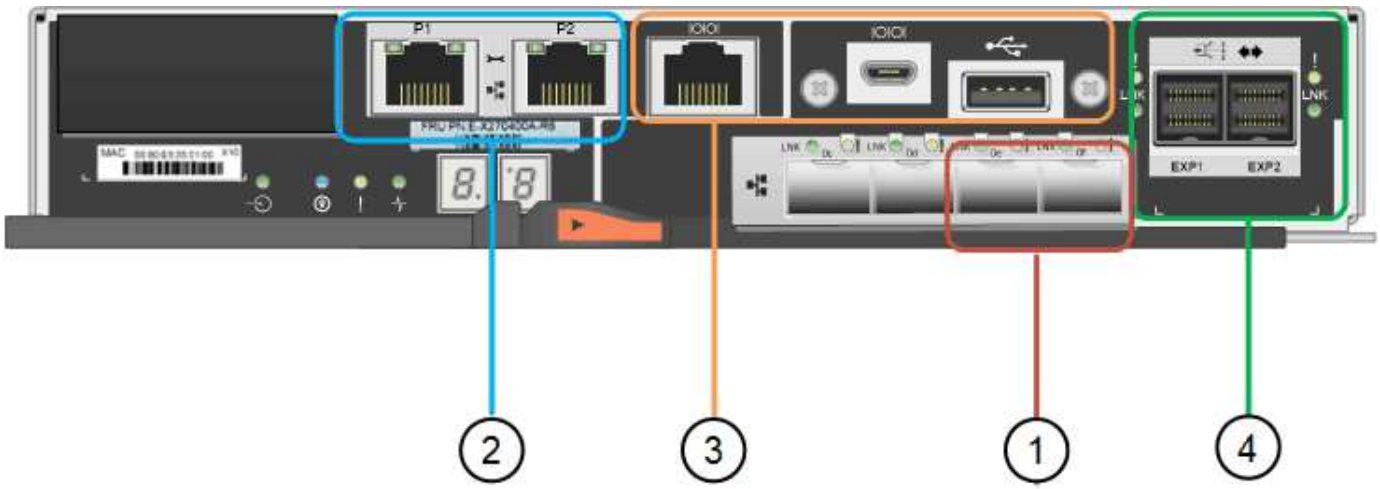
Le contrôleur de stockage E2800 Series présente les caractéristiques suivantes :

- Fonctionne comme contrôleur de stockage pour l'appliance.
- Gère le stockage des données sur les disques.
- Fonctionne en tant que contrôleur E-Series standard en mode simplex.
- Inclut le logiciel SANtricity OS (firmware du contrôleur).
- Inclut SANtricity System Manager pour le matériel de l'appliance de surveillance, la gestion des alertes, la fonction AutoSupport et la sécurité des lecteurs.
- Se connecte au contrôleur E5700SG et fonctionne comme cible.

Connecteurs E2800A



Connecteurs E2800B



Légende	Port	Type	Utiliser
1	Ports d'interconnexion 1 et 2	SFP optique FC 16 Gbit/s	Connectez le contrôleur E2800 au contrôleur E5700SG.

Légende	Port	Type	Utiliser
2	Ports de gestion 1 et 2	Ethernet 1 Gbit (RJ-45)	• Options du port 1 : ◦ Connectez-vous à un réseau de gestion pour activer l'accès TCP/IP direct à SANtricity System Manager ◦ Laissez le câble non câblé pour enregistrer un port de commutateur et une adresse IP. Accédez à SANtricity System Manager à l'aide des interfaces utilisateur Grid Manager ou Storage Grid Appliance installer. **Remarque** : certaines fonctionnalités SANtricity en option, telles que la synchronisation NTP pour des horodatages précis du journal, ne sont pas disponibles lorsque vous choisissez de laisser le port 1 sans fil. **Remarque** : StorageGRID 11.5 ou supérieur et SANtricity 11.70 ou supérieur sont nécessaires lorsque vous quittez le port 1 sans fil. • Le port 2 est réservé au support technique.
3	Ports de diagnostic et de support	• Port série RJ-45 • Port série micro USB • Port USB	Réservé au support technique.
4	Ports d'extension de disque.	12 Gb/s SAS	Non utilisé.

Appareils SG100 et SG1000: Présentation

Le dispositif des services StorageGRID SG100 et l'appliance des services SG1000 peuvent fonctionner en tant que nœud de passerelle et en tant que nœud d'administration pour fournir des services d'équilibrage de charge haute disponibilité dans

un système StorageGRID. Les deux appliances peuvent fonctionner en tant que nœuds de passerelle et de nœud d'administration (principal ou non primaire) à la fois.

Caractéristiques de l'appareil

Les deux modèles de l'appareil de services offrent les fonctionnalités suivantes :

- Le nœud de passerelle ou le nœud d'administration fonctionne pour un système StorageGRID.
- Le programme d'installation de l'appliance StorageGRID simplifie le déploiement et la configuration des nœuds.
- Une fois déployé, peut accéder au logiciel StorageGRID à partir d'un nœud d'administration existant ou d'un logiciel téléchargé vers un disque local. Pour simplifier davantage le processus de déploiement, une version récente du logiciel est préchargée sur l'appareil pendant la fabrication.
- Contrôleur de gestion de la carte mère (BMC) pour le contrôle et le diagnostic de certaines pièces du matériel de l'appliance.
- Possibilité de se connecter aux trois réseaux StorageGRID, y compris le réseau Grid, le réseau d'administration et le réseau client :
  - Le SG100 prend en charge jusqu'à quatre connexions 10 ou 25 GbE au réseau Grid et au réseau client.
  - Le SG1000 prend en charge jusqu'à quatre connexions 10, 25, 40 ou 100 GbE au réseau Grid et au réseau client.

Schémas SG100 et SG1000

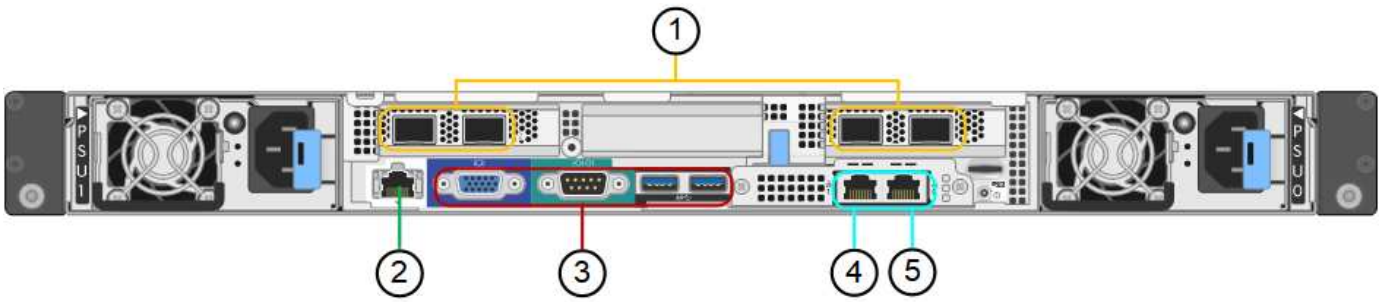
Cette figure montre l'avant du SG100 et du SG1000 avec le cadre retiré. À partir de l'avant, les deux appareils sont identiques, à l'exception du nom du produit sur le cadre.

Les deux disques SSD (Solid-State Drives), indiqués par le contour orange, sont utilisés pour stocker le système d'exploitation StorageGRID et sont mis en miroir avec RAID 1 pour la redondance. Lorsque l'appliance de services SG100 ou SG1000 est configurée comme un nœud d'administration, ces disques servent à stocker les journaux d'audit, les metrics et les tables de bases de données.

Les emplacements de lecteur restants sont vides.

Connecteurs SG100

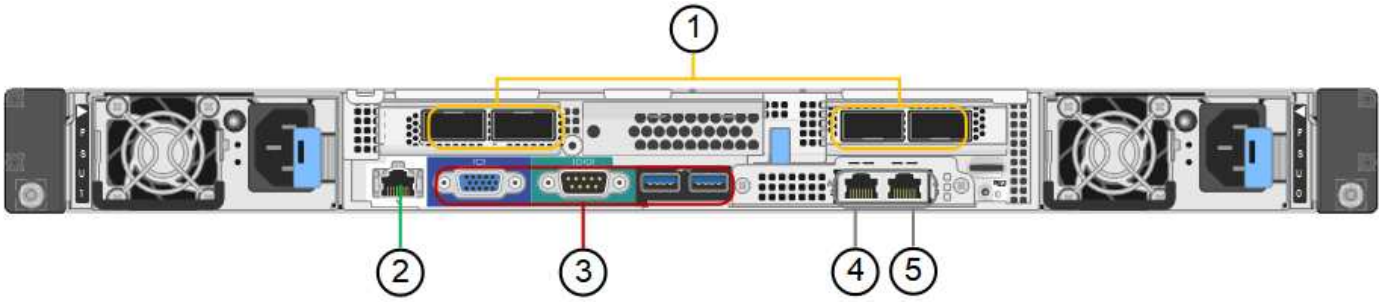
Cette figure montre les connecteurs à l'arrière du SG100.



Légende	Port	Type	Utiliser
1	Ports réseau 1-4	10/25-GbE, selon le type d'émetteur-récepteur SFP ou câble (les modules SFP28 et SFP+ sont pris en charge), la vitesse du switch et la vitesse de liaison configurée	Connectez-vous au réseau Grid et au réseau client pour StorageGRID.
2	Port de gestion BMC	1 GbE (RJ-45)	Se connecte au contrôleur de gestion de la carte de base de l'appliance.
3	Ports de diagnostic et de support	• VGA • Série, 115200 8-N-1 • USB	Réservé au support technique.
4	Port réseau d'administration 1	1 GbE (RJ-45)	Connectez l'appliance au réseau d'administration pour StorageGRID.
5	Port réseau d'administration 2	1 GbE (RJ-45)	Options : • Lien avec le port de gestion 1 pour une connexion redondante au réseau d'administration pour StorageGRID. • Laisser déconnecté et disponible pour l'accès local temporaire (IP 169.254.0.1). • Lors de l'installation, utilisez le port 2 pour la configuration IP si les adresses IP attribuées par DHCP ne sont pas disponibles.

Connecteurs SG1000

Cette figure montre les connecteurs à l'arrière du SG1000.



Légende	Port	Type	Utiliser
1	Ports réseau 1-4	10/25/40/100-GbE, selon le type de câble ou d'émetteur-récepteur, la vitesse du commutateur et la vitesse de liaison configurée. Les protocoles QSFP28 et QSFP+ (40 GbE) sont pris en charge en natif et les émetteurs-récepteurs SFP28/SFP+ peuvent être utilisés avec un QSA (vendu séparément) pour utiliser des vitesses 10 GbE.	Connectez-vous au réseau Grid et au réseau client pour StorageGRID.
2	Port de gestion BMC	1 GbE (RJ-45)	Se connecte au contrôleur de gestion de la carte de base de l'appliance.
3	Ports de diagnostic et de support	• VGA • Série, 115200 8-N-1 • USB	Réservé au support technique.
4	Port réseau d'administration 1	1 GbE (RJ-45)	Connectez l'appliance au réseau d'administration pour StorageGRID.

Légende	Port	Type	Utiliser
5	Port réseau d'administration 2	1 GbE (RJ-45)	Options : • Lien avec le port de gestion 1 pour une connexion redondante au réseau d'administration pour StorageGRID. • Laisser déconnecté et disponible pour l'accès local temporaire (IP 169.254.0.1). • Lors de l'installation, utilisez le port 2 pour la configuration IP si les adresses IP attribuées par DHCP ne sont pas disponibles.

Applications SG100 et SG1000

Vous pouvez configurer les appliances de services StorageGRID de différentes façons pour fournir des services de passerelle ainsi que la redondance de certains services d'administration de grille.

Les appliances peuvent être déployées de plusieurs manières :

- Ajouter à une nouvelle grille ou à une grille existante en tant que nœud de passerelle
- Ajoutez à une nouvelle grille en tant que nœud d'administration principal ou non primaire, ou à une grille existante en tant que nœud d'administration non primaire
- Fonctionnement en tant que nœud passerelle et nœud d'administration (principal ou non primaire) en même temps

L'appliance facilite l'utilisation de groupes haute disponibilité (HA) et d'un équilibrage intelligent de la charge pour les connexions de chemin d'accès aux données S3 ou Swift.

Les exemples suivants décrivent comment optimiser les capacités de l'appliance :

- Utilisez deux appareils SG100 ou SG1000 pour fournir des services de passerelle en les configurant en tant que nœuds de passerelle.

> Ne déployez pas les appliances de services SG100 et SG1000 sur le même site. Cela peut entraîner des performances imprévisibles.

- Utilisez deux appareils SG100 ou SG1000 pour assurer la redondance de certains services d'administration de réseau. Pour ce faire, configurez chaque appliance en tant que nœuds d'administration.
- Utilisez deux appareils SG100 ou deux SG1000 pour fournir des services d'équilibrage de charge et de mise en forme du trafic hautement disponibles accessibles via une ou plusieurs adresses IP virtuelles. Pour ce faire, les appliances sont configurés comme des combinaisons de nœuds d'administration ou de nœuds de passerelle et vous ajoutez les deux nœuds au même groupe haute disponibilité.

Si vous utilisez des nœuds d'administration et des nœuds de passerelle dans le même groupe haute disponibilité, le port Admin nœud seul ne basculera pas. Reportez-vous aux instructions pour "Configuration des groupes haute disponibilité".

Lorsqu'il est utilisé avec des appliances de stockage StorageGRID, les appliances de services SG100 et SG1000 permettent de déployer des grilles d'appliance uniquement, sans dépendance vis-à-vis des hyperviseurs externes ou du matériel de calcul.

Avant l'installation

Préparer le site

Avant d'installer l'appliance, assurez-vous que le site et l'armoire ou le rack que vous souhaitez utiliser correspondent aux spécifications d'une appliance StorageGRID.

Étapes

1. Vérifier que le site répond aux exigences en matière de température, d'humidité, d'altitude, de débit d'air, de dissipation thermique, câblage, alimentation et mise à la terre. Voir la "NetApp Hardware Universe" pour en savoir plus.
2. Vérifiez que votre emplacement fournit la tension correcte de l'alimentation secteur :

Modèle	Conditions requises
SGF6112	100 à 240 volts c.a.
SG6060	240 V c.a.
SGF6024	120 V c.a.
SG5760	240 V c.a.
SG100 et SG1000	120 à 240 volts c.a.

3. Procurez-vous une armoire ou un rack de 19 pouces (48.3 cm) pour les étagères de la taille suivante (sans câbles).

SGF6112

Hauteur	Largeur	Profondeur	Poids maximum
1.70 po (4.31 cm)	18.98 po (48.2 cm)	33.11 po (84.1 cm)	43.83 lb (19.88 kg)

SG6000

Type d'étagère	Hauteur	Largeur	Profondeur	Poids maximum
Tiroir contrôleur E2860 (SG6060)	6.87 po (17.46 cm)	17.66 po (44.86 cm)	38.25 po (97.16 cm)	250 lb (113 kg)
Tiroir d'extension (SG6060) - en option	6.87 po (17.46 cm)	17.66 po (44.86 cm)	38.25 po (97.16 cm)	250 lb (113 kg)
Tiroir contrôleur EF570 (SGF6024)	3.35 po (8.50 cm)	17.66 po (44.86 cm)	19.00 po (48.26 cm)	51.74 lb (23.47 kg)
Contrôleur de calcul SG6000-CN	1.70 po (4.32 cm)	17.32 po (44.0 cm)	32.0 po (81.3 cm)	39 lb (17.7 kg)

SG5700

Modèle de type appliance	Hauteur	Largeur	Profondeur	Poids maximum
SG5712 (12 lecteurs)	3.41 po (8.68 cm)	17.6 po (44.7 cm)	21.1 po (53.6 cm)	63.9 lb (29.0 kg)
SG5760 (60 lecteurs)	6.87 po (17.46 cm)	17.66 po (44.86 cm)	38.25 po (97.16 cm)	250 lb (113 kg)

SG100 et SG1000

Hauteur	Largeur	Profondeur	Poids maximum
1.70 po (4.32 cm)	17.32 po (44.0 cm)	32.0 po (81.3 cm)	39 lb (17.7 kg)

4. Choisissez où vous allez installer l'appareil.

Lors de l'installation du tiroir contrôleur E2860 ou des tiroirs d'extension en option, installez le matériel en bas jusqu'en haut du rack ou de l'armoire afin d'éviter tout basculement de l'équipement. Pour que l'équipement le plus lourd se trouve au bas de l'armoire ou du rack, installez le contrôleur SG6000-CN au-dessus du tiroir du contrôleur E2860 et des tiroirs d'extension.

Avant de valider l'installation, vérifiez que les câbles optiques de 0,5 m livrés avec un système SG6000 ou les câbles que vous fournissez sont suffisamment longs pour la configuration prévue.

5. Installez les commutateurs réseau requis. Voir la "Matrice d'interopérabilité NetApp" pour obtenir des informations sur la compatibilité.

Déballez les boîtes

Avant d'installer votre appareil StorageGRID, déballez toutes les boîtes et comparez le contenu aux éléments figurant sur le bordereau d'expédition.

Appliances SGF6112

Sous-jacent

Élément	À quoi ressemble-t-il
SGF6112	
Kit de rails avec instructions	
Panneau avant	

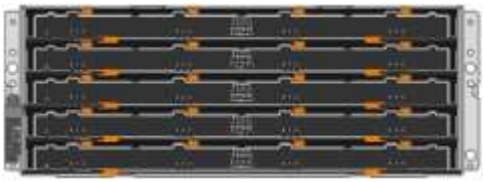
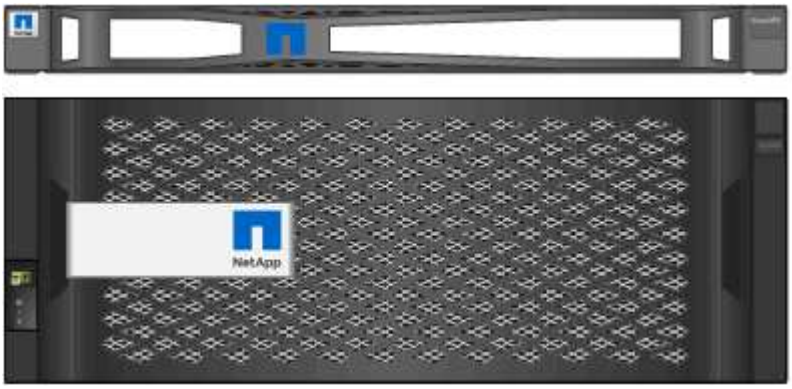
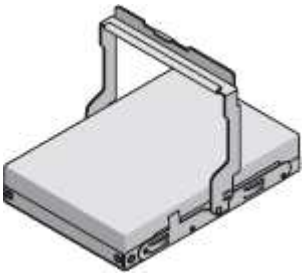
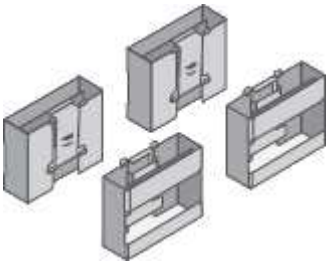
Cordons d'alimentation

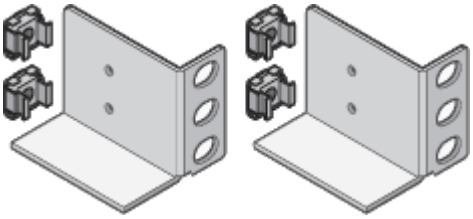
La livraison d'une appliance SGF6112 inclut les cordons d'alimentation suivants.

Il se peut que votre armoire soit équipée de cordons d'alimentation spéciaux à la place des câbles d'alimentation fournis avec l'appliance.

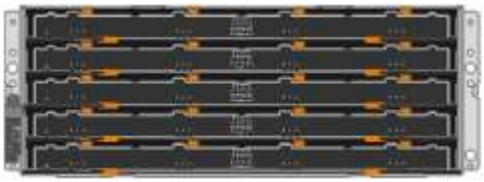
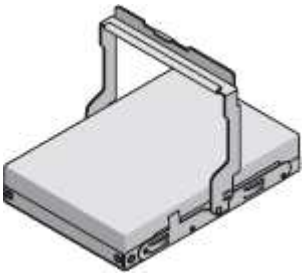
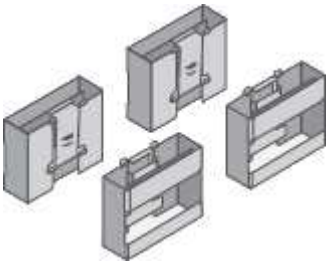
Élément	À quoi ressemble-t-il
Deux cordons d'alimentation pour votre pays	

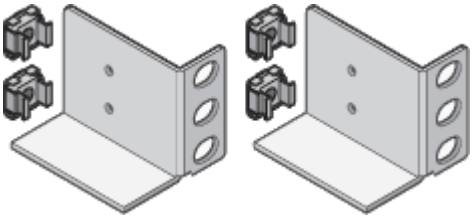
Matériel SG6060

Élément	À quoi ressemble-t-il
Contrôleur SG6000-CN	
Tiroir contrôleur E2860 sans disque installé	
Deux encadrements avant	
Deux kits de rails avec instructions	
60 disques (2 SSD et 58 NL-SAS)	
Quatre poignées	

Élément	À quoi ressemble-t-il
Supports arrière et écrous à cage pour l'installation en rack à trous carrés	

Tiroir d'extension SG6060

Élément	À quoi ressemble-t-il
Tiroir d'extension sans disque installé	
Panneau avant	
60 disques NL-SAS	
Un kit de rails avec instructions	
Quatre poignées	

Élément	À quoi ressemble-t-il
Supports arrière et écrous à cage pour l'installation en rack à trous carrés	

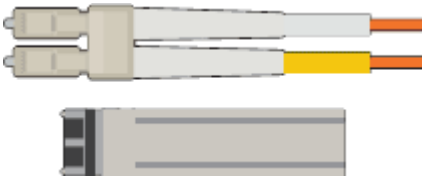
Matériel SGF6024

Élément	À quoi ressemble-t-il
Contrôleur SG6000-CN	
Baie Flash EF570 installée avec 24 disques SSD (Flash	
Deux encadrements avant	
Deux kits de rails avec instructions	
Têtes de gondole des tablettes	

Câbles et connecteurs

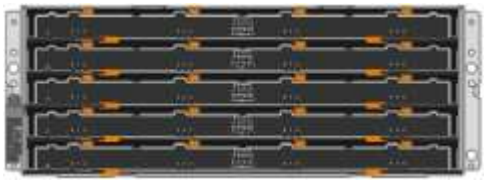
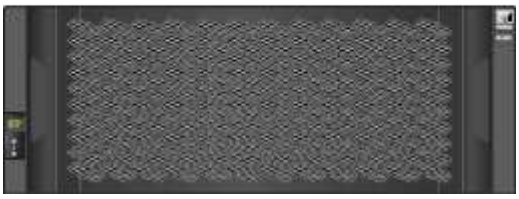
La livraison d'un système SG6000 inclut les câbles et connecteurs suivants.

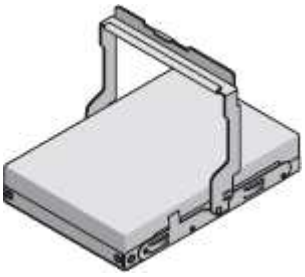
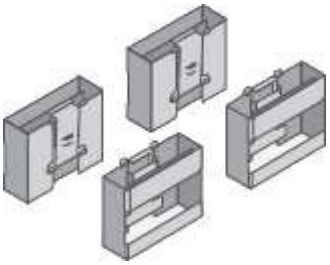
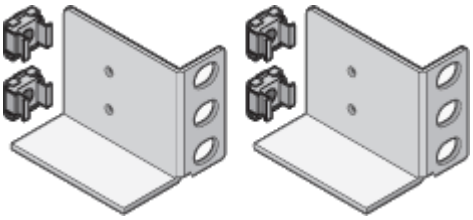
Il se peut que votre armoire soit équipée de cordons d'alimentation spéciaux à la place des câbles d'alimentation fournis avec l'appliance.

Élément	À quoi ressemble-t-il
Quatre cordons d'alimentation pour votre pays	
Câbles optiques et émetteurs-récepteurs SFP	 • Quatre câbles optiques pour les ports d'interconnexion FC • Quatre émetteurs-récepteurs SFP+ prenant en charge le protocole FC 16 Gbit/s.
En option : deux câbles SAS pour connecter chaque tiroir d'extension SG6060	

Appliances SG5700

Sous-jacent

Élément	À quoi ressemble-t-il
Appliance SG5712 avec 12 disques installés	
Appliance SG5760 sans disque installé	
Panneau avant de l'appareil	 

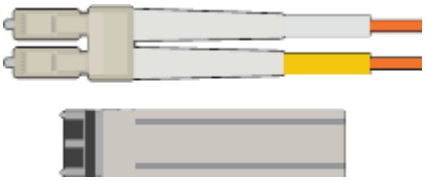
Élément	À quoi ressemble-t-il
Kit de rails avec instructions	
SG5760 : 60 disques	
SG5760 : poignées	
SG5760 : supports arrière et écrous cage pour une installation en rack à trous carrés	

Câbles et connecteurs

La livraison d'une appliance SG5700 inclut les câbles et connecteurs suivants.

Il se peut que votre armoire soit équipée de cordons d'alimentation spéciaux à la place des câbles d'alimentation fournis avec l'appliance.

Élément	À quoi ressemble-t-il
Deux cordons d'alimentation pour votre pays	

Élément	À quoi ressemble-t-il
Câbles optiques et émetteurs-récepteurs SFP	 • Deux câbles optiques pour les ports d'interconnexion FC • Huit émetteurs-récepteurs SFP+, compatibles avec les quatre ports d'interconnexion FC 16 Gbit/s et les quatre ports réseau 10 GbE

Appliances SG100 et SG1000

Sous-jacent

Élément	À quoi ressemble-t-il
SG100 ou SG1000	
Kit de rails avec instructions	

Cordons d'alimentation

La livraison d'une appliance SG100 ou SG1000 inclut les cordons d'alimentation suivants.

Il se peut que votre armoire soit équipée de cordons d'alimentation spéciaux à la place des câbles d'alimentation fournis avec l'appliance.

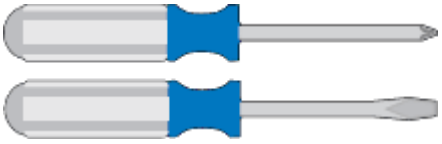
Élément	À quoi ressemble-t-il
Deux cordons d'alimentation pour votre pays	

Procurez-vous des équipements et outils supplémentaires

Avant d'installer une appliance StorageGRID, vérifiez que vous disposez de tous les équipements et outils supplémentaires dont vous avez besoin.

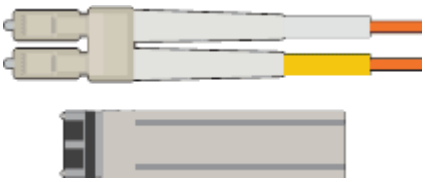
Tous les appareils

Vous avez besoin de l'équipement suivant pour installer et configurer tous les dispositifs.

Élément	À quoi ressemble-t-il
Tournevis	 • N° Phillips 2 tournevis • Tournevis plat moyen
Bracelet antistatique	
L'ordinateur portable de service	 • "Navigateur Web pris en charge" • Client SSH, tel que PuTTY • Port 1 GbE (RJ-45) Certains ports ne prennent pas en charge les débits Ethernet 10/100.
Outils en option	 • Perceuse électrique avec embout Phillips • Lampe de poche

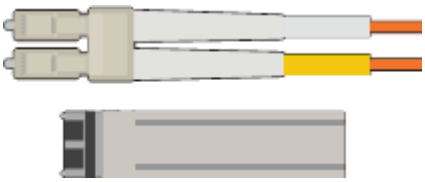
SGF6112

Vous avez besoin de l'équipement supplémentaire suivant pour installer et configurer le matériel SGF6112.

Élément	À quoi ressemble-t-il
Câbles optiques et émetteurs-récepteurs	 • Un à quatre de ces types de câbles : ◦ Twinax/cuivre ◦ Fibre optique • De un à quatre de ces émetteurs-récepteurs/adaptateurs en fonction de la vitesse de liaison (les vitesses mixtes ne sont pas prises en charge) : ◦ SFP+ 10 GbE ◦ 25 GbE SFP28
Câbles Ethernet RJ-45 (Cat5/Cat5e/Cat6/Cat6a)	

SG6000

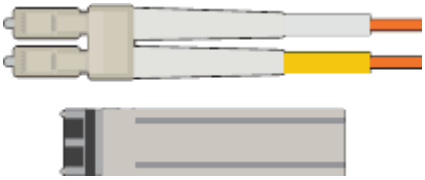
Vous avez besoin de l'équipement supplémentaire suivant pour installer et configurer le matériel SG6000.

Élément	À quoi ressemble-t-il
Câbles optiques et émetteurs-récepteurs SFP	 • Un à quatre de ces types de câbles : ◦ Twinax/cuivre ◦ Fibre optique • Un à quatre de ces émetteurs-récepteurs/cartes, en fonction de la vitesse de liaison (les vitesses mixtes ne sont pas prises en charge) : ◦ SFP+ 10 GbE ◦ 25 GbE SFP28
Câbles Ethernet RJ-45 (Cat5/Cat5e/Cat6)	

Élément	À quoi ressemble-t-il
Outils en option	Levage mécanisé pour les tiroirs de 60 disques

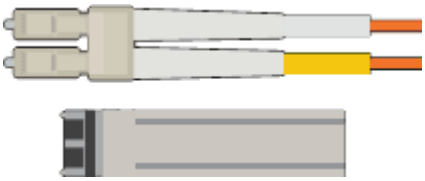
SG5700

Vous avez besoin des équipements supplémentaires suivants pour installer et configurer le matériel SG5700.

Élément	À quoi ressemble-t-il
Câbles optiques et émetteurs-récepteurs SFP	 • Câbles optiques pour les ports 10/25 GbE que vous souhaitez utiliser • Facultatif : les émetteurs-récepteurs SFP28 si vous souhaitez utiliser la vitesse de liaison 25 GbE
Câbles Ethernet	
Outils en option	Levage mécanisé pour SG5760

SG100 et SG1000

Vous avez besoin de l'équipement supplémentaire suivant pour installer et configurer le matériel SG100 et SG1000.

Élément	À quoi ressemble-t-il
Câbles optiques et émetteurs-récepteurs	 • Un à quatre de ces types de câble : ◦ Twinax/cuivre ◦ Fibre optique • De un à quatre de ces émetteurs-récepteurs/adaptateurs en fonction de la vitesse de liaison (les vitesses mixtes ne sont pas prises en charge) : ◦ SG100 : ▪ SFP+ 10 GbE ▪ 25 GbE SFP28 ◦ SG1000 : ▪ Adaptateur QSFP-to-SFP (QSA) et SFP+ 10 GbE ▪ Adaptateur QSFP-to-SFP (QSA) à 25 GbE et SFP28 ▪ QSFP+ 40 GbE ▪ QFSP28 100 GbE
Câbles Ethernet RJ-45 (Cat5/Cat5e/Cat6/Cat6a)	

Navigateurs Web pris en charge

Vous devez utiliser un navigateur Web pris en charge.

Navigateur Web	Version minimale prise en charge
Google Chrome	107
Microsoft Edge	107
Mozilla Firefox	106

Vous devez régler la fenêtre du navigateur sur une largeur recommandée.

Largeur du navigateur	Pixels
Minimum	1024

Largeur du navigateur	Pixels
Optimale	1280

Vérifiez les connexions réseau de l'appliance

Vérifiez les connexions réseau de l'appliance

Avant d'installer l'appliance StorageGRID, vous devez savoir quels réseaux peuvent être connectés à l'appliance et comment les ports de chaque contrôleur sont utilisés. La configuration réseau requise pour StorageGRID est expliquée en détail dans le "Instructions de mise en réseau".

Lorsque vous déployez une appliance StorageGRID en tant que nœud d'un système StorageGRID, vous pouvez la connecter aux réseaux suivants :

- **Réseau Grid pour StorageGRID** : le réseau Grid est utilisé pour tout le trafic StorageGRID interne. Il assure la connectivité entre tous les nœuds de la grille, sur tous les sites et sous-réseaux. Le réseau Grid est requis.
- **Réseau d'administration pour StorageGRID** : le réseau d'administration est un réseau fermé utilisé pour l'administration et la maintenance du système. Le réseau Admin est généralement un réseau privé et n'a pas besoin d'être routable entre les sites. Le réseau d'administration est facultatif.
- **Réseau client pour StorageGRID :** le réseau client est un réseau ouvert utilisé pour fournir un accès aux applications client, y compris S3 et Swift. Le réseau client fournit un accès au protocole client à la grille, de sorte que le réseau Grid puisse être isolé et sécurisé. Vous pouvez configurer le réseau client de sorte que l'appliance soit accessible via ce réseau en utilisant uniquement les ports que vous choisissez d'ouvrir. Le réseau client est facultatif.
- **Réseau de gestion pour SANtricity** (facultatif pour les dispositifs de stockage, non requis pour le SGF6112) : ce réseau permet d'accéder à SANtricity System Manager, ce qui vous permet de surveiller et de gérer les composants matériels de l'appliance et du tiroir du contrôleur de stockage. Ce réseau de gestion peut être le même que le réseau d'administration pour StorageGRID, ou il peut s'agir d'un réseau de gestion indépendant.
- **Réseau de gestion BMC** (facultatif pour SG100, SG1000, SG6000 et SGF6112) : ce réseau permet d'accéder au contrôleur de gestion de la carte de base des appliances SG100, SG1000, SG6000 et SGF6112, ce qui vous permet de surveiller et de gérer les composants matériels de l'appliance. Ce réseau de gestion peut être le même que le réseau d'administration pour StorageGRID, ou il peut s'agir d'un réseau de gestion indépendant.

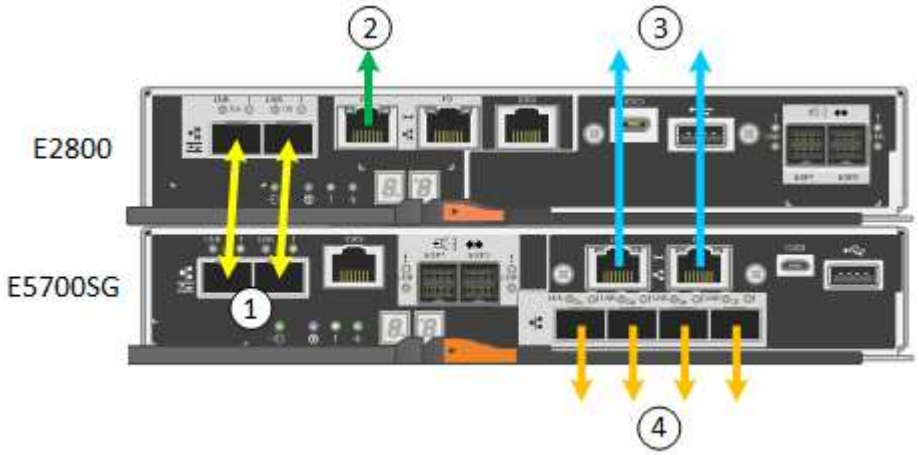
  Si le réseau de gestion BMC facultatif n'est pas connecté, certaines procédures de support et de maintenance seront plus difficiles à réaliser. Vous pouvez ne pas connecter le réseau de gestion BMC, sauf si nécessaire à des fins de support.

> ⓘ Pour plus d'informations sur les réseaux StorageGRID, reportez-vous au "Types de réseau StorageGRID".

Connexions réseau (SG5700)

Lorsque vous installez une appliance SG5700 StorageGRID, vous connectez les deux contrôleurs les uns aux autres et aux réseaux requis.

La figure montre les deux contrôleurs SG5760, avec le contrôleur E2800 en haut et le contrôleur E5700SG en bas. Dans le SG5712, le contrôleur E2800 est à la gauche du contrôleur E5700SG.



Légende	Port	Type de port	Utiliser
1	Deux ports d'interconnexion sur chaque contrôleur	SFP+ optique 16 Gbit/s FC	Connectez les deux contrôleurs les uns aux autres.
2	Port de gestion 1 du contrôleur E2800	1 GbE (RJ-45)	Connexion au réseau sur lequel vous accédez à SANtricity System Manager. Vous pouvez utiliser le réseau d'administration pour StorageGRID ou un réseau de gestion indépendant.
Port de gestion 2 du contrôleur E2800	1 GbE (RJ-45)	Réservé au support technique.	3
Port de gestion 1 du contrôleur E5700SG	1 GbE (RJ-45)	Permet de connecter le contrôleur E5700SG au réseau d'administration pour StorageGRID.	Port de gestion 2 du contrôleur E5700SG

Légende	Port	Type de port	Utiliser
1 GbE (RJ-45)	• Peut être lié avec le port de gestion 1 si vous souhaitez établir une connexion redondante avec le réseau d'administration. • Peut être laissé sans fil et disponible pour un accès local temporaire (IP 169.254.0.1). • Lors de l'installation, peut être utilisé pour connecter le contrôleur E5700SG à un ordinateur portable de service si les adresses IP attribuées par DHCP ne sont pas disponibles.	4	Ports 10/25 GbE 1-4 sur le contrôleur E5700SG

Modes de liaison de port (SGF6112)

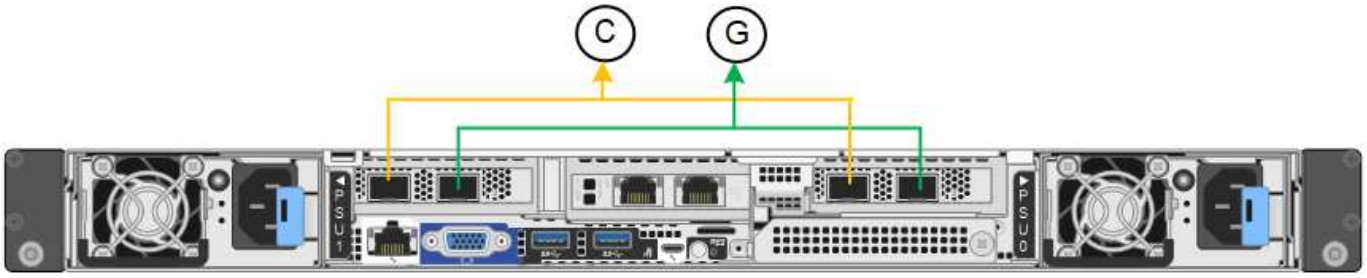
Quand "configuration des liens réseau" Pour l'appliance SGF6112, vous pouvez utiliser la liaison de port pour les ports qui se connectent au réseau Grid et au réseau client en option, ainsi que les ports de gestion 1/10-GbE qui se connectent au réseau Admin en option. La liaison de ports contribue à protéger vos données en fournissant des chemins redondants entre les réseaux StorageGRID et l'appliance.

Modes de liaison réseau

Les ports réseau de l'appliance prennent en charge le mode de liaison de port fixe ou le mode de liaison de port agrégé pour les connexions réseau Grid et réseau client.

Mode de liaison de port fixe

Le mode de liaison de port fixe est la configuration par défaut des ports réseau.



Légende	Quels ports sont liés
C	Les ports 1 et 3 sont liés ensemble pour le réseau client, si ce réseau est utilisé.

Légende	Quels ports sont liés
G	Les ports 2 et 4 sont liés ensemble pour le réseau de grille.

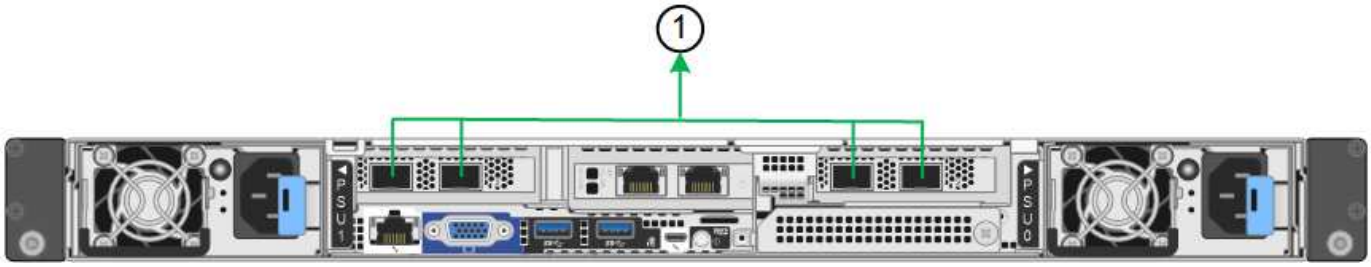
Lors de l'utilisation du mode de liaison de port fixe, les ports peuvent être liés en mode de sauvegarde active ou en mode de protocole de contrôle d'agrégation de liens (LACP 802.3ad).

- En mode de sauvegarde active (valeur par défaut), un seul port est actif à la fois. Si le port actif tombe en panne, son port de sauvegarde fournit automatiquement une connexion de basculement. Le port 4 fournit un chemin de sauvegarde pour le port 2 (réseau Grid) et le port 3 fournit un chemin de sauvegarde pour le port 1 (réseau client).
- En mode LACP, chaque paire de ports forme un canal logique entre l'appliance et le réseau, ce qui permet un débit plus élevé. En cas de défaillance d'un port, l'autre port continue de fournir le canal. Le débit est réduit, mais la connectivité n'est pas affectée.

> Si vous n'avez pas besoin de connexions redondantes, vous ne pouvez utiliser qu'un seul port pour chaque réseau. Cependant, n'oubliez pas que l'alerte **liaison de l'appliance de stockage en panne** peut être déclenchée dans le Gestionnaire de grille après l'installation de StorageGRID, indiquant qu'un câble est débranché. Vous pouvez désactiver cette règle d'alerte en toute sécurité.

Mode de liaison du port agrégé

Le mode de liaison de port agrégé augmente considérablement le débit de chaque réseau StorageGRID et fournit des chemins de basculement supplémentaires.



Légende	Quels ports sont liés
1	Tous les ports connectés sont regroupés en une seule liaison LACP, ce qui permet d'utiliser tous les ports pour le trafic Grid Network et client Network.

Si vous prévoyez d'utiliser le mode de liaison du port agrégé :

- Vous devez utiliser le mode lien réseau LACP.
- Vous devez spécifier une balise VLAN unique pour chaque réseau. Cette balise VLAN sera ajoutée à chaque paquet réseau pour s'assurer que le trafic réseau est acheminé vers le réseau approprié.
- Les ports doivent être connectés aux switchs capables de prendre en charge VLAN et LACP. Si plusieurs commutateurs participent au lien LACP, les switchs doivent prendre en charge les groupes d'agrégation de liens multi-châssis (MLAG), ou un équivalent.
- Vous savez comment configurer les commutateurs pour utiliser VLAN, LACP et MLAG, ou équivalent.

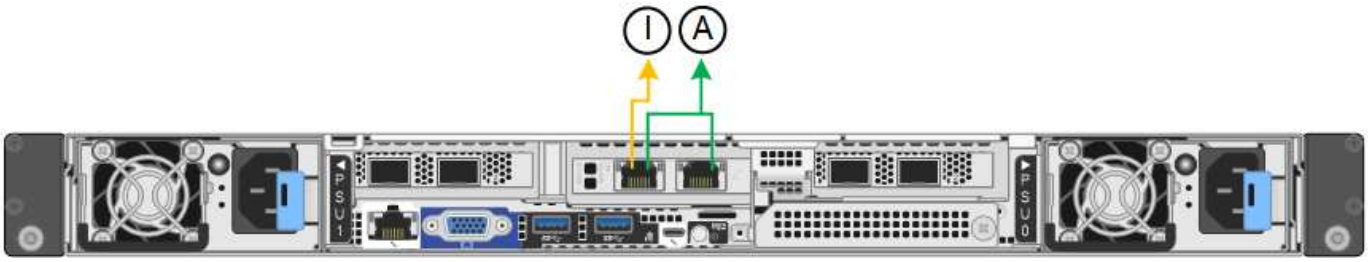
Si vous ne souhaitez pas utiliser les quatre ports, vous pouvez utiliser un, deux ou trois ports. L'utilisation de

plusieurs ports permet d'optimiser la possibilité qu'une certaine connectivité réseau reste disponible en cas de défaillance de l'un des ports.

> Si vous choisissez d'utiliser moins de quatre ports réseau, sachez qu'une alerte **Services Appliance LINK Down** peut être déclenchée dans Grid Manager après l'installation du nœud de l'appliance, ce qui indique qu'un câble est débranché. Vous pouvez désactiver cette règle d'alerte en toute sécurité pour l'alerte déclenchée.

Modes de liaison réseau pour les ports de gestion

Pour les deux ports de gestion 1/10-GbE, vous pouvez choisir le mode de liaison réseau indépendant ou le mode de liaison réseau Active-Backup pour vous connecter au réseau d'administration facultatif.



En mode indépendant, seul le port de gestion de gauche est connecté au réseau Admin. Ce mode ne fournit pas de chemin redondant. Le port de gestion sur la droite est déconnecté et disponible pour les connexions locales temporaires (utilise l'adresse IP 169.254.0.1).

En mode sauvegarde active, les deux ports de gestion sont connectés au réseau Admin. Un seul port est actif à la fois. Si le port actif tombe en panne, son port de sauvegarde fournit automatiquement une connexion de basculement. Le fait de lier ces deux ports physiques à un port de gestion logique fournit un chemin redondant au réseau Admin.

> Si vous devez établir une connexion locale temporaire à l'appliance lorsque les ports de gestion 1/10-GbE sont configurés pour le mode Active-Backup, débranchez les câbles des deux ports de gestion, branchez votre câble temporaire dans le port de gestion situé à droite et accédez au dispositif à l'aide de l'adresse IP 169.254.0.1.

Légende	Mode de liaison réseau
A	Mode de sauvegarde active/active. Les deux ports de gestion sont liés à un port de gestion logique connecté au réseau d'administration.
JE	Mode indépendant. Le port de gauche est connecté au réseau Admin. Le port de droite est disponible pour les connexions locales temporaires (adresse IP 169.254.0.1).

Modes de liaison du port (contrôleur SG6000-CN)

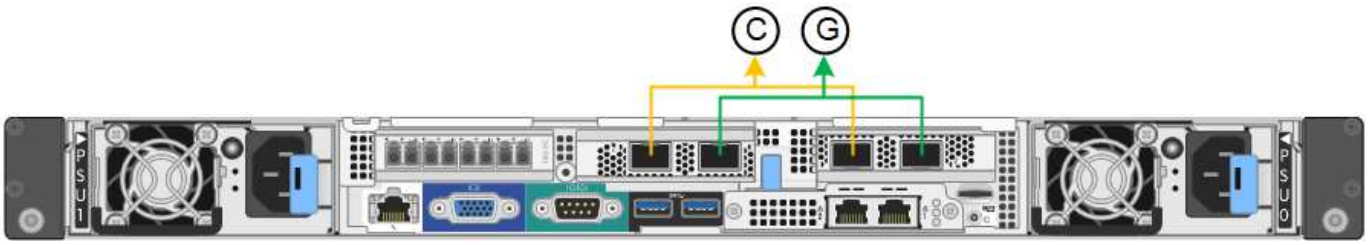
Quand "configuration des liens réseau" Pour le contrôleur SG6000-CN, vous pouvez utiliser la liaison de port pour les ports 10/25-GbE qui se connectent au réseau Grid et au réseau client en option, ainsi que les ports de gestion 1-GbE qui se connectent au réseau Admin en option. La liaison de ports contribue à protéger vos données en fournissant des chemins redondants entre les réseaux StorageGRID et l'appliance.

Modes de liaison réseau pour les ports 10/25 GbE

Les ports réseau 10/25-GbE du contrôleur SG6000-CN prennent en charge le mode de liaison de port fixe ou le mode de liaison de port agrégé pour les connexions réseau Grid et réseau client.

Mode de liaison de port fixe

Le mode fixe est la configuration par défaut pour les ports réseau 10/25 GbE.



Légende	Quels ports sont liés
C	Les ports 1 et 3 sont liés ensemble pour le réseau client, si ce réseau est utilisé.
G	Les ports 2 et 4 sont liés ensemble pour le réseau de grille.

Lors de l'utilisation du mode de liaison de port fixe, les ports peuvent être liés en mode de sauvegarde active ou en mode de protocole de contrôle d'agrégation de liens (LACP 802.3ad).

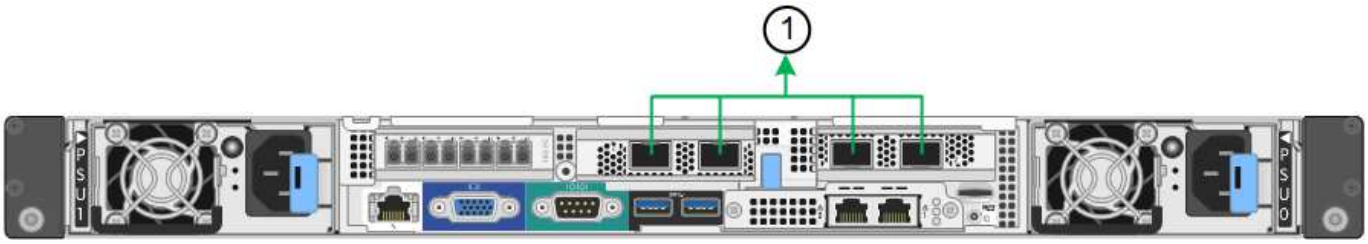
- En mode de sauvegarde active (valeur par défaut), un seul port est actif à la fois. Si le port actif tombe en panne, son port de sauvegarde fournit automatiquement une connexion de basculement. Le port 4 fournit un chemin de sauvegarde pour le port 2 (réseau Grid) et le port 3 fournit un chemin de sauvegarde pour le port 1 (réseau client).
- En mode LACP, chaque paire de ports forme un canal logique entre le contrôleur et le réseau, ce qui permet d'augmenter le débit. En cas de défaillance d'un port, l'autre port continue de fournir le canal. Le débit est réduit, mais la connectivité n'est pas affectée.

> Si vous n'avez pas besoin de connexions redondantes, vous ne pouvez utiliser qu'un seul port pour chaque réseau. Notez cependant qu'une alerte sera déclenchée dans le Grid Manager une fois que StorageGRID a été installé, ce qui indique qu'un lien ne fonctionne pas. Comme ce port est déconnecté à cet effet, vous pouvez désactiver cette alerte en toute sécurité.

Dans le Gestionnaire de grille, sélectionnez **alerte** > **règles**, sélectionnez la règle et cliquez sur **Modifier règle**. Décochez ensuite la case **activé**.

Mode de liaison du port agrégé

Le mode de liaison de port agrégé étend considérablement l'ensemble de chaque réseau StorageGRID et fournit des chemins de basculement supplémentaires.



Légende	Quels ports sont liés
1	Tous les ports connectés sont regroupés en une seule liaison LACP, ce qui permet d'utiliser tous les ports pour le trafic Grid Network et client Network.

Si vous prévoyez d'utiliser le mode de liaison du port agrégé :

- Vous devez utiliser le mode lien réseau LACP.
- Vous devez spécifier une balise VLAN unique pour chaque réseau. Cette balise VLAN sera ajoutée à chaque paquet réseau pour s'assurer que le trafic réseau est acheminé vers le réseau approprié.
- Les ports doivent être connectés aux switchs capables de prendre en charge VLAN et LACP. Si plusieurs commutateurs participent au lien LACP, les switchs doivent prendre en charge les groupes d'agrégation de liens multi-châssis (MLAG), ou un équivalent.
- Vous savez comment configurer les commutateurs pour utiliser VLAN, LACP et MLAG, ou équivalent.

Si vous ne souhaitez pas utiliser les quatre ports 10/25-GbE, vous pouvez utiliser un, deux ou trois ports. L'utilisation de plusieurs ports permet de maximiser la possibilité qu'une certaine connectivité réseau reste disponible en cas de défaillance de l'un des ports 10/25 GbE.

> Si vous choisissez d'utiliser moins de quatre ports, sachez qu'une ou plusieurs alarmes seront déclenchées dans le Gestionnaire de grille après l'installation de StorageGRID, ce qui indique que les câbles sont débranchés. Vous pouvez accuser réception des alarmes en toute sécurité pour les effacer.

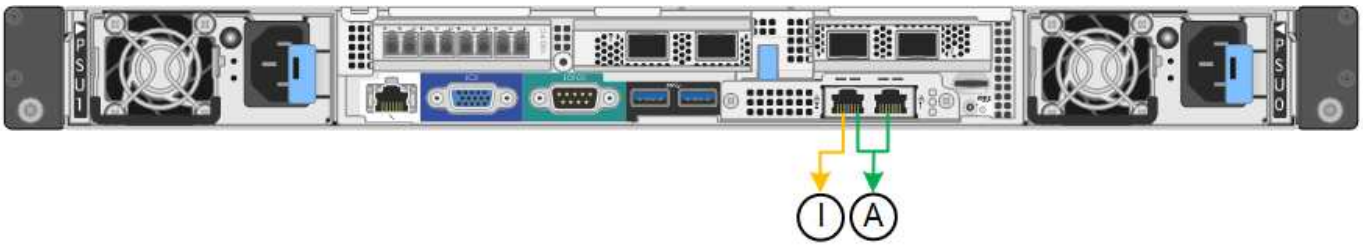
Modes de liaison réseau pour les ports de gestion 1 GbE

Pour les deux ports de gestion 1 GbE du contrôleur SG6000-CN, vous pouvez choisir le mode de liaison réseau indépendant ou le mode de liaison réseau Active-Backup pour vous connecter au réseau d'administration facultatif.

En mode indépendant, seul le port de gestion de gauche est connecté au réseau Admin. Ce mode ne fournit pas de chemin redondant. Le port de gestion de droite n'est pas connecté et disponible pour les connexions locales temporaires (utilise l'adresse IP 169.254.0.1)

En mode sauvegarde active, les deux ports de gestion sont connectés au réseau Admin. Un seul port est actif à la fois. Si le port actif tombe en panne, son port de sauvegarde fournit automatiquement une connexion de basculement. Le fait de lier ces deux ports physiques à un port de gestion logique fournit un chemin redondant au réseau Admin.

> Si vous devez établir une connexion locale temporaire au contrôleur SG6000-CN lorsque les ports de gestion 1 GbE sont configurés pour le mode sauvegarde active, retirez les câbles des deux ports de gestion, branchez votre câble temporaire dans le port de gestion de droite et accédez à l'appliance via l'adresse IP 169.254.0.1.



Légende	Mode de liaison réseau
A	Les deux ports de gestion sont liés à un port de gestion logique connecté au réseau d'administration.
JE	Le port de gauche est connecté au réseau Admin. Le port de droite est disponible pour les connexions locales temporaires (adresse IP 169.254.0.1).

Modes de liaison des ports (contrôleur E5700SG)

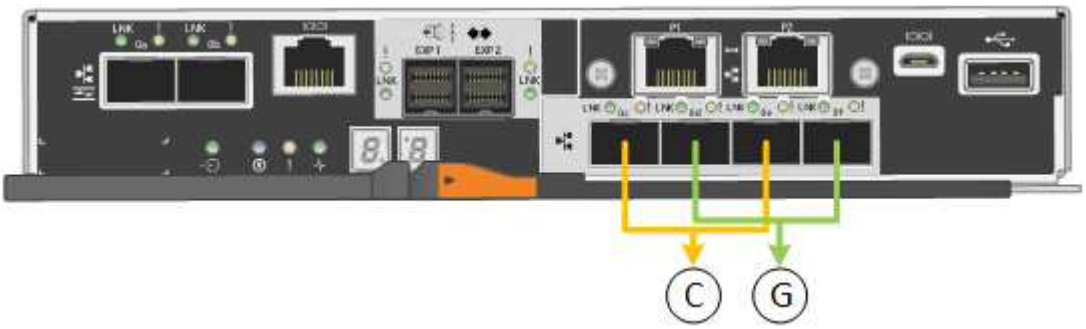
Quand "configuration des liens réseau" Pour le contrôleur E5700SG, vous pouvez utiliser la liaison de port pour les ports 10/25-GbE qui se connectent au réseau Grid et au réseau client en option, ainsi que les ports de gestion 1-GbE qui se connectent au réseau d'administration en option. La liaison de ports contribue à protéger vos données en fournissant des chemins redondants entre les réseaux StorageGRID et l'appliance.

Modes de liaison réseau pour les ports 10/25 GbE

Les ports réseau 10/25-GbE du contrôleur E5700SG prennent en charge le mode de liaison de port fixe ou le mode de liaison de port agrégé pour les connexions réseau Grid et réseau client.

Mode de liaison de port fixe

Le mode fixe est la configuration par défaut pour les ports réseau 10/25 GbE.



Légende	Quels ports sont liés
C	Les ports 1 et 3 sont liés ensemble pour le réseau client, si ce réseau est utilisé.
G	Les ports 2 et 4 sont liés ensemble pour le réseau de grille.

Si vous utilisez le mode liaison de port fixe, vous pouvez utiliser l'un des deux modes de liaison réseau :

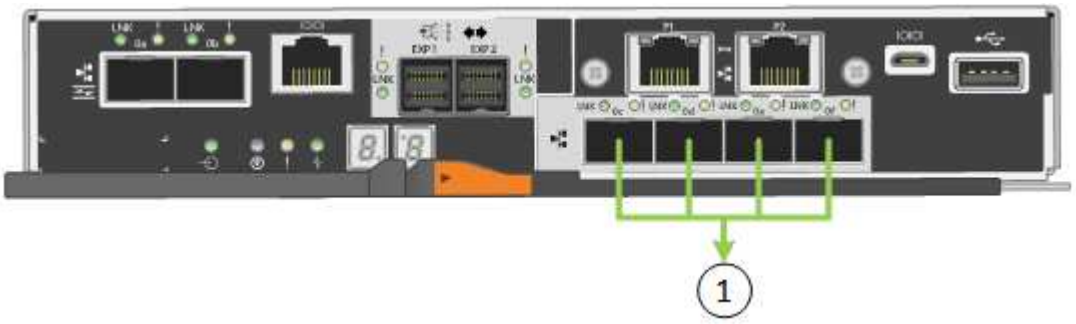
active-Backup ou Link Aggregation Control Protocol (LACP).

- En mode sauvegarde active (par défaut), un seul port est actif à la fois. Si le port actif tombe en panne, son port de sauvegarde fournit automatiquement une connexion de basculement. Le port 4 fournit un chemin de sauvegarde pour le port 2 (réseau Grid) et le port 3 fournit un chemin de sauvegarde pour le port 1 (réseau client).
- En mode LACP, chaque paire de ports forme un canal logique entre le contrôleur et le réseau, ce qui permet d'augmenter le débit. En cas de défaillance d'un port, l'autre port continue de fournir le canal. Le débit est réduit, mais la connectivité n'est pas affectée.

> Si vous n'avez pas besoin de connexions redondantes, vous ne pouvez utiliser qu'un seul port pour chaque réseau. Notez cependant qu'une alarme est déclenchée dans le Gestionnaire de grille après l'installation de StorageGRID, ce qui indique qu'un câble est débranché. Vous pouvez accuser réception de cette alarme en toute sécurité pour l'effacer.

Mode de liaison du port agrégé

Le mode de liaison de port agrégé étend considérablement l'ensemble de chaque réseau StorageGRID et fournit des chemins de basculement supplémentaires.



Légende	Quels ports sont liés
1	Tous les ports connectés sont regroupés en une seule liaison LACP, ce qui permet d'utiliser tous les ports pour le trafic Grid Network et client Network.

Si vous prévoyez d'utiliser le mode de liaison du port agrégé :

- Vous devez utiliser le mode lien réseau LACP.
- Vous devez spécifier une balise VLAN unique pour chaque réseau. Cette balise VLAN sera ajoutée à chaque paquet réseau pour s'assurer que le trafic réseau est acheminé vers le réseau approprié.
- Les ports doivent être connectés aux switchs capables de prendre en charge VLAN et LACP. Si plusieurs commutateurs participent au lien LACP, les switchs doivent prendre en charge les groupes d'agrégation de liens multi-châssis (MLAG), ou un équivalent.
- Vous savez comment configurer les commutateurs pour utiliser VLAN, LACP et MLAG, ou équivalent.

Si vous ne souhaitez pas utiliser les quatre ports 10/25-GbE, vous pouvez utiliser un, deux ou trois ports. L'utilisation de plusieurs ports permet de maximiser la possibilité qu'une certaine connectivité réseau reste disponible en cas de défaillance de l'un des ports 10/25 GbE.

Si vous choisissez d'utiliser moins de quatre ports, sachez qu'une ou plusieurs alarmes seront déclenchées dans le Gestionnaire de grille après l'installation de StorageGRID, ce qui indique que les câbles sont débranchés. Vous pouvez accuser réception des alarmes en toute sécurité pour les effacer.

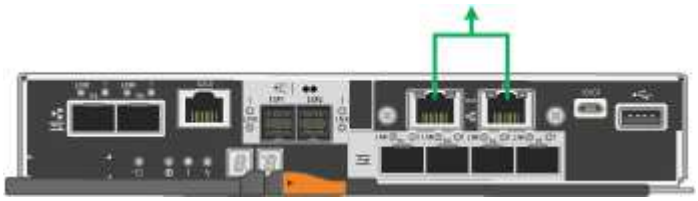
Modes de liaison réseau pour les ports de gestion 1 GbE

Pour les deux ports de gestion 1 GbE du contrôleur E5700SG, vous pouvez choisir le mode de liaison réseau indépendant ou le mode de liaison réseau Active-Backup pour vous connecter au réseau d'administration facultatif.

En mode indépendant, seul le port de gestion 1 est connecté au réseau d'administration. Ce mode ne fournit pas de chemin redondant. Le port de gestion 2 est laissé non câblé et disponible pour les connexions locales temporaires (utilisez l'adresse IP 169.254.0.1)

En mode sauvegarde active, les ports de gestion 1 et 2 sont connectés au réseau Admin. Un seul port est actif à la fois. Si le port actif tombe en panne, son port de sauvegarde fournit automatiquement une connexion de basculement. Le fait de lier ces deux ports physiques à un port de gestion logique fournit un chemin redondant au réseau Admin.

Si vous devez établir une connexion locale temporaire au contrôleur E5700SG lorsque les ports de gestion 1 GbE sont configurés pour le mode sauvegarde active/active, retirez les câbles des deux ports de gestion, branchez votre câble temporaire sur le port de gestion 2 et accédez à l'appliance via l'adresse IP 169.254.0.1.



Modes de liaison de port (SG100 et SG1000)

Lors de la configuration de liaisons réseau pour les appliances SG100 et SG1000, vous pouvez utiliser la liaison de port pour les ports qui se connectent au réseau de grille et au réseau client en option, ainsi que les ports de gestion 1 GbE qui se connectent au réseau d'administration en option. La liaison de ports contribue à protéger vos données en fournissant des chemins redondants entre les réseaux StorageGRID et l'appliance.

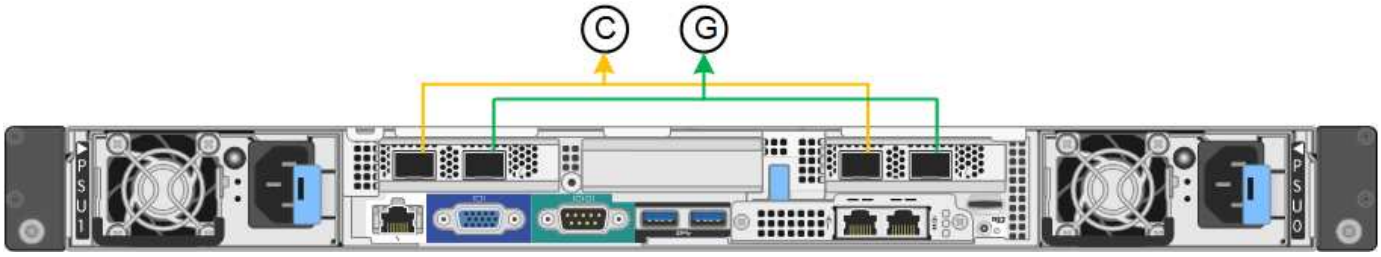
Modes de liaison réseau

Les ports réseau de l'appliance de services prennent en charge le mode de liaison de port fixe ou le mode de liaison de port agrégé pour les connexions réseau Grid et réseau client.

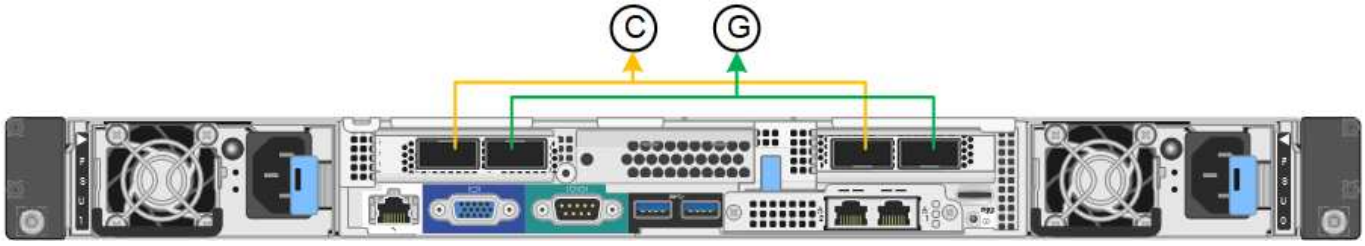
Mode de liaison de port fixe

Le mode de liaison de port fixe est la configuration par défaut des ports réseau. Les figures montrent comment les ports réseau du SG1000 ou du SG100 sont liés en mode de liaison port fixe.

SG100 :



SG1000 :



Légende	Quels ports sont liés
C	Les ports 1 et 3 sont liés ensemble pour le réseau client, si ce réseau est utilisé.
G	Les ports 2 et 4 sont liés ensemble pour le réseau de grille.

Lors de l'utilisation du mode de liaison de port fixe, les ports peuvent être liés en mode de sauvegarde active ou en mode de protocole de contrôle d'agrégation de liens (LACP 802.3ad).

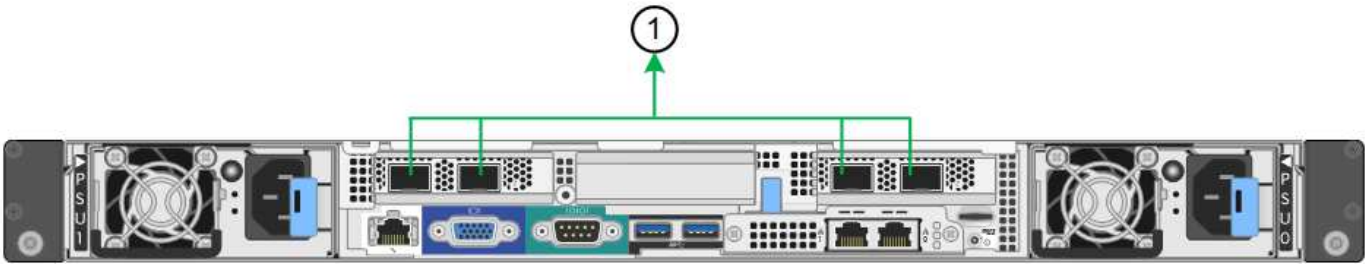
- En mode de sauvegarde active (valeur par défaut), un seul port est actif à la fois. Si le port actif tombe en panne, son port de sauvegarde fournit automatiquement une connexion de basculement. Le port 4 fournit un chemin de sauvegarde pour le port 2 (réseau Grid) et le port 3 fournit un chemin de sauvegarde pour le port 1 (réseau client).
- En mode LACP, chaque paire de ports forme un canal logique entre l'appliance de services et le réseau, ce qui permet d'augmenter le débit. En cas de défaillance d'un port, l'autre port continue de fournir le canal. Le débit est réduit, mais la connectivité n'est pas affectée.

> Si vous n'avez pas besoin de connexions redondantes, vous ne pouvez utiliser qu'un seul port pour chaque réseau. Cependant, n'oubliez pas que l'alerte **Services Appliance LINK** peut être déclenchée dans le Gestionnaire de grille après l'installation de StorageGRID, ce qui indique qu'un câble est débranché. Vous pouvez désactiver cette règle d'alerte en toute sécurité.

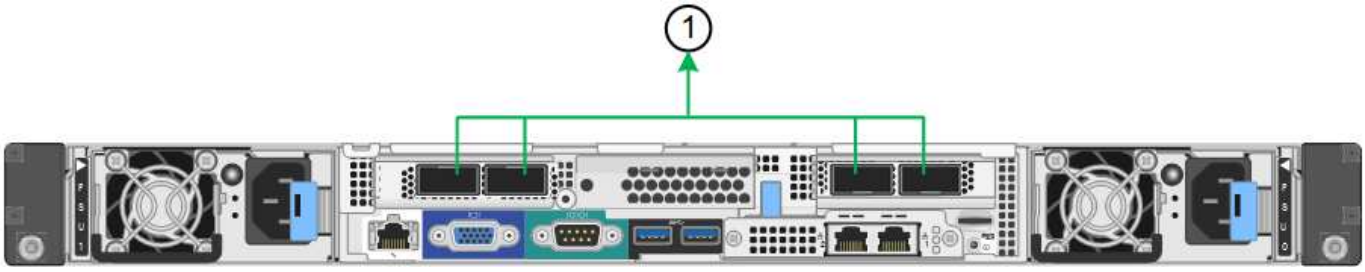
Mode de liaison du port agrégé

Le mode de liaison de port agrégé augmente considérablement le débit de chaque réseau StorageGRID et fournit des chemins de basculement supplémentaires. Ces figures montrent comment les ports réseau sont liés en mode agrégation port bond.

SG100 :



SG1000 :



Légende	Quels ports sont liés
1	Tous les ports connectés sont regroupés en une seule liaison LACP, ce qui permet d'utiliser tous les ports pour le trafic Grid Network et client Network.

Si vous prévoyez d'utiliser le mode de liaison du port agrégé :

- Vous devez utiliser le mode lien réseau LACP.
- Vous devez spécifier une balise VLAN unique pour chaque réseau. Cette balise VLAN sera ajoutée à chaque paquet réseau pour s'assurer que le trafic réseau est acheminé vers le réseau approprié.
- Les ports doivent être connectés aux switchs capables de prendre en charge VLAN et LACP. Si plusieurs commutateurs participent au lien LACP, les switchs doivent prendre en charge les groupes d'agrégation de liens multi-châssis (MLAG), ou un équivalent.
- Vous savez comment configurer les commutateurs pour utiliser VLAN, LACP et MLAG, ou équivalent.

Si vous ne souhaitez pas utiliser les quatre ports, vous pouvez utiliser un, deux ou trois ports. L'utilisation de plusieurs ports permet d'optimiser la possibilité qu'une certaine connectivité réseau reste disponible en cas de défaillance de l'un des ports.

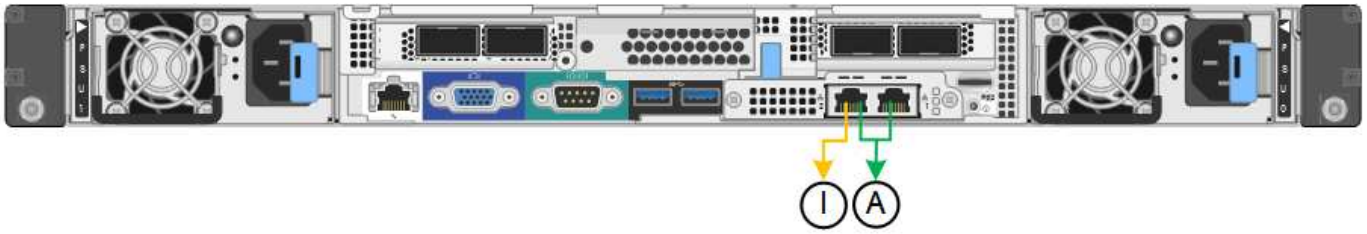
> Si vous choisissez d'utiliser moins de quatre ports réseau, sachez qu'une alerte **Services Appliance LINK Down** peut être déclenchée dans Grid Manager après l'installation du nœud de l'appliance, ce qui indique qu'un câble est débranché. Vous pouvez désactiver cette règle d'alerte en toute sécurité pour l'alerte déclenchée.

Modes de liaison réseau pour les ports de gestion

Pour les deux ports de gestion 1 GbE de l'appliance de services, vous pouvez choisir le mode de liaison réseau indépendante ou le mode de liaison réseau Active-Backup pour vous connecter au réseau d'administration facultatif. Ces figures montrent comment les ports de gestion des appliances sont liés en mode liaison réseau pour le réseau d'administration.

SG100 :

SG1000 :



Légende	Mode de liaison réseau
A	Mode de sauvegarde active/active. Les deux ports de gestion sont liés à un port de gestion logique connecté au réseau d'administration.
JE	Mode indépendant. Le port de gauche est connecté au réseau Admin. Le port de droite est disponible pour les connexions locales temporaires (adresse IP 169.254.0.1).

En mode indépendant, seul le port de gestion de gauche est connecté au réseau Admin. Ce mode ne fournit pas de chemin redondant. Le port de gestion de droite n'est pas connecté et disponible pour les connexions locales temporaires (utilise l'adresse IP 169.254.0.1)

En mode sauvegarde active, les deux ports de gestion sont connectés au réseau Admin. Un seul port est actif à la fois. Si le port actif tombe en panne, son port de sauvegarde fournit automatiquement une connexion de basculement. Le fait de lier ces deux ports physiques à un port de gestion logique fournit un chemin redondant au réseau Admin.

> Si vous devez établir une connexion locale temporaire avec l'appliance de services lorsque les ports de gestion 1 GbE sont configurés pour le mode sauvegarde active, retirez les câbles des deux ports de gestion, branchez votre câble temporaire sur le port de gestion de droite et accédez à l'appliance à l'aide de l'adresse IP 169.254.0.1.

Rassembler les informations d'installation

Collecte des informations d'installation : présentation

Lors de l'installation et de la configuration d'une appliance StorageGRID, vous prenez des décisions et collectez des informations sur les ports de commutation Ethernet, les adresses IP et les modes de liaison port et réseau.

Reportez-vous aux instructions de votre appareil pour déterminer les informations dont vous avez besoin :

- "SGF6112"

- "SG6000"
- "SG5700"
- "SG100 et SG1000"

Vous pouvez également travailler avec votre consultant en services professionnels NetApp afin d'utiliser l'outil ConfigBuilder de NetApp afin de rationaliser et d'automatiser les étapes de configuration. Voir "Automatisez l'installation et la configuration de l'appliance".

Collecte des informations d'installation (SGF6112)

À l'aide des tableaux suivants, notez les informations requises pour chaque réseau que vous connectez à l'appliance. Ces valeurs sont nécessaires pour installer et configurer le matériel.

> Au lieu d'utiliser les tableaux, utilisez le manuel fourni avec ConfigBuilder. Le manuel ConfigBuilder vous permet de télécharger les informations système et de générer un fichier JSON pour effectuer automatiquement certaines étapes de configuration dans le programme d'installation de l'appliance StorageGRID. Voir "Automatisez l'installation et la configuration de l'appliance".

Vérifiez la version de StorageGRID

Avant d'installer une appliance SGF6112, vérifiez que votre système StorageGRID utilise la version requise du logiciel StorageGRID.

Appliance	Version StorageGRID requise
SGF6112	11.7 ou version ultérieure (dernier correctif recommandé)

Ports d'administration et de maintenance

Le réseau d'administration pour StorageGRID est un réseau facultatif, utilisé pour l'administration et la maintenance du système. L'appliance se connecte au réseau d'administration à l'aide des ports suivants de l'appliance.

La figure suivante présente les ports RJ-45 de l'appliance SG6112.

Informations nécessaires	Votre valeur
Réseau admin activé	Choisir une option : • Non • Oui (par défaut)

Informations nécessaires	Votre valeur
Mode de liaison réseau	Choisir une option : • Indépendant (par défaut) • Sauvegarde active-Backup
Port de commutateur pour le port gauche entouré dans le schéma (port actif par défaut pour le mode de liaison réseau indépendante)	
Port de commutateur pour le port droit entouré dans le diagramme (mode de liaison réseau Active-Backup uniquement)	
Adresse MAC du port réseau d'administration **Remarque :** l'étiquette d'adresse MAC située à l'avant de l'appliance répertorie l'adresse MAC du port de gestion BMC. Pour déterminer l'adresse MAC du port réseau Admin, vous devez ajouter **2** au numéro hexadécimal sur l'étiquette. Par exemple, si l'adresse MAC de l'étiquette se termine par **09**, l'adresse MAC du port d'administration se terminera par **0B**. Si l'adresse MAC de l'étiquette se termine dans **(*y*)FF**, l'adresse MAC du port d'administration se terminera dans **(*y*+1)01**. Vous pouvez facilement effectuer ce calcul en ouvrant Calculator sous Windows, en le définissant en mode programmateur, en sélectionnant Hex, en saisissant l'adresse MAC, puis en tapant **+ 2 =**.	
Adresse IP attribuée par DHCP pour le port réseau d'administration, si disponible après la mise sous tension **Remarque :** vous pouvez déterminer l'adresse IP attribuée par DHCP en utilisant l'adresse MAC pour rechercher l'adresse IP attribuée.	• Adresse IPv4 (CIDR) : • Passerelle :
Adresse IP statique que vous envisagez d'utiliser pour le nœud d'appliance sur le réseau d'administration **Remarque :** si votre réseau n'a pas de passerelle, spécifiez la même adresse IPv4 statique pour la passerelle.	• Adresse IPv4 (CIDR) : • Passerelle :
Sous-réseaux du réseau d'administration (CIDR)	

Ports réseau

Les quatre ports réseau de l'appliance se connectent au réseau StorageGRID Grid et au réseau client en option.

Informations nécessaires	Votre valeur
Vitesse de liaison	Pour le SGF6112, choisissez l'une des options suivantes : • Auto (par défaut) • 10 GbE • 25 GbE
Mode de liaison du port	Choisir une option : • Fixe (par défaut) • Agrégat
Port de commutation pour le port 1 (réseau client pour mode fixe)	
Port de commutation pour le port 2 (réseau grille pour mode fixe)	
Port de commutation pour le port 3 (réseau client pour mode fixe)	
Port de commutation pour le port 4 (réseau Grid pour mode fixe)	

Ports réseau de la grille

Le réseau Grid Network pour StorageGRID est un réseau requis, utilisé pour l'ensemble du trafic StorageGRID interne. L'appliance se connecte au réseau Grid à l'aide des quatre ports réseau.

Informations nécessaires	Votre valeur
Mode de liaison réseau	Choisir une option : • Sauvegarde active/active (par défaut) • LACP (802.3ad)
Balisage VLAN activé	Choisir une option : • Non (par défaut) • Oui.
Balise VLAN (si le balisage VLAN est activé)	Entrez une valeur comprise entre 0 et 4095 :
Adresse IP attribuée par DHCP pour le réseau Grid, si disponible après la mise sous tension	• Adresse IPv4 (CIDR) : • Passerelle :

Informations nécessaires	Votre valeur
Adresse IP statique que vous prévoyez d'utiliser pour le nœud de l'appliance sur le réseau Grid **Remarque :** si votre réseau n'a pas de passerelle, spécifiez la même adresse IPv4 statique pour la passerelle.	• Adresse IPv4 (CIDR) : • Passerelle :
Sous-réseaux du réseau de grille (CIDR)	
Réglage de l'unité de transmission maximale (MTU) (facultatif). Vous pouvez utiliser la valeur par défaut 1500 ou définir la valeur MTU sur une valeur adaptée aux trames jumbo, par exemple 9000.	

Ports réseau client

Le réseau client pour StorageGRID est un réseau facultatif, généralement utilisé pour fournir l'accès du protocole client à la grille. Le serveur se connecte au réseau client à l'aide des quatre ports réseau.

Informations nécessaires	Votre valeur
Réseau client activé	Choisir une option : • Non (par défaut) • Oui.
Mode de liaison réseau	Choisir une option : • Sauvegarde active/active (par défaut) • LACP (802.3ad)
Balisage VLAN activé	Choisir une option : • Non (par défaut) • Oui.
Balise VLAN (si le marquage VLAN est activé)	Entrez une valeur comprise entre 0 et 4095 :
Adresse IP attribuée par DHCP pour le réseau client, si disponible après la mise sous tension	• Adresse IPv4 (CIDR) : • Passerelle :
Adresse IP statique que vous prévoyez d'utiliser pour le nœud de l'appliance sur le réseau client **Remarque :** si le réseau client est activé, la route par défaut du serveur utilise la passerelle indiquée ici.	• Adresse IPv4 (CIDR) : • Passerelle :

Ports réseau de gestion BMC

Vous pouvez accéder à l'interface BMC sur l'appliance à l'aide du port de gestion 1 GbE entouré dans le schéma. Ce port prend en charge la gestion à distance du matériel du contrôleur via Ethernet en utilisant la norme IPMI (Intelligent Platform Management interface).

> Vous pouvez activer ou désactiver l'accès IPMI à distance pour tous les dispositifs contenant un contrôleur BMC en utilisant le point de terminaison privé de l'API de gestion, PUT /private/bmc.

La figure suivante présente le port de gestion BMC sur l'appliance SG6112.

Informations nécessaires	Votre valeur
Port de commutateur Ethernet vous vous connectez au port de gestion du contrôleur BMC (encerclé dans le diagramme)	
Adresse IP attribuée par DHCP pour le réseau de gestion BMC, si disponible après la mise sous tension	• Adresse IPv4 (CIDR) : • Passerelle :
Adresse IP statique que vous prévoyez d'utiliser pour le port de gestion BMC	• Adresse IPv4 (CIDR) : • Passerelle :

Informations associées

- "Cable appliance (SGF6112)"
- "Configurez les adresses IP StorageGRID"

Collecte des informations d'installation (SG6000)

À l'aide des tableaux, notez les informations requises pour chaque réseau que vous connectez à l'appliance. Ces valeurs sont nécessaires pour installer et configurer le matériel.

> Au lieu d'utiliser les tableaux, utilisez le manuel fourni avec ConfigBuilder. Le manuel ConfigBuilder vous permet de télécharger les informations système et de générer un fichier JSON pour effectuer automatiquement certaines étapes de configuration dans le programme d'installation de l'appliance StorageGRID. Voir "Automatisez l'installation et la configuration de l'appliance".

Informations nécessaires pour la connexion à SANtricity System Manager sur les contrôleurs de stockage

Vous connectez les deux contrôleurs de stockage de l'appliance (les contrôleurs E2800 Series ou EF570) au réseau de gestion que vous utiliserez pour SANtricity System Manager. Les contrôleurs sont situés sur chaque appliance comme suit :

- SG6060 et SG6060X : le contrôleur A se trouve en haut et le contrôleur B en bas.
- SGF6024 : le contrôleur A est sur la gauche et le contrôleur B sur la droite.

Informations nécessaires	Valeur pour le contrôleur A	Valeur pour le contrôleur B
Port de commutateur Ethernet que vous allez connecter au port de gestion 1 (nommé P1 sur le contrôleur)		
Adresse MAC pour le port de gestion 1 (imprimée sur une étiquette près du port P1)		
Adresse IP attribuée par DHCP pour le port de gestion 1, si disponible après la mise sous tension **Remarque :** si le réseau auquel vous vous connectez au contrôleur de stockage comporte un serveur DHCP, l'administrateur réseau peut utiliser l'adresse MAC pour déterminer l'adresse IP attribuée par le serveur DHCP.		
Adresse IP statique que vous prévoyez d'utiliser pour l'appliance sur le réseau de gestion	Pour IPv4 : • Adresse IPv4 : • Masque de sous-réseau : • Passerelle : Pour IPv6 : • Adresse IPv6 : • Adresse IP routable : • Adresse IP du routeur du contrôleur de stockage :	Pour IPv4 : • Adresse IPv4 : • Masque de sous-réseau : • Passerelle : Pour IPv6 : • Adresse IPv6 : • Adresse IP routable : • Adresse IP du routeur du contrôleur de stockage :
Format d'adresse IP	Choisir une option : • IPv4 • IPv6	Choisir une option : • IPv4 • IPv6
Vitesse et mode duplex **Remarque :** vous devez vous assurer que le commutateur Ethernet du réseau de gestion SANtricity System Manager est défini sur négociation automatique.	Doit être : • Négociation automatique (par défaut)	Doit être : • Négociation automatique (par défaut)

Informations nécessaires pour connecter le contrôleur SG6000-CN au réseau Admin

Le réseau d'administration pour StorageGRID est un réseau facultatif, utilisé pour l'administration et la maintenance du système. Le dispositif se connecte au réseau d'administration à l'aide des ports de gestion 1 GbE suivants sur le contrôleur SG6000-CN.

Informations nécessaires	Votre valeur
Réseau admin activé	Choisir une option : • Non • Oui (par défaut)
Mode de liaison réseau	Choisir une option : • Indépendant (par défaut) • Sauvegarde active-Backup
Port de commutation pour le port gauche dans le cercle rouge du schéma (port actif par défaut pour le mode de liaison réseau indépendante)	
Port de commutateur pour le port droit dans le cercle rouge du schéma (mode liaison réseau Active-Backup uniquement)	
Adresse MAC du port réseau d'administration **Remarque :** l'étiquette d'adresse MAC située à l'avant du contrôleur SG6000-CN répertorie l'adresse MAC du port de gestion BMC. Pour déterminer l'adresse MAC du port réseau Admin, vous devez ajouter **2** au numéro hexadécimal sur l'étiquette. Par exemple, si l'adresse MAC de l'étiquette se termine par **09**, l'adresse MAC du port d'administration se terminera par **0B**. Si l'adresse MAC de l'étiquette se termine dans **(*y*)FF**, l'adresse MAC du port d'administration se terminera dans **(*y*+1)01**. Vous pouvez facilement effectuer ce calcul en ouvrant Calculator sous Windows, en le définissant en mode programmateur, en sélectionnant Hex, en saisissant l'adresse MAC, puis en tapant **+ 2 =**.	
Adresse IP attribuée par DHCP pour le port réseau d'administration, si disponible après la mise sous tension **Remarque :** vous pouvez déterminer l'adresse IP attribuée par DHCP en utilisant l'adresse MAC pour rechercher l'adresse IP attribuée.	• Adresse IPv4 (CIDR) : • Passerelle :

Informations nécessaires	Votre valeur
Adresse IP statique que vous envisagez d'utiliser pour le nœud de stockage de l'appliance sur le réseau d'administration **Remarque :** si votre réseau n'a pas de passerelle, spécifiez la même adresse IPv4 statique pour la passerelle.	• Adresse IPv4 (CIDR) : • Passerelle :
Sous-réseaux du réseau d'administration (CIDR)	

Informations nécessaires pour connecter et configurer les ports 10/25 GbE sur le contrôleur SG6000-CN

Les quatre ports 10/25 GbE du contrôleur SG6000-CN se connectent au réseau de réseau StorageGRID et au réseau client en option.

Informations nécessaires	Votre valeur
Vitesse de liaison	Choisir une option : • Auto (par défaut) • 10 GbE • 25 GbE
Mode de liaison du port	Choisir une option : • Fixe (par défaut) • Agrégat
Port de commutation pour le port 1 (réseau client pour mode fixe)	
Port de commutation pour le port 2 (réseau grille pour mode fixe)	
Port de commutation pour le port 3 (réseau client pour mode fixe)	
Port de commutation pour le port 4 (réseau Grid pour mode fixe)	

Informations nécessaires pour connecter le contrôleur SG6000-CN au réseau Grid

Le réseau Grid Network pour StorageGRID est un réseau requis, utilisé pour l'ensemble du trafic StorageGRID interne. L'appareil se connecte au réseau Grid à l'aide des ports 10/25 GbE du contrôleur SG6000-CN.

Informations nécessaires	Votre valeur
Mode de liaison réseau	Choisir une option : • Sauvegarde active/active (par défaut) • LACP (802.3ad)
Balisage VLAN activé	Choisir une option : • Non (par défaut) • Oui.
Balise VLAN (si le marquage VLAN est activé)	Entrez une valeur comprise entre 0 et 4095 :
Adresse IP attribuée par DHCP pour le réseau Grid, si disponible après la mise sous tension	• Adresse IPv4 (CIDR) : • Passerelle :
Adresse IP statique que vous prévoyez d'utiliser pour le noeud de stockage de l'appliance sur le réseau Grid **Remarque :** si votre réseau n'a pas de passerelle, spécifiez la même adresse IPv4 statique pour la passerelle.	• Adresse IPv4 (CIDR) : • Passerelle :
Sous-réseaux du réseau de grille (CIDR)	

Informations nécessaires pour connecter le contrôleur SG6000-CN au réseau client

Le réseau client pour StorageGRID est un réseau facultatif, généralement utilisé pour fournir l'accès du protocole client à la grille. L'appliance se connecte au réseau client à l'aide des ports 10/25 GbE du contrôleur SG6000-CN.

Informations nécessaires	Votre valeur
Réseau client activé	Choisir une option : • Non (par défaut) • Oui.
Mode de liaison réseau	Choisir une option : • Sauvegarde active/active (par défaut) • LACP (802.3ad)

Informations nécessaires	Votre valeur
Balisage VLAN activé	Choisir une option : • Non (par défaut) • Oui.
Balise VLAN (si le marquage VLAN est activé)	Entrez une valeur comprise entre 0 et 4095 :
Adresse IP attribuée par DHCP pour le réseau client, si disponible après la mise sous tension	• Adresse IPv4 (CIDR) : • Passerelle :
Adresse IP statique que vous prévoyez d'utiliser pour le noeud de stockage de l'appliance sur le réseau client **Remarque :** si le réseau client est activé, la route par défaut du contrôleur utilisera la passerelle indiquée ici.	• Adresse IPv4 (CIDR) : • Passerelle :

Informations nécessaires pour connecter le contrôleur SG6000-CN au réseau de gestion BMC

Vous pouvez accéder à l'interface BMC sur le contrôleur SG6000-CN à l'aide du port de gestion 1 GbE suivant. Ce port prend en charge la gestion à distance du matériel du contrôleur via Ethernet en utilisant la norme IPMI (Intelligent Platform Management interface).

Vous pouvez activer ou désactiver l'accès IPMI à distance pour tous les dispositifs contenant un contrôleur BMC en utilisant le point de terminaison privé de l'API de gestion, PUT /private/bmc.

Informations nécessaires	Votre valeur
Port de commutateur Ethernet vous vous connectez au port de gestion du contrôleur BMC (encerclé dans le diagramme)	
Adresse IP attribuée par DHCP pour le réseau de gestion BMC, si disponible après la mise sous tension	• Adresse IPv4 (CIDR) : • Passerelle :
Adresse IP statique que vous prévoyez d'utiliser pour le port de gestion BMC	• Adresse IPv4 (CIDR) : • Passerelle :

Informations associées

- "Contrôleurs SG6000"
- "Vérifiez les connexions réseau de l'appliance"

- "Modes de liaison du port (contrôleur SG6000-CN)"
- "Cable appliance (SG6000)"
- "Configurez les adresses IP StorageGRID"

Collecte d'informations sur l'installation (SG5700)

À l'aide des tableaux, notez les informations requises pour chaque réseau que vous connectez à l'appliance. Ces valeurs sont nécessaires pour installer et configurer le matériel.

> Au lieu d'utiliser les tableaux, utilisez le manuel fourni avec ConfigBuilder. Le manuel ConfigBuilder vous permet de télécharger les informations système et de générer un fichier JSON pour effectuer automatiquement certaines étapes de configuration dans le programme d'installation de l'appliance StorageGRID. Voir "Automatisez l'installation et la configuration de l'appliance".

Informations nécessaires pour la connexion à SANtricity System Manager sur le contrôleur E2800

Vous connectez le contrôleur E2800 Series au réseau de gestion que vous utiliserez pour SANtricity System Manager.

Informations nécessaires	Votre valeur
Port de commutateur Ethernet vous connectez au port de gestion 1	
Adresse MAC pour le port de gestion 1 (imprimée sur une étiquette près du port P1)	
Adresse IP attribuée par DHCP pour le port de gestion 1, si disponible après la mise sous tension **Remarque :** si le réseau auquel vous vous connectez au contrôleur E2800 comporte un serveur DHCP, l'administrateur réseau peut utiliser l'adresse MAC pour déterminer l'adresse IP attribuée par le serveur DHCP.	
Vitesse et mode duplex **Remarque :** vous devez vous assurer que le commutateur Ethernet du réseau de gestion SANtricity System Manager est défini sur négociation automatique.	Doit être : • Négociation automatique (par défaut)
Format d'adresse IP	Choisir une option : • IPv4 • IPv6

Informations nécessaires	Votre valeur
Adresse IP statique que vous prévoyez d'utiliser pour l'appliance sur le réseau de gestion	Pour IPv4 : • Adresse IPv4 : • Masque de sous-réseau : • Passerelle : Pour IPv6 : • Adresse IPv6 : • Adresse IP routable : • Adresse IP du routeur du contrôleur E2800 :

Informations nécessaires pour connecter le contrôleur E5700SG au réseau Admin

Le réseau d'administration pour StorageGRID est un réseau facultatif, utilisé pour l'administration et la maintenance du système. Le dispositif se connecte au réseau d'administration via les ports de gestion 1 GbE du contrôleur E5700SG.

Informations nécessaires	Votre valeur
Réseau admin activé	Choisir une option : • Non • Oui (par défaut)
Mode de liaison réseau	Choisir une option : • Indépendant • Sauvegarde active-Backup
Port de commutation pour le port 1	
Port de commutation pour le port 2 (mode de liaison réseau Active-Backup uniquement)	
Adresse IP attribuée par DHCP pour le port de gestion 1, si disponible après la mise sous tension **Remarque :** si le réseau d'administration comprend un serveur DHCP, le contrôleur E5700SG affiche l'adresse IP attribuée par DHCP sur son affichage à sept segments après son démarrage. Vous pouvez également déterminer l'adresse IP attribuée par DHCP en utilisant l'adresse MAC pour rechercher l'adresse IP attribuée.	• Adresse IPv4 (CIDR) : • Passerelle :

Informations nécessaires	Votre valeur
Adresse IP statique que vous envisagez d'utiliser pour le nœud de stockage de l'appliance sur le réseau d'administration **Remarque :** si votre réseau n'a pas de passerelle, spécifiez la même adresse IPv4 statique pour la passerelle.	• Adresse IPv4 (CIDR) : • Passerelle :
Sous-réseaux du réseau d'administration (CIDR)	

Informations nécessaires pour la connexion et la configuration des ports 10/25 GbE sur le contrôleur E5700SG

Les quatre ports 10/25 GbE du contrôleur E5700SG se connectent au réseau Grid et au réseau client StorageGRID.

Voir "Modes de liaison des ports (contrôleur E5700SG)".

Informations nécessaires	Votre valeur
Vitesse de liaison **Remarque :** si vous sélectionnez 25 GbE, installez les émetteurs-récepteurs SPF28. La négociation automatique n'est pas prise en charge, vous devez donc également configurer les ports et les commutateurs connectés pour 25 GbE.	Choisir une option : • 10 GbE (par défaut) • 25 GbE
Mode de liaison du port	Choisir une option : • Fixe (par défaut) • Agrégat
Port de commutation pour le port 1 (réseau client)	
Port de commutation pour le port 2 (réseau Grid)	
Port de commutation pour le port 3 (réseau client)	
Port de commutation pour le port 4 (réseau Grid)	

Informations nécessaires pour connecter le contrôleur E5700SG au réseau Grid

Le réseau Grid Network pour StorageGRID est un réseau requis, utilisé pour l'ensemble du trafic StorageGRID interne. L'appliance se connecte au réseau Grid à l'aide des ports 10/25 GbE du contrôleur E5700SG.

Voir "Modes de liaison des ports (contrôleur E5700SG)".

Informations nécessaires	Votre valeur
Mode de liaison réseau	Choisir une option : • Sauvegarde active/active (par défaut) • LACP (802.3ad)
Balisage VLAN activé	Choisir une option : • Non (par défaut) • Oui.
Balise VLAN (si le marquage VLAN est activé)	Entrez une valeur comprise entre 0 et 4095 :
Adresse IP attribuée par DHCP pour le réseau Grid, si disponible après la mise sous tension **Remarque :** si le réseau Grid comprend un serveur DHCP, le contrôleur E5700SG affiche l'adresse IP attribuée par DHCP pour le réseau Grid sur son affichage à sept segments après son démarrage.	• Adresse IPv4 (CIDR) : • Passerelle :
Adresse IP statique que vous prévoyez d'utiliser pour le noeud de stockage de l'appliance sur le réseau Grid **Remarque :** si votre réseau n'a pas de passerelle, spécifiez la même adresse IPv4 statique pour la passerelle.	• Adresse IPv4 (CIDR) : • Passerelle :
Sous-réseaux du réseau de grille (CIDR) **Remarque :** si le réseau client n'est pas activé, la route par défaut du contrôleur utilisera la passerelle indiquée ici.	

Informations nécessaires pour connecter le contrôleur E5700SG au réseau client

Le réseau client pour StorageGRID est un réseau facultatif, généralement utilisé pour fournir l'accès du protocole client à la grille. L'appliance se connecte au réseau client à l'aide des ports 10/25 GbE du contrôleur E5700SG.

Voir "Modes de liaison des ports (contrôleur E5700SG)".

Informations nécessaires	Votre valeur
Réseau client activé	Choisir une option : • Non (par défaut) • Oui.

Informations nécessaires	Votre valeur
Mode de liaison réseau	Choisir une option : • Sauvegarde active/active (par défaut) • LACP (802.3ad)
Balisage VLAN activé	Choisir une option : • Non (par défaut) • Oui.
Balise VLAN (Si le marquage VLAN est activé)	Entrez une valeur comprise entre 0 et 4095 :
Adresse IP attribuée par DHCP pour le réseau client, si disponible après la mise sous tension	• Adresse IPv4 (CIDR) : • Passerelle :
Adresse IP statique que vous prévoyez d'utiliser pour le noeud de stockage de l'appliance sur le réseau client **Remarque :** si le réseau client est activé, la route par défaut du contrôleur utilisera la passerelle indiquée ici.	• Adresse IPv4 (CIDR) : • Passerelle :

Informations associées

- "Connexions réseau (SG5700)"
- "Modes de liaison des ports (contrôleur E5700SG)"
- "Configuration du matériel (SG5700)"

Collecte des informations d'installation (SG100 et SG1000)

À l'aide des tableaux, notez les informations requises pour chaque réseau que vous connectez à l'appliance. Ces valeurs sont nécessaires pour installer et configurer le matériel.

> Au lieu d'utiliser les tableaux, utilisez le manuel fourni avec ConfigBuilder. Le manuel ConfigBuilder vous permet de télécharger les informations système et de générer un fichier JSON pour effectuer automatiquement certaines étapes de configuration dans le programme d'installation de l'appliance StorageGRID. Voir "Automatisez l'installation et la configuration de l'appliance".

Vérifiez la version de StorageGRID

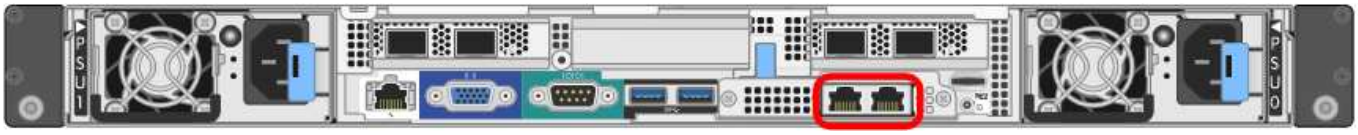
Avant d'installer une appliance de services SG100 ou SG1000, vérifiez que votre système StorageGRID utilise la version requise du logiciel StorageGRID.

Appliance	Version StorageGRID requise
SG1000	11.3 ou ultérieure (dernier correctif recommandé)
SG100	11.4 ou ultérieure (dernier correctif recommandé)

Ports d'administration et de maintenance

Le réseau d'administration pour StorageGRID est un réseau facultatif, utilisé pour l'administration et la maintenance du système. L'appliance se connecte au réseau d'administration à l'aide des ports de gestion 1 GbE suivants de l'appliance.

Ports RJ-45 SG100 :



Ports RJ-45 SG1000 :

Informations nécessaires	Votre valeur
Réseau admin activé	Choisir une option : • Non • Oui (par défaut)
Mode de liaison réseau	Choisir une option : • Indépendant (par défaut) • Sauvegarde active-Backup
Port de commutateur pour le port gauche entouré dans le schéma (port actif par défaut pour le mode de liaison réseau indépendante)	
Port de commutateur pour le port droit entouré dans le diagramme (mode de liaison réseau Active-Backup uniquement)	

Informations nécessaires	Votre valeur
Adresse MAC du port réseau d'administration **Remarque :** l'étiquette d'adresse MAC située à l'avant de l'appliance répertorie l'adresse MAC du port de gestion BMC. Pour déterminer l'adresse MAC du port Admin Network, ajoutez **2** au nombre hexadécimal figurant sur l'étiquette. Par exemple, si l'adresse MAC de l'étiquette se termine par **09**, l'adresse MAC du port d'administration se terminera par **0B**. Si l'adresse MAC de l'étiquette se termine dans **(*y*)FF**, l'adresse MAC du port d'administration se terminera dans **(*y*+1)01**. Vous pouvez facilement effectuer ce calcul en ouvrant Calculator sous Windows, en le définissant en mode programmateur, en sélectionnant Hex, en saisissant l'adresse MAC, puis en tapant **+ 2 =**.	
Adresse IP attribuée par DHCP pour le port réseau d'administration, si disponible après la mise sous tension **Remarque :** vous pouvez déterminer l'adresse IP attribuée par DHCP en utilisant l'adresse MAC pour rechercher l'adresse IP attribuée.	• Adresse IPv4 (CIDR) : • Passerelle :
Adresse IP statique que vous envisagez d'utiliser pour le nœud d'appliance sur le réseau d'administration **Remarque :** si votre réseau n'a pas de passerelle, spécifiez la même adresse IPv4 statique pour la passerelle.	• Adresse IPv4 (CIDR) : • Passerelle :
Sous-réseaux du réseau d'administration (CIDR)	

Ports réseau

Les quatre ports réseau de l'appliance se connectent au réseau StorageGRID Grid et au réseau client en option.

Informations nécessaires	Votre valeur
Vitesse de liaison	Pour le SG100, choisissez l'une des options suivantes : • Auto (par défaut) • 10 GbE • 25 GbE Pour le SG1000, choisissez l'une des options suivantes : • Auto (par défaut) • 10 GbE • 25 GbE • 40 GbE • 100 GbE **Remarque :** pour les vitesses SG1000, 10 et 25 GbE, il faut utiliser des adaptateurs QSA.
Mode de liaison du port	Choisir une option : • Fixe (par défaut) • Agrégat
Port de commutation pour le port 1 (réseau client pour mode fixe)	
Port de commutation pour le port 2 (réseau grille pour mode fixe)	
Port de commutation pour le port 3 (réseau client pour mode fixe)	
Port de commutation pour le port 4 (réseau Grid pour mode fixe)	

Ports réseau de la grille

Le réseau Grid Network pour StorageGRID est un réseau requis, utilisé pour l'ensemble du trafic StorageGRID interne. L'appliance se connecte au réseau Grid à l'aide des quatre ports réseau.

Informations nécessaires	Votre valeur
Mode de liaison réseau	Choisir une option : • Sauvegarde active/active (par défaut) • LACP (802.3ad)

Informations nécessaires	Votre valeur
Balisage VLAN activé	Choisir une option : • Non (par défaut) • Oui.
Balise VLAN (si le marquage VLAN est activé)	Entrez une valeur comprise entre 0 et 4095 :
Adresse IP attribuée par DHCP pour le réseau Grid, si disponible après la mise sous tension	• Adresse IPv4 (CIDR) : • Passerelle :
Adresse IP statique que vous prévoyez d'utiliser pour le nœud de l'appliance sur le réseau Grid **Remarque :** si votre réseau n'a pas de passerelle, spécifiez la même adresse IPv4 statique pour la passerelle.	• Adresse IPv4 (CIDR) : • Passerelle :
Sous-réseaux du réseau de grille (CIDR)	
Paramètre MTU (maximum transmission Unit) (facultatif)vous pouvez utiliser la valeur par défaut de 1500, ou définir la MTU sur une valeur adaptée aux trames jumbo, comme 9000.	

Ports réseau client

Le réseau client pour StorageGRID est un réseau facultatif, généralement utilisé pour fournir l'accès du protocole client à la grille. Le serveur se connecte au réseau client à l'aide des quatre ports réseau.

Informations nécessaires	Votre valeur
Réseau client activé	Choisir une option : • Non (par défaut) • Oui.
Mode de liaison réseau	Choisir une option : • Sauvegarde active/active (par défaut) • LACP (802.3ad)
Balisage VLAN activé	Choisir une option : • Non (par défaut) • Oui.

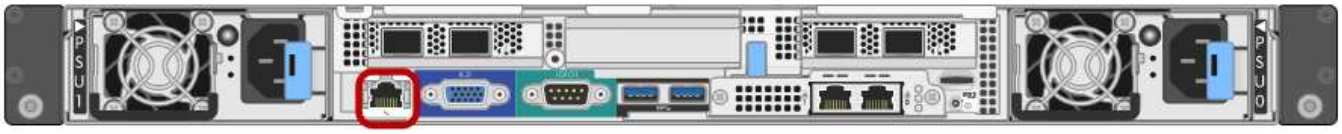
Informations nécessaires	Votre valeur
Balise VLAN (si le balisage VLAN est activé)	Entrez une valeur comprise entre 0 et 4095 :
Adresse IP attribuée par DHCP pour le réseau client, si disponible après la mise sous tension	• Adresse IPv4 (CIDR) : • Passerelle :
Adresse IP statique que vous prévoyez d'utiliser pour le nœud de l'appliance sur le réseau client **Remarque :** si le réseau client est activé, la route par défaut du serveur utilise la passerelle indiquée ici.	• Adresse IPv4 (CIDR) : • Passerelle :

Ports réseau de gestion BMC

Vous pouvez accéder à l'interface BMC de l'appliance de services à l'aide du port de gestion 1 GbE entouré dans le schéma. Ce port prend en charge la gestion à distance du matériel du contrôleur via Ethernet en utilisant la norme IPMI (Intelligent Platform Management interface).

> Vous pouvez activer ou désactiver l'accès IPMI à distance pour tous les dispositifs contenant un contrôleur BMC en utilisant le point de terminaison privé de l'API de gestion, PUT /private/bmc.

Port de gestion du contrôleur BMC SG100 :



Port de gestion du contrôleur BMC SG1000 :

Informations nécessaires	Votre valeur
Port de commutateur Ethernet vous vous connectez au port de gestion du contrôleur BMC (encerclé dans le diagramme)	
Adresse IP attribuée par DHCP pour le réseau de gestion BMC, si disponible après la mise sous tension	• Adresse IPv4 (CIDR) : • Passerelle :
Adresse IP statique que vous prévoyez d'utiliser pour le port de gestion BMC	• Adresse IPv4 (CIDR) : • Passerelle :

Informations associées

- "Cable appliance (SG100 et SG1000)"
- "Configurez les adresses IP StorageGRID"

Automatisez l'installation et la configuration de l'appliance

L'automatisation de l'installation et de la configuration peut être utile pour déployer plusieurs instances StorageGRID ou une instance StorageGRID complexe et de grande taille.

Automatisez l'installation et la configuration de vos appliances StorageGRID à l'aide des outils NetApp StorageGRID. Une fois que vous avez installé et configuré les appliances, vous pouvez le faire "Automatisez la configuration de l'ensemble du système StorageGRID".

Vous pouvez automatiser la configuration des éléments suivants :

- Réseau Grid, réseau d'administration et adresses IP du réseau client
- Interface BMC
- Liens réseau
  - Mode de liaison du port
  - Mode de liaison réseau
  - Vitesse de liaison

Options d'automatisation

Pour automatiser l'installation et la configuration de l'appliance, utilisez une ou plusieurs des options suivantes :

- Générez un fichier JSON contenant les détails de la configuration. Collaborez avec votre consultant en services professionnels NetApp pour utiliser le "Outil NetApp ConfigBuilder" pour effectuer ces étapes :

Étape	Consultez les services professionnels NetApp	Utilisez ConfigBuilder
1	Obtenir le numéro de commande	
2		Télécharger le manuel
3	Compléter le manuel	
4		Télécharger le classeur
5		Générer un fichier JSON
6	Téléchargez le fichier JSON vers l'appliance	

  Vous pouvez utiliser le même fichier JSON pour configurer plusieurs appliances.

  La configuration de l'appliance à l'aide d'un fichier JSON téléchargé est souvent plus efficace que d'effectuer la configuration manuellement, en particulier si vous devez configurer de nombreux nœuds.

L'exécution manuelle de la configuration nécessite l'utilisation de plusieurs pages dans le programme d'installation de l'appliance StorageGRID et l'application du fichier de configuration pour chaque nœud un par un.

- Si vous êtes un utilisateur avancé, vous pouvez utiliser les scripts StorageGRID Python suivants pour installer et configurer votre système :
  - `configure-sga.py`: Automatisez l'installation et la configuration de vos appareils. Voir Automatisez l'installation et la configuration de l'appliance à l'aide du script configure-sga.py.
  - `configure-storagegrid.py`: Configurer les autres composants de l'ensemble du système StorageGRID (la « grille »). Voir "Automatisez la configuration de StorageGRID".

> Vous pouvez utiliser directement les scripts Python d'automatisation StorageGRID, ou utiliser ces scripts en tant qu'exemples de l'utilisation de l'API REST d'installation de StorageGRID dans les outils de déploiement et de configuration que vous développez vous-même. Reportez-vous aux instructions pour "Téléchargement et extraction des fichiers d'installation de StorageGRID".

Automatisez la configuration de l'appliance avec le programme d'installation de l'appliance StorageGRID

Une fois que vous avez généré un fichier JSON, vous pouvez automatiser la configuration d'une ou plusieurs appliances en utilisant le programme d'installation de l'appliance StorageGRID pour télécharger le fichier JSON.

Avant de commencer

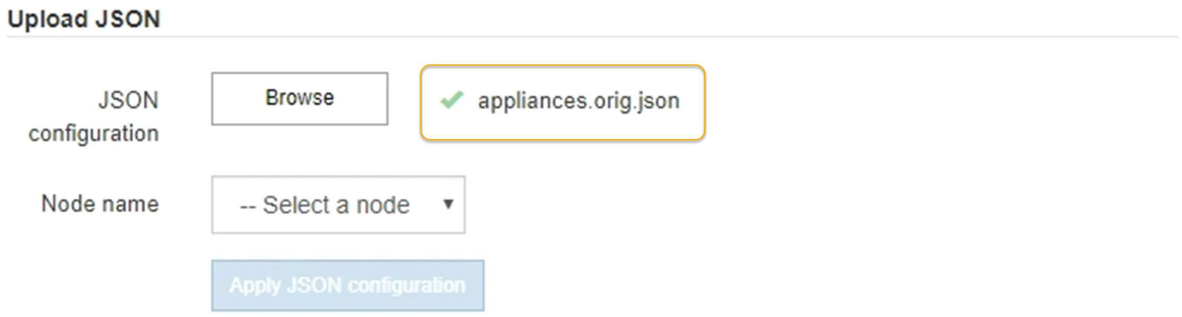
- L'appliance a été installée dans un rack, connectée à vos réseaux et sous tension.
- Vous avez Généré le fichier JSON En collaboration avec votre consultant en services professionnels NetApp.
- Votre appareil contient la dernière version du micrologiciel compatible avec StorageGRID 11.5 ou une version ultérieure.
- Vous êtes connecté au programme d'installation de l'appliance StorageGRID sur l'appliance que vous configurez à l'aide d'un "navigateur web pris en charge".

Étapes

1. Dans le programme d'installation de l'appareil StorageGRID, sélectionnez **Avancé** > **mettre à jour la configuration de l'appareil**. La page mise à jour de la configuration de l'appliance s'affiche.
2. Recherchez et sélectionnez le fichier JSON avec la configuration que vous souhaitez télécharger.

   Le fichier est téléchargé et validé. Une fois le processus de validation terminé, le nom du fichier s'affiche à côté d'une coche verte.

> Vous risquez de perdre la connexion à l'appliance si la configuration du fichier JSON inclut des sections pour `link_config`, `networks`, ou les deux. Si vous n'êtes pas reconnecté dans un délai d'une minute, saisissez à nouveau l'URL de l'appliance en utilisant l'une des autres adresses IP attribuées à l'appliance.



La liste déroulante **Nom de nœud** contient les noms de nœud de niveau supérieur définis dans le fichier JSON.

> Si le fichier n'est pas valide, le nom du fichier s'affiche en rouge et un message d'erreur s'affiche dans une bannière jaune. Le fichier non valide n'est pas appliqué à l'appliance. ConfigBuilder vérifie que vous disposez d'un fichier JSON valide.

3. Sélectionnez un noeud dans la liste déroulante **Nom de noeud**.

   Le bouton **Apply JSON configuration** est activé.

4. Sélectionnez **appliquer la configuration JSON**.

   La configuration est appliquée au nœud sélectionné.

Automatisez l'installation et la configuration de l'appliance à l'aide du script configure-sga.py

Si vous êtes un utilisateur avancé, vous pouvez utiliser le `configure-sga.py` Script permettant d'automatiser la plupart des tâches d'installation et de configuration des nœuds d'appliance StorageGRID, notamment l'installation et la configuration d'un nœud d'administration principal. Ce script peut être utile si vous avez un grand nombre d'appliances à configurer.

Vous pouvez également utiliser le script pour générer un fichier JSON qui contient les informations de configuration de l'appliance. Vous pouvez télécharger le fichier JSON vers le programme d'installation de l'appliance StorageGRID pour configurer tous les nœuds d'appliance en même temps. Vous pouvez également modifier le fichier JSON, puis le télécharger pour appliquer une nouvelle configuration à un ou plusieurs dispositifs.

> Cette procédure s'adresse aux utilisateurs expérimentés ayant de l'expérience dans l'utilisation d'interfaces de ligne de commande. C'est également possible Utilisez le programme d'installation de l'appliance StorageGRID pour automatiser la configuration.

Avant de commencer

- L'appliance a été installée dans un rack, connectée à vos réseaux et sous tension.
- Vous avez Généré le fichier JSON En collaboration avec votre consultant en services professionnels NetApp.
- Votre appareil contient la dernière version du micrologiciel compatible avec StorageGRID 11.5 ou une version ultérieure.
- Vous avez configuré l'adresse IP du réseau d'administration de l'appliance.

- Vous avez téléchargé le `configure-sga.py` fichier. Le fichier est inclus dans l'archive d'installation ou vous pouvez y accéder en cliquant sur **aide** > **script d'installation de l'appliance** dans le programme d'installation de l'appliance StorageGRID.

Étapes

1. Connectez-vous à la machine Linux que vous utilisez pour exécuter le script Python.
2. Pour obtenir de l'aide générale sur la syntaxe du script et pour afficher la liste des paramètres disponibles, entrez les informations suivantes :

   ```
   configure-sga.py --help
   ```

   Le `configure-sga.py` script utilise cinq sous-commandes :

   - `advanced` Pour les interactions avancées avec l'appliance StorageGRID, notamment la configuration BMC, et la création d'un fichier JSON contenant la configuration actuelle de l'appliance
   - `configure` Pour configurer le mode RAID, le nom du nœud et les paramètres réseau
   - `install` Pour démarrer une installation StorageGRID
   - `monitor` Pour contrôler une installation StorageGRID
   - `reboot` pour redémarrer l'appliance

     Si vous entrez une sous-commande (avancé, configurez, installez, surveillez ou redémarrez), suivie de l'argument `--help` option vous obtenez un autre texte d'aide fournissant plus de détails sur les options disponibles dans cette sous-commande :
     `configure-sga.py` *`subcommand`* `--help`

     Si vous le souhaitez Sauvegardez la configuration de l'appliance dans un fichier JSON, assurez-vous que les noms de nœuds respectent les exigences suivantes :

     - Chaque nom de nœud est unique si vous souhaitez configurer automatiquement tous les nœuds d'appliance à l'aide d'un fichier JSON.
     - Doit être un nom d'hôte valide contenant au moins 1 et 32 caractères.
     - Peut utiliser des lettres, des chiffres et des tirets.
     - Impossible de commencer ou de terminer par un tiret.
     - Ne peut pas contenir uniquement des chiffres.
3. Pour appliquer la configuration du fichier JSON à l'appliance, entrez la commande suivante, où *`SGA-INSTALL-IP`* L'adresse IP du réseau d'administration de l'appliance, *`json-file-name`* Est le nom du fichier JSON, et *`node-name-inside-json-file`* est le nom du nœud sur lequel la configuration est appliquée :
   `configure-sga.py advanced --restore-file` *`json-file-name`* `--restore-node` *`node-name-inside-json-file SGA-INSTALL-IP`*
4. Pour vérifier la configuration actuelle du nœud de l'appliance, entrez l'emplacement suivant *`SGA-INSTALL-IP`* Adresse IP du réseau d'administration de l'appliance :
   `configure-sga.py configure` *`SGA-INSTALL-IP`*

   Les résultats indiquent les informations IP actuelles de l'appliance, y compris l'adresse IP du noeud d'administration principal et les informations sur les réseaux Admin, Grid et client.

```
Connecting to +https://10.224.2.30:8443+ (Checking version and
connectivity.)
2021/02/25 16:25:11: Performing GET on /api/versions... Received 200
2021/02/25 16:25:11: Performing GET on /api/v2/system-info... Received
200
2021/02/25 16:25:11: Performing GET on /api/v2/admin-connection...
Received 200
2021/02/25 16:25:11: Performing GET on /api/v2/link-config... Received
200
2021/02/25 16:25:11: Performing GET on /api/v2/networks... Received 200
2021/02/25 16:25:11: Performing GET on /api/v2/system-config... Received
200

  StorageGRID Appliance
    Name:        LAB-SGA-2-30
    Node type:   storage

  StorageGRID primary Admin Node
    IP:        172.16.1.170
    State:     unknown
    Message:   Initializing...
    Version:   Unknown

  Network Link Configuration
    Link Status
          Link      State      Speed (Gbps)
          ----      -----      -----
          1         Up         10
          2         Up         10
          3         Up         10
          4         Up         10
          5         Up         1
          6         Down       N/A

    Link Settings
        Port bond mode:      FIXED
        Link speed:          10GBE

        Grid Network:        ENABLED
            Bonding mode:    active-backup
            VLAN:            novlan
            MAC Addresses:   00:a0:98:59:8e:8a  00:a0:98:59:8e:82

        Admin Network:       ENABLED
            Bonding mode:    no-bond
            MAC Addresses:   00:80:e5:29:70:f4
```

```
        Client Network:      ENABLED
            Bonding mode:    active-backup
            VLAN:            novlan
            MAC Addresses:   00:a0:98:59:8e:89  00:a0:98:59:8e:81

  Grid Network
    CIDR:      172.16.2.30/21 (Static)
    MAC:       00:A0:98:59:8E:8A
    Gateway:   172.16.0.1
    Subnets:   172.17.0.0/21
               172.18.0.0/21
               192.168.0.0/21
    MTU:       1500

  Admin Network
    CIDR:      10.224.2.30/21 (Static)
    MAC:       00:80:E5:29:70:F4
    Gateway:   10.224.0.1
    Subnets:   10.0.0.0/8
               172.19.0.0/16
               172.21.0.0/16
    MTU:       1500

  Client Network
    CIDR:      47.47.2.30/21 (Static)
    MAC:       00:A0:98:59:8E:89
    Gateway:   47.47.0.1
    MTU:       2000

#####################################################################
#####   If you are satisfied with this configuration,    #####
##### execute the script with the "install" sub-command. #####
#####################################################################
```

5. Si vous devez modifier l'une des valeurs de la configuration actuelle, utilisez le `configure` sous-commande pour les mettre à jour. Par exemple, si vous souhaitez modifier l'adresse IP utilisée par l'appliance pour la connexion au nœud d'administration principal à `172.16.2.99`, saisissez les informations suivantes :

```
configure-sga.py configure --admin-ip 172.16.2.99 _SGA-INSTALL-IP_
```

6. si vous souhaitez sauvegarder la configuration de l'appliance dans un fichier JSON, utilisez les options avancées et `backup-file` sous-commandes. Par exemple, si vous souhaitez sauvegarder la configuration d'une appliance avec une adresse IP *`SGA-INSTALL-IP`* à un fichier nommé `appliance-SG1000.json`, entrez les informations suivantes :

`configure-sga.py advanced --backup-file appliance-SG1000.json SGA-INSTALL-IP`

Le fichier JSON contenant les informations de configuration est écrit dans le même répertoire que celui où vous avez exécuté le script à partir de.

> Vérifiez que le nom de nœud supérieur dans le fichier JSON généré correspond au nom de l'appliance. N'apportez aucune modification à ce fichier à moins d'être un utilisateur expérimenté et d'avoir une compréhension approfondie des API StorageGRID.

7. Lorsque vous êtes satisfait de la configuration de l'appliance, utilisez le `install` et `monitor` sous-commandes pour installer l'appliance :
`configure-sga.py install --monitor SGA-INSTALL-IP`
8. Si vous souhaitez redémarrer l'appareil, entrez les valeurs suivantes :
`configure-sga.py reboot SGA-INSTALL-IP`

Automatisez la configuration de StorageGRID

Une fois que vous avez installé et configuré les nœuds grid, vous pouvez automatiser la configuration du système StorageGRID.

Avant de commencer

- Vous connaissez l'emplacement des fichiers suivants à partir de l'archive d'installation.

Nom du fichier	Description
configure-storagegrid.py	Script Python utilisé pour automatiser la configuration
configurez-storagegrid.sample.json	Exemple de fichier de configuration à utiliser avec le script
configurez-storagegrid.blank.json	Fichier de configuration vierge à utiliser avec le script

- Vous avez créé un `configure-storagegrid.json` fichier de configuration. Pour créer ce fichier, vous pouvez modifier l'exemple de fichier de configuration (`configure-storagegrid.sample.json`) ou le fichier de configuration vierge (`configure-storagegrid.blank.json`).

Description de la tâche

Vous pouvez utiliser le `configure-storagegrid.py` Script Python et le `configure-storagegrid.json` Fichier de configuration pour automatiser la configuration de votre système StorageGRID.

> Vous pouvez également configurer le système à l'aide du "Gestionnaire de grille" ou le "API d'installation".

Étapes

1. Connectez-vous à la machine Linux que vous utilisez pour exécuter le script Python.
2. Accédez au répertoire dans lequel vous avez extrait l'archive d'installation.

Par exemple :
`cd StorageGRID-Webscale-version/platform`

où *platform* est `debs`, `rpms`, ou `vsphere`.

3. Exécutez le script Python et utilisez le fichier de configuration que vous avez créé.

   Par exemple :

```
./configure-storagegrid.py ./configure-storagegrid.json --start-install
```

Une fois que vous avez terminé

Un progiciel de récupération `.zip` le fichier est généré pendant le processus de configuration et il est téléchargé dans le répertoire où vous exécutez le processus d'installation et de configuration. Vous devez sauvegarder le fichier de package de restauration afin de pouvoir restaurer le système StorageGRID en cas de défaillance d'un ou plusieurs nœuds de la grille. Par exemple, copiez-le dans un emplacement sécurisé, sauvegardé sur le réseau et dans un emplacement de stockage cloud sécurisé.

> Le fichier du progiciel de récupération doit être sécurisé car il contient des clés de cryptage et des mots de passe qui peuvent être utilisés pour obtenir des données du système StorageGRID.

Si vous avez spécifié que des mots de passe aléatoires doivent être générés, vous devez extraire le `Passwords.txt` Fichier et recherche les mots de passe requis pour accéder au système StorageGRID.

```
######################################################################
##### The StorageGRID "recovery package" has been downloaded as: #####
#####           ./sgws-recovery-package-994078-rev1.zip          #####
#####   Safeguard this file as it will be needed in case of a    #####
#####                 StorageGRID node recovery.                 #####
######################################################################
```

Votre système StorageGRID est installé et configuré lorsqu'un message de confirmation s'affiche.

```
StorageGRID has been configured and installed.
```

Présentation de l'installation des API REST

StorageGRID fournit deux API REST pour effectuer des tâches d'installation : l'API d'installation de StorageGRID et l'API du programme d'installation de l'appliance StorageGRID.

Les deux API utilisent la plate-forme swagger open source API pour fournir la documentation de l'API. Swagger permet aux développeurs et aux non-développeurs d'interagir avec l'API dans une interface utilisateur qui illustre la façon dont l'API répond aux paramètres et aux options. Cette documentation suppose que vous êtes familiarisé avec les technologies Web standard et le format de données JSON.

Toutes les opérations d'API que vous effectuez à l'aide de la page Web API Docs sont des opérations en direct. Veillez à ne pas créer, mettre à jour ou supprimer des données de configuration ou d'autres données par erreur.

Chaque commande de l'API REST inclut l'URL de l'API, une action HTTP, tous les paramètres d'URL requis ou facultatifs et une réponse de l'API attendue.

API d'installation de StorageGRID

L'API d'installation de StorageGRID n'est disponible que lors de la configuration initiale du système StorageGRID et si vous devez effectuer une restauration du nœud d'administration principal. L'API d'installation est accessible via HTTPS depuis le Grid Manager.

Pour accéder à la documentation de l'API, accédez à la page Web d'installation sur le nœud d'administration principal et sélectionnez **aide** > **documentation de l'API** dans la barre de menus.

L'API d'installation de StorageGRID comprend les sections suivantes :

- **Config** : opérations liées à la version du produit et aux versions de l'API. Vous pouvez lister la version du produit ainsi que les versions principales de l'API prises en charge par cette version.
- **GRID** : opérations de configuration au niveau de la grille. Vous pouvez obtenir et mettre à jour les paramètres de la grille, y compris les détails de la grille, les sous-réseaux de la grille, les mots de passe de la grille et les adresses IP des serveurs NTP et DNS.
- **Nœuds** : opérations de configuration au niveau des nœuds. Vous pouvez récupérer une liste de nœuds de la grille, supprimer un nœud de la grille, configurer un nœud de la grille, afficher un nœud de la grille et réinitialiser la configuration d'un nœud de la grille.
- **Provision**: Opérations de provisionnement. Vous pouvez démarrer l'opération de provisionnement et afficher l'état de cette opération.
- **Recovery** : opérations de restauration du noeud Admin principal. Vous pouvez réinitialiser les informations, télécharger le progiciel de restauration, démarrer la récupération et afficher l'état de l'opération de récupération.
- **Recovery-package**: Opérations pour télécharger le progiciel de récupération.
- **Sites** : opérations de configuration au niveau du site. Vous pouvez créer, afficher, supprimer et modifier un site.

API du programme d'installation de l'appliance StorageGRID

L'API du programme d'installation de l'appliance StorageGRID est accessible via HTTPS à partir de `*Controller_IP*:8443`.

Pour accéder à la documentation de l'API, accédez au programme d'installation de l'appliance StorageGRID sur l'appliance et sélectionnez **aide** > **API Docs** dans la barre de menus.

L'API du programme d'installation de l'appliance StorageGRID comprend les sections suivantes :

- **Clone** : opérations de configuration et de contrôle du clonage des nœuds.
- **Cryptage** : opérations de gestion du cryptage et d'affichage de l'état du cryptage.
- **Configuration matérielle** : opérations permettant de configurer les paramètres système sur le matériel connecté.
- **Installation** : opérations de démarrage de l'installation de l'appareil et de surveillance de l'état de

l'installation.

- **Mise en réseau** : opérations liées à la configuration du réseau Grid, Admin et client pour une appliance StorageGRID et les paramètres du port de l'appliance.
- **Setup** : opérations pour faciliter la configuration initiale de l'appliance, y compris les demandes d'obtenir des informations sur le système et de mettre à jour l'adresse IP du nœud d'administration principal.
- **Support** : opérations de redémarrage du contrôleur et d'obtention des journaux.
- **Update-config** : opérations de mise à jour de la configuration de l'appliance StorageGRID.
- **Mise à niveau** : opérations liées à la mise à niveau du micrologiciel de l'appareil.
- **Uploadsg** : opérations de téléchargement des fichiers d'installation StorageGRID.

Installer le matériel de fixation

Enregistrez le matériel

L'enregistrement du matériel offre des avantages de support.

Étapes

1. Recherchez le numéro de série du châssis de l'appliance. Pour les appliances SG6000, le numéro de série du châssis se trouve sur le tiroir du contrôleur de stockage.

   Vous trouverez le numéro sur le bordereau d'expédition, dans votre e-mail de confirmation ou sur l'appareil après le déballage.

   L'appliance de stockage SG6000 comporte plusieurs numéros de série. Le numéro de série figurant sur le tiroir du contrôleur de stockage doit être enregistré et utilisé si vous appelez pour obtenir une assistance ou une réparation sur l'appliance SG6000.

2. Accédez au site de support NetApp à l'adresse "mysupport.netapp.com".
3. Déterminez si vous devez enregistrer le matériel :

Si vous êtes…	Suivez ces étapes…
Client NetApp existant	a. Connectez-vous à l'aide de votre nom d'utilisateur et de votre mot de passe. b. Sélectionnez **produits** > **Mes produits**. c. Vérifiez que le nouveau numéro de série est répertorié. d. Si ce n'est pas le cas, suivez les instructions destinées aux nouveaux clients NetApp.

Si vous êtes…	Suivez ces étapes…
Nouveau client NetApp	a. Cliquez sur **s'inscrire maintenant** et créez un compte. b. Sélectionnez **produits** > **Enregistrer les produits**. c. Entrez le numéro de série du produit et les détails demandés. Une fois votre inscription approuvée, vous pouvez télécharger tout logiciel requis. La procédure d'approbation peut prendre jusqu'à 24 heures.

Installez-le dans l'armoire ou sur le rack

Installation dans l'armoire ou le rack (SGF6112)

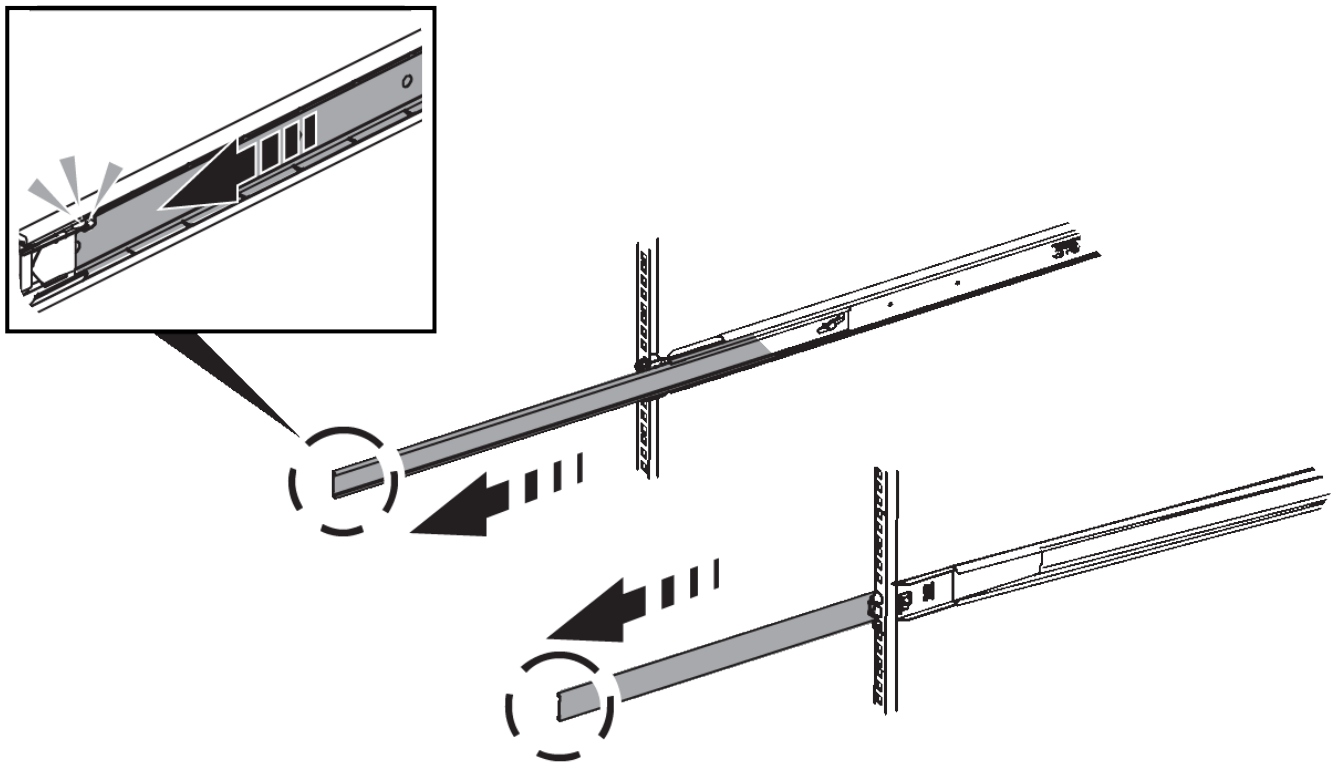
Vous installez un ensemble de rails pour l'appareil dans votre armoire ou rack, puis faites glisser l'appareil sur les rails.

Avant de commencer

- Vous avez passé en revue le document consignes de sécurité inclus dans la boîte et compris les précautions à prendre pour déplacer et installer le matériel.
- Les instructions sont fournies avec le kit de rails.

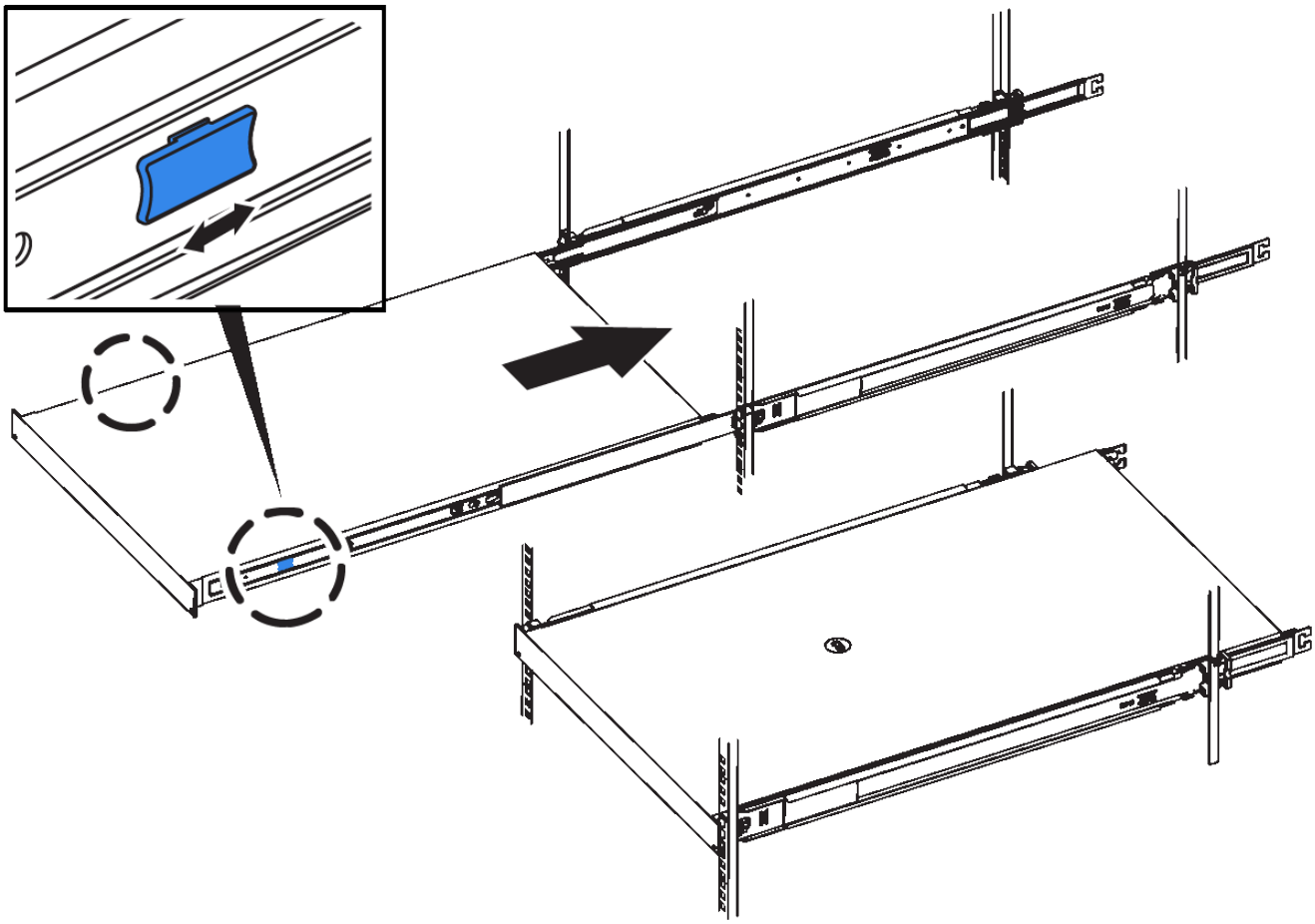
Étapes

1. Suivez attentivement les instructions du kit de rails pour installer les rails dans votre armoire ou rack.
2. Sur les deux rails installés dans l'armoire ou le rack, étendez les pièces mobiles des rails jusqu'à ce que vous entendiez un clic.



3. Insérez l’appareil dans les rails.
4. Faites glisser l’appareil dans l’armoire ou le rack.

   Lorsque vous ne pouvez plus déplacer l’appareil, tirez sur les loquets bleus des deux côtés du châssis pour faire glisser l’appareil complètement vers l’intérieur.



5. Serrez les vis imperdables du panneau avant de l’appareil pour fixer l’appareil dans le rack.

> Ne fixez le cadre avant qu’après avoir mis l’appareil sous tension.

SG6000

Installation dans l’armoire ou le rack (SG6000)

Pour les SGSGSGF6024 et SGF6024, vous installez des rails dans votre armoire ou rack et faites glisser le tiroir contrôleur, les tiroirs d’extension éventuels et le contrôleur de calcul sur les rails. Pour les SG6060, n’installez pas les disques dans chaque shelf avant que les shelfs soient installés.

Modèle	Installer	Pour plus d'informations
SG6060	tiroir contrôleur de 60 disques et tiroir d'extension de 60 disques	"Installez les tiroirs de 60 disques"
SG6060	60 disques dans chaque tiroir	"Installez les lecteurs"
SGF6024	tiroir contrôleur de 24 disques	"Installez les tiroirs de 24 disques"
SG6060 et SGF6024	Contrôleur de calcul SG6000-CN	"Installer le contrôleur SG6000-CN"

Installation des tiroirs de 60 disques (SG6060)

Vous installez un ensemble de rails pour le tiroir contrôleur E2860 dans votre armoire ou votre rack, puis faites glisser le tiroir contrôleur sur les rails. Si vous installez des tiroirs d'extension de 60 disques, la même procédure s'applique.

Avant de commencer

- Vous avez passé en revue le document consignes de sécurité inclus dans la boîte et compris les précautions à prendre pour déplacer et installer le matériel.
- Les instructions sont fournies avec le kit de rails.

Chaque tiroir de 60 disques pèse environ 60 kg (132 lb) sans disque installé. Quatre personnes ou un dispositif de levage mécanisé sont nécessaires pour déplacer la tablette en toute sécurité.

Pour éviter d'endommager le matériel, ne déplacez jamais le tiroir si des disques sont installés. Vous devez retirer tous les disques avant de déplacer le tiroir.

Lors de l'installation du tiroir contrôleur E2860 ou des tiroirs d'extension en option, installez le matériel en bas jusqu'en haut du rack ou de l'armoire afin d'éviter tout basculement de l'équipement. Pour que l'équipement le plus lourd se trouve au bas de l'armoire ou du rack, installez le contrôleur SG6000-CN au-dessus du tiroir du contrôleur E2860 et des tiroirs d'extension.

Avant de valider l'installation, vérifiez que les câbles optiques de 0,5 m fournis avec l'appliance ou les câbles que vous fournissez sont suffisamment longs pour la disposition prévue.

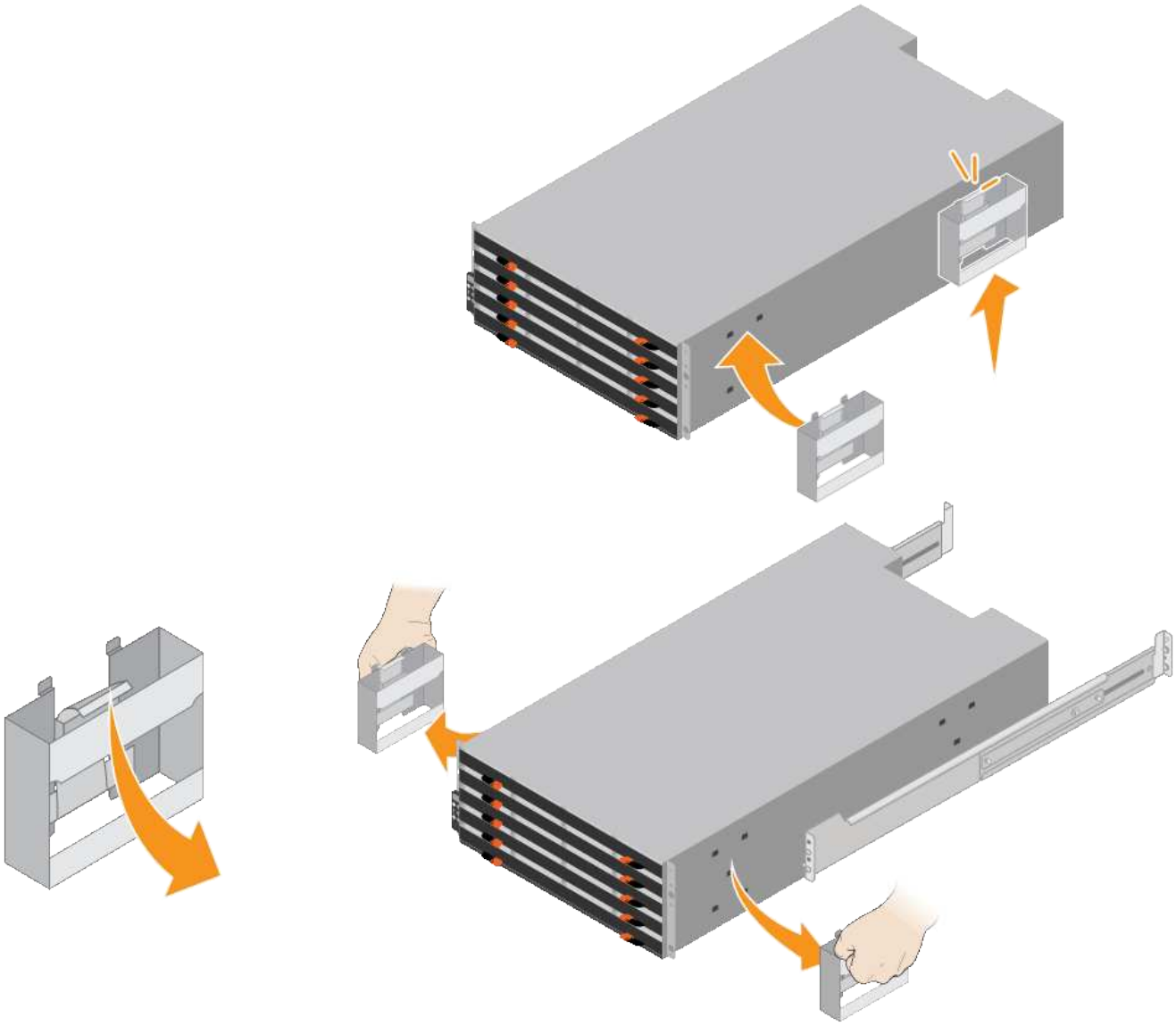
Étapes

1. Suivez attentivement les instructions du kit de rails pour installer les rails dans votre armoire ou rack.

   Pour les armoires à trous carrés, installez d'abord les écrous cage fournis pour fixer l'avant et l'arrière du shelf à l'aide de vis.

2. Retirez la boîte d'emballage extérieure de l'appareil. Pliez ensuite les rabats du boîtier intérieur.
3. Si vous soulevez l'appareil à la main, fixez les quatre poignées sur les côtés du châssis.

   Poussez sur chaque poignée jusqu'à ce qu'elle s'enclenche.



4. Placez l’arrière de la tablette (extrémité avec les connecteurs) sur les rails.
5. En soutenant le shelf par le bas, faites-le glisser dans l’armoire. Si vous utilisez les poignées, utilisez les loquets du pouce pour détacher une poignée à la fois lorsque vous faites glisser la tablette vers l’intérieur.

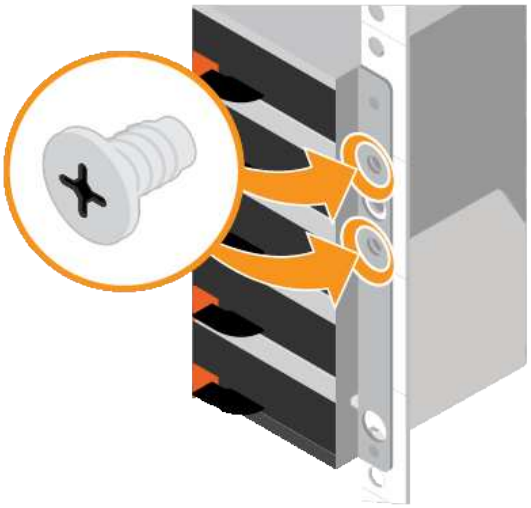
   Pour retirer les poignées, tirez le loquet de déverrouillage, poussez-le vers le bas, puis tirez-le hors de la tablette.

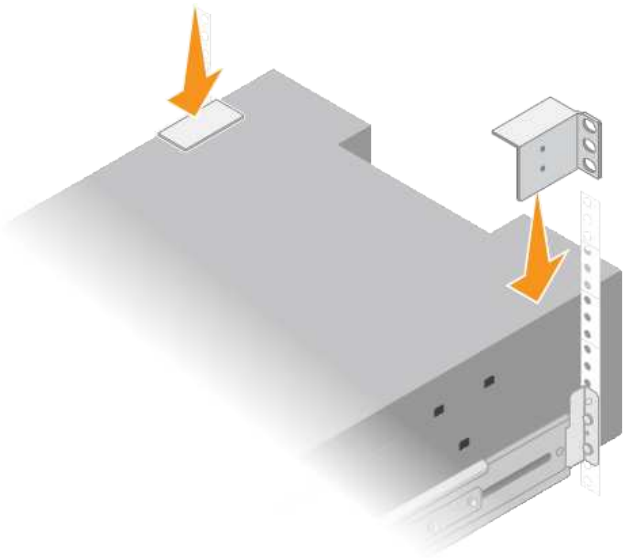
6. Fixez le shelf à l’avant de l’armoire.

   Insérez les vis dans les premier et troisième trous du haut de la tablette des deux côtés.

7. Fixez le shelf à l’arrière de l’armoire.

   Placez deux supports arrière de chaque côté de la section supérieure arrière de la tablette. Insérez les vis dans le premier et le troisième trous de chaque support.





8. Répétez ces étapes pour tous les tiroirs d'extension.

Installation des disques (SG6060)

Après avoir installé le tiroir de 60 disques dans une armoire ou un rack, installez les 60 disques dans le tiroir. Le numéro d'expédition du tiroir contrôleur E2860 comprend deux disques SSD que vous devez installer dans le tiroir supérieur du tiroir contrôleur. Chaque tiroir d'extension en option comprend 60 disques durs et aucun disque SSD.

Avant de commencer

Vous avez installé le tiroir contrôleur E2860 ou deux tiroirs d'extension optionnels (un ou deux) dans l'armoire ou le rack.

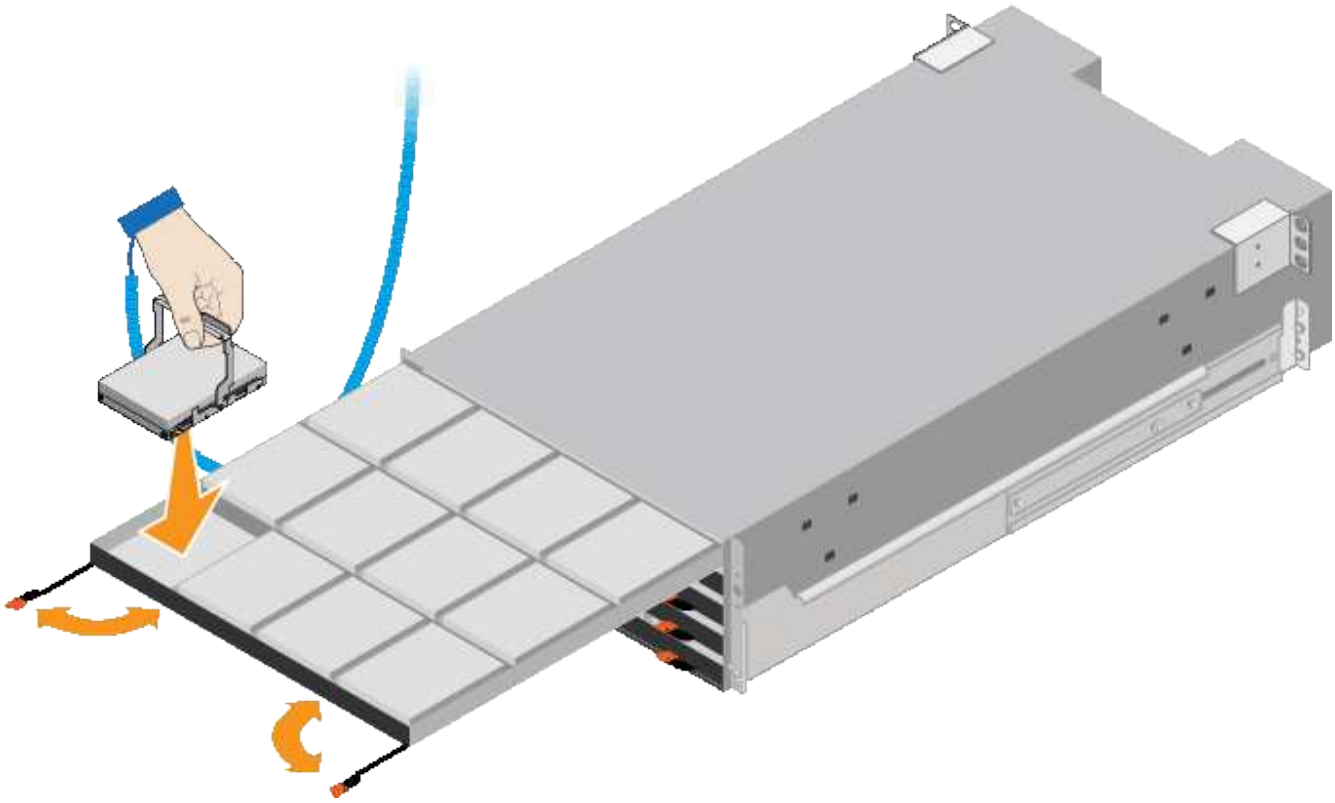
> Pour éviter d'endommager le matériel, ne déplacez jamais le tiroir si des disques sont installés. Vous devez retirer tous les disques avant de déplacer le tiroir.

Étapes

1. Enroulez l'extrémité du bracelet antistatique autour de votre poignet et fixez l'extrémité du clip à une masse métallique afin d'éviter toute décharge statique.
2. Retirez les disques de leur emballage.
3. Relâchez les leviers du tiroir d'entraînement supérieur et faites glisser le tiroir vers l'extérieur à l'aide des leviers.
4. Recherchez les deux disques SSD.

   > Les tiroirs d'extension n'utilisent pas de disques SSD.

5. Relever chaque poignée d'entraînement en position verticale.
6. Installez les deux disques SSD dans les logements 0 et 1 (les deux premiers logements le long du côté gauche du tiroir).
7. Positionnez doucement chaque disque dans son slot, et abaissez la poignée de lecteur relevée jusqu'à ce qu'il s'enclenche en position.



8. Installez 10 disques durs dans le tiroir supérieur.
9. Faites glisser le tiroir vers l'intérieur en appuyant sur le centre et en fermant doucement les deux leviers.

> Arrêtez de pousser le tiroir si vous vous sentez grippé. Utilisez les leviers de déverrouillage à l'avant du tiroir pour le faire glisser vers l'arrière. Réinsérez ensuite le tiroir avec précaution dans la fente.

10. Répétez ces étapes pour installer des disques durs dans les quatre autres tiroirs.

> Vous devez installer les 60 disques pour assurer le bon fonctionnement.

11. Fixez le panneau avant sur le shelf.
12. Si vous disposez de tiroirs d'extension, répétez cette procédure pour installer 12 disques durs dans chaque tiroir de chaque tiroir d'extension.
13. Reportez-vous aux instructions d'installation du SG6000-CN dans une armoire ou un rack.

Installation des tiroirs de 24 disques (SGF6024)

Vous installez un ensemble de rails pour le tiroir contrôleur EF570 dans votre armoire ou votre rack, puis faites glisser la baie sur les rails.

Avant de commencer

- Vous avez passé en revue le document consignes de sécurité inclus dans la boîte et compris les précautions à prendre pour déplacer et installer le matériel.
- Les instructions sont fournies avec le kit de rails.

Étapes

1. Suivez attentivement les instructions du kit de rails pour installer les rails dans votre armoire ou rack.

   Pour les armoires à trous carrés, installez d'abord les écrous cage fournis pour fixer l'avant et l'arrière du shelf à l'aide de vis.

2. Retirez la boîte d'emballage extérieure de l'appareil. Pliez ensuite les rabats du boîtier intérieur.
3. Placez l'arrière de la tablette (extrémité avec les connecteurs) sur les rails.

   Une étagère entièrement chargée pèse environ 24 kg (52 lb). Deux personnes sont nécessaires pour déplacer le boîtier en toute sécurité.

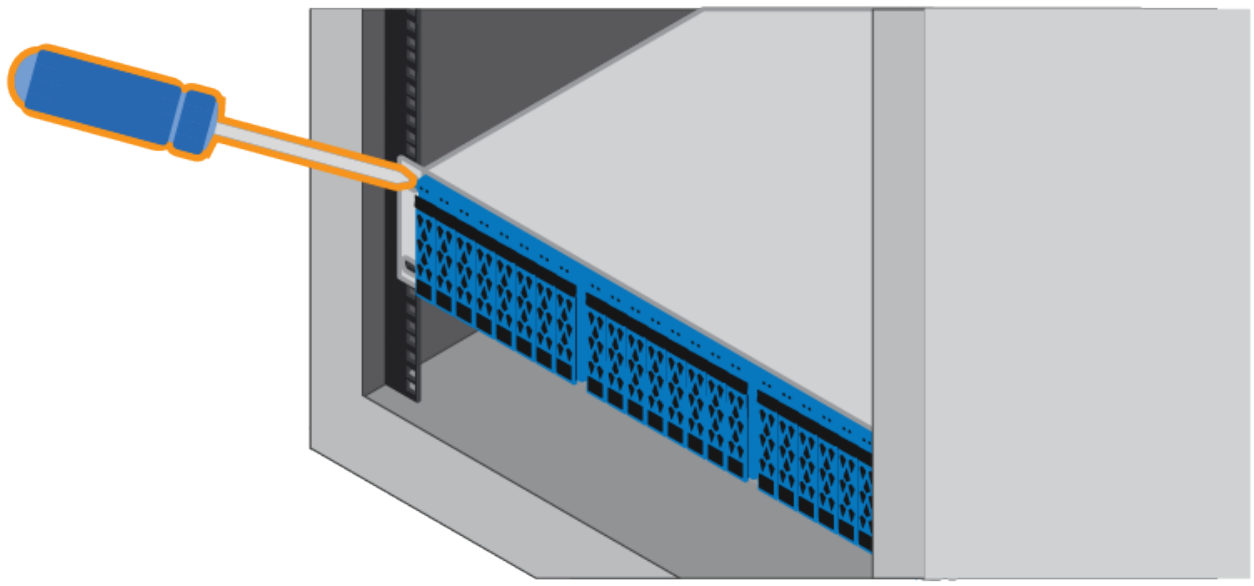
4. Faites glisser avec précaution le boîtier tout au long des rails.

   Vous devrez peut-être ajuster les rails pour vous assurer que le boîtier glisse complètement sur les rails.

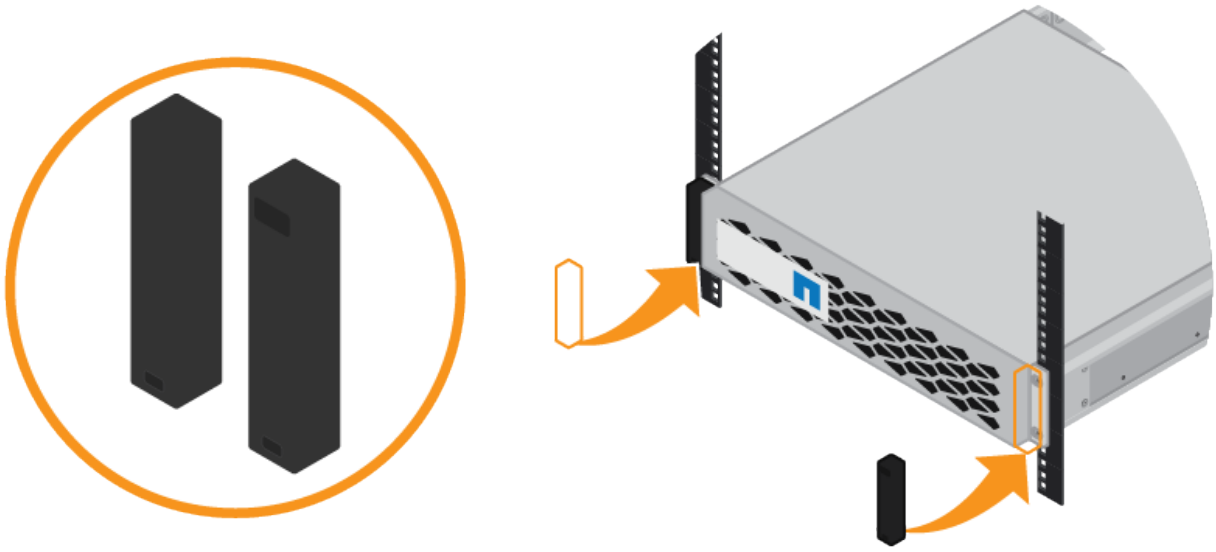
   Ne placez pas d'équipement supplémentaire sur les rails après avoir installé le boîtier. Les rails ne sont pas conçus pour supporter un poids supplémentaire.

   Le cas échéant, vous devrez peut-être retirer les capuchons d'extrémité du tiroir ou le cadre du système pour fixer le boîtier sur le montant du rack. Si oui, vous devez remplacer les caches d'extrémité ou le cadre lorsque vous avez terminé.

5. Fixez le boîtier à l'avant de l'armoire ou du rack et des rails en insérant deux vis M5 à travers les supports de montage (préinstallés de chaque côté de l'avant du boîtier), les trous du rack ou de l'armoire système et les trous à l'avant des rails.



6. Fixez le boîtier à l'arrière des rails en insérant deux vis M5 dans les supports du boîtier et du support du kit de rails.
7. Le cas échéant, remettez en place les caches d'extrémité des tablettes ou le cadre du système.



Installation du contrôleur SG6000-CN (SGSG6060 et SG6024)

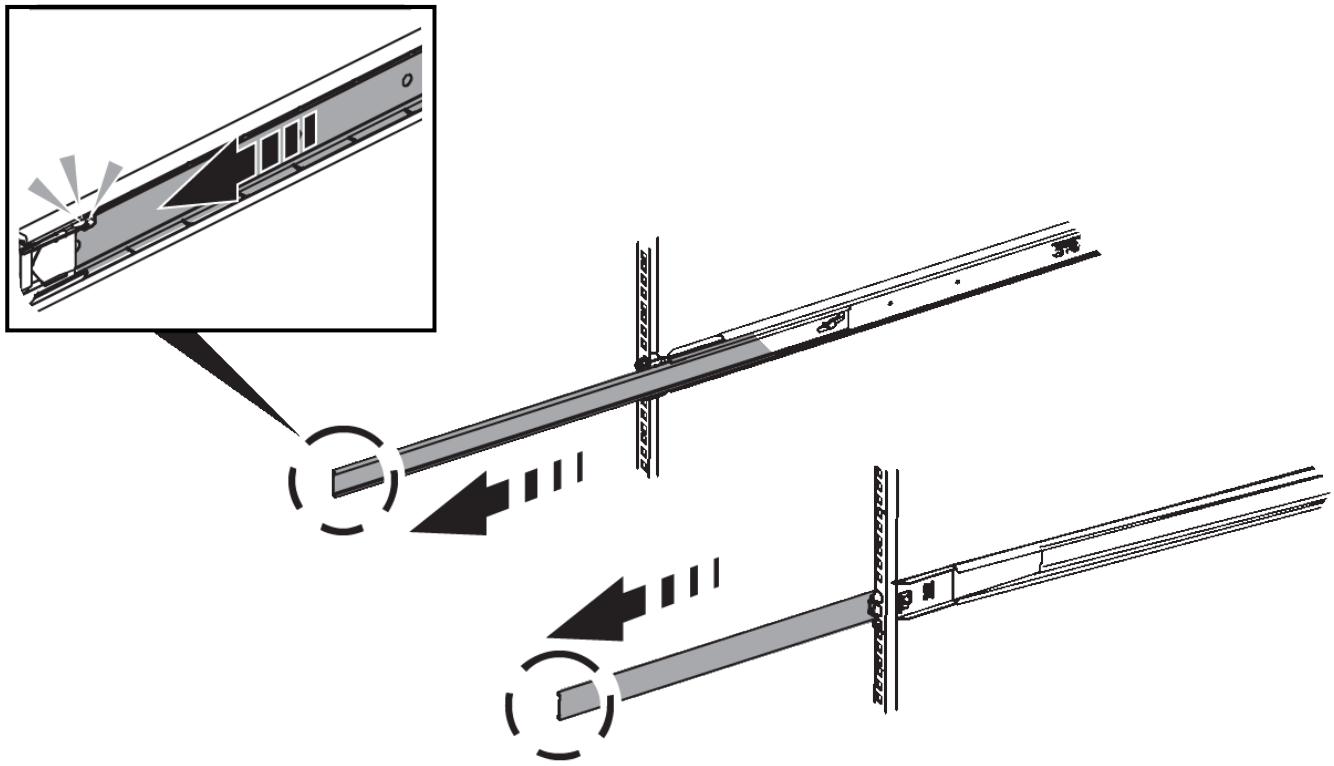
Vous installez un ensemble de rails pour le contrôleur SG6000-CN dans votre armoire ou rack, puis faites glisser le contrôleur sur les rails.

Avant de commencer

- Vous avez passé en revue le document consignes de sécurité inclus dans la boîte et compris les précautions à prendre pour déplacer et installer le matériel.
- Les instructions sont fournies avec le kit de rails.
- Vous avez installé le tiroir contrôleur E2860 et ses disques ou le tiroir contrôleur EF570.

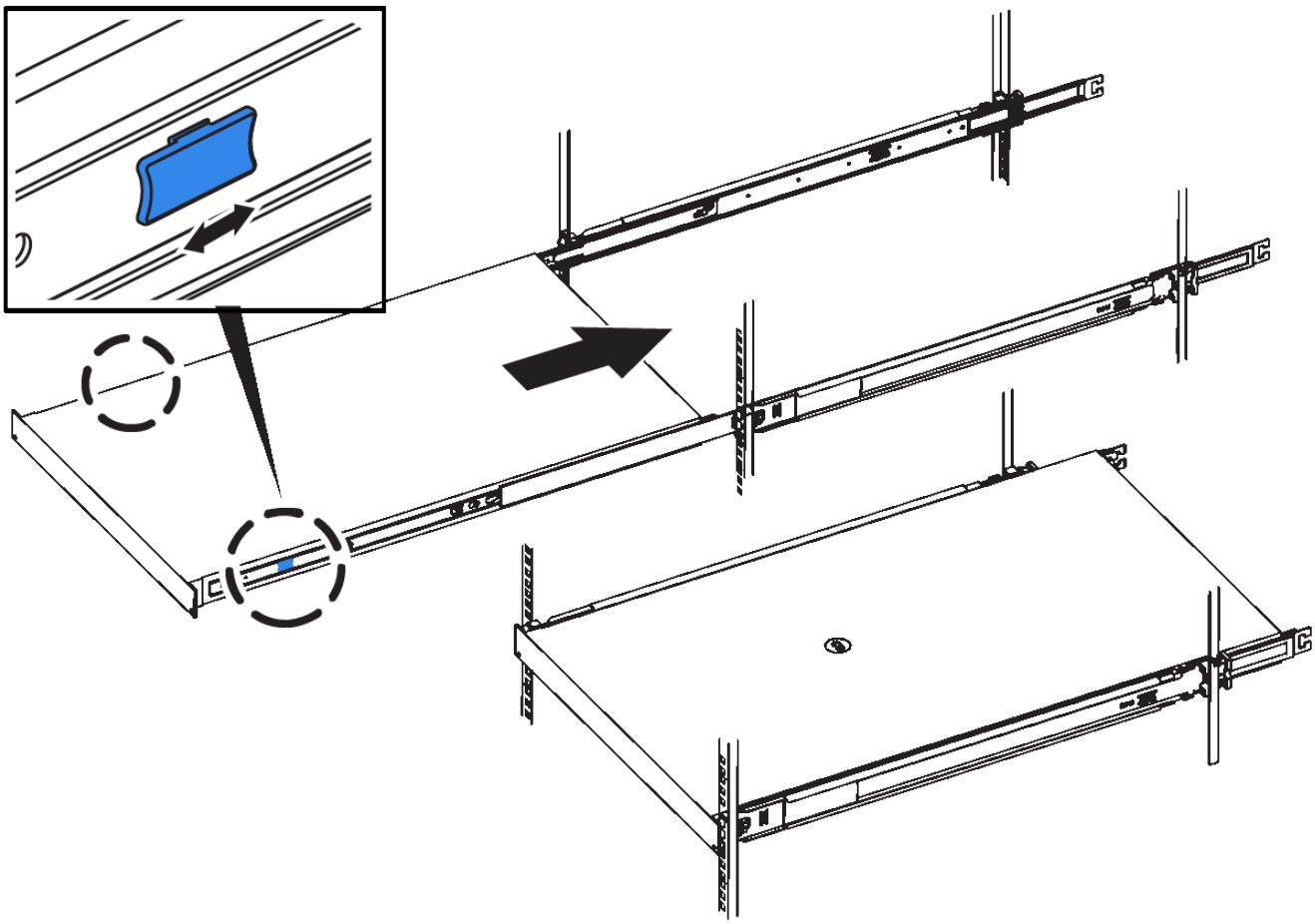
Étapes

1. Suivez attentivement les instructions du kit de rails pour installer les rails dans votre armoire ou rack.
2. Sur les deux rails installés dans l'armoire ou le rack, étendez les pièces mobiles des rails jusqu'à ce que vous entendiez un clic.



3. Insérez le contrôleur SG6000-CN dans les rails.
4. Faites glisser le contrôleur dans l’armoire ou le rack.

   Lorsque vous ne pouvez plus déplacer le contrôleur, tirez sur les loquets bleus des deux côtés du châssis pour faire glisser le contrôleur complètement vers l’intérieur.



Ne fixez le panneau avant qu'après la mise sous tension du contrôleur.

5. Serrez les vis imperdables du panneau avant du contrôleur pour fixer le contrôleur dans le rack.

Installation dans l'armoire ou le rack (SG5700)

Vous installez un ensemble de rails dans votre armoire ou rack, puis faites glisser l'appareil sur les rails. Si vous disposez d'un SG5760, installez les lecteurs après l'installation de l'appliance.

Avant de commencer

- Vous avez passé en revue le document consignes de sécurité inclus dans la boîte et compris les précautions à prendre pour déplacer et installer le matériel.
- Les instructions sont fournies avec le kit de rails.

Installer SG5712

Procédez comme suit pour installer une appliance SG5712 dans un rack ou une armoire.

Le SG5712 pèse environ 29 kg (64 lb) lorsqu'il est entièrement chargé avec des disques. Deux personnes ou un dispositif de levage mécanisé sont nécessaires pour déplacer le SG5712 en toute sécurité.

Installez le matériel depuis le bas du rack ou de l'armoire, ou montez le rack pour éviter que l'équipement ne bascule.

Étapes

1. Suivez les instructions du kit de rails pour installer les rails.
2. Placez l'arrière de l'appareil (l'extrémité avec les connecteurs) sur les rails.
3. Faites glisser avec précaution l'appareil jusqu'au fond de l'armoire ou du rack.
4. Fixez l'appareil à l'armoire ou au rack conformément aux instructions du kit de rails.
5. Fixez le panneau à l'avant.

Installer SG5760

Suivez ces étapes pour installer une appliance SG5760 et tout tiroir d'extension dans un rack ou une armoire.

Installez le matériel depuis le bas du rack ou de l'armoire, ou montez le rack pour éviter que l'équipement ne bascule.

Le SG5760 pèse environ 60 kg (132 lb) et n'a pas de disque installé. Quatre personnes ou un dispositif de levage mécanisé sont nécessaires pour déplacer en toute sécurité un SG5760 vide.

Pour éviter d'endommager le matériel, ne déplacez jamais un SG5760 si des lecteurs sont installés. Vous devez retirer tous les disques avant de déplacer le tiroir.

Étapes

1. Suivez les instructions du kit de rails pour installer les rails dans votre armoire ou rack.
2. Préparez-vous à déplacer l'appareil :
   a. Retirez la boîte d'emballage extérieure.
   b. Pliez les rabats de la boîte intérieure vers le bas.
   c. Si vous soulevez le SG5760 à la main, fixez les quatre poignées sur les côtés du châssis.

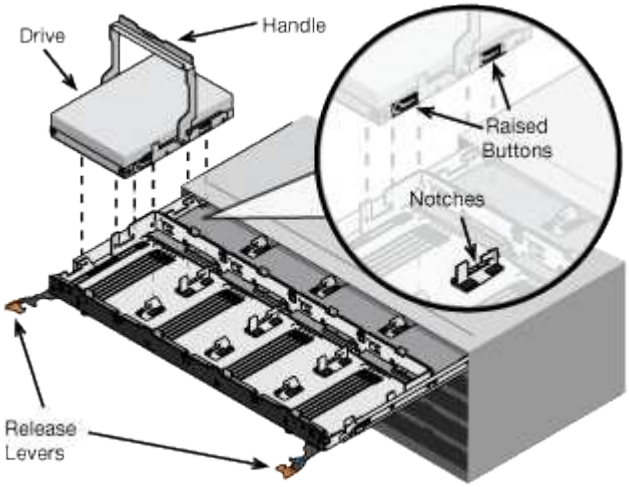
      Vous retirez ces poignées lorsque vous faites glisser l'appareil sur les rails.
3. Si votre armoire est dotée d'un trou carré, installez les écrous de cage de manière à pouvoir fixer l'avant et l'arrière du shelf à l'aide de vis.
4. Placez l'arrière de l'appareil (l'extrémité avec les connecteurs) sur les rails.
5. Tout en maintenant l'appareil par le bas, faites-le glisser dans le rack ou l'armoire.

   Utilisez les loquets pour retirer les poignées lorsque vous faites glisser l'appareil.
6. Fixez l'appareil à l'avant du rack en insérant deux vis dans le premier et le troisième trou (en partant du haut) de chaque côté.
7. Fixez l'appareil à l'arrière du rack ou de l'armoire à l'aide des supports.

8. Installez 12 disques dans chacun des cinq tiroirs.

   Vous devez installer les 60 disques pour assurer le bon fonctionnement.

   a. Placez le bracelet antistatique et retirez les lecteurs de leur emballage.
   b. Relâchez les leviers du tiroir d'entraînement supérieur et faites glisser le tiroir vers l'extérieur à l'aide des leviers.
   c. Relevez la poignée du lecteur à la verticale et alignez les boutons du lecteur avec les encoches du tiroir.



   d. Appuyez doucement sur le haut du lecteur, faites pivoter la poignée du lecteur vers le bas jusqu'à ce qu'il s'enclenche.
   e. Après avoir installé les 12 premiers lecteurs, faites glisser le tiroir vers l'intérieur en poussant sur le centre et en fermant doucement les deux leviers.
   f. Répétez ces étapes pour les quatre autres tiroirs.

9. Fixez le cadre avant.

Installation dans l'armoire ou le rack (SG100 et SG1000)

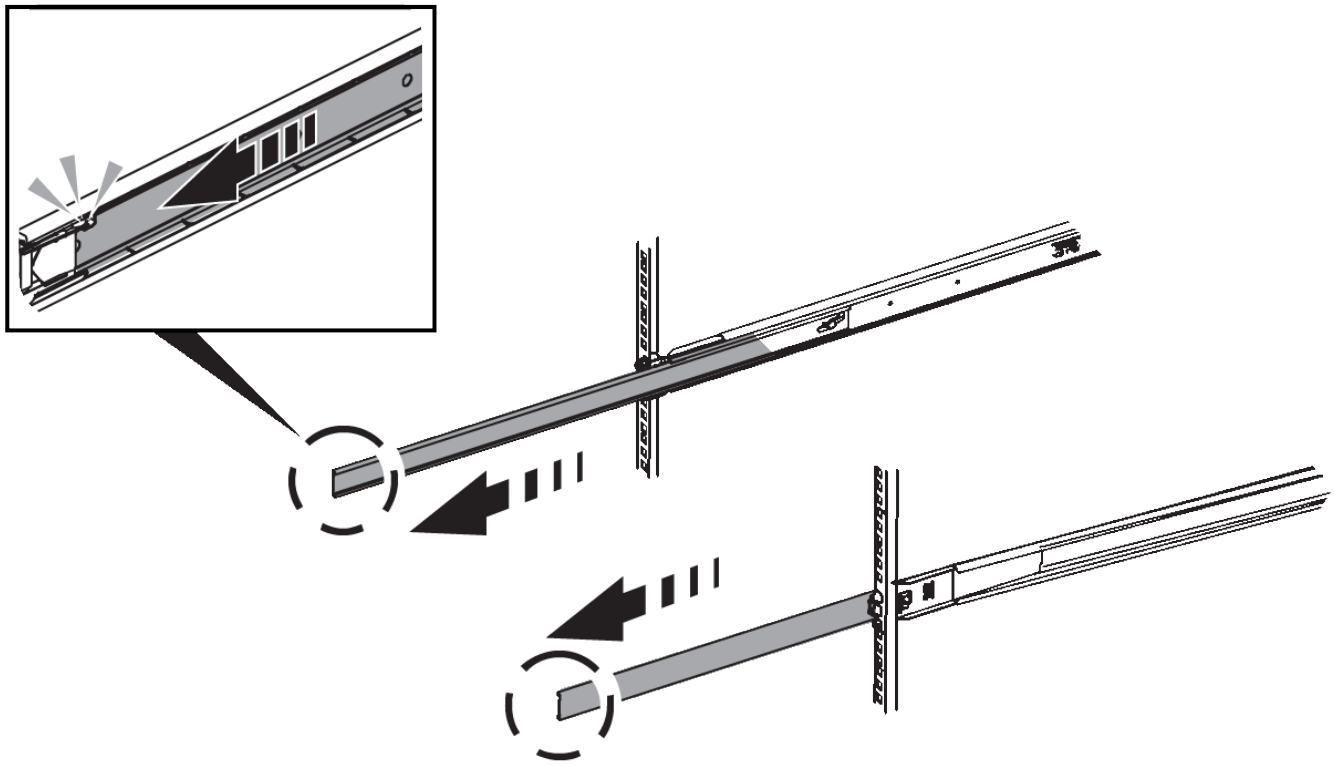
Vous installez un ensemble de rails pour l'appareil dans votre armoire ou rack, puis faites glisser l'appareil sur les rails.

Avant de commencer

- Vous avez passé en revue le document consignes de sécurité inclus dans la boîte et compris les précautions à prendre pour déplacer et installer le matériel.
- Les instructions sont fournies avec le kit de rails.

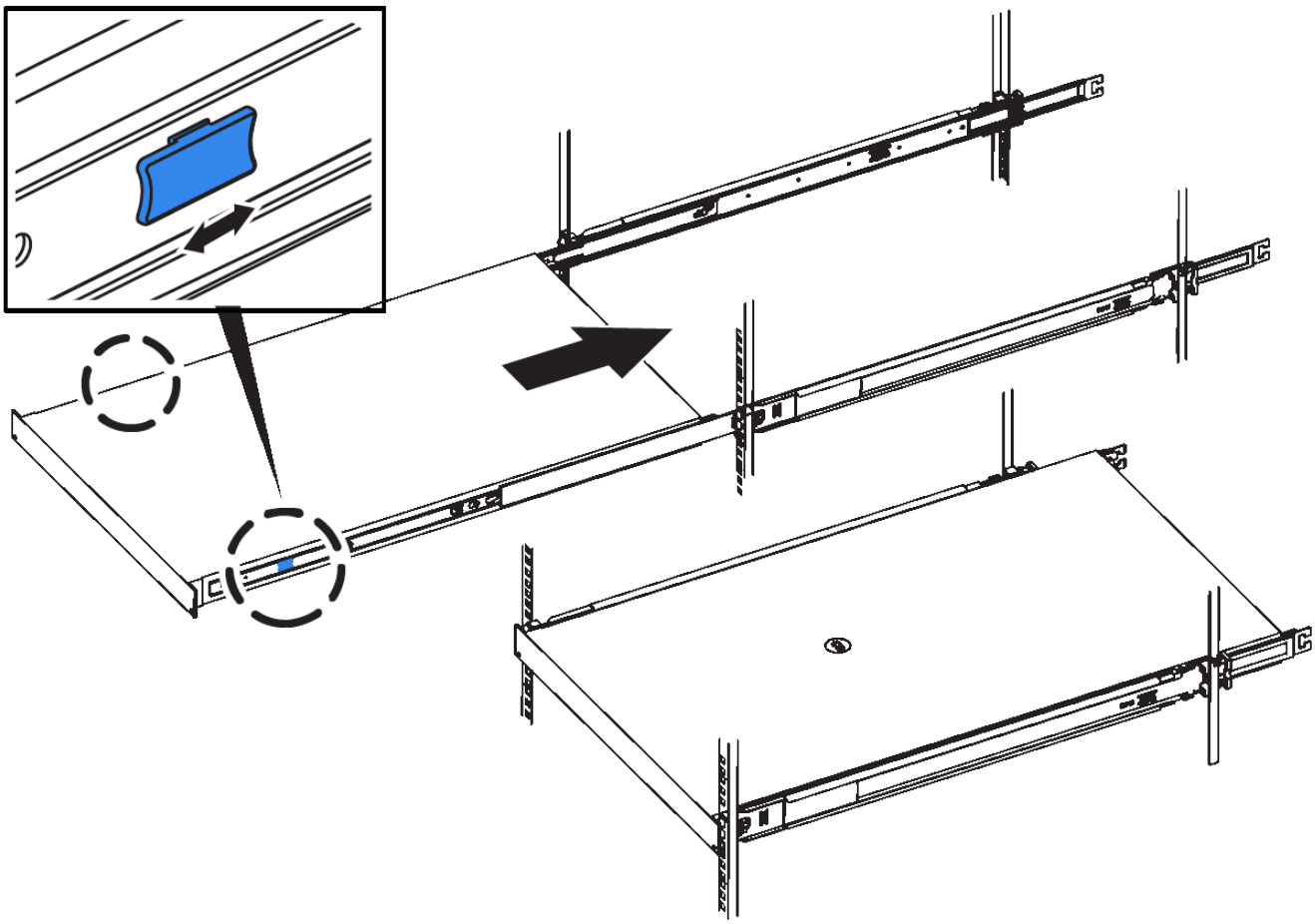
Étapes

1. Suivez attentivement les instructions du kit de rails pour installer les rails dans votre armoire ou rack.
2. Sur les deux rails installés dans l'armoire ou le rack, étendez les pièces mobiles des rails jusqu'à ce que vous entendiez un clic.



3. Insérez l’appareil dans les rails.
4. Faites glisser l’appareil dans l’armoire ou le rack.

   Lorsque vous ne pouvez plus déplacer l’appareil, tirez sur les loquets bleus des deux côtés du châssis pour faire glisser l’appareil complètement vers l’intérieur.



Ne fixez le cadre avant qu'après avoir mis l'appareil sous tension.

Appareil câblé

Cable appliance (SGF6112)

Vous connectez le port de gestion de l'appliance à l'ordinateur portable de service et connectez les ports réseau de l'appliance au réseau de réseau et au réseau client en option pour StorageGRID.

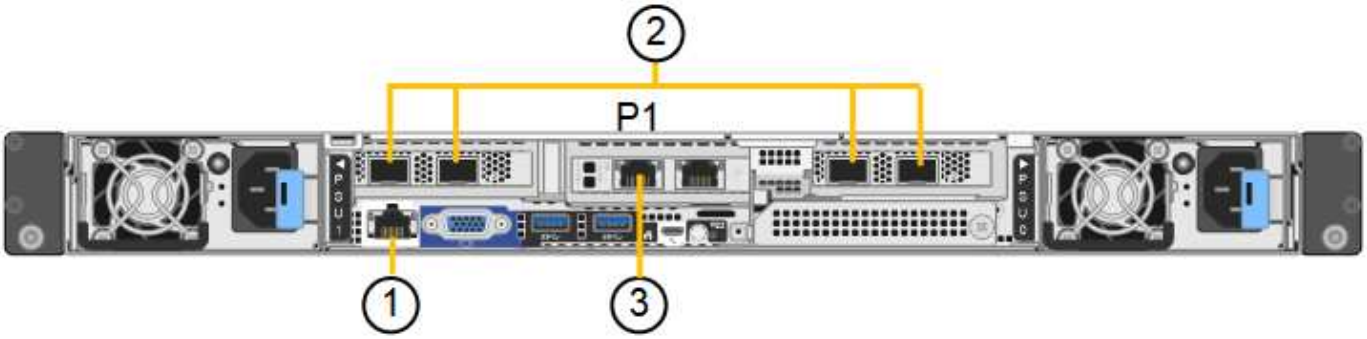
Avant de commencer

- Vous disposez d'un câble Ethernet RJ-45 pour connecter le port de gestion.
- Vous avez l'une des options suivantes pour les ports réseau. Ces éléments ne sont pas fournis avec l'appareil.
  - Un à quatre câbles TwinAx pour la connexion des quatre ports réseau.
  - Un à quatre émetteurs-récepteurs SFP+ ou SFP28 si vous prévoyez d'utiliser des câbles optiques pour les ports.

Risque d'exposition au rayonnement laser — ne démontez ou ne retirez aucune partie d'un émetteur-récepteur SFP. Vous pourriez être exposé à un rayonnement laser.

Description de la tâche

Les figures suivantes illustrent les ports situés à l'arrière du SGF6112.



Légende	Port	Type de port	Utiliser
1	Port de gestion BMC de l'appliance	1 GbE (RJ-45)	Se connecte au réseau sur lequel vous accédez à l'interface BMC.
2	Quatre ports réseau 10/25-GbE sur l'appliance		Connectez-vous au réseau Grid et au réseau client pour StorageGRID.
3	Port réseau d'administration de l'appliance (étiqueté P1 dans la figure)	1 GbE (RJ-45) **Important:** ce port fonctionne uniquement à 1/10-GbE (RJ-45) et ne prend pas en charge les vitesses de 100 mégabits.	Permet de connecter l'appliance au réseau d'administration pour StorageGRID.
	Port RJ-45 le plus à droite de l'appareil	1 GbE (RJ-45) **Important:** ce port fonctionne uniquement à 1/10-GbE (RJ-45) et ne prend pas en charge les vitesses de 100 mégabits.	• Peut être lié avec le port de gestion 1 si vous souhaitez établir une connexion redondante avec le réseau d'administration. • Peut être laissée déconnectée et disponible pour l'accès local temporaire (IP 169.254.0.1). • Pendant l'installation, peut être utilisé pour connecter l'appliance à un ordinateur portable de service si les adresses IP attribuées par DHCP ne sont pas disponibles.

Étapes

1. Connectez le port de gestion BMC de l'appliance au réseau de gestion à l'aide d'un câble Ethernet.

   Bien que cette connexion soit facultative, elle est recommandée pour faciliter l'assistance.

2. Connectez les ports réseau de l'appareil aux commutateurs réseau appropriés à l'aide de câbles TwinAx ou de câbles optiques et d'émetteurs-récepteurs.

Les quatre ports réseau doivent utiliser la même vitesse de liaison.

Vitesse de liaison SGF6112 (GbE)	Équipement requis
10	Émetteur-récepteur SFP+
25	Émetteur-récepteur SFP28

- Si vous prévoyez d'utiliser le mode de liaison de port fixe (par défaut), connectez les ports aux réseaux StorageGRID Grid et client, comme indiqué dans le tableau.

Port	Se connecte à…
Orifice 1	Réseau client (facultatif)
Orifice 2	Réseau Grid
Orifice 3	Réseau client (facultatif)
Orifice 4	Réseau Grid

- Si vous prévoyez d'utiliser le mode de liaison du port de l'agrégat, connectez un ou plusieurs ports réseau à un ou plusieurs commutateurs. Vous devez connecter au moins deux des quatre ports pour éviter d'avoir un point de défaillance unique. Si vous utilisez plusieurs switchs pour une liaison LACP unique, les switchs doivent prendre en charge MLAG ou équivalent.

3. Si vous envisagez d'utiliser le réseau d'administration pour StorageGRID, connectez le port réseau d'administration de l'appliance au réseau d'administration à l'aide d'un câble Ethernet.

Cable appliance (SG6000)

Vous connectez les contrôleurs de stockage au contrôleur SG6000-CN, connectez les ports de gestion des trois contrôleurs et connectez les ports réseau du contrôleur SG6000-CN au réseau Grid et au réseau client en option pour StorageGRID.

Avant de commencer

- Les quatre câbles optiques fournis avec l'appareil permettent de connecter les deux contrôleurs de stockage au contrôleur SG6000-CN.
- Vous disposez de câbles Ethernet RJ-45 (quatre minimum) pour connecter les ports de gestion.
- Vous avez l'une des options suivantes pour les ports réseau. Ces éléments ne sont pas fournis avec l'appareil.
  - Un à quatre câbles TwinAx pour la connexion des quatre ports réseau.
  - Un à quatre émetteurs-récepteurs SFP+ ou SFP28 si vous prévoyez d'utiliser des câbles optiques pour les ports.

Risque d'exposition au rayonnement laser — ne démontez ou ne retirez aucune partie d'un émetteur-récepteur SFP. Vous pourriez être exposé à un rayonnement laser.

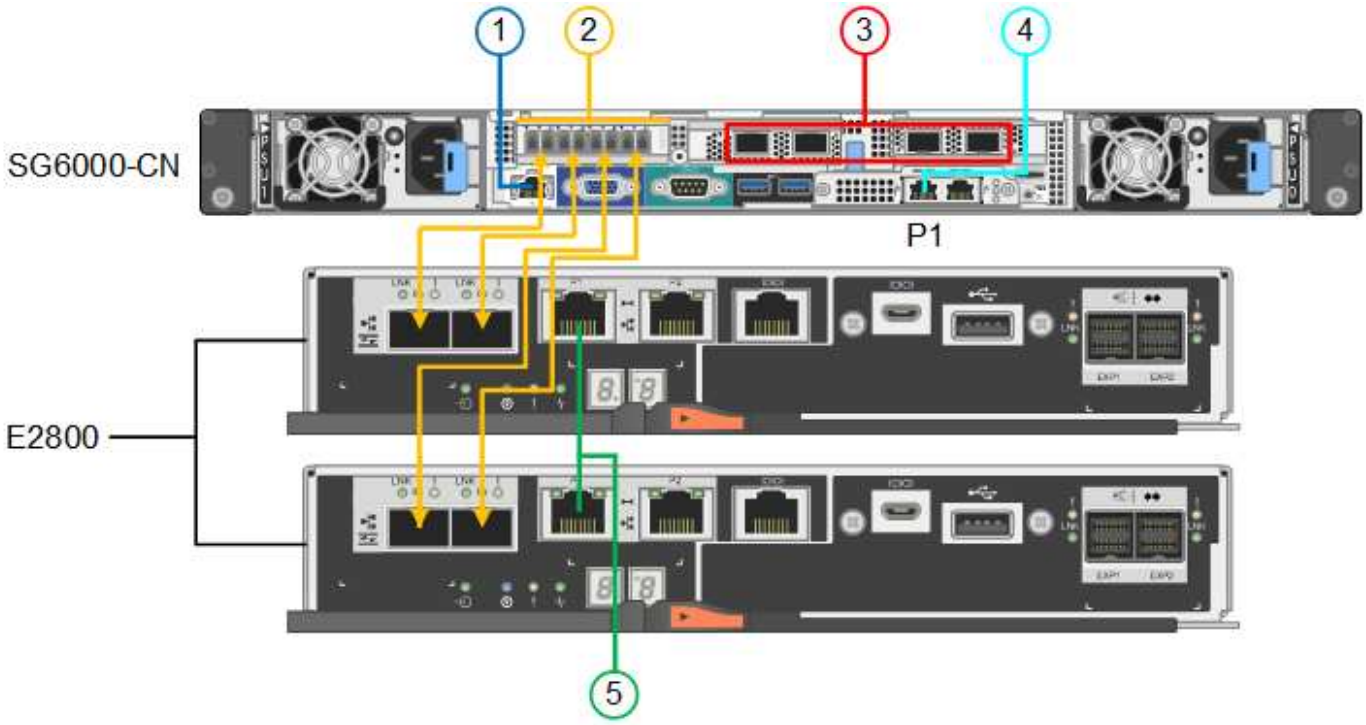
Description de la tâche

Les figures suivantes illustrent les trois contrôleurs des appliances SG6060 et SG6060X, avec le contrôleur de calcul SG6000-CN en haut et les deux contrôleurs de stockage E2800 en bas. Le SG6060 utilise des contrôleurs E2800A et le SG606060X utilise des contrôleurs E2800B.

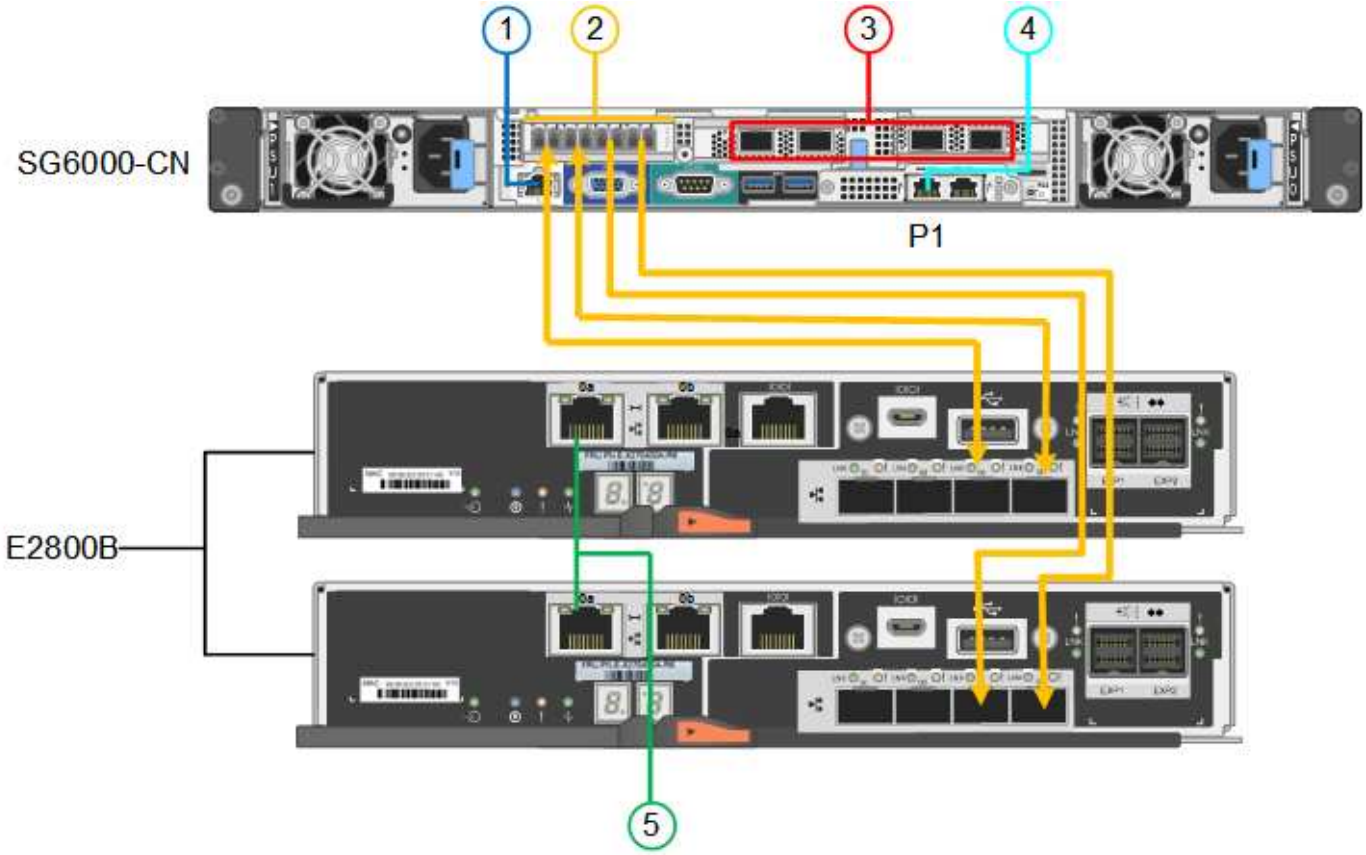
Les deux versions du contrôleur E2800 présentent les mêmes spécifications et fonctionnent, à l'exception de l'emplacement des ports d'interconnexion.

N'utilisez pas de contrôleur E2800A et E2800B dans le même appareil.

Connexions SG6060 :

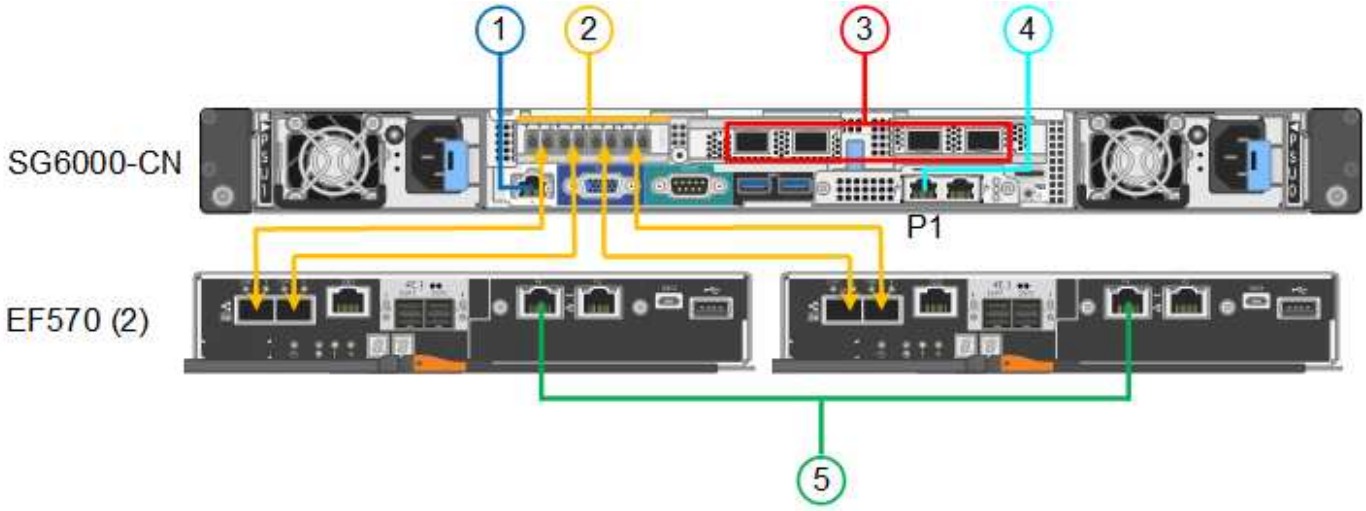


Connexions SG606060X :



La figure suivante présente les trois contrôleurs de l'appliance SGF6024, avec le contrôleur de calcul SG6000-CN en haut et les deux contrôleurs de stockage EF570 en dessous du contrôleur de calcul.

Connexions SGF6024 :



Légende	Port	Type de port	Utiliser
1	Port de gestion BMC sur le contrôleur SG6000-CN	1 GbE (RJ-45)	Se connecte au réseau sur lequel vous accédez à l'interface BMC.

Légende	Port	Type de port	Utiliser
2	Ports de connexion FC : • 4 sur le contrôleur SG6000-CN • 2 sur chaque contrôleur de stockage	SFP+ optique FC 16 Gbit/s	Connectez chaque contrôleur de stockage au contrôleur SG6000-CN.
3	Quatre ports réseau sur le contrôleur SG6000-CN	10/25 GbE	Connectez-vous au réseau Grid et au réseau client pour StorageGRID.
4	Port réseau d'administration du contrôleur SG6000-CN (étiqueté P1 dans la figure)	1 GbE (RJ-45) **Important :** ce port fonctionne uniquement à 1000 BaseT/full et ne prend pas en charge les vitesses de 10 ou 100 mégabits.	Permet de connecter le contrôleur SG6000-CN au réseau Admin pour StorageGRID.
	Port RJ-45 le plus à droite du contrôleur SG6000-CN	1 GbE (RJ-45) **Important :** ce port fonctionne uniquement à 1000 BaseT/full et ne prend pas en charge les vitesses de 10 ou 100 mégabits.	• Peut être lié avec le port de gestion 1 si vous souhaitez établir une connexion redondante avec le réseau d'administration. • Peut être laissé sans fil et disponible pour un accès local temporaire (IP 169.254.0.1). • Pendant l'installation, peut être utilisé pour connecter le contrôleur SG6000-CN à un ordinateur portable de service si les adresses IP attribuées par DHCP ne sont pas disponibles.
5	Le port de gestion 1 de chaque contrôleur de stockage	1 GbE (RJ-45)	Connexion au réseau sur lequel vous accédez à SANtricity System Manager.
	Port de gestion 2 sur chaque contrôleur de stockage	1 GbE (RJ-45)	Réservé au support technique.

Étapes

1. Connectez le port de gestion BMC du contrôleur SG6000-CN au réseau de gestion à l'aide d'un câble Ethernet.

   Bien que cette connexion soit facultative, elle est recommandée pour faciliter l'assistance.

2. Connectez les deux ports FC de chaque contrôleur de stockage aux ports FC du contrôleur SG6000-CN, à l'aide de quatre câbles optiques et de quatre émetteurs-récepteurs SFP+ pour les contrôleurs de stockage.
3. Connectez les ports réseau du contrôleur SG6000-CN aux commutateurs réseau appropriés, à l'aide de câbles TwinAx ou de câbles optiques et d'émetteurs-récepteurs SFP+ ou SFP28.

> Les quatre ports réseau doivent utiliser la même vitesse de liaison. Installez des émetteurs-récepteurs SFP+ si vous prévoyez d'utiliser des vitesses de liaison 10 GbE. Installez des émetteurs-récepteurs SFP28 si vous prévoyez d'utiliser des vitesses de liaison 25 GbE.

   - Si vous prévoyez d'utiliser le mode de liaison de port fixe (par défaut), connectez les ports aux réseaux StorageGRID Grid et client, comme indiqué dans le tableau.

Port	Se connecte à…
Orifice 1	Réseau client (facultatif)
Orifice 2	Réseau Grid
Orifice 3	Réseau client (facultatif)
Orifice 4	Réseau Grid

   - Si vous prévoyez d'utiliser le mode de liaison du port de l'agrégat, connectez un ou plusieurs ports réseau à un ou plusieurs commutateurs. Vous devez connecter au moins deux des quatre ports pour éviter d'avoir un point de défaillance unique. Si vous utilisez plusieurs switchs pour une liaison LACP unique, les switchs doivent prendre en charge MLAG ou équivalent.
4. Si vous prévoyez d'utiliser le réseau d'administration pour StorageGRID, connectez le port réseau d'administration du contrôleur SG6000-CN au réseau d'administration à l'aide d'un câble Ethernet.
5. Si vous prévoyez d'utiliser le réseau de gestion pour le Gestionnaire système SANtricity, connectez le port de gestion 1 (P1) de chaque contrôleur de stockage (le port RJ-45 de gauche) au réseau de gestion pour le Gestionnaire système SANtricity, à l'aide d'un câble Ethernet.

   N'utilisez pas le port de gestion 2 (P2) sur les contrôleurs de stockage (le port RJ-45 sur la droite). Ce port est réservé au support technique.

Informations associées

"Modes de liaison du port (contrôleur SG6000-CN)"

Appliance pour câble (SG5700)

Vous connectez les deux contrôleurs, connectez les ports de gestion de chaque contrôleur et connectez les ports 10/25-GbE du contrôleur E5700SG au réseau Grid et au réseau client en option pour StorageGRID.

Avant de commencer

- Vous avez déballé les éléments suivants, fournis avec l'appareil :
  - Deux cordons d'alimentation.
  - Deux câbles optiques pour les ports d'interconnexion FC sur les contrôleurs.

- Huit émetteurs-récepteurs SFP+ prenant en charge le protocole FC 10 GbE ou 16 Gbit/s. Les émetteurs-récepteurs peuvent être utilisés avec les deux ports d'interconnexion des deux contrôleurs et avec les quatre ports réseau 10/25 GbE du contrôleur E5700SG, à condition que vous souhaitiez que les ports réseau utilisent une vitesse de liaison 10 GbE.

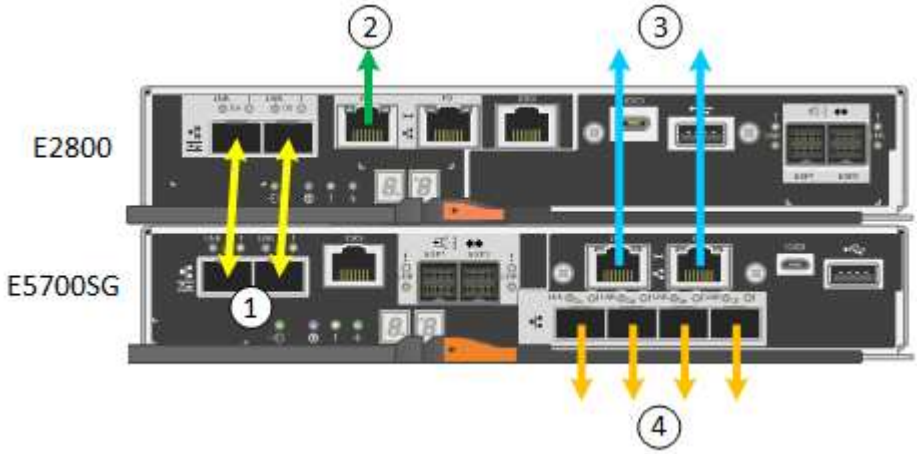
- Vous avez obtenu les éléments suivants, qui ne sont pas fournis avec l'appareil :
  - Un à quatre câbles optiques pour les ports 10/25 GbE que vous prévoyez d'utiliser.
  - Un à quatre émetteurs-récepteurs SFP28 si vous prévoyez d'utiliser une vitesse de liaison 25 GbE.
  - Câbles Ethernet pour la connexion des ports de gestion.

Risque d'exposition au rayonnement laser — ne démontez ou ne retirez aucune partie d'un émetteur-récepteur SFP. Vous pourriez être exposé à un rayonnement laser.

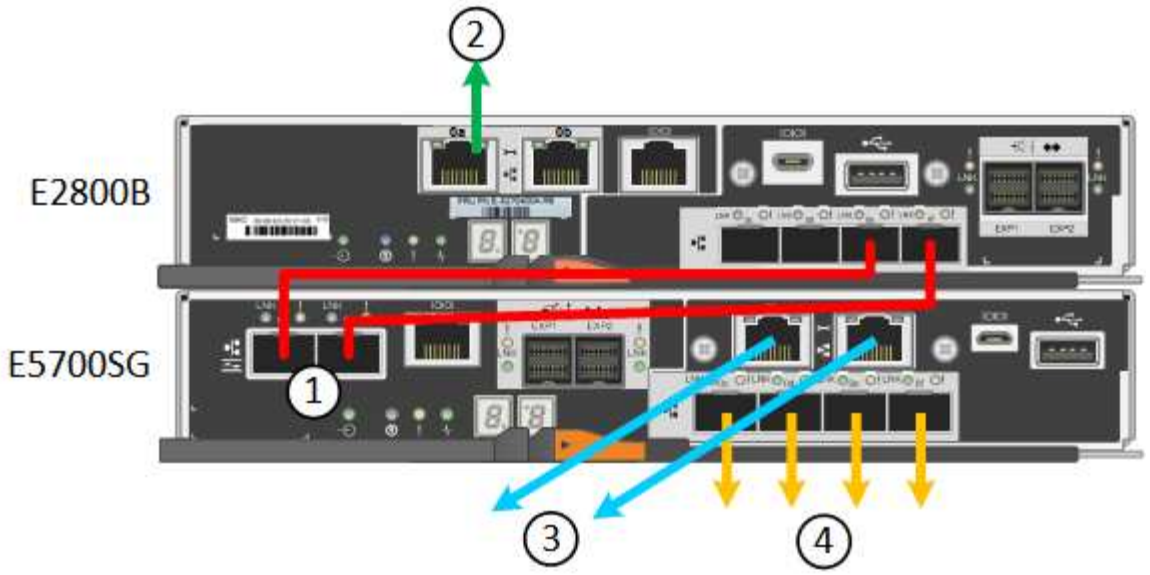
Description de la tâche

Les chiffres montrent les deux contrôleurs des modèles SG5760 et S260X, avec le contrôleur de stockage de la gamme E2800 en haut et le contrôleur E5700SG en bas. Dans le SG5712 et dans la résolution 12X, le contrôleur de stockage de la gamme E2800 se trouve à gauche du contrôleur E5700SG, lorsqu'il est vue depuis l'arrière.

Connexions SG5760 :



Connexions SG5760X :



Légende	Port	Type de port	Utiliser
1	Deux ports d'interconnexion sur chaque contrôleur	SFP+ optique 16 Gbit/s FC	Connectez les deux contrôleurs les uns aux autres.
2	Port de gestion 1 sur le contrôleur E2800 Series	1 GbE (RJ-45)	Connexion au réseau sur lequel vous accédez à SANtricity System Manager. Vous pouvez utiliser le réseau d'administration pour StorageGRID ou un réseau de gestion indépendant.
2	Port de gestion 2 sur le contrôleur E2800 Series	1 GbE (RJ-45)	Réservé au support technique.
3	Port de gestion 1 du contrôleur E5700SG	1 GbE (RJ-45)	Permet de connecter le contrôleur E5700SG au réseau d'administration pour StorageGRID.

Légende	Port	Type de port	Utiliser
3	Port de gestion 2 du contrôleur E5700SG	1 GbE (RJ-45)	• Peut être lié avec le port de gestion 1 si vous souhaitez établir une connexion redondante avec le réseau d'administration. • Peut être laissé sans fil et disponible pour un accès local temporaire (IP 169.254.0.1). • Lors de l'installation, peut être utilisé pour connecter le contrôleur E5700SG à un ordinateur portable de service si les adresses IP attribuées par DHCP ne sont pas disponibles.
4	Ports 10/25 GbE 1-4 sur le contrôleur E5700SG	10 GbE ou 25 GbE **Remarque :** les émetteurs-récepteurs SFP+ inclus avec l'appareil prennent en charge les vitesses de liaison 10 GbE. Si vous souhaitez utiliser des vitesses de liaison 25 GbE pour les quatre ports réseau, vous devez fournir des émetteurs-récepteurs SFP28.	Connectez-vous au réseau Grid et au réseau client pour StorageGRID. Voir "Modes de liaison des ports (contrôleur E5700SG)".

Étapes

1. Connectez le contrôleur E2800 au contrôleur E5700SG à l'aide de deux câbles optiques et de quatre des huit émetteurs-récepteurs SFP+.

Connecter ce port…	Vers ce port…
Port d'interconnexion 1 du contrôleur E2800	Port d'interconnexion 1 du contrôleur E5700SG
Port d'interconnexion 2 du contrôleur E2800	Port d'interconnexion 2 du contrôleur E5700SG

2. Si vous prévoyez d'utiliser SANtricity System Manager, connectez le port de gestion 1 (P1) du contrôleur E2800 (port RJ-45 de gauche) au réseau de gestion de SANtricity System Manager à l'aide d'un câble Ethernet.

   N'utilisez pas le port de gestion 2 (P2) du contrôleur E2800 (port RJ-45 sur la droite). Ce port est réservé au support technique.

3. Si vous avez l'intention d'utiliser le réseau d'administration pour StorageGRID, connectez le port de gestion

1 du contrôleur E5700SG (le port RJ-45 sur la gauche) au réseau d'administration à l'aide d'un câble Ethernet.

Si vous avez l'intention d'utiliser le mode de liaison réseau de sauvegarde active pour le réseau d'administration, connectez le port de gestion 2 du contrôleur E5700SG (le port RJ-45 sur la droite) au réseau d'administration à l'aide d'un câble Ethernet.

4. Connectez les ports 10/25 GbE du contrôleur E5700SG aux switchs réseau appropriés, à l'aide de câbles optiques et d'émetteurs-récepteurs SFP+ ou SFP28.

   Tous les ports doivent utiliser la même vitesse de liaison. Installez des émetteurs-récepteurs SFP+ si vous prévoyez d'utiliser des vitesses de liaison 10 GbE. Installez des émetteurs-récepteurs SFP28 si vous prévoyez d'utiliser des vitesses de liaison 25 GbE.

   - Si vous prévoyez d'utiliser le mode de liaison de port fixe (par défaut), connectez les ports aux réseaux StorageGRID Grid et client, comme indiqué dans le tableau.

Port	Se connecte à…
Orifice 1	Réseau client (facultatif)
Orifice 2	Réseau Grid
Orifice 3	Réseau client (facultatif)
Orifice 4	Réseau Grid

   - Si vous prévoyez d'utiliser le mode de liaison du port de l'agrégat, connectez un ou plusieurs ports réseau à un ou plusieurs commutateurs. Vous devez connecter au moins deux des quatre ports pour éviter d'avoir un point de défaillance unique. Si vous utilisez plusieurs switchs pour une liaison LACP unique, les switchs doivent prendre en charge MLAG ou équivalent.

Informations associées

"Accédez au programme d'installation de l'appliance StorageGRID"

Cable appliance (SG100 et SG1000)

Vous devez connecter le port de gestion de l'appliance à l'ordinateur portable de service et connecter les ports réseau de l'appliance au réseau Grid et au réseau client optionnel pour StorageGRID.

Avant de commencer

- Vous disposez d'un câble Ethernet RJ-45 pour connecter le port de gestion.
- Vous avez l'une des options suivantes pour les ports réseau. Ces éléments ne sont pas fournis avec l'appareil.
  - Un à quatre câbles TwinAx pour la connexion des quatre ports réseau.
  - Pour le SG100, un à quatre émetteurs-récepteurs SFP+ ou SFP28 si vous prévoyez d'utiliser des câbles optiques pour les ports.
  - Pour le SG1000, un à quatre émetteurs-récepteurs QSFP+ ou QSFP28 si vous prévoyez d'utiliser des

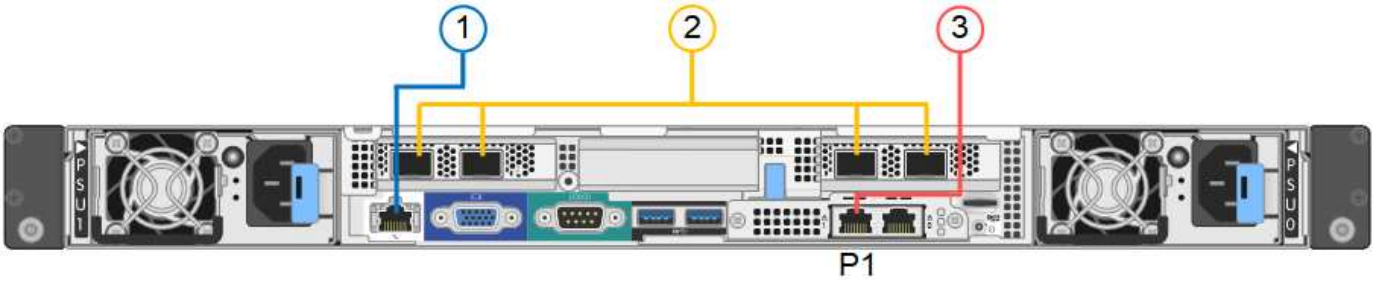
câbles optiques pour les ports.

Risque d'exposition au rayonnement laser — ne démontez ou ne retirez aucune partie d'un émetteur-récepteur SFP ou QSFP. Vous pourriez être exposé à un rayonnement laser.

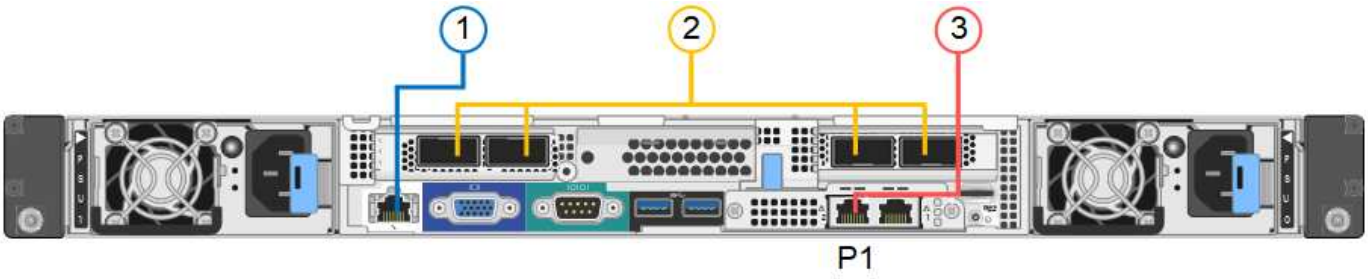
Description de la tâche

Les figures suivantes montrent les ports situés à l'arrière de l'appareil.

Connexions des ports SG100 :



Connexions du port SG1000 :



Légende	Port	Type de port	Utiliser
1	Port de gestion BMC de l'appliance	1 GbE (RJ-45)	Se connecte au réseau sur lequel vous accédez à l'interface BMC.
2	Quatre ports réseau sur l'appliance	• Pour le SG100 : 10/25-GbE • Pour le SG1000 : 10/25/40/100-GbE	Connectez-vous au réseau Grid et au réseau client pour StorageGRID.
3	Port réseau d'administration de l'appliance (étiqueté P1 dans les figures)	1 GbE (RJ-45) **Important :** ce port fonctionne uniquement à 1000 BaseT/full et ne prend pas en charge les vitesses de 10 ou 100 mégabits.	Permet de connecter l'appliance au réseau d'administration pour StorageGRID.

Légende	Port	Type de port	Utiliser
	Port RJ-45 le plus à droite de l'appareil	1 GbE (RJ-45) **Important :** ce port fonctionne uniquement à 1000 BaseT/full et ne prend pas en charge les vitesses de 10 ou 100 mégabits.	• Peut être lié avec le port de gestion 1 si vous souhaitez établir une connexion redondante avec le réseau d'administration. • Peut être laissée déconnectée et disponible pour l'accès local temporaire (IP 169.254.0.1). • Pendant l'installation, peut être utilisé pour connecter l'appliance à un ordinateur portable de service si les adresses IP attribuées par DHCP ne sont pas disponibles.

Étapes

1. Connectez le port de gestion BMC de l'appliance au réseau de gestion à l'aide d'un câble Ethernet.

   Bien que cette connexion soit facultative, elle est recommandée pour faciliter l'assistance.

2. Connectez les ports réseau de l'appareil aux commutateurs réseau appropriés à l'aide de câbles TwinAx ou de câbles optiques et d'émetteurs-récepteurs.

   Les quatre ports réseau doivent utiliser la même vitesse de liaison. Consultez le tableau suivant pour connaître l'équipement requis pour votre matériel et la vitesse de liaison.

Vitesse de liaison SG100 (GbE)	Équipement requis
10	Émetteur-récepteur SFP+
25	Émetteur-récepteur SFP28

Vitesse de liaison SG1000 (GbE)	Équipement requis
10	Emetteur-récepteur QSA et SFP+
25	Emetteur-récepteur QSA et SFP28
40	Émetteur-récepteur QSFP+
100	Emetteur-récepteur QFSP28

   - Si vous prévoyez d'utiliser le mode de liaison de port fixe (par défaut), connectez les ports aux réseaux StorageGRID Grid et client, comme indiqué dans le tableau.

Port	Se connecte à…
Orifice 1	Réseau client (facultatif)

Port	Se connecte à…
Orifice 2	Réseau Grid
Orifice 3	Réseau client (facultatif)
Orifice 4	Réseau Grid

- Si vous prévoyez d'utiliser le mode de liaison du port de l'agrégat, connectez un ou plusieurs ports réseau à un ou plusieurs commutateurs. Vous devez connecter au moins deux des quatre ports pour éviter d'avoir un point de défaillance unique. Si vous utilisez plusieurs switchs pour une liaison LACP unique, les switchs doivent prendre en charge MLAG ou équivalent.

3. Si vous envisagez d'utiliser le réseau d'administration pour StorageGRID, connectez le port réseau d'administration de l'appliance au réseau d'administration à l'aide d'un câble Ethernet.

Branchez les câbles d'alimentation et mettez le système sous tension

Branchement des câbles d'alimentation et mise sous tension (SGF6112)

Après avoir branché les câbles réseau, vous êtes prêt à alimenter l'appareil.

Étapes

1. Connectez un cordon d'alimentation à chacune des deux unités d'alimentation de l'appareil.
2. Branchez ces deux cordons d'alimentation à deux unités de distribution d'alimentation différentes dans l'armoire ou le rack.
3. Si le bouton d'alimentation situé à l'avant de l'appareil n'est pas allumé en bleu, appuyez sur le bouton pour mettre l'appareil sous tension.

   N'appuyez pas de nouveau sur le bouton d'alimentation pendant le processus de mise sous tension.

   Le voyant du bloc d'alimentation doit être allumé en vert sans clignoter.

4. En cas d'erreur, corrigez tout problème.
5. Si vous avez retiré le cadre avant, fixez-le à l'appareil.

Informations associées

"Afficher les indicateurs d'état"

Branchement des câbles d'alimentation et alimentation (SG6000)

Une fois les câbles réseau connectés, vous pouvez alimenter le contrôleur SG6000-CN et les deux contrôleurs de stockage ou les tiroirs d'extension en option.

Étapes

1. Vérifier que les deux contrôleurs du tiroir de contrôleur de stockage sont éteints

Risque d'électrocution — avant de connecter les cordons d'alimentation, assurez-vous que les interrupteurs d'alimentation de chacun des deux contrôleurs de stockage sont éteints.

2. Si vous disposez de tiroirs d'extension, vérifiez que les deux boutons d'alimentation du module sont éteints.

> **Risque d'électrocution** — avant de connecter les cordons d'alimentation, assurez-vous que les deux commutateurs d'alimentation de chacun des étagères d'extension sont éteints.

3. Connectez un cordon d'alimentation à chacune des deux unités d'alimentation du contrôleur SG6000-CN.
4. Branchez ces deux cordons d'alimentation à deux unités de distribution d'alimentation différentes dans l'armoire ou le rack.
5. Connectez un cordon d'alimentation à chacune des deux unités d'alimentation du tiroir de contrôleur de stockage.
6. Si vous disposez de tiroirs d'extension, connectez un cordon d'alimentation à chacune des deux unités d'alimentation de chaque tiroir d'extension.
7. Connectez les deux câbles d'alimentation de chaque tiroir de stockage (y compris les tiroirs d'extension en option) à deux unités PDU différentes dans l'armoire ou le rack.
8. Si le bouton d'alimentation situé à l'avant du contrôleur SG6000-CN n'est pas actuellement allumé en bleu, appuyez sur le bouton pour mettre le contrôleur sous tension.

   N'appuyez pas de nouveau sur le bouton d'alimentation pendant le processus de mise sous tension.

9. Allumer les deux boutons d'alimentation à l'arrière du tiroir du contrôleur de stockage. Si vous avez des tiroirs d'extension, mettez les deux commutateurs d'alimentation sur tension pour chaque tiroir.
   - N'éteignez pas les interrupteurs d'alimentation pendant le processus de mise sous tension.
   - Au premier démarrage, les ventilateurs du tiroir de contrôleur de stockage et les tiroirs d'extension en option peuvent être très bruyants. Le bruit est normal au démarrage.
10. Une fois les composants démarrés, vérifiez leur état.
    - Vérifiez l'affichage des sept segments à l'arrière de chaque contrôleur de stockage. Pour plus d'informations, reportez-vous à l'article sur l'affichage des codes d'état de démarrage.
    - Vérifiez que le bouton d'alimentation situé à l'avant du contrôleur SG6000-CN est allumé.
11. En cas d'erreur, corrigez tout problème.
12. Si vous avez déposé le cadre avant, fixez-le au contrôleur SG6000-CN.

Informations associées

- "Afficher les indicateurs d'état"
- "Réinstallez le contrôleur SG6000-CN dans l'armoire ou le rack"

Branchement des câbles d'alimentation et mise en œuvre de l'alimentation (SG5700)

Lorsque vous mettez l'appliance sous tension, les deux contrôleurs démarrent.

Avant de commencer

Les deux interrupteurs doivent être éteints avant de brancher l'appareil.

> **Risque d'électrocution** — avant de brancher les cordons d'alimentation, assurez-vous que les deux interrupteurs de l'appareil sont éteints.

Étapes

1. Vérifiez que les deux interrupteurs de l'appareil sont éteints.
2. Branchez les deux cordons d'alimentation à l'appareil.
3. Connectez les deux cordons d'alimentation à différentes unités de distribution de l'alimentation dans l'armoire ou le rack.
4. Allumez les deux interrupteurs de l'appareil.
   - N'éteignez pas les interrupteurs d'alimentation pendant le processus de mise sous tension.
   - Les ventilateurs sont très bruyants lors du premier démarrage. Le bruit est normal au démarrage.
5. Une fois les contrôleurs démarrés, vérifiez leur affichage à sept segments.

Branchement des câbles d'alimentation et application de l'alimentation (SG100 et SG1000)

Après avoir branché les câbles réseau, vous êtes prêt à alimenter l'appareil.

Étapes

1. Connectez un cordon d'alimentation à chacune des deux unités d'alimentation de l'appareil.
2. Branchez ces deux cordons d'alimentation à deux unités de distribution d'alimentation différentes dans l'armoire ou le rack.
3. Si le bouton d'alimentation situé à l'avant de l'appareil n'est pas allumé en bleu, appuyez sur le bouton pour mettre l'appareil sous tension.

   N'appuyez pas de nouveau sur le bouton d'alimentation pendant le processus de mise sous tension.
4. En cas d'erreur, corrigez tout problème.
5. Si vous avez retiré le cadre avant, fixez-le à l'appareil.

Informations associées

"Afficher les indicateurs d'état"

Afficher les indicateurs d'état et les codes

Les appareils et les contrôleurs comprennent des indicateurs qui vous aident à déterminer l'état des composants de l'appliance.

SGF6112

L'appliance inclut des indicateurs qui vous permettent de déterminer l'état du contrôleur de l'appliance et des disques SSD :

- Voyants et boutons de l'appareil
- Codes de démarrage généraux
- Indicateurs SSD

Utilisez ces informations pour vous aider "Dépanner l'installation matérielle du SGF6112".

Voyants et boutons de l'appareil

La figure suivante montre les voyants et les boutons de l'appareil SG6112.

Légende	Afficher	État
1	Bouton d'alimentation	• Bleu : l'appareil est sous tension. • Éteint : l'appareil est hors tension.
2	Bouton de réinitialisation	Utilisez ce bouton pour effectuer une réinitialisation matérielle du contrôleur.
3	Bouton identifier	A l'aide du contrôleur BMC, ce bouton peut être défini sur clignotant, activé (fixe) ou Désactivé. • Bleu clignotant : identifie l'appliance dans l'armoire ou le rack. • Bleu, fixe : identifie l'appliance dans l'armoire ou le rack. • Éteint : l'appareil n'est pas visuellement identifiable dans l'armoire ou le rack.
4	Voyant d'état	• Orange, fixe : une erreur s'est produite. **Note:** pour afficher les codes de démarrage et d'erreur, "Accédez à l'interface BMC". • OFF : aucune erreur n'est présente.
5	PFR	Ce voyant n'est pas utilisé par l'appareil SGF6112 et reste éteint.

Codes de démarrage généraux

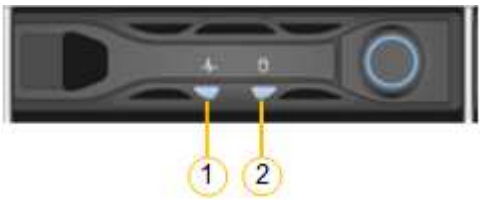
Lors du démarrage ou après une réinitialisation matérielle de l'appareil, les événements suivants se produisent :

1. Le contrôleur BMC (Baseboard Management Controller) consigne les codes de la séquence de démarrage, y compris les erreurs qui se produisent.
2. Le bouton d'alimentation s'allume.
3. Si des erreurs se produisent au démarrage, le voyant d'alarme s'allume.

   Pour afficher les codes de démarrage et d'erreur, "Accédez à l'interface BMC".

Indicateurs SSD

La figure suivante montre les voyants des disques SSD de l'appliance SG6112.



LED	Afficher	État
1	État/défaut du lecteur	• Bleu (continu) : le lecteur est en ligne • Orange (fixe) : panne de disque • OFF : l'emplacement est vide **Remarque :** si un nouveau disque SSD en fonctionnement est inséré dans un nœud StorageGRID SGF6112 en fonctionnement, les voyants du disque SSD doivent clignoter au début, mais cessent de clignoter dès que le système détermine que le disque dur a suffisamment de capacité et qu'il est fonctionnel.
2	Entraînement actif	Bleu (clignotant) : accès au lecteur

SG6000

Les contrôleurs de l'appliance SG6000 comprennent des indicateurs qui vous aident à déterminer l'état du contrôleur de l'appliance :

- Voyants et boutons d'état sur le contrôleur SG6000-CN
- Codes de démarrage généraux
- Codes d'état de démarrage pour les contrôleurs de stockage SG6000

Utilisez ces informations pour vous aider "Dépannage de l'installation du SG6000".

Voyants et boutons d'état sur le contrôleur SG6000-CN

Le contrôleur SG6000-CN comprend des indicateurs qui vous aident à déterminer l'état du contrôleur, y compris les voyants et boutons suivants.

La figure suivante montre les indicateurs d'état et les boutons du contrôleur SG6000-CN.

Légende	Afficher	Description
1	Bouton d'alimentation	• Bleu : le contrôleur est sous tension. • OFF : le contrôleur est hors tension.
2	Bouton de réinitialisation	*Aucun indicateur* Utilisez ce bouton pour effectuer une réinitialisation matérielle du contrôleur.
3	Bouton identifier	• Bleu clignotant ou fixe : identifie le contrôleur dans l'armoire ou le rack. • OFF : le contrôleur n'est pas visuellement identifiable dans l'armoire ou le rack. Ce bouton peut être configuré pour clignoter, allumé (continu) ou éteint.
4	Voyant d'alarme	• Orange : une erreur s'est produite. **Note:** pour afficher les codes de démarrage et d'erreur, "Accédez à l'interface BMC". • OFF : aucune erreur n'est présente.

Codes de démarrage généraux

Lors du démarrage ou après une réinitialisation matérielle du contrôleur SG6000-CN, les événements suivants se produisent :

1. Le contrôleur BMC (Baseboard Management Controller) consigne les codes de la séquence de démarrage, y compris les erreurs qui se produisent.
2. Le bouton d'alimentation s'allume.
3. Si des erreurs se produisent au démarrage, le voyant d'alarme s'allume.

   Pour afficher les codes de démarrage et d'erreur, "Accédez à l'interface BMC".

Codes d'état de démarrage pour les contrôleurs de stockage SG6000

Chaque contrôleur de stockage dispose d'un affichage à sept segments qui fournit des codes d'état lors

de la mise sous tension du contrôleur. Les codes d'état sont identiques pour le contrôleur E2800 et le contrôleur EF570.

Pour obtenir une description de ces codes, consultez les informations de surveillance du système E-Series pour votre type de contrôleur de stockage.

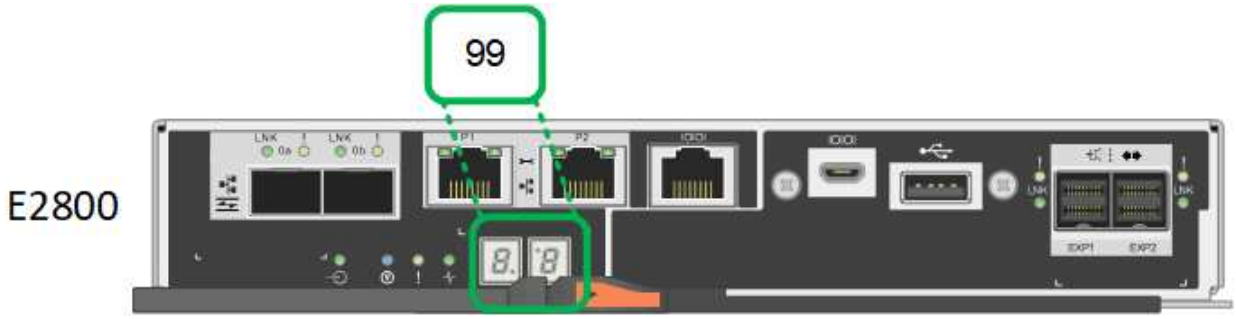
Étapes

1. Pendant le démarrage, surveillez la progression en affichant les codes affichés sur l'affichage à sept segments pour chaque contrôleur de stockage.

   L'affichage à sept segments sur chaque contrôleur de stockage indique la séquence répétée **OS**, **SD**, ***blank*** pour indiquer que le contrôleur exécute un traitement en début de journée.

2. Une fois les contrôleurs démarrés, vérifiez que chaque contrôleur de stockage indique 99, qui est l'ID par défaut d'un tiroir contrôleur E-Series.

   Vérifiez que cette valeur s'affiche sur les deux contrôleurs de stockage, comme illustré dans cet exemple.



3. Si l'un des contrôleurs ou les deux affichent d'autres valeurs, reportez-vous à la section "Dépannage de l'installation matérielle (SG6000 ou SG5700)" et confirmez que vous avez correctement effectué les étapes d'installation. Si vous ne parvenez pas à résoudre le problème, contactez le support technique.

Informations associées

- "Support NetApp"
- "Mettez le contrôleur SG6000-CN sous tension et vérifiez son fonctionnement"

SG5700

Les contrôleurs de l'appareil incluent des indicateurs qui vous aident à déterminer l'état du contrôleur de l'appareil :

- Codes d'état de démarrage de l'appliance SG5700
- Voyants d'état sur le contrôleur E5700SG
- Codes de démarrage généraux
- Codes de démarrage du contrôleur E5700SG
- Codes d'erreur du contrôleur E5700SG

Utilisez ces informations pour vous aider "Dépannez l'installation du matériel SG5700".

Codes d’état de démarrage de l’appliance SG5700

Les affichages à sept segments de chaque contrôleur affichent les codes d’état et d’erreur lors de la mise sous tension de l’appareil.

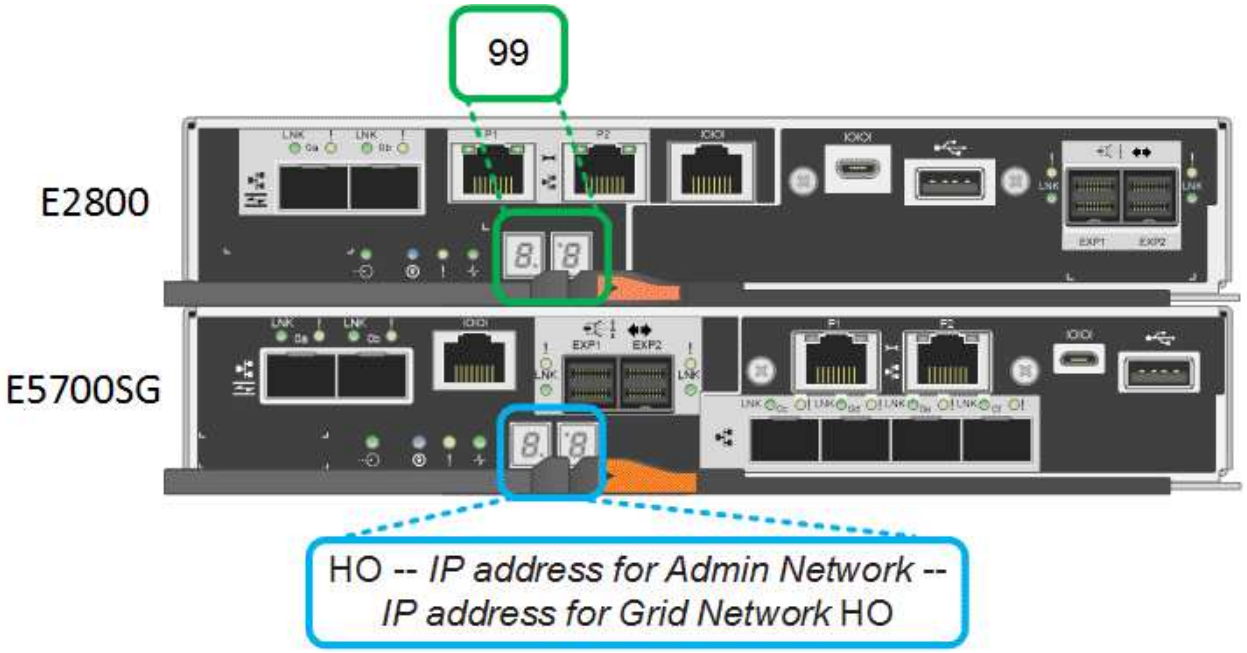
Le contrôleur E2800 et le contrôleur E5700SG affichent des États et des codes d’erreur différents.

Pour comprendre la signification de ces codes, consultez les ressources suivantes :

Contrôleur	Référence
Contrôleur E2800	*E5700 et E2800 System Monitoring Guide* **Remarque :** les codes répertoriés pour le contrôleur E-Series E5700 ne s’appliquent pas au contrôleur E5700SG de l’appliance.
Contrôleur E5700SG	"Indicateurs d’état sur le contrôleur E5700SG"

Étapes

1. Pendant le démarrage, surveillez la progression en affichant les codes affichés sur les affichages à sept segments.
   - L’écran à sept segments du contrôleur E2800 affiche la séquence répétée **OS**, **SD**, ***blank*** pour indiquer qu’il effectue un traitement en début de journée.
   - L’affichage à sept segments du contrôleur E5700SG montre une séquence de codes se terminant par **AA** et **FF**.
2. Une fois les contrôleurs démarrés, vérifiez que les sept segments affichent la valeur suivante :



Contrôleur	Affichage à sept segments
Contrôleur E2800	Indique 99, qui est l’ID par défaut d’un tiroir contrôleur E-Series.

Contrôleur	Affichage à sept segments
Contrôleur E5700SG	Affiche **HO**, suivie d'une séquence répétée de deux nombres. `HO -- IP address for Admin Network -- IP address for Grid Network HO` Dans la séquence, le premier jeu de chiffres est l'adresse IP attribuée par DHCP pour le port de gestion 1 du contrôleur. Cette adresse est utilisée pour connecter le contrôleur au réseau Admin pour StorageGRID. Le second jeu de chiffres est l'adresse IP attribuée par DHCP utilisée pour connecter l'appareil au réseau de grille pour StorageGRID. **Remarque :** si une adresse IP n'a pas pu être attribuée à l'aide de DHCP, 0.0.0.0 s'affiche.

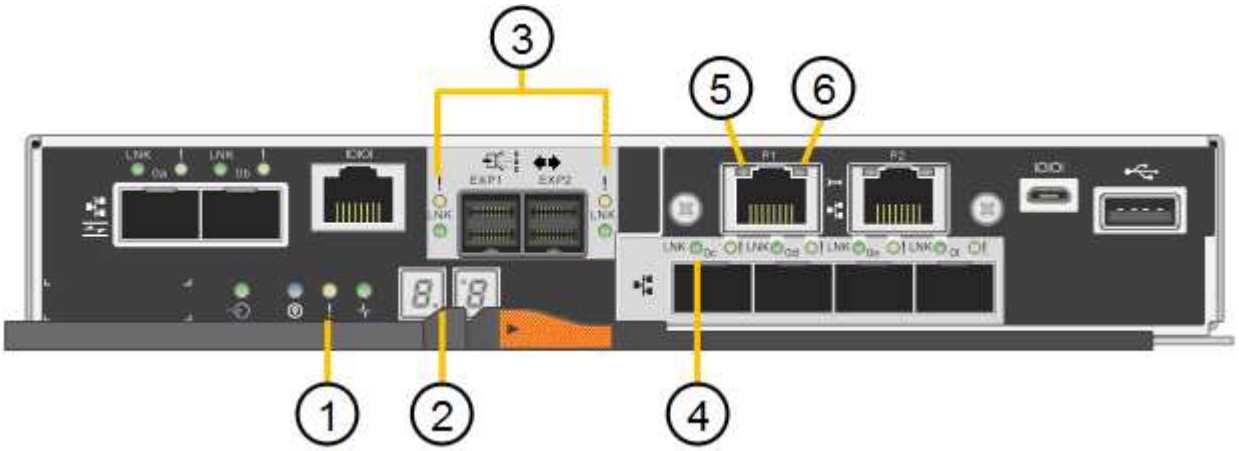
3. Si les affichages à sept segments affichent d'autres valeurs, voir "Dépannage de l'installation matérielle (SG6000 ou SG5700)" et confirmez que vous avez correctement effectué les étapes d'installation. Si vous ne parvenez pas à résoudre le problème, contactez le support technique.

Voyants d'état sur le contrôleur E5700SG

L'écran à sept segments et les voyants du contrôleur E5700SG indiquent les codes d'état et d'erreur pendant la mise sous tension et l'initialisation du matériel. Vous pouvez utiliser ces affichages pour déterminer l'état et résoudre les erreurs.

Une fois le programme d'installation de l'appliance StorageGRID démarré, il est conseillé de vérifier régulièrement les voyants d'état du contrôleur E5700SG.

La figure suivante présente les voyants d'état du contrôleur E5700SG.



Légende	Afficher	Description
1	LED d’avertissement	Orange : le contrôleur est défectueux et nécessite l’intervention de l’opérateur, ou le script d’installation est introuvable. OFF : le contrôleur fonctionne normalement.
2	Affichage à sept segments	Affiche un code de diagnostic Les séquences d’affichage à sept segments permettent de comprendre les erreurs et l’état de fonctionnement de l’appareil.
3	Voyants d’avertissement du port d’extension	Orange : ces voyants sont toujours orange (aucune liaison établie) car le dispositif n’utilise pas les ports d’extension.
4	Voyants d’état de la liaison du port hôte	Vert : le lien fonctionne. OFF : le lien ne fonctionne pas.
5	Voyants d’état de la liaison Ethernet	Vert : un lien est établi. Désactivé : aucun lien n’est établi.
6	LED d’activités Ethernet	Vert : la liaison entre le port de gestion et le périphérique auquel il est connecté (par exemple, un commutateur Ethernet) est active. Éteint : il n’y a pas de lien entre le contrôleur et le périphérique connecté. Vert clignotant : activité Ethernet.

Codes de démarrage généraux

Lors du démarrage ou après une réinitialisation matérielle de l’appareil, les événements suivants se produisent :

1. L’affichage à sept segments sur le contrôleur E5700SG montre une séquence générale de codes qui n’est pas spécifique au contrôleur. La séquence générale se termine par les codes AA et FF.
2. Les codes de démarrage spécifiques au contrôleur E5700SG apparaissent.

Codes de démarrage du contrôleur E5700SG

Lors d’un démarrage normal de l’appareil, l’écran à sept segments du contrôleur E5700SG affiche les codes suivants dans l’ordre indiqué :

Code	Indique
BONJOUR	Le script de démarrage principal a démarré.
PP	Le système vérifie si le FPGA doit être mis à jour.
HP	Le système vérifie si le micrologiciel du contrôleur 10/25-GbE doit être mis à jour.
RB	Le système redémarre après l'application des mises à jour du firmware.
FP	Les vérifications de mise à jour du micrologiciel du sous-système matériel sont terminées. Les services de communication inter-contrôleurs sont en cours de démarrage.
IL	Le système attend la connectivité avec le contrôleur E2800 et la synchronisation avec le système d'exploitation SANtricity. **Remarque :** si cette procédure de démarrage n'est pas en cours au-delà de cette étape, vérifier les connexions entre les deux contrôleurs.
PC	Le système recherche les données d'installation StorageGRID existantes.
HO	Le programme d'installation de l'appliance StorageGRID est en cours d'exécution.
HAUTE DISPONIBILITÉ	StorageGRID est en cours d'exécution.

Codes d'erreur du contrôleur E5700SG

Ces codes représentent des conditions d'erreur qui peuvent s'afficher sur le contrôleur E5700SG au démarrage de l'appareil. Des codes hexadécimaux supplémentaires à deux chiffres sont affichés si des erreurs matérielles spécifiques de bas niveau se produisent. Si l'un de ces codes persiste pendant plus d'une seconde ou deux, ou si vous ne parvenez pas à résoudre l'erreur en suivant l'une des procédures de dépannage prescrites, contactez le support technique.

Code	Indique
22	Aucun enregistrement d'amorçage maître trouvé sur un périphérique d'amorçage.
23	Le disque flash interne n'est pas connecté.
2A, 2B	Bus bloqué, impossible de lire les données du démon DIMM.
40	Modules DIMM non valides.
41	Modules DIMM non valides.

Code	Indique
42	Échec du test de la mémoire.
51	Échec de lecture du SPD.
92 à 96	Initialisation du bus PCI.
A0 à A3	Initialisation du lecteur SATA.
AB	Autre code d'amorçage.
AE	Démarrage du système d'exploitation.
EA	Échec de la formation DDR4.
E8	Aucune mémoire installée.
UE	Le script d'installation est introuvable.
EP	L'installation ou la communication avec le contrôleur E2800 est défectueuse.

Informations associées

- "Support NetApp"
- "Guide de surveillance des systèmes E5700 et E2800"

SG100 et SG1000

L'appliance inclut des indicateurs qui vous permettent de déterminer l'état du contrôleur de l'appliance et des deux disques SSD :

- Voyants et boutons de l'appareil
- Codes de démarrage généraux
- Indicateurs SSD

Utilisez ces informations pour vous aider "Dépanner l'installation matérielle des systèmes SG100 et SG1000".

Voyants et boutons de l'appareil

La figure suivante montre les indicateurs d'état et les boutons sur les SG100 et SG1000.

Légende	Afficher	État
1	Bouton d'alimentation	• Bleu : l'appareil est sous tension. • Éteint : l'appareil est hors tension.
2	Bouton de réinitialisation	Utilisez ce bouton pour effectuer une réinitialisation matérielle du contrôleur.
3	Bouton identifier	Ce bouton peut être configuré pour clignoter, allumé (continu) ou éteint. • Bleu clignotant : identifie l'appliance dans l'armoire ou le rack. • Bleu, fixe : identifie l'appliance dans l'armoire ou le rack. • Éteint : l'appareil n'est pas visuellement identifiable dans l'armoire ou le rack.
4	Voyant d'alarme	• Orange, fixe : une erreur s'est produite. **Note:** pour afficher les codes de démarrage et d'erreur, "Accédez à l'interface BMC". • OFF : aucune erreur n'est présente.

Codes de démarrage généraux

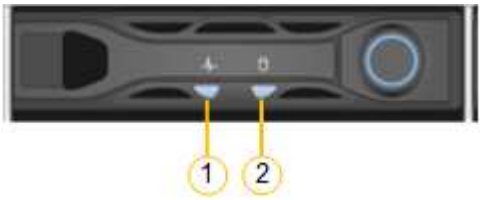
Lors du démarrage ou après une réinitialisation matérielle de l'appareil, les événements suivants se produisent :

1. Le contrôleur BMC (Baseboard Management Controller) consigne les codes de la séquence de démarrage, y compris les erreurs qui se produisent.
2. Le bouton d'alimentation s'allume.
3. Si des erreurs se produisent au démarrage, le voyant d'alarme s'allume.

   Pour afficher les codes de démarrage et d'erreur, "Accédez à l'interface BMC".

Indicateurs SSD

La figure suivante montre les voyants des disques SSD du SG100 et du SG1000.



LED	Afficher	État
1	État/défaut du lecteur	• Bleu (continu) : le lecteur est en ligne • Orange (clignotant) : échec du lecteur • OFF : l'emplacement est vide
2	Entraînement actif	Bleu (clignotant) : accès au lecteur

Configurer le matériel

Configuration du matériel : présentation

Après avoir mis l'appareil sous tension, vous configurez les connexions réseau qui seront utilisées par StorageGRID.

Configurez les connexions réseau requises

Pour tous les dispositifs, vous devez effectuer plusieurs tâches pour configurer les connexions réseau requises, telles que :

- Accédez au programme d'installation de l'appliance
- Configurer les liaisons réseau
- Vérifiez les connexions réseau au niveau des ports

Configuration supplémentaire éventuellement nécessaire

Selon le type d'appliance que vous configurez, une configuration matérielle supplémentaire peut être nécessaire.

SANtricity System Manager

Pour SG6000 et SG5700, vous configurez SANtricity System Manager. Le logiciel SANtricity est utilisé pour contrôler le matériel de ces dispositifs.

Interface BMC

Les appliances suivantes ont une interface BMC qui doit être configurée :

- SGF6112
- SG6000
- SG1000
- SG100

Configuration facultative

- Appliances de stockage

    - Configurez le logiciel SANtricity System Manager (SG6000 et SG5700) que vous utiliserez pour surveiller le matériel
    - Changer de mode RAID
- Appliances de services
    - Accédez à l'interface BMC pour les SG100 et SG1000 et le contrôleur SG6000-CN

Configurer les connexions StorageGRID

Accédez au programme d'installation de l'appliance StorageGRID

Vous devez accéder au programme d'installation de l'appliance StorageGRID pour vérifier la version du programme d'installation et configurer les connexions entre l'appliance et les trois réseaux StorageGRID : le réseau Grid, le réseau d'administration (facultatif) et le réseau client (facultatif).

Avant de commencer

- Vous utilisez n'importe quel client de gestion pouvant vous connecter au réseau d'administration StorageGRID ou vous disposez d'un ordinateur portable de service.
- Le client ou l'ordinateur portable de service a un "navigateur web pris en charge".
- L'appliance de services ou le contrôleur de l'appliance de stockage est connecté à tous les réseaux StorageGRID que vous souhaitez utiliser.
- Vous connaissez l'adresse IP, la passerelle et le sous-réseau de l'appliance de services ou du contrôleur d'appliance de stockage sur ces réseaux.
- Vous avez configuré les commutateurs réseau que vous prévoyez d'utiliser.

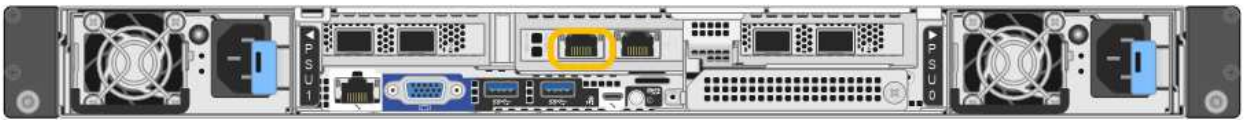
Description de la tâche

Pour accéder initialement au programme d'installation de l'appliance StorageGRID, vous pouvez utiliser l'adresse IP attribuée par DHCP pour le port réseau d'administration sur l'appliance de services ou le contrôleur de l'appliance de stockage (en supposant qu'il est connecté au réseau d'administration). vous pouvez également connecter un ordinateur portable de service directement à l'appliance de services ou au contrôleur de l'appliance de stockage.

Étapes

1. Si possible, utilisez l'adresse DHCP du port Admin Network sur l'appliance de services ou le contrôleur de l'appliance de stockage. Le port réseau d'administration est mis en surbrillance dans la figure suivante. (Utilisez l'adresse IP sur le réseau Grid si le réseau Admin n'est pas connecté.)

SGF6112



SG6000-CN

E5700SG

Pour le modèle E5700SG, vous pouvez effectuer l'une des opérations suivantes :

- Regardez l'affichage à sept segments sur le contrôleur E5700SG. Si les ports 1 et 10/25-GbE 2 et 4 du contrôleur E5700SG sont connectés à des réseaux avec des serveurs DHCP, le contrôleur tente d'obtenir des adresses IP attribuées de manière dynamique lors de la mise sous tension du boîtier. Une fois le processus de mise sous tension terminé, l'affichage à sept segments indique **HO**, suivi d'une séquence répétée de deux nombres.

  ```
  HO -- IP address for Admin Network -- IP address for Grid Network
  HO
  ```

  Dans l'ordre :

  - Le premier jeu de chiffres est l'adresse DHCP du nœud de stockage de l'appliance sur le réseau Admin, s'il est connecté. Cette adresse IP est attribuée au port de gestion 1 du contrôleur E5700SG.
  - Le second jeu de chiffres correspond à l'adresse DHCP du nœud de stockage de l'appliance sur le réseau Grid. Cette adresse IP est attribuée aux ports 10/25-GbE 2 et 4 lorsque vous mettez l'appliance sous tension pour la première fois.

    Si une adresse IP n'a pas pu être attribuée à l'aide de DHCP, 0.0.0.0 s'affiche.

SG100

SG1000

a. Repérez l'étiquette d'adresse MAC située à l'avant de l'appliance de services ou de stockage et déterminez l'adresse MAC du port réseau d'administration.

L'étiquette d'adresse MAC répertorie l'adresse MAC du port de gestion BMC.

Pour déterminer l'adresse MAC du port Admin Network, ajoutez **2** au nombre hexadécimal figurant sur l'étiquette. Par exemple, si l'adresse MAC de l'étiquette se termine par **09**, l'adresse MAC du port d'administration se terminera par **0B**. Si l'adresse MAC de l'étiquette se termine dans **(*y*)FF**, l'adresse MAC du port d'administration se terminera dans **(*y*+1)01**. Vous pouvez facilement effectuer ce calcul en ouvrant Calculator sous Windows, en le définissant en mode programmateur, en sélectionnant Hex, en saisissant l'adresse MAC, puis en tapant **+ 2 =**.

b. Indiquez l'adresse MAC à votre administrateur réseau pour qu'il puisse rechercher l'adresse DHCP de l'appliance sur le réseau d'administration.

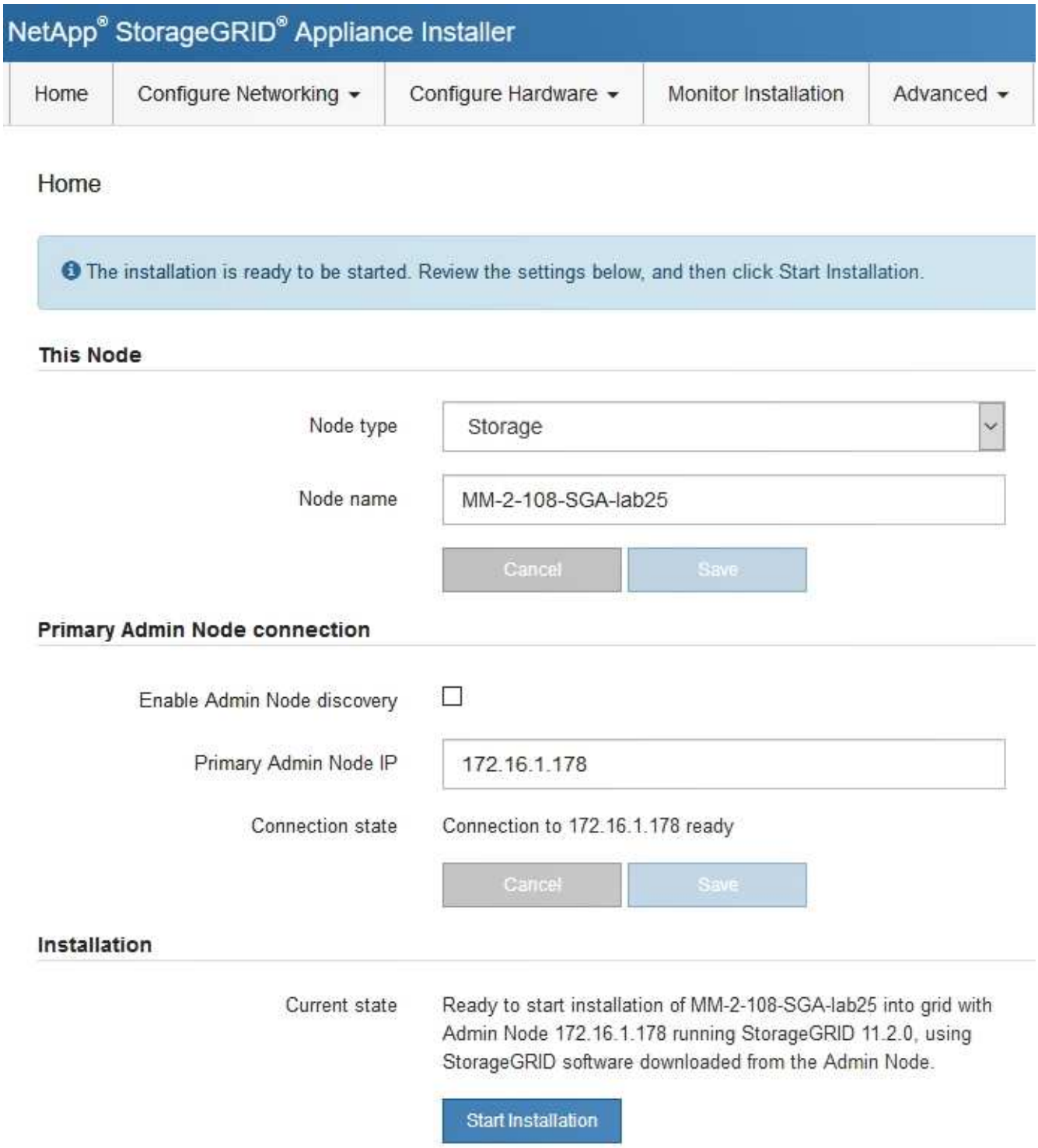
c. Dans le client, saisissez cette URL pour le programme d'installation de l'appliance StorageGRID : **`https://Appliance_IP:8443`**

Pour *`Appliance_IP`*, Utilisez l'adresse DHCP (utilisez l'adresse IP du réseau d'administration si vous l'avez).

d. Si vous êtes invité à recevoir une alerte de sécurité, affichez et installez le certificat à l'aide de l'assistant d'installation du navigateur.

L'alerte n'apparaît pas la prochaine fois que vous accédez à cette URL.

La page d'accueil du programme d'installation de l'appliance StorageGRID s'affiche. Les informations et les messages affichés lorsque vous accédez pour la première fois à cette page dépendent de la manière dont votre appareil est actuellement connecté aux réseaux StorageGRID. Des messages d'erreur peuvent s'afficher et seront résolus dans les étapes suivantes.



2. Si vous ne parvenez pas à obtenir une adresse IP à l'aide de DHCP, vous pouvez utiliser une connexion lien-local.

SGF6112

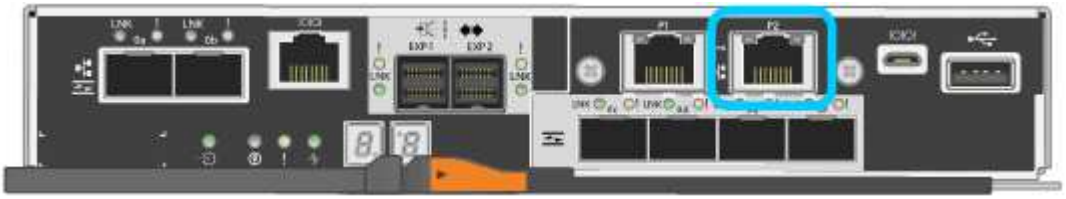
Connectez un ordinateur portable de service directement au port RJ-45 le plus à droite de l'appareil, à l'aide d'un câble Ethernet.

SG6000-CN

Connectez un ordinateur portable de service directement au port RJ-45 le plus à droite du contrôleur SG6000-CN, à l'aide d'un câble Ethernet.

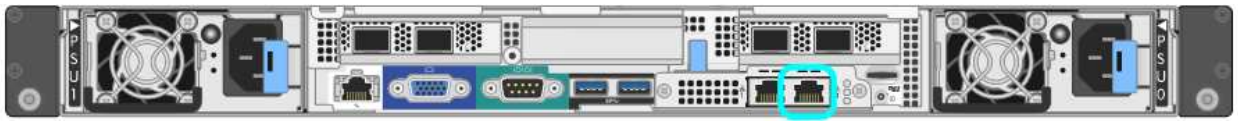
E5700SG

Connectez l'ordinateur portable de service au port de gestion 2 du contrôleur E5700SG à l'aide d'un câble Ethernet.



SG100

Connectez un ordinateur portable de service directement au port RJ-45 le plus à droite de l'appareil de services à l'aide d'un câble Ethernet.



SG1000

Connectez un ordinateur portable de service directement au port RJ-45 le plus à droite de l'appareil de services à l'aide d'un câble Ethernet.

a. Ouvrez un navigateur Web sur l'ordinateur portable de service.

b. Entrez l'URL suivante pour le programme d'installation de l'appliance StorageGRID :
`https://169.254.0.1:8443`

La page d'accueil du programme d'installation de l'appliance StorageGRID s'affiche. Les informations et les messages affichés lorsque vous accédez pour la première fois à cette page dépendent de la manière dont votre appareil est actuellement connecté aux réseaux StorageGRID. Des messages

d’erreur peuvent s’afficher et seront résolus dans les étapes suivantes.

Si vous ne pouvez pas accéder à la page d’accueil via une connexion lien-local, configurez l’adresse IP de l’ordinateur portable de service en tant que `169.254.0.2`, et réessayez.

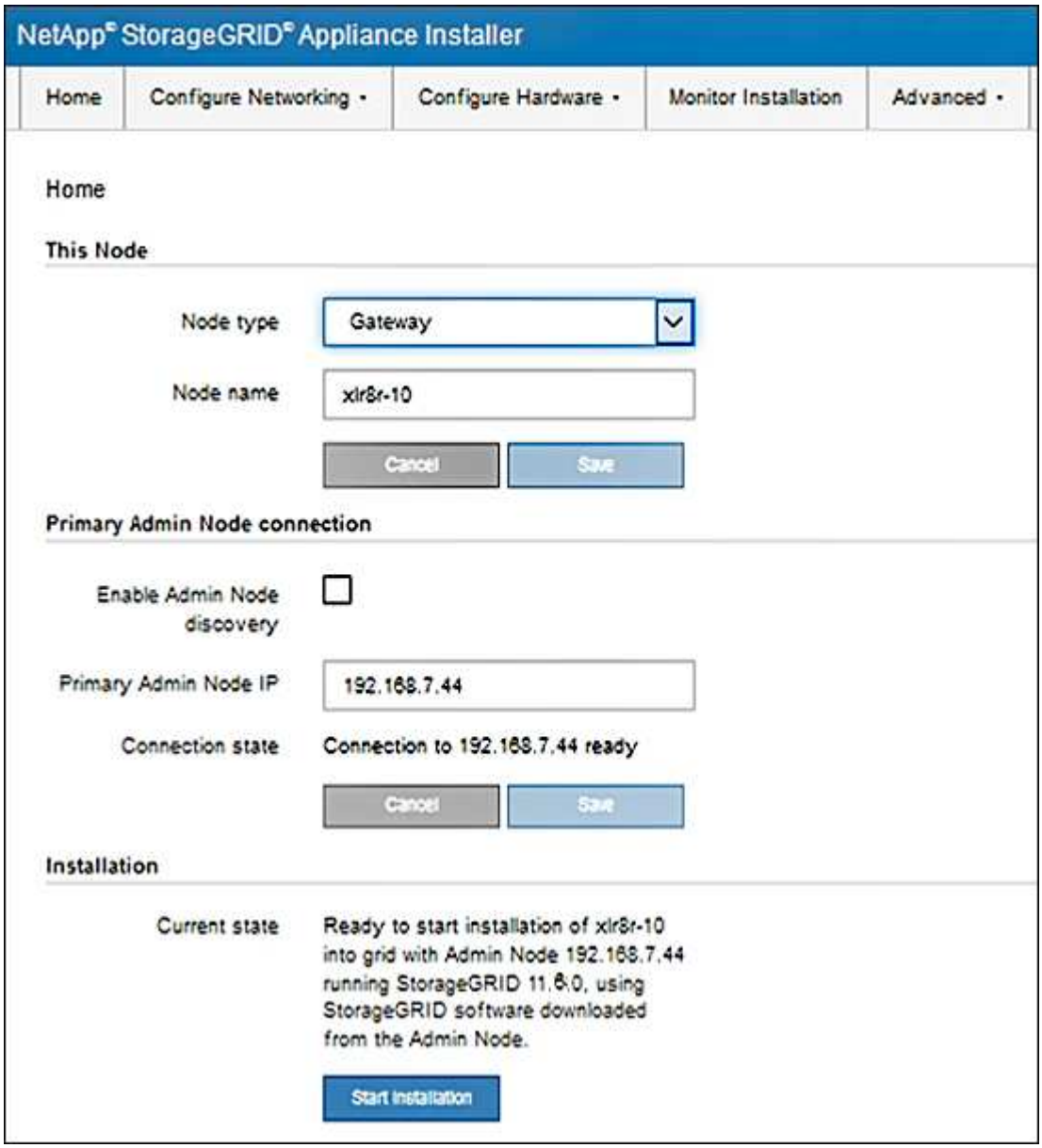
Une fois que vous avez terminé

Après avoir accédé au programme d’installation de l’appliance StorageGRID :

- Vérifiez que la version du programme d’installation de l’appliance StorageGRID installée sur l’appliance correspond à la version logicielle installée sur votre système StorageGRID. Mettez à niveau le programme d’installation de l’appliance StorageGRID, si nécessaire.

  "Vérifiez et mettez à niveau la version du programme d’installation de l’appliance StorageGRID"

- Vérifiez tous les messages affichés sur la page d’accueil du programme d’installation de l’appliance StorageGRID et configurez la configuration du lien et la configuration IP, selon les besoins.



Vérifiez et mettez à niveau la version du programme d'installation de l'appliance StorageGRID

La version du programme d'installation de l'appliance StorageGRID sur l'appliance doit correspondre à la version logicielle installée sur votre système StorageGRID pour s'assurer que toutes les fonctionnalités StorageGRID sont prises en charge.

Avant de commencer

Vous avez accédé au programme d'installation de l'appliance StorageGRID.

Description de la tâche

Les appliances StorageGRID sont préinstallées en usine avec le programme d'installation de l'appliance StorageGRID. Si vous ajoutez une appliance à un système StorageGRID récemment mis à niveau, vous devrez peut-être mettre à niveau manuellement le programme d'installation de l'appliance StorageGRID avant d'installer l'appliance en tant que nouveau nœud.

Le programme d'installation de l'appliance StorageGRID se met automatiquement à niveau lorsque vous effectuez une mise à niveau vers une nouvelle version de StorageGRID. Vous n'avez pas besoin de mettre à niveau le programme d'installation de l'appliance StorageGRID sur les nœuds d'appliance installés. Cette procédure est uniquement requise lorsque vous installez une appliance qui contient une version antérieure du programme d'installation de l'appliance StorageGRID.

Étapes

1. Dans le programme d'installation de l'appliance StorageGRID, sélectionnez **Avancé** > **mise à niveau du micrologiciel**.
2. Comparez la version actuelle du micrologiciel avec la version logicielle installée sur votre système StorageGRID. (En haut de Grid Manager, sélectionnez l'icône d'aide et sélectionnez **About**.)

   Le second chiffre des deux versions doit correspondre. Par exemple, si votre système StorageGRID exécute la version 11.**6**.*x*.*y*, la version du programme d'installation de l'appliance StorageGRID doit être 3.**6**.*z*.

3. Si l'appliance dispose d'une version de niveau inférieur du programme d'installation de l'appliance StorageGRID, passez à "Téléchargement NetApp : appliance StorageGRID".

   Connectez-vous avec le nom d'utilisateur et le mot de passe de votre compte NetApp.

4. Téléchargez la version appropriée du fichier **support pour les appliances StorageGRID** et le fichier de somme de contrôle correspondant.

   Le fichier de support des appliances StorageGRID est un `.zip` Archive contenant les versions de micrologiciel actuelles et précédentes pour tous les modèles d'appliance StorageGRID.

   Après avoir téléchargé le fichier de support des appliances StorageGRID, extrayez le `.zip` Archivez et consultez le fichier README pour obtenir des informations importantes sur l'installation du programme d'installation de l'appliance StorageGRID.

5. Suivez les instructions de la page mise à niveau du micrologiciel du programme d'installation de votre appliance StorageGRID pour effectuer les opérations suivantes :
   a. Téléchargez le fichier de support approprié (image du micrologiciel) pour votre type de contrôleur. Certaines versions de micrologiciel nécessitent également le téléchargement d'un fichier de somme de contrôle. Si vous êtes invité à entrer un fichier de checksum, il peut également être trouvé dans le fichier support pour les appliances StorageGRID.

b. Mettre à niveau la partition inactive.

c. Redémarrez et permutez les partitions.

d. Téléchargez à nouveau le fichier de support approprié (image du micrologiciel) pour votre type de contrôleur. Certaines versions de micrologiciel nécessitent également le téléchargement d'un fichier de somme de contrôle. Si vous êtes invité à entrer un fichier de checksum, il peut également être trouvé dans le fichier support pour les appliances StorageGRID.

e. Mettez à niveau la deuxième partition (inactive).

Informations associées

"Accès au programme d'installation de l'appliance StorageGRID"

Configurer les liaisons réseau

Vous pouvez configurer des liaisons réseau pour les ports utilisés pour connecter l'appliance au réseau Grid, au réseau client et au réseau Admin. Vous pouvez définir la vitesse de liaison ainsi que les modes de port et de liaison réseau.

Si vous utilisez ConfigBuilder pour générer un fichier JSON, vous pouvez configurer automatiquement les liens réseau. Voir "Automatisez l'installation et la configuration de l'appliance".

Avant de commencer

- Vous avez "obtenu l'équipement supplémentaire" requis pour votre type de câble et votre vitesse de liaison.
- Vous avez installé les émetteurs-récepteurs appropriés dans les ports, en fonction de la vitesse de liaison que vous prévoyez d'utiliser.
- Vous avez connecté les ports réseau à des commutateurs qui prennent en charge la vitesse choisie.

Si vous prévoyez d'utiliser le mode de liaison de port d'agrégat, le mode de liaison réseau LACP ou le balisage VLAN :

- Vous avez connecté les ports réseau de l'appliance à des commutateurs capables de prendre en charge VLAN et LACP.
- Si plusieurs commutateurs participent au lien LACP, les commutateurs prennent en charge les groupes d'agrégation de liens multi-châssis (MLAG), ou un équivalent.
- Vous comprenez comment configurer les commutateurs pour utiliser VLAN, LACP et MLAG ou équivalent.
- Vous connaissez la balise VLAN unique à utiliser pour chaque réseau. Cette balise VLAN sera ajoutée à chaque paquet réseau pour s'assurer que le trafic réseau est acheminé vers le réseau approprié.

Description de la tâche

Vous ne devez configurer les paramètres de la page Configuration des liens que si vous souhaitez utiliser un paramètre autre que celui par défaut.

La politique de hachage de transmission LACP est layer2+3.

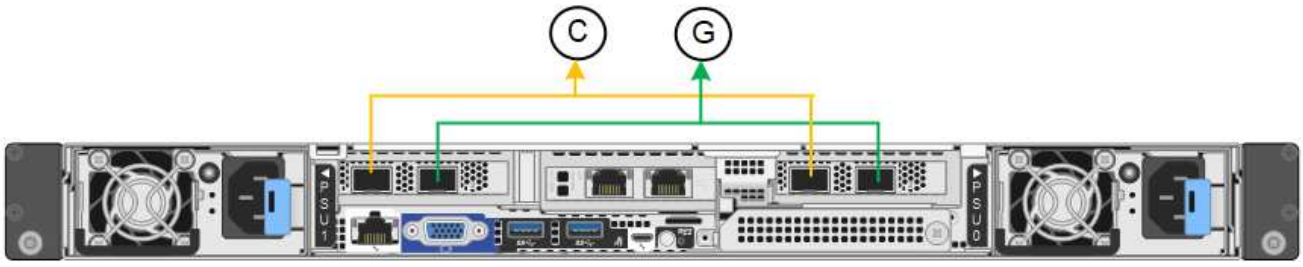
Les figures et les tableaux résument les options pour le mode de liaison du port et le mode de liaison du réseau pour chaque appliance. Pour plus d'informations, reportez-vous aux sections suivantes :

- "Modes de liaison de port (SGF6112)"
- "Modes de liaison de port (SG6000-CN)"
- "Modes de liaison du port (E5700SG)"
- "Modes de liaison de port (SG1000 et SG100)"

SGF6112

Mode de liaison port fixe (par défaut)

La figure montre comment les quatre ports réseau sont liés en mode de liaison port fixe (configuration par défaut).



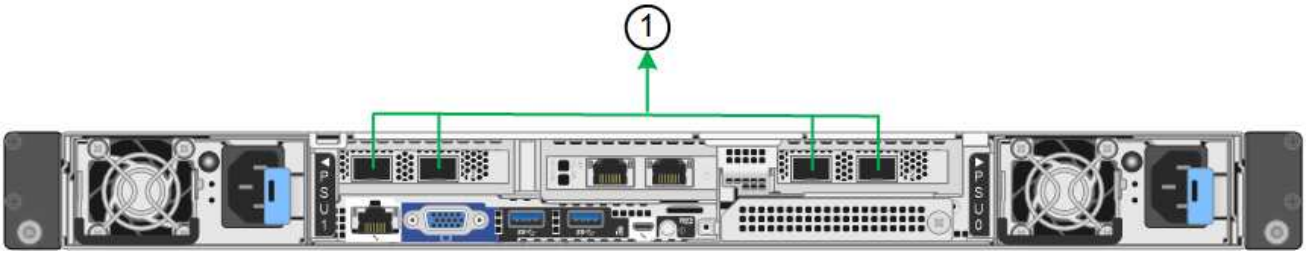
Légende	Quels ports sont liés
C	Les ports 1 et 3 sont liés ensemble pour le réseau client, si ce réseau est utilisé.
G	Les ports 2 et 4 sont liés ensemble pour le réseau de grille.

Le tableau récapitule les options de configuration des ports réseau. Vous ne devez configurer les paramètres de la page Configuration des liens que si vous souhaitez utiliser un paramètre autre que celui par défaut.

Mode de liaison réseau	Réseau client désactivé (par défaut)	Réseau client activé
Sauvegarde active/active (par défaut)	• Les ports 2 et 4 utilisent une liaison de sauvegarde active pour le réseau Grid. • Les ports 1 et 3 ne sont pas utilisés. • Une balise VLAN est facultative.	• Les ports 2 et 4 utilisent une liaison de sauvegarde active pour le réseau Grid. • Les ports 1 et 3 utilisent une liaison de sauvegarde active pour le réseau client. • Les balises VLAN peuvent être spécifiées pour les deux réseaux pour le confort de l'administrateur réseau.
LACP (802.3ad)	• Les ports 2 et 4 utilisent une liaison LACP pour le réseau Grid. • Les ports 1 et 3 ne sont pas utilisés. • Une balise VLAN est facultative.	• Les ports 2 et 4 utilisent une liaison LACP pour le réseau Grid. • Les ports 1 et 3 utilisent une liaison LACP pour le réseau client. • Les balises VLAN peuvent être spécifiées pour les deux réseaux pour le confort de l'administrateur réseau.

Mode de liaison du port agrégé

La figure montre comment les quatre ports réseau sont liés en mode agrégation de liens de port.



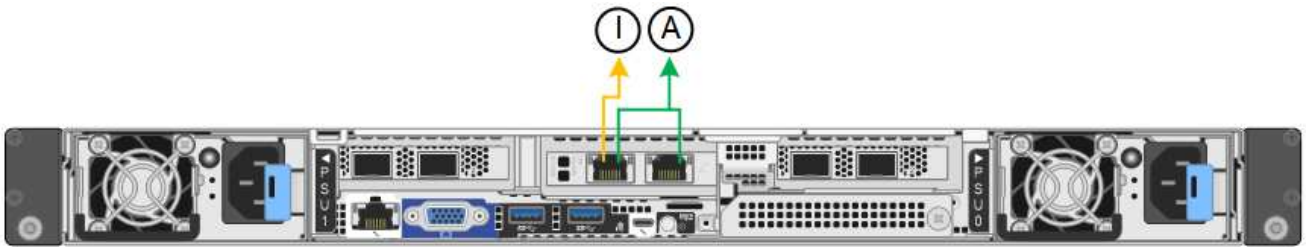
Légende	Quels ports sont liés
1	Les quatre ports sont regroupés en une seule liaison LACP, ce qui permet d'utiliser tous les ports pour le trafic Grid Network et client Network.

Le tableau récapitule les options de configuration des ports réseau. Vous ne devez configurer les paramètres de la page Configuration des liens que si vous souhaitez utiliser un paramètre autre que celui par défaut.

Mode de liaison réseau	Réseau client désactivé (par défaut)	Réseau client activé
LACP (802.3ad) uniquement	• Les ports 1-4 utilisent une liaison LACP unique pour le réseau Grid. • Une balise VLAN unique identifie les paquets réseau Grid.	• Les ports 1-4 utilisent une liaison LACP unique pour le réseau Grid et le réseau client. • Deux balises VLAN permettent de isoler les paquets réseau Grid des paquets réseau client.

Mode de liaison réseau Active-Backup pour les ports de gestion

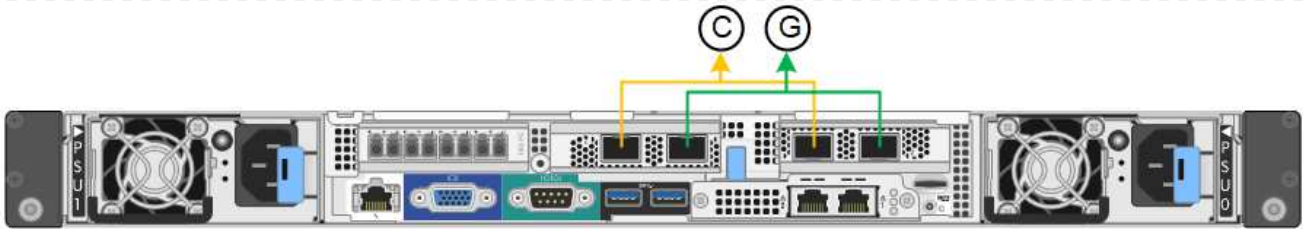
Cette figure montre comment les deux ports de gestion 1 GbE du SGF6112 sont liés en mode liaison réseau Active-Backup pour le réseau d'administration.



SG6000

Mode de liaison port fixe (par défaut)

Cette figure montre comment les quatre ports réseau sont liés en mode de liaison port fixe (configuration par défaut)



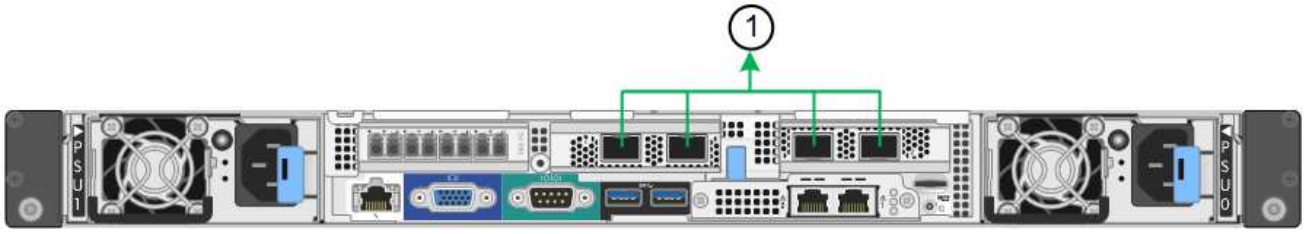
Légende	Quels ports sont liés
C	Les ports 1 et 3 sont liés ensemble pour le réseau client, si ce réseau est utilisé.
G	Les ports 2 et 4 sont liés ensemble pour le réseau de grille.

Le tableau récapitule les options de configuration des ports réseau. Vous ne devez configurer les paramètres de la page Configuration des liens que si vous souhaitez utiliser un paramètre autre que celui par défaut.

Mode de liaison réseau	Réseau client désactivé (par défaut)	Réseau client activé
Sauvegarde active/active (par défaut)	• Les ports 2 et 4 utilisent une liaison de sauvegarde active pour le réseau Grid. • Les ports 1 et 3 ne sont pas utilisés. • Une balise VLAN est facultative.	• Les ports 2 et 4 utilisent une liaison de sauvegarde active pour le réseau Grid. • Les ports 1 et 3 utilisent une liaison de sauvegarde active pour le réseau client. • Les balises VLAN peuvent être spécifiées pour les deux réseaux pour le confort de l'administrateur réseau.
LACP (802.3ad)	• Les ports 2 et 4 utilisent une liaison LACP pour le réseau Grid. • Les ports 1 et 3 ne sont pas utilisés. • Une balise VLAN est facultative.	• Les ports 2 et 4 utilisent une liaison LACP pour le réseau Grid. • Les ports 1 et 3 utilisent une liaison LACP pour le réseau client. • Les balises VLAN peuvent être spécifiées pour les deux réseaux pour le confort de l'administrateur réseau.

Mode de liaison du port agrégé

Cette figure montre comment les quatre ports réseau sont liés en mode de liaison de port agrégé.



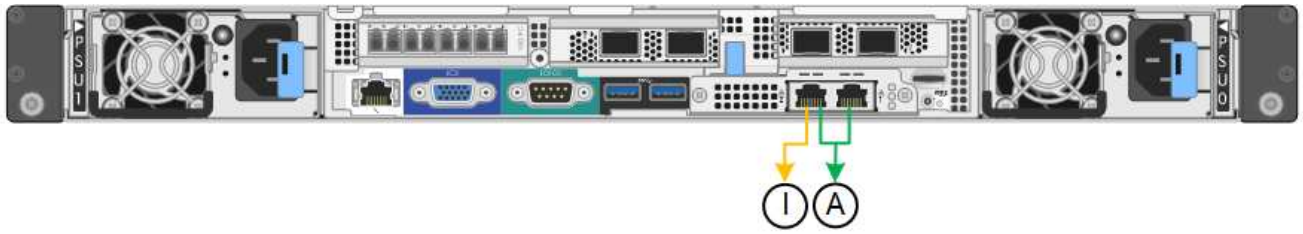
Légende	Quels ports sont liés
1	Les quatre ports sont regroupés en une seule liaison LACP, ce qui permet d'utiliser tous les ports pour le trafic Grid Network et client Network.

Le tableau récapitule les options de configuration des ports réseau. Vous ne devez configurer les paramètres de la page Configuration des liens que si vous souhaitez utiliser un paramètre autre que celui par défaut.

Mode de liaison réseau	Réseau client désactivé (par défaut)	Réseau client activé
LACP (802.3ad) uniquement	• Les ports 1-4 utilisent une liaison LACP unique pour le réseau Grid. • Une balise VLAN unique identifie les paquets réseau Grid.	• Les ports 1-4 utilisent une liaison LACP unique pour le réseau Grid et le réseau client. • Deux balises VLAN permettent de isoler les paquets réseau Grid des paquets réseau client.

Mode de liaison réseau Active-Backup pour les ports de gestion

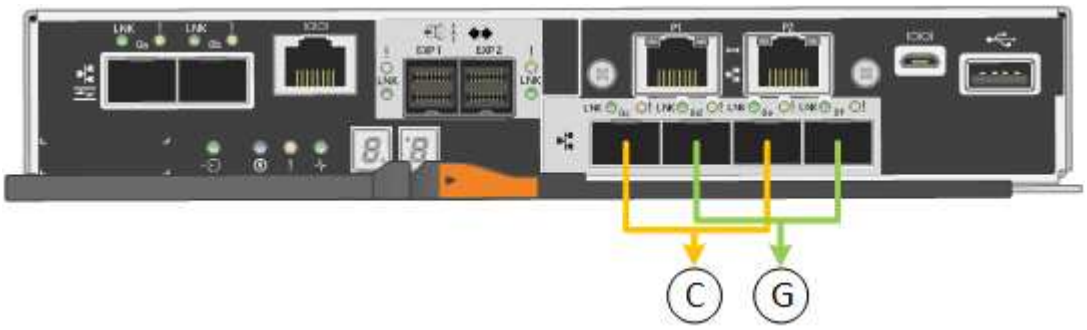
Cette figure montre comment les deux ports de gestion 1 GbE du contrôleur SG6000-CN sont liés en mode de liaison réseau Active-Backup pour le réseau Admin.



SG5700

Mode de liaison port fixe (par défaut)

Cette figure montre comment les quatre ports 10/25 GbE sont liés en mode de liaison de port fixe (configuration par défaut).



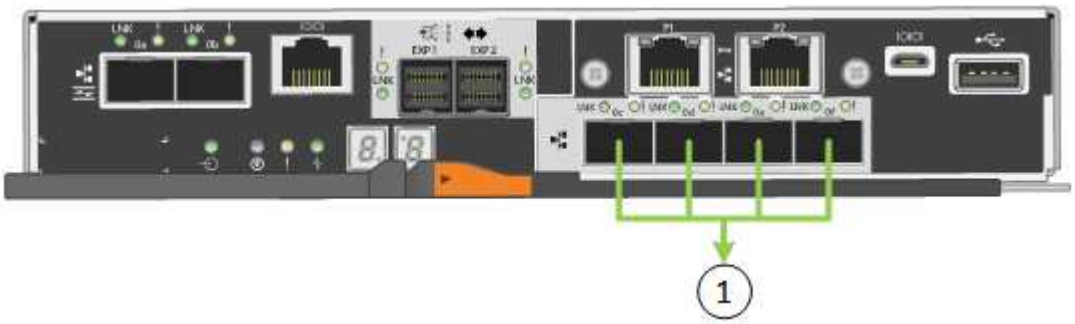
Légende	Quels ports sont liés
C	Les ports 1 et 3 sont liés ensemble pour le réseau client, si ce réseau est utilisé.
G	Les ports 2 et 4 sont liés ensemble pour le réseau de grille.

Le tableau récapitule les options de configuration des quatre ports 10/25-GbE. Vous ne devez configurer les paramètres de la page Configuration des liens que si vous souhaitez utiliser un paramètre autre que celui par défaut.

Mode de liaison réseau	Réseau client désactivé (par défaut)	Réseau client activé
Sauvegarde active/active (par défaut)	• Les ports 2 et 4 utilisent une liaison de sauvegarde active pour le réseau Grid. • Les ports 1 et 3 ne sont pas utilisés. • Une balise VLAN est facultative.	• Les ports 2 et 4 utilisent une liaison de sauvegarde active pour le réseau Grid. • Les ports 1 et 3 utilisent une liaison de sauvegarde active pour le réseau client. • Les balises VLAN peuvent être spécifiées pour les deux réseaux pour le confort de l'administrateur réseau.
LACP (802.3ad)	• Les ports 2 et 4 utilisent une liaison LACP pour le réseau Grid. • Les ports 1 et 3 ne sont pas utilisés. • Une balise VLAN est facultative.	• Les ports 2 et 4 utilisent une liaison LACP pour le réseau Grid. • Les ports 1 et 3 utilisent une liaison LACP pour le réseau client. • Les balises VLAN peuvent être spécifiées pour les deux réseaux pour le confort de l'administrateur réseau.

Mode de liaison du port agrégé

Cette figure montre comment les quatre ports 10/25 GbE sont liés en mode de liaison de port agrégé.



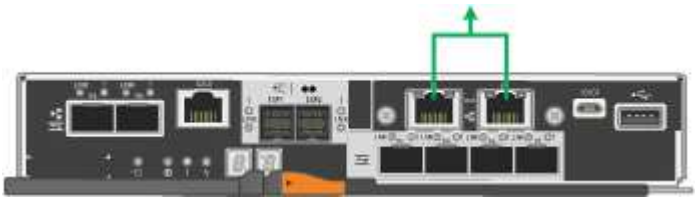
Légende	Quels ports sont liés
1	Les quatre ports sont regroupés en une seule liaison LACP, ce qui permet d'utiliser tous les ports pour le trafic Grid Network et client Network.

Le tableau récapitule les options de configuration des quatre ports 10/25-GbE. Vous ne devez configurer les paramètres de la page Configuration des liens que si vous souhaitez utiliser un paramètre autre que celui par défaut.

Mode de liaison réseau	Réseau client désactivé (par défaut)	Réseau client activé
LACP (802.3ad) uniquement	• Les ports 1-4 utilisent une liaison LACP unique pour le réseau Grid. • Une balise VLAN unique identifie les paquets réseau Grid.	• Les ports 1-4 utilisent une liaison LACP unique pour le réseau Grid et le réseau client. • Deux balises VLAN permettent de isoler les paquets réseau Grid des paquets réseau client.

Mode de liaison réseau Active-Backup pour les ports de gestion

Cette figure montre comment les deux ports de gestion 1 GbE du contrôleur E5700SG sont liés en mode de liaison réseau Active-Backup pour le réseau d'administration.

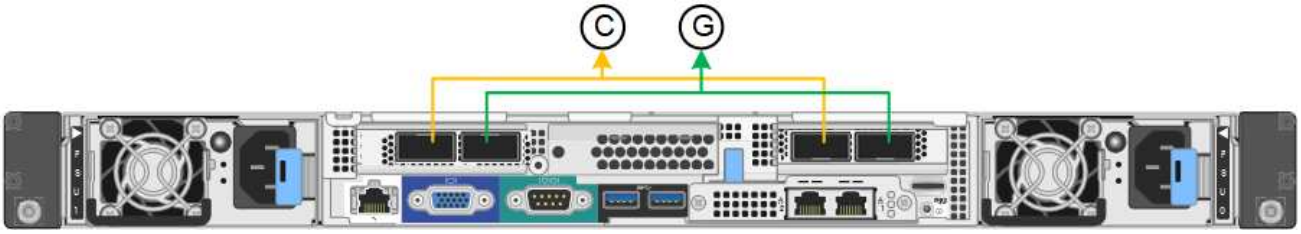


SG100 et SG1000

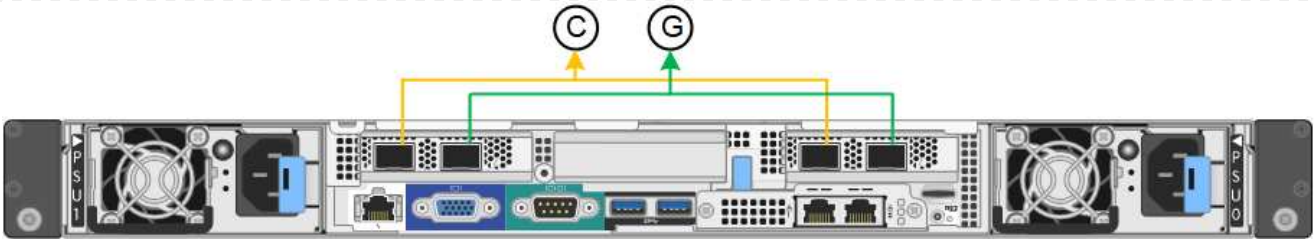
Mode de liaison port fixe (par défaut)

Les figures montrent comment les quatre ports réseau du SG1000 ou du SG100 sont liés en mode de liaison port fixe (configuration par défaut).

SG1000 :



SG100 :



Légende	Quels ports sont liés
C	Les ports 1 et 3 sont liés ensemble pour le réseau client, si ce réseau est utilisé.
G	Les ports 2 et 4 sont liés ensemble pour le réseau de grille.

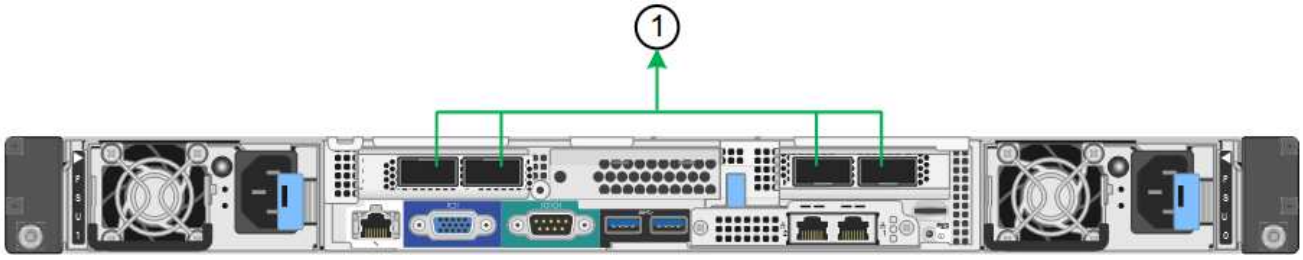
Le tableau récapitule les options de configuration des quatre ports réseau. Vous ne devez configurer les paramètres de la page Configuration des liens que si vous souhaitez utiliser un paramètre autre que celui par défaut.

Mode de liaison réseau	Réseau client désactivé (par défaut)	Réseau client activé
Sauvegarde active/active (par défaut)	• Les ports 2 et 4 utilisent une liaison de sauvegarde active pour le réseau Grid. • Les ports 1 et 3 ne sont pas utilisés. • Une balise VLAN est facultative.	• Les ports 2 et 4 utilisent une liaison de sauvegarde active pour le réseau Grid. • Les ports 1 et 3 utilisent une liaison de sauvegarde active pour le réseau client. • Les balises VLAN peuvent être spécifiées pour les deux réseaux pour le confort de l'administrateur réseau.
LACP (802.3ad)	• Les ports 2 et 4 utilisent une liaison LACP pour le réseau Grid. • Les ports 1 et 3 ne sont pas utilisés. • Une balise VLAN est facultative.	• Les ports 2 et 4 utilisent une liaison LACP pour le réseau Grid. • Les ports 1 et 3 utilisent une liaison LACP pour le réseau client. • Les balises VLAN peuvent être spécifiées pour les deux réseaux pour le confort de l'administrateur réseau.

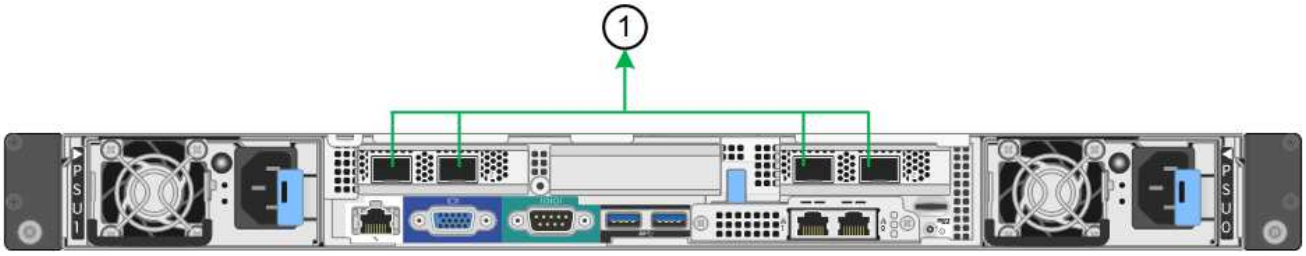
Mode de liaison du port agrégé

Ces figures montrent comment les quatre ports réseau sont liés en mode agrégation port bond.

SG1000 :



SG100 :



Légende	Quels ports sont liés
1	Les quatre ports sont regroupés en une seule liaison LACP, ce qui permet d'utiliser tous les ports pour le trafic Grid Network et client Network.

Le tableau récapitule les options de configuration des quatre ports réseau. Vous ne devez configurer les paramètres de la page Configuration des liens que si vous souhaitez utiliser un paramètre autre que celui par défaut.

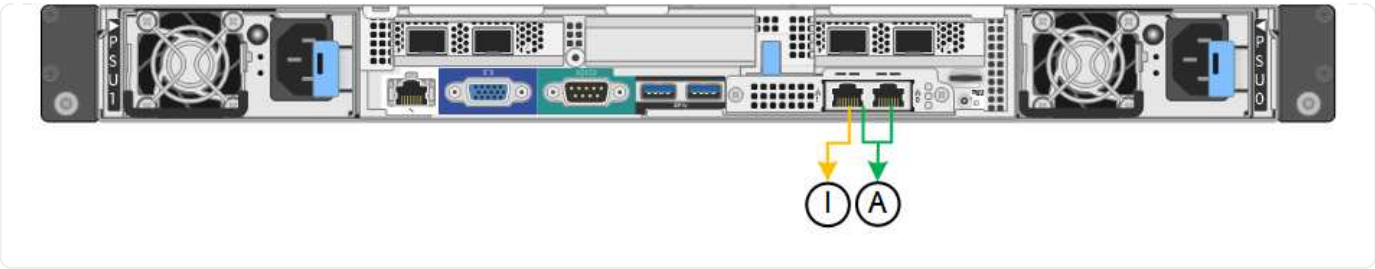
Mode de liaison réseau	Réseau client désactivé (par défaut)	Réseau client activé
LACP (802.3ad) uniquement	• Les ports 1-4 utilisent une liaison LACP unique pour le réseau Grid. • Une balise VLAN unique identifie les paquets réseau Grid.	• Les ports 1-4 utilisent une liaison LACP unique pour le réseau Grid et le réseau client. • Deux balises VLAN permettent de isoler les paquets réseau Grid des paquets réseau client.

Mode de liaison réseau Active-Backup pour les ports de gestion

Ces figures montrent comment les deux ports de gestion 1 GbE des dispositifs sont liés en mode liaison réseau Active-Backup pour le réseau d'administration.

SG1000 :

SG100 :



Étapes

1. Dans la barre de menus du programme d'installation de l'appliance StorageGRID, cliquez sur **configurer réseau** > **Configuration lien**.

   La page Configuration de la liaison réseau affiche un schéma de votre appliance avec le réseau et les ports de gestion numérotés.

   Le tableau État de la liaison répertorie l'état de la liaison, la vitesse de la liaison et les autres statistiques des ports numérotés.

   La première fois que vous accédez à cette page :

   - **Vitesse de liaison** est définie sur **Auto**.
   - **Le mode de liaison de port** est défini sur **fixe**.
   - **Le mode de liaison réseau** est défini sur **Active-Backup** pour le réseau de grille.
   - Le **réseau d'administration** est activé et le mode de liaison réseau est défini sur **indépendant**.
   - Le **réseau client** est désactivé.

2. Sélectionnez la vitesse de liaison des ports réseau dans la liste déroulante **Link Speed**.

   Les commutateurs réseau que vous utilisez pour le réseau Grid et le réseau client doivent également prendre en charge et être configurés pour cette vitesse. Vous devez utiliser les adaptateurs ou émetteurs-récepteurs appropriés pour la vitesse de liaison configurée. Utilisez la vitesse de liaison automatique lorsque cela est possible car cette option négocie à la fois la vitesse de liaison et le mode de correction d'erreur de marche avant (FEC) avec le partenaire de liaison.

   Si vous prévoyez d'utiliser la vitesse de liaison 25 GbE pour les ports réseau SG6000 ou SG5700 :

   - Utilisez les émetteurs-récepteurs SFP28 et les câbles TwinAx SFP28 ou les câbles optiques.
   - Pour le SG6000, sélectionnez **Auto** dans la liste déroulante **vitesse de liaison**.
   - Pour l'appliance SG5700, sélectionnez **25GbE** dans la liste déroulante **vitesse de liaison**.

3. Activez ou désactivez les réseaux StorageGRID que vous souhaitez utiliser.

   Le réseau Grid est requis. Vous ne pouvez pas désactiver ce réseau.

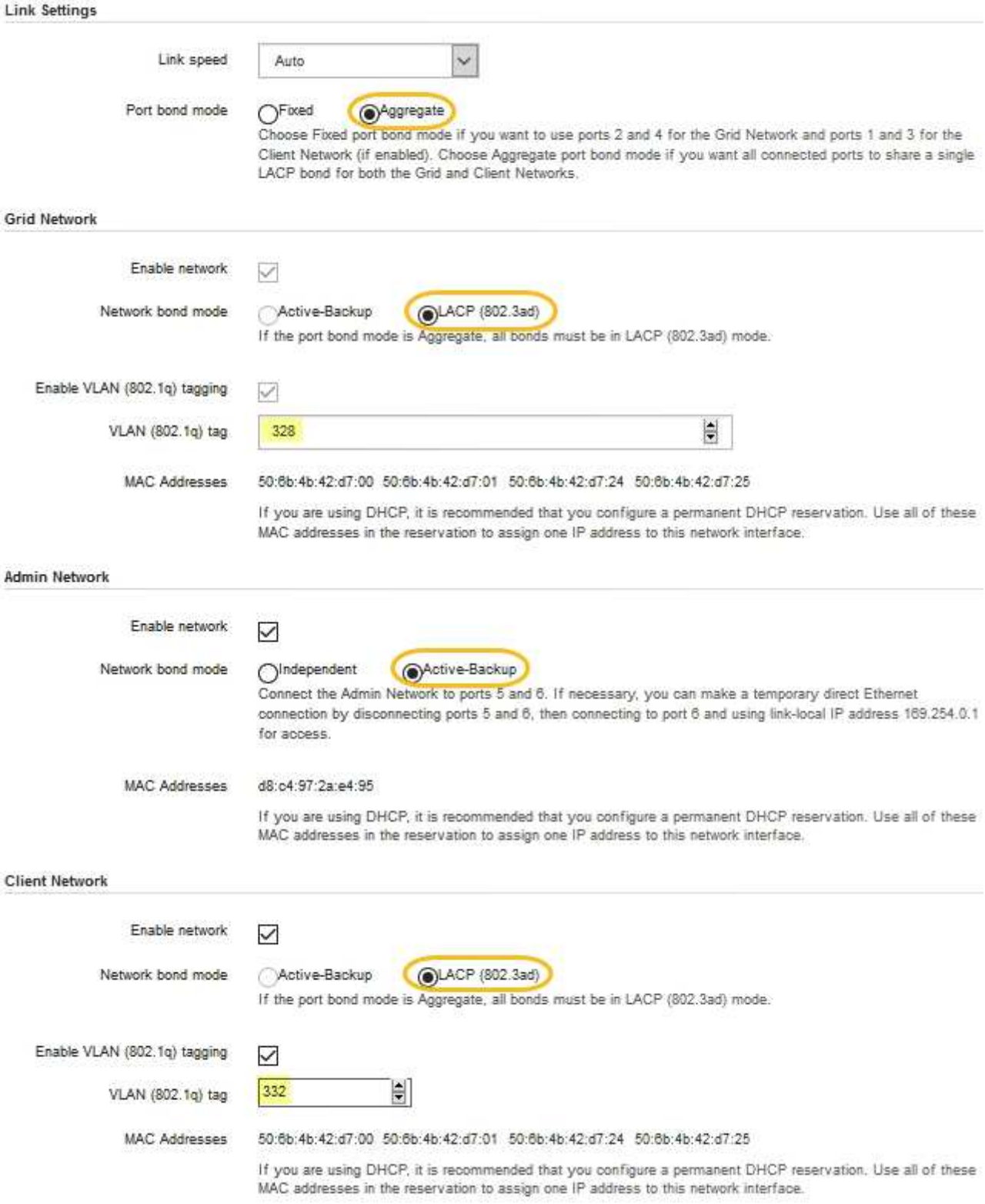
   a. Si le serveur n'est pas connecté au réseau d'administration, décochez la case **Activer le réseau** pour le réseau d'administration.
   b. Si le serveur est connecté au réseau client, cochez la case **Activer le réseau** pour le réseau client.

      Les paramètres réseau du client pour les ports de carte réseau de données sont maintenant affichés.

4. Reportez-vous au tableau et configurez le mode de liaison de port et le mode de liaison réseau.

Cet exemple montre :

- **Agrégat** et **LACP** sélectionnés pour la grille et les réseaux clients. Vous devez spécifier une balise VLAN unique pour chaque réseau. Vous pouvez sélectionner des valeurs comprises entre 0 et 4095.
- **Sauvegarde active** sélectionnée pour le réseau d'administration.



5. Lorsque vous êtes satisfait de vos sélections, cliquez sur **Enregistrer**.

Vous risquez de perdre votre connexion si vous avez apporté des modifications au réseau ou au lien auquel vous êtes connecté. Si vous n'êtes pas reconnecté dans un délai d'une minute, saisissez à nouveau l'URL du programme d'installation de l'appliance StorageGRID à l'aide de l'une des autres adresses IP attribuées à l'appliance : **`https://appliance_IP:8443`**

Configurez les adresses IP StorageGRID

Le programme d'installation de l'appliance StorageGRID vous permet de configurer les adresses IP et les informations de routage utilisées pour l'appliance de services ou le nœud de stockage de l'appliance sur les réseaux StorageGRID Grid, Admin et client.

Si vous utilisez ConfigBuilder pour générer un fichier JSON, vous pouvez configurer automatiquement les adresses IP. Voir "Automatisez l'installation et la configuration de l'appliance".

Description de la tâche

Vous devez attribuer une adresse IP statique à l'appliance sur chaque réseau connecté ou attribuer un bail permanent à l'adresse sur le serveur DHCP.

Pour modifier la configuration de la liaison, reportez-vous aux instructions suivantes :

- "Modifier la configuration de la liaison de l'appliance SGF6112"
- "Modifier la configuration de la liaison du contrôleur SG6000-CN"
- "Modifier la configuration de liaison du contrôleur E5700SG"
- "Modifier la configuration de la liaison de l'appliance de services SG100 ou SG1000"

Étapes

1. Dans le programme d'installation de l'appliance StorageGRID, sélectionnez **configurer le réseau** > **Configuration IP**.

   La page Configuration IP s'affiche.

2. Pour configurer le réseau de grille, sélectionnez **statique** ou **DHCP** dans la section **réseau de grille** de la page.
3. Si vous avez sélectionné **statique**, procédez comme suit pour configurer le réseau de grille :
   a. Entrez l'adresse IPv4 statique à l'aide de la notation CIDR.
   b. Entrez la passerelle.

      Si votre réseau ne dispose pas d'une passerelle, saisissez à nouveau la même adresse IPv4 statique.

   c. Si vous souhaitez utiliser des trames jumbo, remplacez le champ MTU par une valeur adaptée aux trames jumbo, comme 9000. Sinon, conservez la valeur par défaut 1500.

      La valeur MTU du réseau doit correspondre à la valeur configurée sur le port du commutateur auquel le nœud est connecté. Dans le cas contraire, des problèmes de performances réseau ou une perte de paquets peuvent se produire.

Pour des performances réseau optimales, tous les nœuds doivent être configurés avec des valeurs MTU similaires sur leurs interfaces réseau Grid. L'alerte **Grid Network MTU mismatch** est déclenchée en cas de différence importante dans les paramètres MTU pour le réseau Grid sur les nœuds individuels. Les valeurs MTU ne doivent pas nécessairement être identiques pour tous les types de réseau.

d. Cliquez sur **Enregistrer**.

Lorsque vous modifiez l'adresse IP, la passerelle et la liste des sous-réseaux peuvent également changer.

Si vous perdez votre connexion au programme d'installation de l'appliance StorageGRID, entrez à nouveau l'URL en utilisant la nouvelle adresse IP statique que vous venez d'attribuer. Par exemple, `https://appliance_IP:8443`

e. Vérifiez que la liste des sous-réseaux du réseau Grid est correcte.

Si vous avez des sous-réseaux de grille, la passerelle de réseau de grille est requise. Tous les sous-réseaux de la grille spécifiés doivent être accessibles via cette passerelle. Ces sous-réseaux du réseau Grid doivent également être définis dans la liste de sous-réseaux du réseau Grid sur le nœud d'administration principal lorsque vous démarrez l'installation de StorageGRID.

La route par défaut n'est pas répertoriée. Si le réseau client n'est pas activé, la route par défaut utilise la passerelle réseau Grid.

- Pour ajouter un sous-réseau, cliquez sur l'icône d'insertion ➕ à droite de la dernière entrée.
- Pour supprimer un sous-réseau inutilisé, cliquez sur l'icône Supprimer ✖.

f. Cliquez sur **Enregistrer**.

4. Si vous avez sélectionné **DHCP**, procédez comme suit pour configurer le réseau de grille :

a. Après avoir sélectionné le bouton radio **DHCP**, cliquez sur **Enregistrer**.

Les champs **adresse IPv4**, **passerelle** et **sous-réseaux** sont automatiquement renseignés. Si le serveur DHCP est configuré pour attribuer une valeur MTU, le champ **MTU** est renseigné avec cette valeur et le champ devient en lecture seule.

Votre navigateur Web est automatiquement redirigé vers la nouvelle adresse IP pour le programme d'installation de l'appliance StorageGRID.

b. Vérifiez que la liste des sous-réseaux du réseau Grid est correcte.

Si vous avez des sous-réseaux de grille, la passerelle de réseau de grille est requise. Tous les sous-réseaux de la grille spécifiés doivent être accessibles via cette passerelle. Ces sous-réseaux du réseau Grid doivent également être définis dans la liste de sous-réseaux du réseau Grid sur le nœud d'administration principal lorsque vous démarrez l'installation de StorageGRID.

La route par défaut n'est pas répertoriée. Si le réseau client n'est pas activé, la route par défaut utilise la passerelle réseau Grid.

- Pour ajouter un sous-réseau, cliquez sur l'icône d'insertion ➕ à droite de la dernière entrée.
- Pour supprimer un sous-réseau inutilisé, cliquez sur l'icône Supprimer ✖.

c. Si vous souhaitez utiliser des trames jumbo, remplacez le champ MTU par une valeur adaptée aux trames jumbo, comme 9000. Sinon, conservez la valeur par défaut 1500.

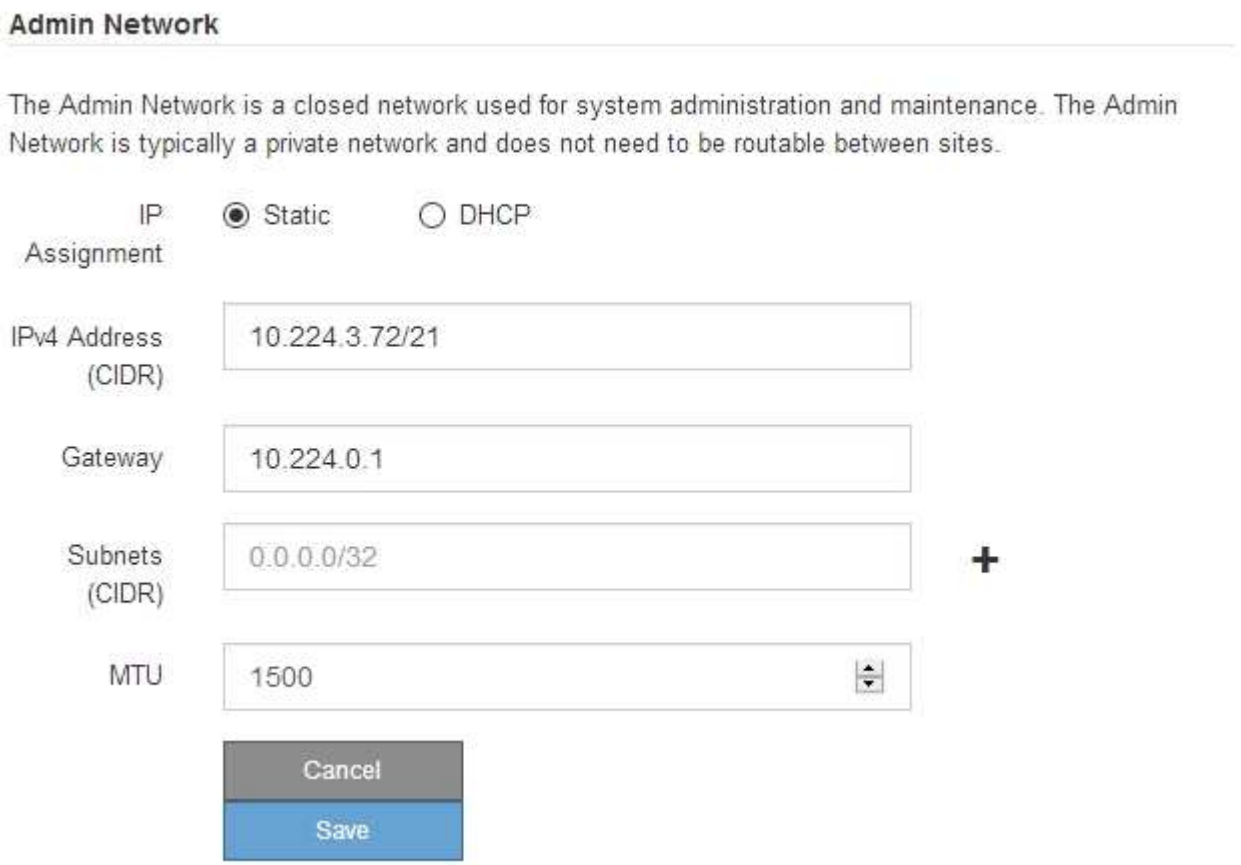
> La valeur MTU du réseau doit correspondre à la valeur configurée sur le port du commutateur auquel le nœud est connecté. Dans le cas contraire, des problèmes de performances réseau ou une perte de paquets peuvent se produire.

> Pour des performances réseau optimales, tous les nœuds doivent être configurés avec des valeurs MTU similaires sur leurs interfaces réseau Grid. L'alerte **Grid Network MTU mismatch** est déclenchée en cas de différence importante dans les paramètres MTU pour le réseau Grid sur les nœuds individuels. Les valeurs MTU ne doivent pas nécessairement être identiques pour tous les types de réseau.

a. Cliquez sur **Enregistrer**.

5. Pour configurer le réseau d'administration, sélectionnez **statique** ou **DHCP** dans la section **réseau d'administration** de la page.

> Pour configurer le réseau d'administration, activez le réseau d'administration sur la page Configuration de la liaison.



6. Si vous avez sélectionné **statique**, procédez comme suit pour configurer le réseau d'administration :

a. Saisissez l'adresse IPv4 statique, en utilisant la notation CIDR, pour le port de gestion 1 de l'appliance.

Le port de gestion 1 se trouve à gauche des deux ports RJ45 1 GbE situés à l'extrémité droite de l'appliance.

b. Entrez la passerelle.

   Si votre réseau ne dispose pas d'une passerelle, saisissez à nouveau la même adresse IPv4 statique.

c. Si vous souhaitez utiliser des trames jumbo, remplacez le champ MTU par une valeur adaptée aux trames jumbo, comme 9000. Sinon, conservez la valeur par défaut 1500.

   > La valeur MTU du réseau doit correspondre à la valeur configurée sur le port du commutateur auquel le nœud est connecté. Dans le cas contraire, des problèmes de performances réseau ou une perte de paquets peuvent se produire.

d. Cliquez sur **Enregistrer**.

   Lorsque vous modifiez l'adresse IP, la passerelle et la liste des sous-réseaux peuvent également changer.

   Si vous perdez votre connexion au programme d'installation de l'appliance StorageGRID, entrez à nouveau l'URL en utilisant la nouvelle adresse IP statique que vous venez d'attribuer. Par exemple, **`https://appliance:8443`**

e. Vérifiez que la liste des sous-réseaux du réseau Admin est correcte.

   Vous devez vérifier que tous les sous-réseaux peuvent être atteints à l'aide de la passerelle fournie.

   > La route par défaut ne peut pas être établie pour utiliser la passerelle réseau Admin.

   - Pour ajouter un sous-réseau, cliquez sur l'icône d'insertion ➕ à droite de la dernière entrée.
   - Pour supprimer un sous-réseau inutilisé, cliquez sur l'icône Supprimer ✖.

f. Cliquez sur **Enregistrer**.

7. Si vous avez sélectionné **DHCP**, procédez comme suit pour configurer le réseau d'administration :

   a. Après avoir sélectionné le bouton radio **DHCP**, cliquez sur **Enregistrer**.

      Les champs **adresse IPv4**, **passerelle** et **sous-réseaux** sont automatiquement renseignés. Si le serveur DHCP est configuré pour attribuer une valeur MTU, le champ **MTU** est renseigné avec cette valeur et le champ devient en lecture seule.

      Votre navigateur Web est automatiquement redirigé vers la nouvelle adresse IP pour le programme d'installation de l'appliance StorageGRID.

   b. Vérifiez que la liste des sous-réseaux du réseau Admin est correcte.

      Vous devez vérifier que tous les sous-réseaux peuvent être atteints à l'aide de la passerelle fournie.

      > La route par défaut ne peut pas être établie pour utiliser la passerelle réseau Admin.

      - Pour ajouter un sous-réseau, cliquez sur l'icône d'insertion ➕ à droite de la dernière entrée.
      - Pour supprimer un sous-réseau inutilisé, cliquez sur l'icône Supprimer ✖.

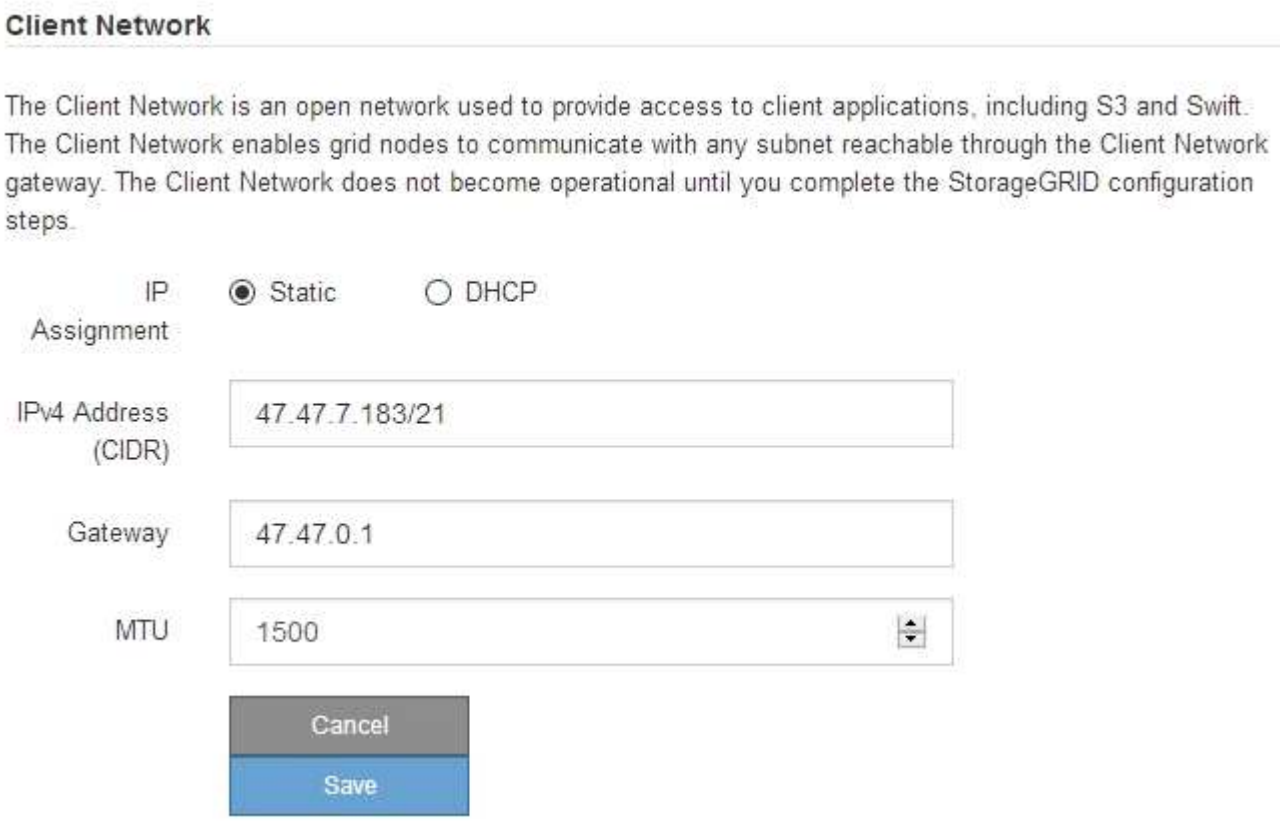
   c. Si vous souhaitez utiliser des trames jumbo, remplacez le champ MTU par une valeur adaptée aux trames jumbo, comme 9000. Sinon, conservez la valeur par défaut 1500.

La valeur MTU du réseau doit correspondre à la valeur configurée sur le port du commutateur auquel le nœud est connecté. Dans le cas contraire, des problèmes de performances réseau ou une perte de paquets peuvent se produire.

d. Cliquez sur **Enregistrer**.

8. Pour configurer le réseau client, sélectionnez **statique** ou **DHCP** dans la section **réseau client** de la page.

Pour configurer le réseau client, activez le réseau client sur la page Configuration de la liaison.



9. Si vous avez sélectionné **statique**, procédez comme suit pour configurer le réseau client :

a. Entrez l'adresse IPv4 statique à l'aide de la notation CIDR.

b. Cliquez sur **Enregistrer**.

c. Vérifiez que l'adresse IP de la passerelle du réseau client est correcte.

Si le réseau client est activé, la route par défaut s'affiche. La route par défaut utilise la passerelle réseau client et ne peut pas être déplacée vers une autre interface lorsque le réseau client est activé.

d. Si vous souhaitez utiliser des trames jumbo, remplacez le champ MTU par une valeur adaptée aux trames jumbo, comme 9000. Sinon, conservez la valeur par défaut 1500.

La valeur MTU du réseau doit correspondre à la valeur configurée sur le port du commutateur auquel le nœud est connecté. Dans le cas contraire, des problèmes de performances réseau ou une perte de paquets peuvent se produire.

e. Cliquez sur **Enregistrer**.

10. Si vous avez sélectionné **DHCP**, procédez comme suit pour configurer le réseau client :

    a. Après avoir sélectionné le bouton radio **DHCP**, cliquez sur **Enregistrer**.

       Les champs **adresse IPv4** et **passerelle** sont automatiquement renseignés. Si le serveur DHCP est configuré pour attribuer une valeur MTU, le champ **MTU** est renseigné avec cette valeur et le champ devient en lecture seule.

    Votre navigateur Web est automatiquement redirigé vers la nouvelle adresse IP pour le programme d'installation de l'appliance StorageGRID.

    a. Vérifiez que la passerelle est correcte.

       > Si le réseau client est activé, la route par défaut s'affiche. La route par défaut utilise la passerelle réseau client et ne peut pas être déplacée vers une autre interface lorsque le réseau client est activé.

    b. Si vous souhaitez utiliser des trames jumbo, remplacez le champ MTU par une valeur adaptée aux trames jumbo, comme 9000. Sinon, conservez la valeur par défaut 1500.

       > La valeur MTU du réseau doit correspondre à la valeur configurée sur le port du commutateur auquel le nœud est connecté. Dans le cas contraire, des problèmes de performances réseau ou une perte de paquets peuvent se produire.

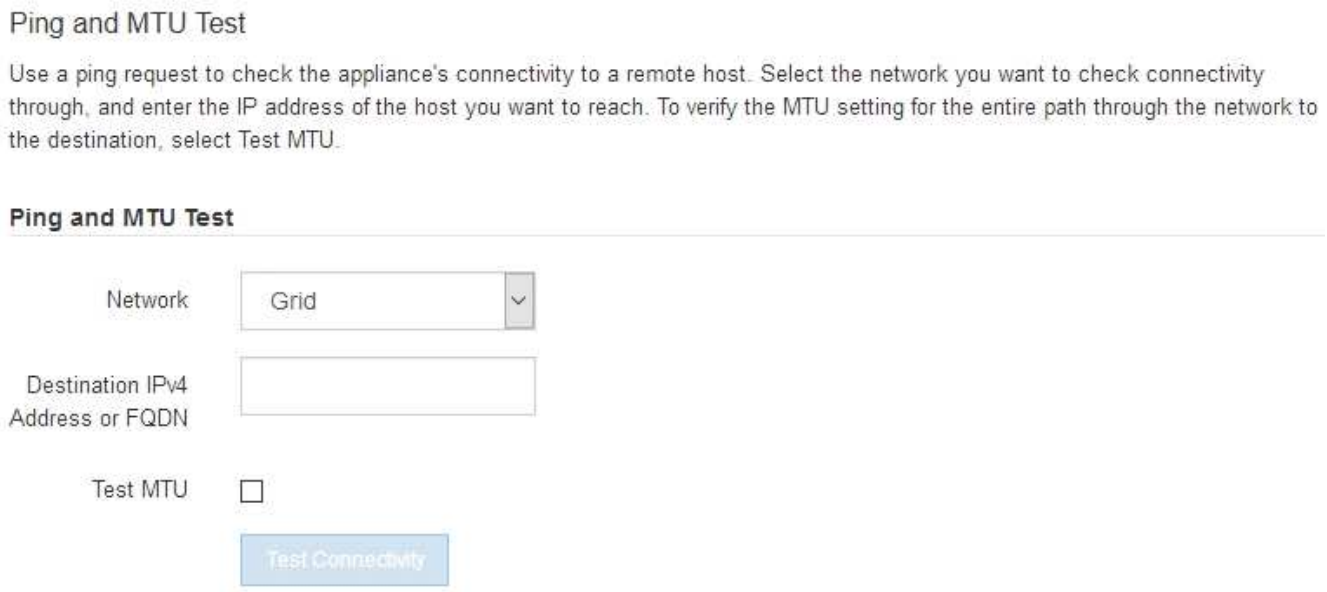
Vérifiez les connexions réseau

Vérifiez que vous pouvez accéder aux réseaux StorageGRID que vous utilisez à partir de l'appliance. Pour valider le routage via des passerelles réseau, vous devez tester la connectivité entre le programme d'installation de l'appliance StorageGRID et les adresses IP sur différents sous-réseaux. Vous pouvez également vérifier le paramètre MTU.

Étapes

1. Dans la barre de menus du programme d'installation de l'appliance StorageGRID, cliquez sur **configurer réseau** > **Test Ping et MTU**.

   La page Test Ping et MTU s'affiche.



2. Dans la liste déroulante **Network**, sélectionnez le réseau à tester : grid, Admin ou client.
3. Saisissez l'adresse IPv4 ou le nom de domaine complet (FQDN) d'un hôte sur ce réseau.

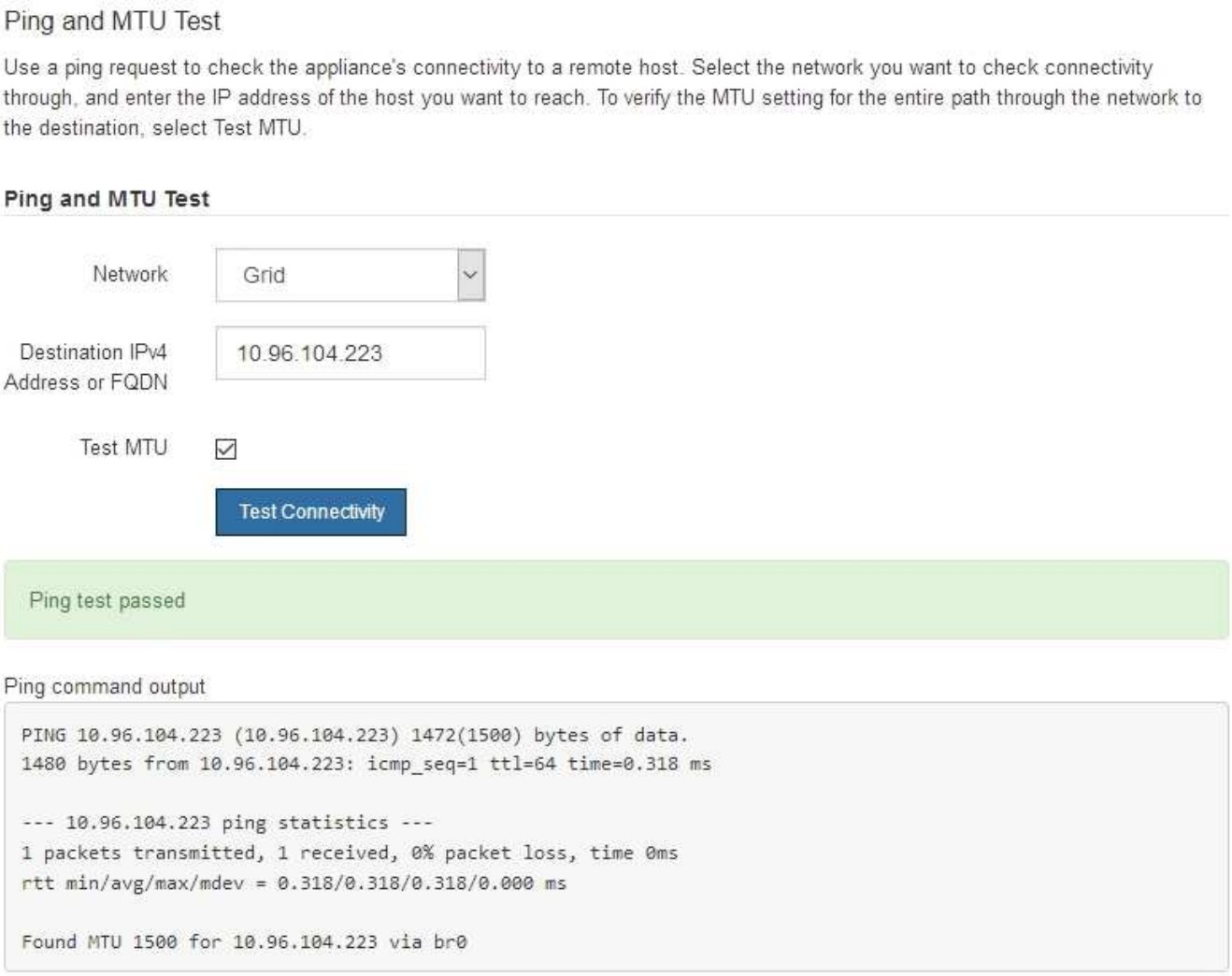
   Par exemple, vous pouvez envoyer une requête ping à la passerelle sur le réseau ou au nœud d'administration principal.

4. Si vous le souhaitez, cochez la case **Test MTU** pour vérifier le paramètre MTU pour l'ensemble du chemin passant par le réseau jusqu'à la destination.

   Par exemple, vous pouvez tester le chemin d'accès entre le nœud d'appliance et un nœud sur un autre site.

5. Cliquez sur **Tester la connectivité**.

   Si la connexion réseau est valide, le message « test Ping réussi » s'affiche, avec la sortie de la commande ping répertoriée.



Informations associées

- "Configurer les liaisons réseau"
- "Modifier le paramètre MTU"

Vérifiez les connexions réseau au niveau des ports

Pour vous assurer que l'accès entre le programme d'installation de l'appliance StorageGRID et d'autres nœuds n'est pas obstrué par des pare-feu, vérifiez que le programme d'installation de l'appliance StorageGRID peut se connecter à un port TCP spécifique ou à un ensemble de ports sur l'adresse IP ou la plage d'adresses spécifiée.

Description de la tâche

À l'aide de la liste des ports fournis dans le programme d'installation de l'appliance StorageGRID, vous pouvez tester la connectivité entre l'appliance et les autres nœuds de votre réseau Grid.

En outre, vous pouvez tester la connectivité sur les réseaux Admin et client et sur les ports UDP, tels que ceux utilisés pour les serveurs NFS ou DNS externes. Pour obtenir la liste de ces ports, reportez-vous au "référence de port réseau".

Les ports réseau de la grille répertoriés dans le tableau de connectivité des ports ne sont valides que pour StorageGRID version 11.7.0. Pour vérifier quels ports sont corrects pour chaque type de nœud, consultez toujours les instructions réseau relatives à votre version de StorageGRID.

Étapes

1. Dans le programme d'installation de l'appliance StorageGRID, cliquez sur **configurer le réseau** > **Test de connectivité du port (nmap)**.

   La page Test de connectivité du port s'affiche.

   Le tableau de connectivité des ports répertorie les types de nœuds qui nécessitent une connectivité TCP sur le réseau Grid. Pour chaque type de nœud, le tableau répertorie les ports du réseau Grid qui doivent être accessibles à votre appliance.

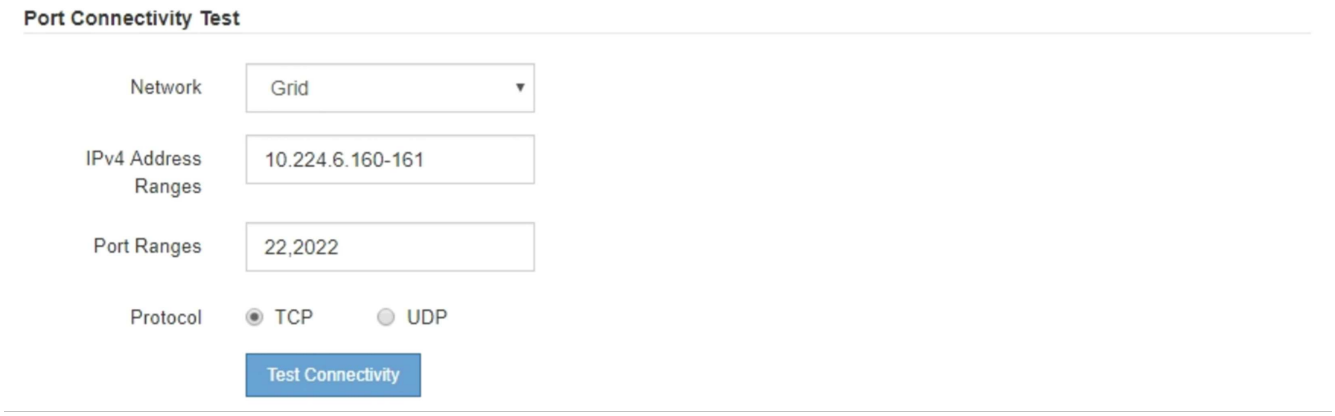
   Vous pouvez tester la connectivité entre les ports de l'appliance répertoriés dans le tableau et les autres nœuds de votre réseau Grid Network.

2. Dans la liste déroulante **Network**, sélectionnez le réseau à tester : **Grid**, **Admin** ou **client**.
3. Spécifiez une plage d'adresses IPv4 pour les hôtes sur ce réseau.

   Par exemple, vous pouvez sonder la passerelle sur le réseau ou le nœud d'administration principal.

   Spécifiez une plage à l'aide d'un tiret, comme indiqué dans l'exemple.

4. Entrez un numéro de port TCP, une liste de ports séparés par des virgules ou une plage de ports.

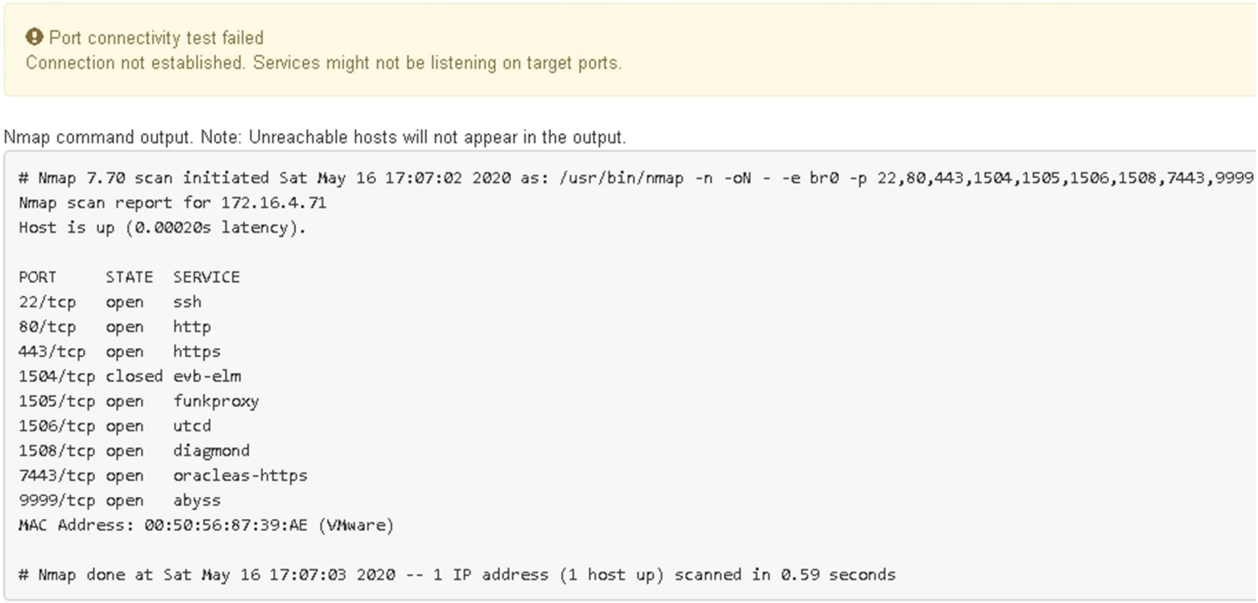


5. Cliquez sur **Tester la connectivité**.

   - Si les connexions réseau au niveau du port sélectionnées sont valides, le message « Test de connectivité du port réussi » s'affiche en vert. Le résultat de la commande nmap est répertorié sous la bannière.

- Si une connexion réseau au niveau du port est établie à l'hôte distant, mais que l'hôte n'écoute pas sur un ou plusieurs des ports sélectionnés, le message « échec du test de connectivité du port » s'affiche en jaune. Le résultat de la commande nmap est répertorié sous la bannière.

  Tout port distant auquel l'hôte n'écoute pas a l'état « fermé ». Par exemple, cette bannière jaune peut s'afficher lorsque le nœud auquel vous essayez de vous connecter est dans un état préinstallé et que le service NMS StorageGRID n'est pas encore exécuté sur ce nœud.



- Si une connexion réseau au niveau du port ne peut pas être établie pour un ou plusieurs ports sélectionnés, le message « échec du test de connectivité du port » apparaît dans une bannière rouge. Le résultat de la commande nmap est répertorié sous la bannière.

  La bannière rouge indique qu'une tentative de connexion TCP à un port de l'hôte distant a été effectuée, mais rien n'a été renvoyé à l'expéditeur. Lorsqu'aucune réponse n'est renvoyée, le port a l'état « filtré » et est probablement bloqué par un pare-feu.

  Les ports « fermés » sont également répertoriés.

Configuration de SANtricity System Manager (SG6000 et SG5700)

Vous pouvez utiliser SANtricity System Manager pour surveiller l'état des contrôleurs de stockage, des disques de stockage et d'autres composants matériels du tiroir du contrôleur de stockage. Vous pouvez également configurer un proxy pour E-Series AutoSupport qui vous permet d'envoyer des messages AutoSupport depuis le dispositif sans utiliser le port de gestion.

Configuration et accès à SANtricity System Manager

Vous devrez peut-être accéder à SANtricity System Manager sur le contrôleur de stockage pour contrôler le matériel du tiroir du contrôleur de stockage ou configurer les baies E-Series AutoSupport.

Avant de commencer

- Vous utilisez un "navigateur web pris en charge".
- Pour accéder au Gestionnaire système SANtricity via le Gestionnaire de grille, vous avez installé StorageGRID et vous disposez de l'autorisation d'administrateur de l'appliance de stockage ou de l'autorisation d'accès racine.
- Pour accéder au Gestionnaire système SANtricity à l'aide du programme d'installation de l'appliance StorageGRID, vous disposez du nom d'utilisateur et du mot de passe de l'administrateur du Gestionnaire système SANtricity.
- Pour accéder au Gestionnaire système SANtricity directement à l'aide d'un navigateur Web, vous disposez du nom d'utilisateur et du mot de passe de l'administrateur du Gestionnaire système SANtricity.

> ⓘ Vous devez disposer du micrologiciel SANtricity 8.70 ou supérieur pour accéder au Gestionnaire système SANtricity à l'aide du Gestionnaire de grille ou du programme d'installation de l'appliance StorageGRID. Vous pouvez vérifier la version de votre micrologiciel à l'aide du programme d'installation de l'appliance StorageGRID et en sélectionnant **aide** > **à propos**.

L'accès à SANtricity System Manager à partir de Grid Manager ou du programme d'installation de l'appliance n'est généralement destiné qu'au contrôle de votre matériel et à la configuration des baies E-Series AutoSupport. De nombreuses fonctionnalités et opérations dans SANtricity System Manager, telles que la mise à niveau du firmware, ne s'appliquent pas à la surveillance de l'appliance StorageGRID. Pour éviter tout problème, suivez toujours les instructions d'installation et de maintenance du matériel de votre appareil.

Description de la tâche

Il existe trois façons d'accéder à SANtricity System Manager, en fonction de l'étape du processus d'installation et de configuration dans laquelle vous vous trouvez :

- Si l'appliance n'a pas encore été déployée en tant que nœud dans votre système StorageGRID, utilisez l'onglet Avancé du programme d'installation de l'appliance StorageGRID.

  Une fois le nœud déployé, vous ne pouvez plus utiliser le programme d'installation de l'appliance StorageGRID pour accéder à SANtricity System Manager.

- Si l'appliance a été déployée en tant que nœud dans votre système StorageGRID, utilisez l'onglet SANtricity System Manager sur la page nœuds de Grid Manager.
- Si vous ne pouvez pas utiliser le programme d'installation de l'appliance StorageGRID ou le Gestionnaire de grille, vous pouvez accéder directement au Gestionnaire système SANtricity à l'aide d'un navigateur Web connecté au port de gestion.

Cette procédure comprend les étapes de votre accès initial à SANtricity System Manager. Si vous avez déjà configuré SANtricity System Manager, rendez-vous sur le étape de configuration des alertes matérielles.

L'utilisation de Grid Manager ou du programme d'installation de l'appliance StorageGRID vous permet d'accéder à SANtricity System Manager sans avoir à configurer ni à connecter le port de gestion de l'appliance.

Vous utilisez SANtricity System Manager pour contrôler les éléments suivants :

- Des données de performances telles que les performances au niveau des baies de stockage, la latence d'E/S, l'utilisation du CPU et le débit
- État des composants matériels
- Fonctions de support, y compris l'affichage des données de diagnostic

Vous pouvez utiliser SANtricity System Manager pour configurer les paramètres suivants :

- Alertes par e-mail, alertes SNMP ou syslog correspondant aux composants du tiroir de contrôleur de stockage
- Paramètres de la gamme E-Series AutoSupport pour les composants du tiroir contrôleur de stockage.

  Pour en savoir plus sur les systèmes E-Series AutoSupport, consultez "Site de documentation sur les systèmes NetApp E-Series".

- Clés de sécurité du lecteur, qui sont nécessaires pour déverrouiller des lecteurs sécurisés (cette étape est requise si la fonction de sécurité du lecteur est activée)
- Mot de passe d'administrateur pour accéder à SANtricity System Manager

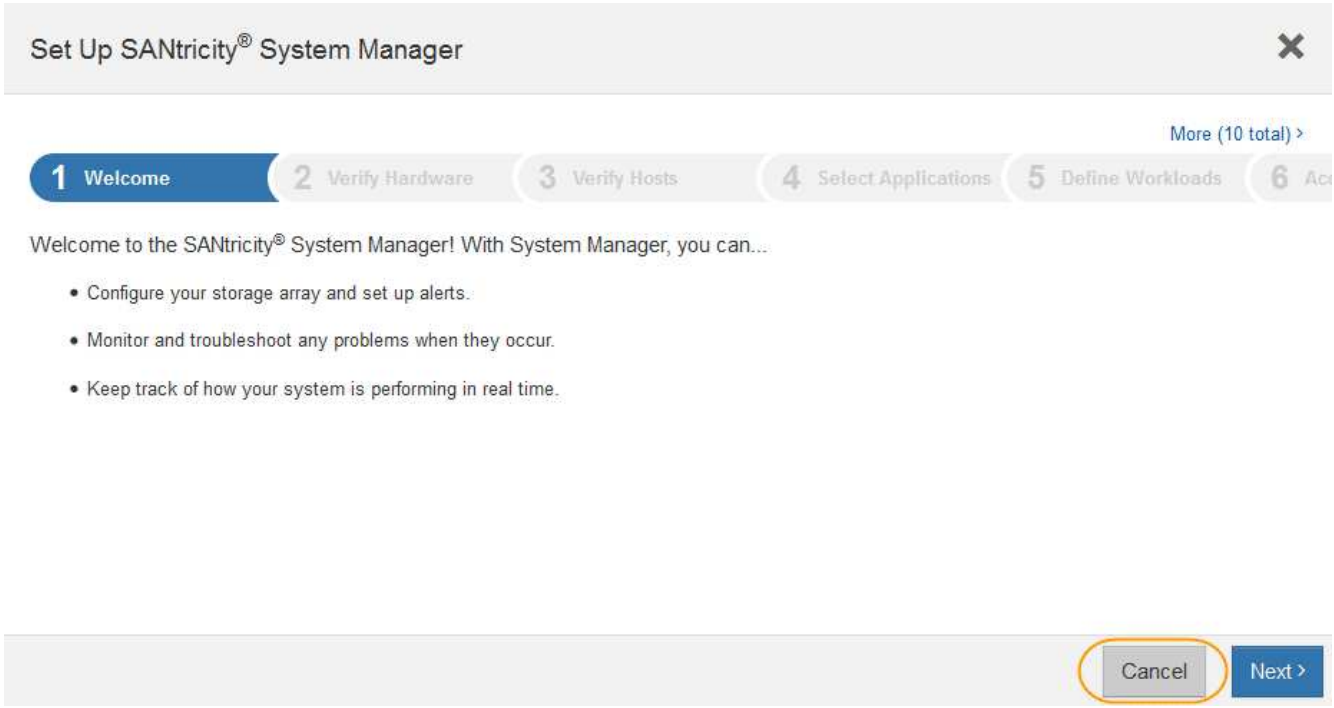
Étapes

1. Effectuez l'une des opérations suivantes :
   - Utilisez le programme d'installation de l'appliance StorageGRID et sélectionnez **Avancé** > **Gestionnaire système SANtricity**
   - Utilisez Grid Manager et sélectionnez **NODES** > ***appliance Storage Node*** > **SANtricity System Manager**

   > Si ces options ne sont pas disponibles ou si la page de connexion n'apparaît pas, utilisez le Adresses IP des contrôleurs de stockage. Accédez à SANtricity System Manager en naviguant sur l'adresse IP du contrôleur de stockage.

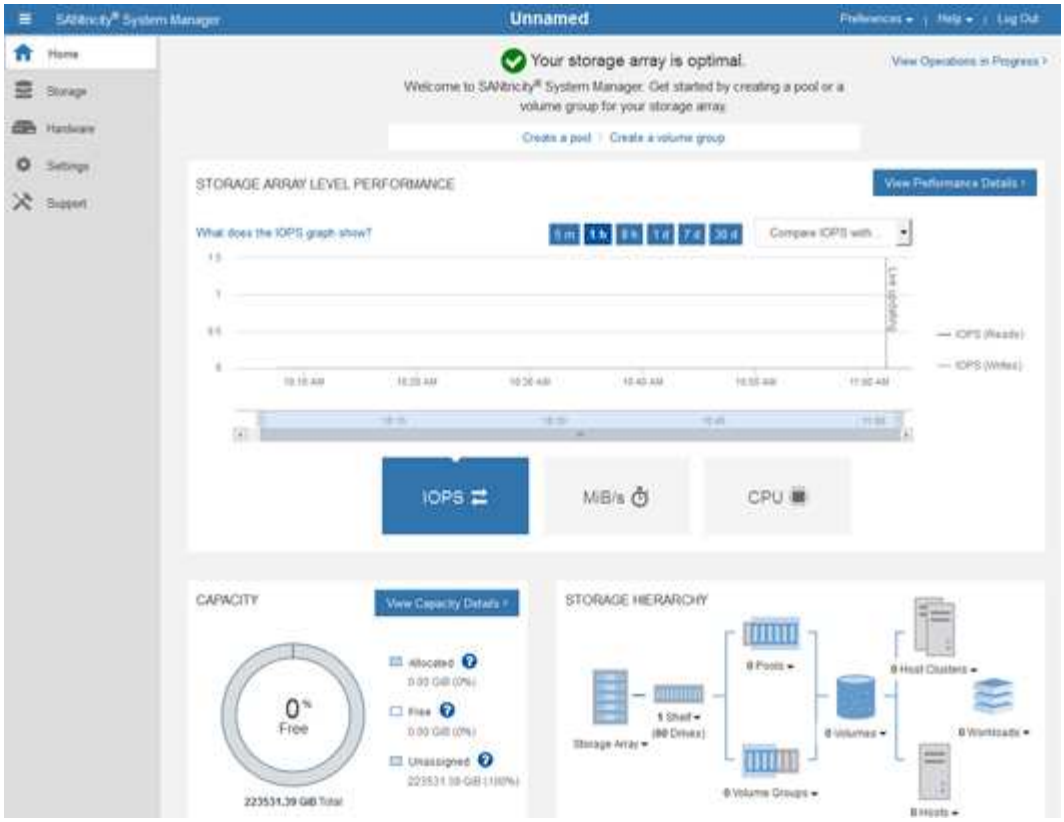
2. Définissez ou saisissez le mot de passe administrateur.

   SANtricity System Manager utilise un mot de passe d'administrateur unique qui est partagé entre tous les utilisateurs.



3. Sélectionnez **Annuler** pour fermer l'assistant.

   > Ne suivez pas l'assistant de configuration d'une appliance StorageGRID.



4. configurer les alertes matérielles.
   a. Sélectionnez **aide** pour accéder à l'aide en ligne de SANtricity System Manager.
   b. Utilisez la section **Paramètres** > **alertes** de l'aide en ligne pour en savoir plus sur les alertes.
   c. Suivez les instructions « Comment faire » pour configurer les alertes par e-mail, les alertes SNMP ou les alertes syslog.
5. Gérez AutoSupport pour les composants du tiroir contrôleur de stockage.
   a. Sélectionnez **aide** pour accéder à l'aide en ligne de SANtricity System Manager.
   b. Utilisez la section **SUPPORT** > **Centre de support** de l'aide en ligne pour en savoir plus sur la fonction AutoSupport.
   c. Suivez les instructions « Comment faire » pour gérer AutoSupport.

      Pour obtenir des instructions spécifiques sur la configuration d'un proxy StorageGRID pour l'envoi de messages AutoSupport E-Series sans utiliser le port de gestion, reportez-vous au "instructions de configuration des paramètres de proxy de stockage".
6. Si la fonction sécurité du lecteur est activée pour l'appliance, créez et gérez la clé de sécurité.
   a. Sélectionnez **aide** pour accéder à l'aide en ligne de SANtricity System Manager.
   b. Utilisez la section **Paramètres** > **système** > **gestion des clés de sécurité** de l'aide en ligne pour en savoir plus sur la sécurité des lecteurs.
   c. Suivez les instructions « Comment faire » pour créer et gérer la clé de sécurité.
7. Si vous le souhaitez, modifiez le mot de passe administrateur.
   a. Sélectionnez **aide** pour accéder à l'aide en ligne de SANtricity System Manager.
   b. Utilisez la section **Accueil** > **Administration de la matrice de stockage** de l'aide en ligne pour en savoir plus sur le mot de passe administrateur.

c. Suivez les instructions « Comment faire » pour modifier le mot de passe.

Révision de l'état du matériel dans SANtricity System Manager

Vous pouvez utiliser SANtricity System Manager pour surveiller et gérer chaque composant matériel du tiroir de contrôleur de stockage, et pour examiner les informations de diagnostic et d'environnement sur le matériel, comme la température des composants et les problèmes liés aux disques.

Avant de commencer

- Vous utilisez un "navigateur web pris en charge".
- Pour accéder au Gestionnaire système SANtricity via le Gestionnaire de grille, vous disposez de l'autorisation d'administrateur de l'appliance de stockage ou de l'autorisation d'accès racine.
- Pour accéder au Gestionnaire système SANtricity à l'aide du programme d'installation de l'appliance StorageGRID, vous disposez du nom d'utilisateur et du mot de passe de l'administrateur du Gestionnaire système SANtricity.
- Pour accéder au Gestionnaire système SANtricity directement à l'aide d'un navigateur Web, vous disposez du nom d'utilisateur et du mot de passe de l'administrateur du Gestionnaire système SANtricity.

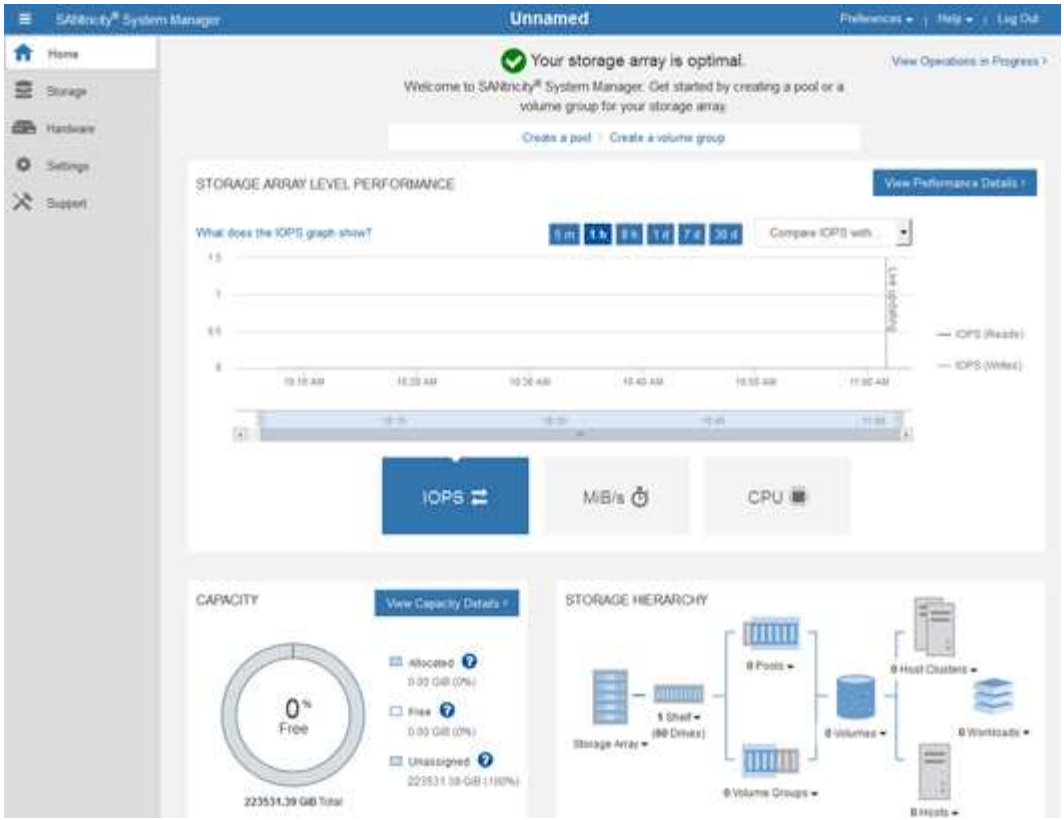
> Vous devez disposer du micrologiciel SANtricity 8.70 ou supérieur pour accéder au Gestionnaire système SANtricity à l'aide du Gestionnaire de grille ou du programme d'installation de l'appliance StorageGRID.

> L'accès à SANtricity System Manager à partir de Grid Manager ou du programme d'installation de l'appliance n'est généralement destiné qu'au contrôle de votre matériel et à la configuration des baies E-Series AutoSupport. De nombreuses fonctionnalités et opérations dans SANtricity System Manager, telles que la mise à niveau du firmware, ne s'appliquent pas à la surveillance de l'appliance StorageGRID. Pour éviter tout problème, suivez toujours les instructions d'installation et de maintenance du matériel de votre appareil.

Étapes

1. Accédez à SANtricity System Manager.
2. Entrez le nom d'utilisateur et le mot de passe de l'administrateur si nécessaire.
3. Cliquez sur **Annuler** pour fermer l'assistant de configuration et afficher la page d'accueil de SANtricity System Manager.

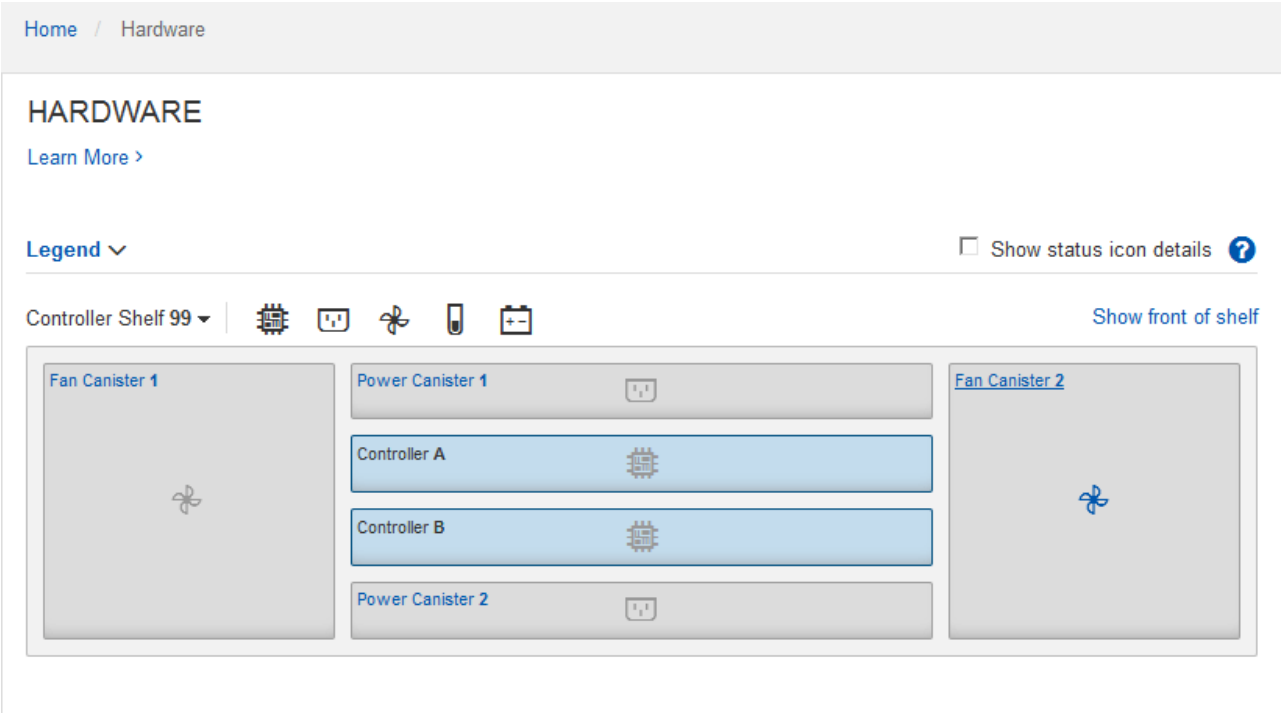
   La page d'accueil de SANtricity System Manager s'affiche. Dans SANtricity System Manager, le tiroir contrôleur est appelé baie de stockage.



4. Consultez les informations affichées pour le matériel de l'appareil et vérifiez que tous les composants matériels ont un état optimal.

   a. Cliquez sur l'onglet **matériel**.

   b. Cliquez sur **Afficher le verso de la tablette**.



À l'arrière, il est possible de voir les deux contrôleurs de stockage, la batterie de chaque contrôleur de stockage, les deux blocs d'alimentation, les deux blocs de ventilation et les tiroirs d'extension (le cas

échéant). Vous pouvez également afficher la température des composants.

a. Pour afficher les paramètres de chaque contrôleur de stockage, sélectionnez le contrôleur et sélectionnez **Afficher les paramètres** dans le menu contextuel.
b. Pour afficher les paramètres des autres composants à l'arrière du tiroir, sélectionnez le composant à afficher.
c. Cliquez sur **Afficher le recto de la tablette**, puis sélectionnez le composant que vous souhaitez afficher.

   Depuis l'avant du tiroir, vous pouvez afficher les disques et les tiroirs disques du tiroir contrôleur de stockage ou des tiroirs d'extension (le cas échéant).

Si l'état d'un composant nécessite une intervention, suivez les étapes du gourou de la restauration pour résoudre le problème ou contacter le support technique.

Définissez les adresses IP des contrôleurs de stockage à l'aide du programme d'installation de l'appliance StorageGRID

Le port de gestion 1 de chaque contrôleur de stockage connecte l'appliance au réseau de gestion pour SANtricity System Manager. Si vous ne pouvez pas accéder à SANtricity System Manager à partir du programme d'installation de l'appliance StorageGRID, définissez une adresse IP statique pour chaque contrôleur de stockage afin de vous assurer que vous ne perdez pas votre connexion de gestion au matériel et le firmware du contrôleur dans le tiroir contrôleur.

Avant de commencer

- Vous utilisez n'importe quel client de gestion pouvant vous connecter au réseau d'administration StorageGRID ou vous disposez d'un ordinateur portable de service.
- L'ordinateur portable client ou de service dispose d'un navigateur Web pris en charge.

Description de la tâche

Les adresses attribuées par DHCP peuvent être modifiées à tout moment. Attribuez des adresses IP statiques aux contrôleurs pour garantir une accessibilité cohérente.

> Suivez cette procédure uniquement si vous n'avez pas accès au Gestionnaire système SANtricity à partir du programme d'installation de l'appliance StorageGRID (**Avancé** > **Gestionnaire système SANtricity**) ou du Gestionnaire de grille (**NOEUDS** > **Gestionnaire système SANtricity**).

Étapes

1. Dans le client, entrez l'URL du programme d'installation de l'appliance StorageGRID : **`https://Appliance_Controller_IP:8443`**

   Pour *`Appliance_Controller_IP`*, Utilisez l'adresse IP du serveur sur tout réseau StorageGRID.

   La page d'accueil du programme d'installation de l'appliance StorageGRID s'affiche.

2. Sélectionnez **configurer le matériel** > **Configuration réseau du contrôleur de stockage**.

   La page Configuration réseau du contrôleur de stockage s'affiche.

3. Selon la configuration de votre réseau, sélectionnez **Enabled** pour IPv4, IPv6 ou les deux.

4. Notez l'adresse IPv4 qui s'affiche automatiquement.

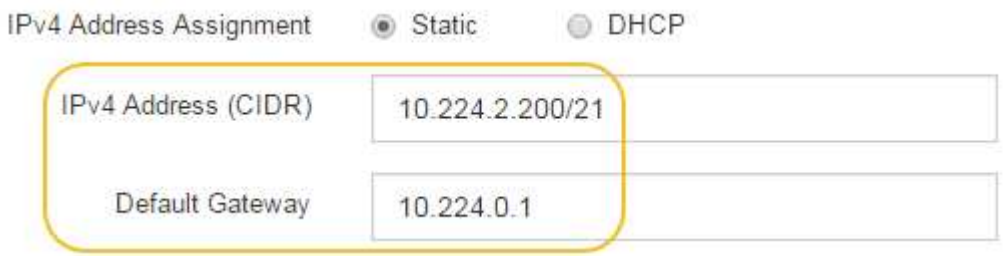
   DHCP est la méthode par défaut d'assignation d'une adresse IP au port de gestion du contrôleur de stockage.

   L'affichage des valeurs DHCP peut prendre quelques minutes.

5. Vous pouvez également définir une adresse IP statique pour le port de gestion du contrôleur de stockage.

   Vous devez attribuer une adresse IP statique au port de gestion ou attribuer un bail permanent à l'adresse sur le serveur DHCP.

   a. Sélectionnez **statique**.
   b. Saisissez l'adresse IPv4 à l'aide de la notation CIDR.
   c. Saisissez la passerelle par défaut.



   d. Cliquez sur **Enregistrer**.

      L'application de vos modifications peut prendre quelques minutes.

   Lorsque vous vous connectez à SANtricity System Manager, vous utiliserez la nouvelle adresse IP statique comme URL :
   `https://Storage_Controller_IP`

Configuration de l'interface BMC (SGF6112, SG6000, SG100 et SG1000)

Interface BMC : présentation (SGF6112, SG6000, SG100 et SG1000)

L'interface utilisateur du contrôleur BMC (Baseboard Management Controller) sur le système SGF6112, SG6000 ou services fournit des informations sur l'état du matériel et vous permet de configurer les paramètres SNMP et d'autres options pour les appliances.

Utilisez les procédures suivantes de cette section pour configurer le contrôleur BMC lors de l'installation de l'appliance :

- "Modifier le mot de passe admin ou root de l'interface BMC"
- "Définissez l'adresse IP du port de gestion BMC"
- "Accéder à l'interface BMC"
- "Configurer les paramètres SNMP"
- "Configurez les notifications par e-mail pour les alertes BMC"

> Si l'appliance a déjà été installée dans une grille et exécute le logiciel StorageGRID, procédez comme suit :
>
> - "Mettez l'appareil en mode de maintenance" Pour accéder au programme d'installation de l'appliance StorageGRID.
> - Voir "Définissez l'adresse IP du port de gestion BMC" Pour plus d'informations sur l'accès à l'interface BMC à l'aide du programme d'installation de l'appliance StorageGRID.

Modifier le mot de passe admin ou root de l'interface BMC

Pour des raisons de sécurité, vous devez modifier le mot de passe de l'administrateur ou de l'utilisateur root du contrôleur BMC.

Avant de commencer

Le client de gestion utilise un "navigateur web pris en charge".

Description de la tâche

Lorsque vous installez l'appliance pour la première fois, le contrôleur BMC utilise un mot de passe par défaut pour l'administrateur ou l'utilisateur root. Vous devez modifier le mot de passe de l'administrateur ou de l'utilisateur root pour sécuriser votre système.

L'utilisateur par défaut dépend de la date d'installation de l'appliance StorageGRID. L'utilisateur par défaut est **admin** pour les nouvelles installations et **root** pour les anciennes installations.

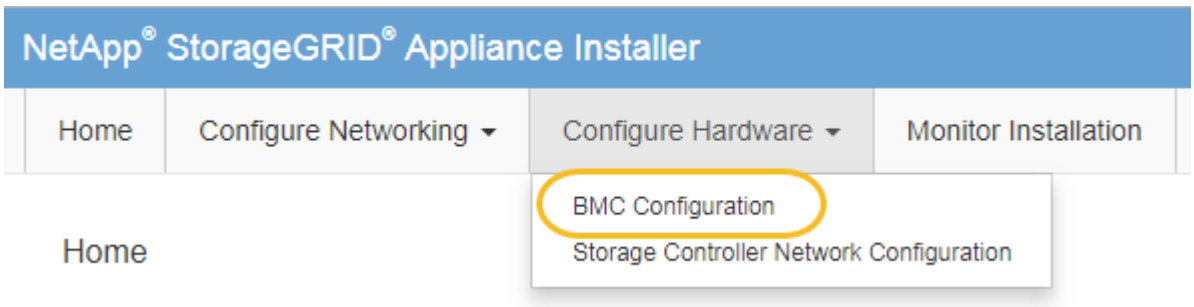
Étapes

1. Dans le client, entrez l'URL du programme d'installation de l'appliance StorageGRID : **`https://Appliance_IP:8443`**

   Pour *`Appliance_IP`*, Utilisez l'adresse IP du serveur sur tout réseau StorageGRID.

   La page d'accueil du programme d'installation de l'appliance StorageGRID s'affiche.

2. Sélectionnez **configurer le matériel** > **BMC Configuration**.



   La page Configuration du contrôleur de gestion de la carte mère s'affiche.

3. Entrez un nouveau mot de passe pour le compte admin ou root dans les deux champs prévus à cet effet.
4. Cliquez sur **Enregistrer**.

Définissez l'adresse IP du port de gestion BMC

Avant de pouvoir accéder à l'interface BMC, configurez l'adresse IP du port de gestion BMC sur le contrôleur SGF6112, SG6000-CN ou les appliances de services.

Si vous utilisez ConfigBuilder pour générer un fichier JSON, vous pouvez configurer automatiquement les adresses IP. Voir "Automatisez l'installation et la configuration de l'appliance".

Avant de commencer

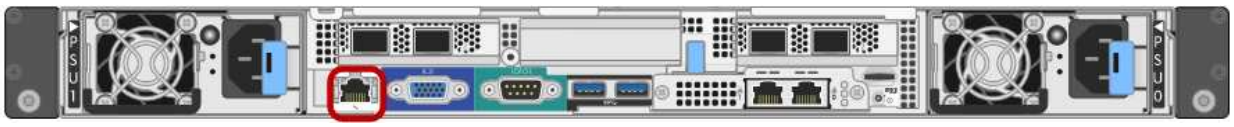
- Le client de gestion utilise un "navigateur web pris en charge".
- Vous utilisez n'importe quel client de gestion pouvant se connecter à un réseau StorageGRID.
- Le port de gestion BMC est connecté au réseau de gestion que vous souhaitez utiliser.

SG6112

SG6000

SG1000

SG100



Description de la tâche

Pour des raisons de prise en charge, le port de gestion BMC permet un accès matériel de faible niveau.

> Vous ne devez connecter ce port qu'à un réseau de gestion interne sécurisé, fiable et. Si aucun réseau de ce type n'est disponible, laissez le port BMC déconnecté ou bloqué, à moins qu'une connexion BMC ne soit demandée par le support technique.

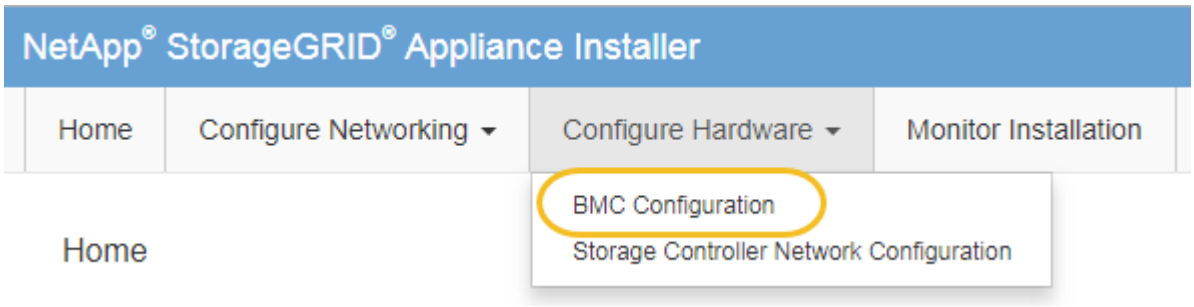
Étapes

1. Dans le client, entrez l'URL du programme d'installation de l'appliance StorageGRID :
   `https://Appliance_IP:8443`

Pour `Appliance_IP`, Utilisez l'adresse IP du serveur sur tout réseau StorageGRID.

La page d'accueil du programme d'installation de l'appliance StorageGRID s'affiche.

2. Sélectionnez **configurer le matériel** > **BMC Configuration**.

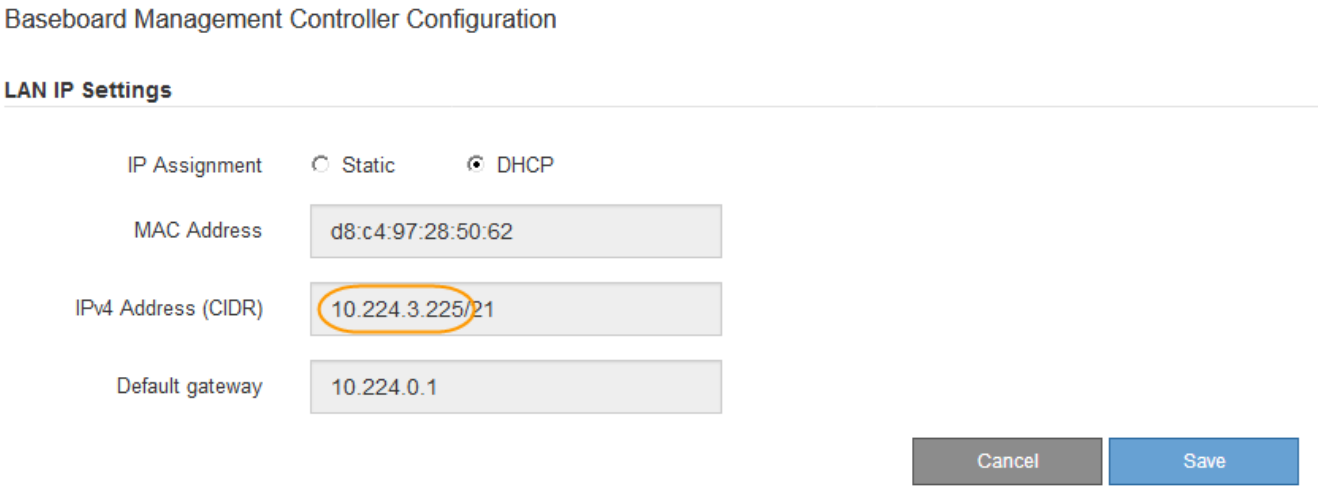


La page Configuration du contrôleur de gestion de la carte mère s'affiche.

3. Notez l'adresse IPv4 qui s'affiche automatiquement.

DHCP est la méthode par défaut pour attribuer une adresse IP à ce port.

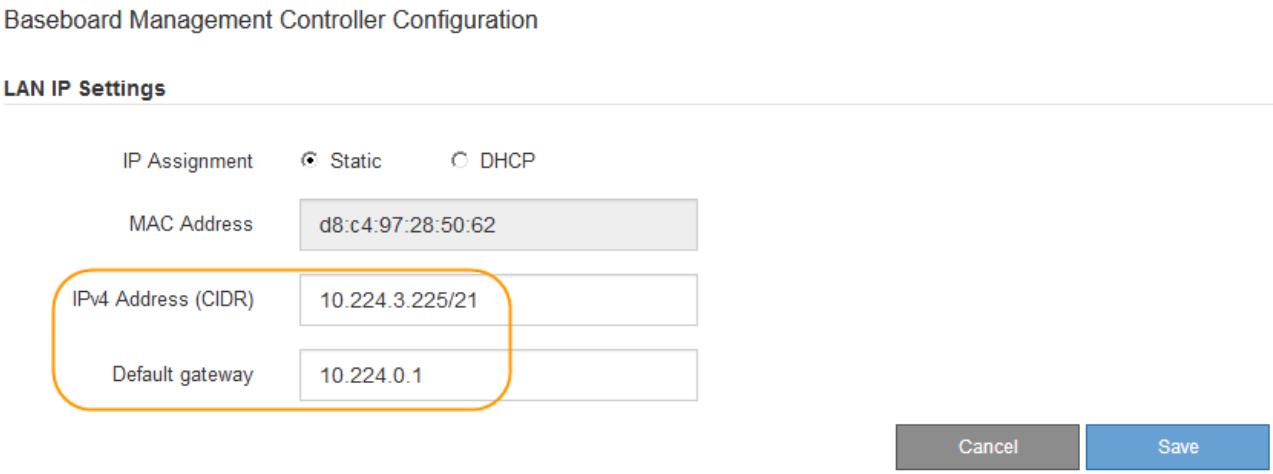
L'affichage des valeurs DHCP peut prendre quelques minutes.



4. Vous pouvez également définir une adresse IP statique pour le port de gestion BMC.

Vous devez attribuer une adresse IP statique au port de gestion BMC ou attribuer un bail permanent à l'adresse sur le serveur DHCP.

a. Sélectionnez **statique**.
b. Saisissez l'adresse IPv4 à l'aide de la notation CIDR.
c. Saisissez la passerelle par défaut.



d. Cliquez sur **Enregistrer**.

L'application de vos modifications peut prendre quelques minutes.

Accéder à l'interface BMC

Vous pouvez accéder à l'interface du contrôleur BMC à l'aide de l'adresse IP DHCP ou statique du port de gestion du contrôleur BMC sur les modèles d'appliance suivants :

- SGF6112
- SG6000
- SG1000
- SG100

Avant de commencer

- Le client de gestion utilise un "navigateur web pris en charge".
- Le port de gestion BMC de l'appliance est connecté au réseau de gestion que vous prévoyez d'utiliser.

SGF6112

SG6000

SG1000

SG100

Étapes

1. Entrez l'URL de l'interface BMC :
   `https://BMC_Port_IP`

   Pour *`BMC_Port_IP`*, Utilisez l'adresse DHCP ou l'adresse IP statique pour le port de gestion BMC.

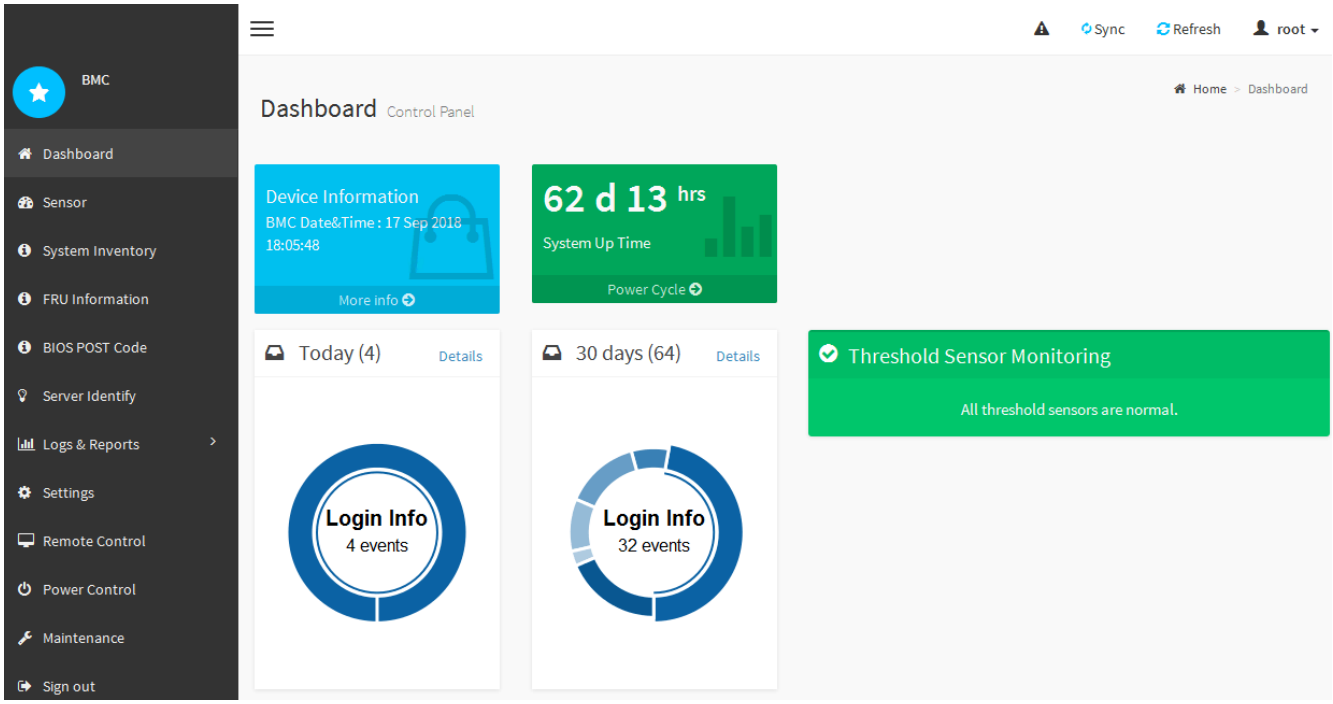
   La page de connexion BMC s'affiche.

   > Si vous n'avez pas encore configuré `BMC_Port_IP`, suivez les instructions de la section "Configurer l'interface BMC". Si vous ne pouvez pas suivre cette procédure en raison d'un problème matériel et si vous n'avez pas encore configuré d'adresse IP BMC, vous pourrez peut-être continuer à accéder au contrôleur BMC. Par défaut, le contrôleur BMC obtient une adresse IP à l'aide de DHCP. Si le protocole DHCP est activé sur le réseau BMC, votre administrateur réseau peut fournir l'adresse IP attribuée au contrôleur BMC MAC, qui est imprimée sur l'étiquette située à l'avant de l'appliance. Si DHCP n'est pas activé sur le réseau BMC, le BMC ne répond pas au bout de quelques minutes et se attribue l'IP statique par défaut `192.168.0.120`. Vous devrez peut-être connecter votre ordinateur portable directement au port BMC et modifier le paramètre réseau pour attribuer à votre ordinateur portable une adresse IP telle que `192.168.0.200/24`, afin de naviguer jusqu'à `192.168.0.120`.

2. Entrez le nom d'utilisateur et le mot de passe admin ou root, en utilisant le mot de passe que vous avez défini "mot de passe racine par défaut modifié":

   > L'utilisateur par défaut dépend de la date d'installation de l'appliance StorageGRID. L'utilisateur par défaut est **admin** pour les nouvelles installations et **root** pour les anciennes installations.

3. Sélectionnez **se connecter**.



4. Vous pouvez également créer d'autres utilisateurs en sélectionnant **Paramètres** > **gestion des utilisateurs** et en cliquant sur tout utilisateur « désactivé ».

> Lorsque les utilisateurs se connectant pour la première fois, ils peuvent être invités à modifier leur mot de passe pour une sécurité accrue.

Configurer les paramètres SNMP pour le contrôleur BMC

Si vous connaissez la configuration de SNMP pour le matériel, vous pouvez utiliser l'interface BMC pour configurer les paramètres SNMP des appliances SGF6112, SG6000 et services. Vous pouvez fournir des chaînes de communauté sécurisées, activer le Trap SNMP et spécifier jusqu'à cinq destinations SNMP.

Avant de commencer

- Vous savez comment accéder au tableau de bord BMC.
- Vous avez de l'expérience dans la configuration des paramètres SNMP pour les équipements SNMPv1-v2c.

> Les paramètres BMC définis lors de cette procédure peuvent ne pas être préservés en cas de défaillance de l'appliance et doivent être remplacés. Assurez-vous d'avoir un enregistrement de tous les paramètres que vous avez appliqués afin de pouvoir les réappliquer facilement après un remplacement de matériel si nécessaire.

Étapes

1. Dans le tableau de bord BMC, sélectionnez **Paramètres** > **Paramètres SNMP**.
2. Sur la page Paramètres SNMP, sélectionnez **Activer SNMP V1/V2**, puis fournissez une chaîne de communauté en lecture seule et une chaîne de communauté en lecture-écriture.

La chaîne de communauté en lecture seule est comme un ID utilisateur ou un mot de passe. Vous devez modifier cette valeur pour empêcher les intrus d'obtenir des informations sur la configuration de votre réseau. La chaîne de communauté lecture-écriture protège le périphérique contre les modifications non autorisées.

3. Vous pouvez également sélectionner **Activer le recouvrement** et saisir les informations requises.

> Entrez l'adresse IP de destination pour chaque interruption SNMP utilisant une adresse IP. Les noms de domaine complets ne sont pas pris en charge.

Activez les interruptions si vous souhaitez que l'appliance envoie des notifications immédiates à une console SNMP lorsqu'elle est dans un état inhabituel. Selon le périphérique, des interruptions peuvent indiquer des pannes matérielles de différents composants, des conditions de liaison vers le haut/bas, des seuils de température dépassés ou un trafic élevé.

4. Vous pouvez également cliquer sur **Envoyer piège de test** pour tester vos paramètres.
5. Si les paramètres sont corrects, cliquez sur **Enregistrer**.

Configurez les notifications par e-mail pour les alertes BMC

Si vous souhaitez envoyer des notifications par e-mail lorsque des alertes se produisent, utilisez l'interface BMC pour configurer les paramètres SMTP, les utilisateurs, les destinations LAN, les stratégies d'alerte et les filtres d'événements.

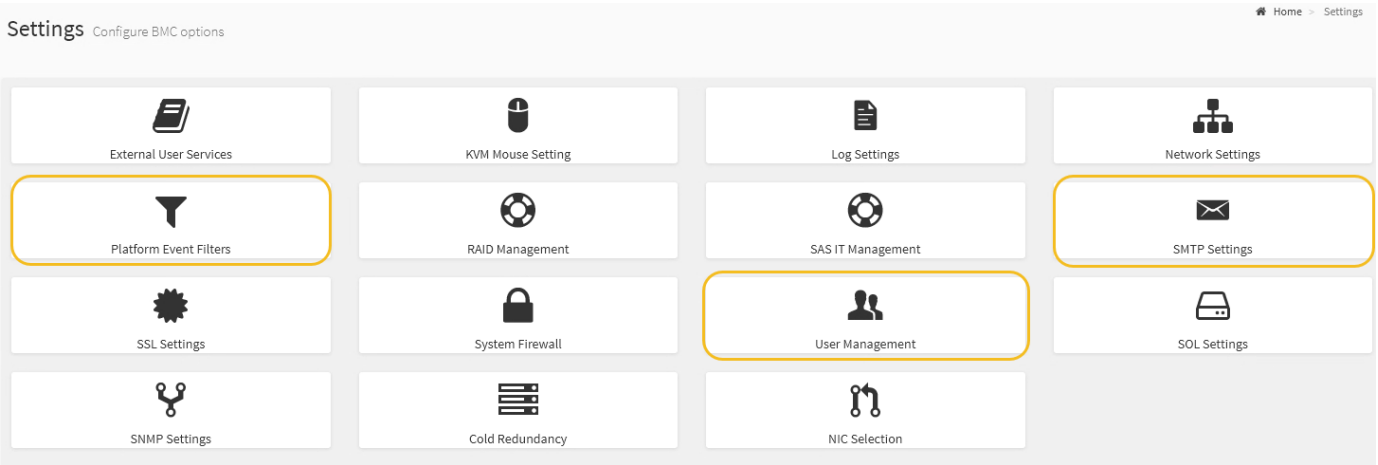
> Les paramètres BMC définis par cette procédure peuvent ne pas être conservés si le contrôleur SG6000-CN ou l'appliance de services tombe en panne et doit être remplacée. Assurez-vous d'avoir un enregistrement de tous les paramètres que vous avez appliqués afin de pouvoir les réappliquer facilement après un remplacement de matériel si nécessaire.

Avant de commencer

Vous savez comment accéder au tableau de bord BMC.

Description de la tâche

Dans l'interface BMC, vous utilisez les options **Paramètres SMTP**, **gestion des utilisateurs** et **filtres d'événements de la plate-forme** de la page Paramètres pour configurer les notifications par e-mail.



Étapes

1. "Configurer les paramètres SNMP pour le contrôleur BMC".
   a. Sélectionnez **Paramètres** > **Paramètres SMTP**.
   b. Pour l'ID e-mail de l'expéditeur, saisissez une adresse e-mail valide.

      Cette adresse e-mail est fournie comme adresse de lorsque le contrôleur BMC envoie un e-mail.

2. Configurez les utilisateurs pour recevoir des alertes.
   a. Dans le tableau de bord BMC, sélectionnez **Paramètres** > **User Management**.
   b. Ajoutez au moins un utilisateur pour recevoir des notifications d'alerte.

      L'adresse e-mail que vous configurez pour un utilisateur est l'adresse à laquelle le contrôleur BMC envoie des notifications d'alerte. Par exemple, vous pouvez ajouter un utilisateur générique, tel que « utilisateur de notification », et utiliser l'adresse électronique d'une liste de diffusion par courrier électronique de l'équipe d'assistance technique.

3. Configurez la destination du réseau local pour les alertes.
   a. Sélectionnez **Paramètres** > **filtres d'événements plateforme** > **destinations LAN**.
   b. Configurez au moins une destination LAN.
      - Sélectionnez **Email** comme Type de destination.
      - Pour le nom d'utilisateur BMC, sélectionnez un nom d'utilisateur que vous avez ajouté précédemment.
      - Si vous avez ajouté plusieurs utilisateurs et que vous souhaitez qu'ils reçoivent tous des e-mails de notification, ajoutez une destination LAN pour chaque utilisateur.
   c. Envoyer une alerte de test.
4. Configurez les règles d'alerte afin de définir le moment et l'emplacement d'envoi des alertes par le contrôleur BMC.
   a. Sélectionnez **Paramètres** > **filtres d'événements de plateforme** > **stratégies d'alerte**.
   b. Configurez au moins une règle d'alerte pour chaque destination LAN.
      - Pour Numéro de groupe de polices, sélectionnez **1**.
      - Pour l'action de police, sélectionnez **toujours envoyer l'alerte à cette destination**.
      - Pour le canal LAN, sélectionnez **1**.
      - Dans le sélecteur de destination, sélectionnez la destination LAN de la stratégie.
5. Configurez les filtres d'événements pour diriger les alertes pour différents types d'événements vers les utilisateurs appropriés.
   a. Sélectionnez **Paramètres** > **filtres d'événements de plate-forme** > **filtres d'événements**.
   b. Pour Numéro de groupe de police d'alerte, entrez **1**.
   c. Créez des filtres pour chaque événement auquel vous souhaitez que le groupe de stratégies d'alerte soit averti.
      - Vous pouvez créer des filtres d'événements pour les actions de puissance, les événements de capteur spécifiques ou tous les événements.
      - Si vous n'êtes pas certain des événements à surveiller, sélectionnez **tous les capteurs** pour Type de capteur et **tous les événements** pour Options d'événements. Si vous recevez des notifications indésirables, vous pouvez modifier vos sélections ultérieurement.

Facultatif : activez le chiffrement de nœud

Si vous activez le chiffrement des nœuds, les disques de votre appliance peuvent être protégés par le chiffrement sécurisé des serveurs de gestion des clés (KMS) contre les pertes physiques ou la suppression du site. Vous devez sélectionner et activer le chiffrement des nœuds lors de l'installation de l'appliance. Vous ne pouvez pas désactiver le chiffrement de nœud après le démarrage du processus de chiffrement KMS.

Si vous utilisez ConfigBuilder pour générer un fichier JSON, vous pouvez activer le chiffrement de nœud automatiquement. Voir "Automatisez l'installation et la configuration de l'appliance".

Avant de commencer

Passez en revue les informations sur "Configuration de KMS".

Description de la tâche

Une appliance pour laquelle le chiffrement des nœuds est activé se connecte au serveur de gestion externe des clés (KMS) configuré pour le site StorageGRID. Chaque cluster KMS (ou KMS) gère les clés de chiffrement pour tous les nœuds d'appliance du site. Ces clés cryptent et décrypter les données sur chaque disque d'une appliance sur laquelle le cryptage des nœuds est activé.

Un KMS peut être configuré dans Grid Manager avant ou après l'installation de l'appliance dans StorageGRID. Pour plus d'informations, consultez les informations sur la configuration du KMS et de l'appliance dans les instructions d'administration de StorageGRID.

- Si un KMS est configuré avant l'installation de l'appliance, le chiffrement contrôlé par KMS commence lorsque vous activez le chiffrement des nœuds sur l'appliance et l'ajoutez à un site StorageGRID où le KMS est configuré.
- Si un KMS n'est pas configuré avant l'installation de l'appliance, le chiffrement contrôlé par KMS est appliqué sur chaque appliance pour que le chiffrement des nœuds soit activé dès qu'un KMS est configuré et disponible pour le site qui contient le nœud d'appliance.

> Lorsqu'un dispositif est installé et que le chiffrement de nœud est activé, une clé temporaire est attribuée. Les données de l'appliance ne sont pas protégées tant que l'appliance n'est pas connectée au système de gestion des clés (KMS) et qu'une clé de sécurité KMS n'est pas installée. Voir la "Présentation de la configuration de l'appliance KM" pour plus d'informations.

Sans la clé KMS requise pour décrypter le disque, les données de l'appliance ne peuvent pas être récupérées et sont perdues. C'est le cas lorsque la clé de déchiffrement ne peut pas être récupérée à partir du KMS. La clé devient inaccessible si un client efface la configuration KMS, une clé KMS expire, la connexion au KMS est perdue ou l'appliance est supprimée du système StorageGRID dans lequel ses clés KMS sont installées.

Étapes

1. Ouvrez un navigateur et entrez l'une des adresses IP du contrôleur de calcul de l'appliance.

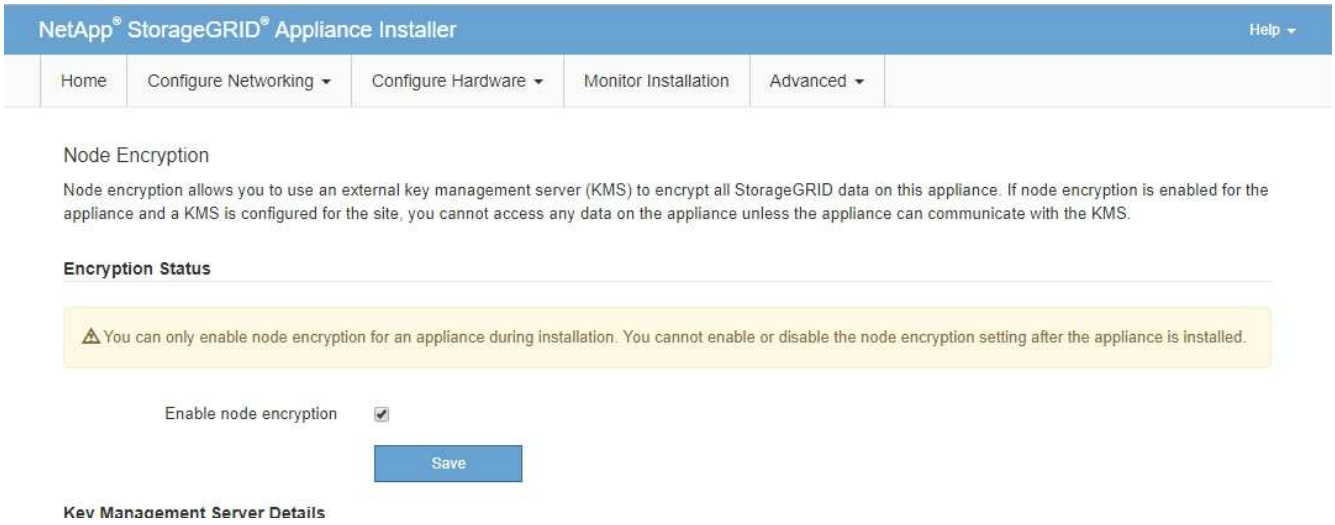
   `https://Controller_IP:8443`

   `Controller_IP` Est l'adresse IP du contrôleur de calcul (pas le contrôleur de stockage) sur l'un des trois réseaux StorageGRID.

   La page d'accueil du programme d'installation de l'appliance StorageGRID s'affiche.

Une fois l'appliance chiffrée à l'aide d'une clé KMS, les disques de l'appliance ne peuvent pas être déchiffrés sans utiliser la même clé KMS.

2. Sélectionnez **configurer le matériel** > **cryptage de nœud**.



3. Sélectionnez **Activer le cryptage de noeud**.

   Avant l'installation de l'appliance, vous pouvez effacer **Activer le chiffrement de nœud** sans risque de perte de données. Lorsque l'installation commence, le nœud de l'appliance accède aux clés de chiffrement KMS dans votre système StorageGRID et commence le chiffrement des disques. Une fois l'appliance installée, vous ne pouvez pas désactiver le chiffrement des nœuds.

   Après avoir ajouté une appliance sur laquelle le chiffrement des nœuds est activé sur un site StorageGRID doté d'un KMS, vous ne pouvez pas arrêter d'utiliser le chiffrement KMS pour le nœud.

4. Sélectionnez **Enregistrer**.
5. Déployez l'appliance en tant que nœud dans votre système StorageGRID.

   Le chiffrement CONTRÔLÉ PAR UNE DISTANCE DE 1 KM commence lorsque l'appliance accède aux clés KMS configurées pour votre site StorageGRID. Le programme d'installation affiche des messages de progression pendant le processus de chiffrement KMS, ce qui peut prendre quelques minutes selon le nombre de volumes de disque dans l'appliance.

   L'appliance est au départ configurée avec une clé de chiffrement aléatoire non KMS attribuée à chaque volume de disque. Les disques sont chiffrés à l'aide de cette clé de chiffrement temporaire, qui n'est pas sécurisée, tant que l'appliance sur laquelle le chiffrement de nœud est activé n'a pas accès aux clés KMS configurées pour votre site StorageGRID.

Une fois que vous avez terminé

Vous pouvez afficher l'état du chiffrement de nœud, les détails KMS et les certificats utilisés lorsque le nœud d'appliance est en mode de maintenance. Voir "Surveillez le chiffrement des nœuds en mode de maintenance" pour plus d'informations.

Facultatif : modifier le mode RAID

Sur certains modèles d'appliance, vous pouvez changer de mode RAID sur l'appliance pour répondre à vos besoins en stockage et en restauration. Vous ne pouvez modifier le mode qu'avant de déployer l'appliance Storage Node.

Si vous utilisez ConfigBuilder pour générer un fichier JSON, vous pouvez modifier le mode RAID automatiquement. Voir "Automatisez l'installation et la configuration de l'appliance".

Description de la tâche

Si votre appliance est prise en charge, vous pouvez choisir l'une des options de configuration de volume suivantes :

- **DDP** : ce mode utilise deux disques de parité pour huit disques de données. Il s'agit du mode par défaut et recommandé pour tous les appareils. Par rapport au niveau RAID 6, les pools de disques dynamiques offrent de meilleures performances du système, un temps de reconstruction réduit après une panne disque et une gestion simplifiée. Ils assurent également la protection contre la perte de tiroirs dans les appliances SG5760.

> Les DDP ne protègent pas la perte de tiroirs dans les appliances SG6060 en raison des deux disques SSD. La protection contre la perte des tiroirs est effective dans toutes les étagères d'extension ajoutées à une SG6060.

- **DDP16** : ce mode utilise deux disques de parité pour chaque 16 disques de données, ce qui améliore l'efficacité du stockage par rapport au pool DDP. Par rapport à RAID 6, DDP16 offre de meilleures performances système, des délais de reconstruction réduits après une panne disque, une gestion simplifiée et une efficacité de stockage comparable. Pour utiliser le mode DDP16, votre configuration doit contenir au moins 20 lecteurs. Le DDP16 n'offre pas de protection contre les pertes de tiroirs.
- **RAID6** : ce mode utilise deux lecteurs de parité pour chaque disque de données de 16 ou plus. Il s'agit d'un schéma de protection matérielle qui utilise des bandes de parité sur chaque disque et autorise deux pannes de disque au sein de l'ensemble RAID avant la perte de données. Pour utiliser le mode RAID 6, votre configuration doit contenir au moins 20 lecteurs. Bien que RAID 6 puisse améliorer l'efficacité du stockage de l'appliance par rapport à des pools de disques dynamiques, il n'est pas recommandé dans la plupart des environnements StorageGRID.

> Si un volume a déjà été configuré ou si StorageGRID a été installé précédemment, la modification du mode RAID entraîne le retrait et le remplacement des volumes. Toutes les données présentes sur ces volumes seront perdues.

SG6000

Avant de commencer

- Vous utilisez n'importe quel client pouvant vous connecter à StorageGRID.
- Le client a un "navigateur web pris en charge".

Étapes

1. Ouvrez un navigateur et entrez l'une des adresses IP du contrôleur de calcul de l'appliance.

   `https://Controller_IP:8443`

   `Controller_IP` Est l'adresse IP du contrôleur de calcul (pas le contrôleur de stockage) sur l'un des trois réseaux StorageGRID.

   La page d'accueil du programme d'installation de l'appliance StorageGRID s'affiche.

2. Sélectionnez **Avancé** > **mode RAID**.
3. Sur la page **configurer le mode RAID**, sélectionnez le mode RAID souhaité dans la liste déroulante mode.
4. Cliquez sur **Enregistrer**.

SG5760

Avant de commencer

- Vous avez un SG5760 avec 60 disques. Si vous disposez d'un SG5712, vous devez utiliser le mode DDP par défaut.
- Vous utilisez n'importe quel client pouvant vous connecter à StorageGRID.
- Le client a un "navigateur web pris en charge".

Étapes

1. À l'aide de l'ordinateur portable de service, ouvrez un navigateur Web et accédez au programme d'installation de l'appliance StorageGRID :
   `https://E5700SG_Controller_IP:8443`

   Où *`E5700SG_Controller_IP`* Est l'une des adresses IP du contrôleur E5700SG.

2. Sélectionnez **Avancé** > **mode RAID**.
3. Sur la page **configurer le mode RAID**, sélectionnez le mode RAID souhaité dans la liste déroulante mode.
4. Cliquez sur **Enregistrer**.

Informations associées

"Site de documentation sur les systèmes NetApp E-Series"

Facultatif : remappage des ports réseau pour l'appliance

Vous pouvez éventuellement remapper les ports internes d'un nœud d'appliance sur différents ports externes. Par exemple, il peut être nécessaire de remappage les ports en raison d'un problème de pare-feu.

Avant de commencer

- Vous avez déjà accédé au programme d'installation de l'appliance StorageGRID.

Description de la tâche

Vous ne pouvez pas utiliser de ports remappés pour les terminaux d'équilibrage de charge. Si vous devez supprimer un port remappé, suivez les étapes de la section "Supprimer les mappages de port".

Étapes

1. Dans le programme d'installation de l'appliance StorageGRID, sélectionnez **configurer la mise en réseau** > **Remap ports**.

   La page Port de remise à neuf s'affiche.

2. Dans la liste déroulante **Network**, sélectionnez le réseau du port que vous souhaitez remappage : grid, Admin ou client.
3. Dans la liste déroulante **Protocol**, sélectionnez le protocole IP : TCP ou UDP.
4. Dans la zone de liste déroulante **Remap Direction**, sélectionnez la direction du trafic que vous souhaitez remappage pour ce port : entrant, sortant ou bidirectionnel.
5. Pour **Port d'origine**, entrez le numéro du port que vous souhaitez remappage.
6. Pour **mappé sur le port**, entrez le numéro du port que vous souhaitez utiliser à la place.
7. Sélectionnez **Ajouter une règle**.

   Le nouveau mappage de port est ajouté à la table et le remappage est immédiatement pris en compte.

8. Pour supprimer un mappage de port, sélectionnez le bouton radio de la règle que vous souhaitez supprimer, puis sélectionnez **Supprimer la règle sélectionnée**.

Déployez le nœud de l'appliance

Déployez le nœud de stockage de l'appliance

Après avoir installé et configuré l'appliance de stockage, vous pouvez la déployer en tant que nœud de stockage dans un système StorageGRID. Lorsque vous déployez une appliance en tant que nœud de stockage, utilisez le programme d'installation de l'appliance StorageGRID inclus sur l'appliance.

Avant de commencer

- Si vous clonez un nœud d'appliance, continuez à suivre les instructions de la section "clonage des nœuds de l'appliance" processus.
- L'appliance a été installée dans un rack ou une armoire, connectée à vos réseaux et sous tension.
- Les liens réseau, les adresses IP et le remappage des ports (si nécessaire) ont été configurés pour le serveur à l'aide du programme d'installation de l'appliance StorageGRID.
- Vous connaissez l'une des adresses IP attribuées au contrôleur de calcul de l'appliance. Vous pouvez utiliser l'adresse IP de n'importe quel réseau StorageGRID connecté.
- Le nœud d'administration principal du système StorageGRID a été déployé.
- Tous les sous-réseaux de réseau Grid répertoriés sur la page de configuration IP du programme d'installation de l'appliance StorageGRID ont été définis dans la liste de sous-réseaux de réseau de grille sur le nœud d'administration principal.

- Vous avez un ordinateur portable de service avec un navigateur Web pris en charge.

Description de la tâche

Chaque appliance de stockage fonctionne comme un seul nœud de stockage. Tout appareil peut se connecter au réseau Grid, au réseau Admin et au réseau client

Pour déployer un nœud de stockage d'appliance dans un système StorageGRID, accédez au programme d'installation de l'appliance StorageGRID et effectuez les opérations suivantes :

- Vous spécifiez ou confirmez l'adresse IP du nœud d'administration principal et le nom du nœud de stockage.
- Vous démarrez le déploiement et attendez que les volumes soient configurés et que le logiciel soit installé.
- Une fois l'installation interrompue pendant une pause dans les tâches d'installation de l'appliance, vous reprenez l'installation en vous connectant au Gestionnaire de grille, en approuvant tous les nœuds de la grille et en complétant les processus d'installation et de déploiement de StorageGRID.

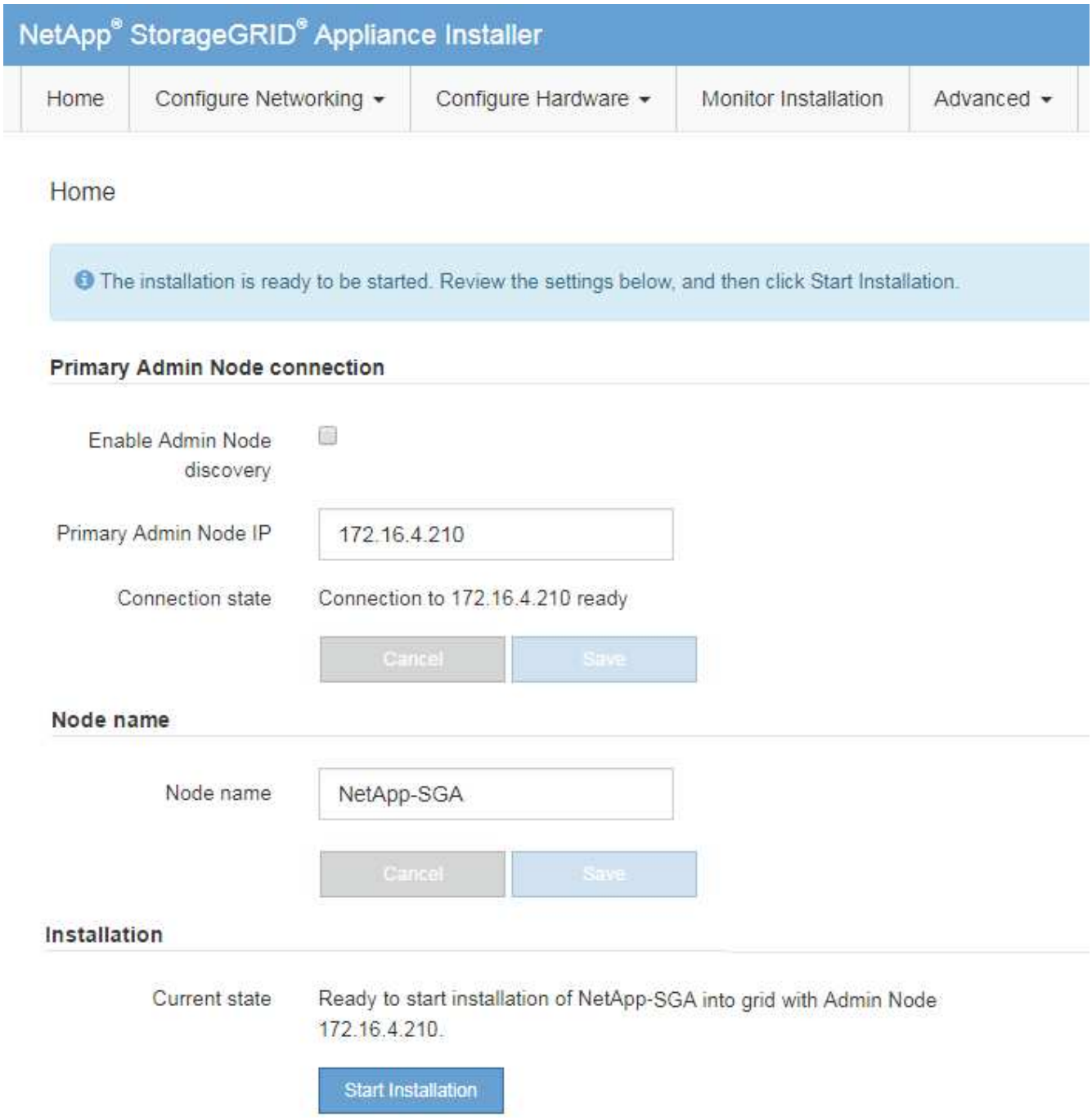
> Si vous devez déployer plusieurs nœuds d'appliance à la fois, vous pouvez automatiser le processus d'installation à l'aide du `configure-sga.py` Script d'installation de l'appliance.

- Si vous effectuez une opération d'extension ou de récupération, suivez les instructions appropriées :
  - Pour ajouter un nœud de stockage d'appliance à un système StorageGRID existant, reportez-vous aux instructions de "ajout de nœuds grid".
  - Pour déployer un nœud de stockage d'appliance dans le cadre d'une opération de restauration, reportez-vous aux instructions "Restauration d'un nœud de stockage d'appliance".

Étapes

1. Ouvrez un navigateur et entrez l'une des adresses IP du contrôleur de calcul de l'appliance.
   `https://Controller_IP:8443`

   La page d'accueil du programme d'installation de l'appliance StorageGRID s'affiche.



2. Dans la section **connexion au noeud d'administration principal**, déterminez si vous devez spécifier l'adresse IP du noeud d'administration principal.

   Si vous avez déjà installé d'autres nœuds dans ce centre de données, le programme d'installation de l'appliance StorageGRID peut détecter automatiquement cette adresse IP, en supposant que le nœud d'administration principal, ou au moins un autre nœud de grille avec ADMIN_IP configuré, soit présent sur le même sous-réseau.

3. Si cette adresse IP n'apparaît pas ou si vous devez la modifier, spécifiez l'adresse :

Option	Description
Entrée IP manuelle	a. Décochez la case **Activer la découverte du noeud d'administration**. b. Saisissez l'adresse IP manuellement. c. Cliquez sur **Enregistrer**. d. Attendez que l'état de connexion de la nouvelle adresse IP soit prêt.
Détection automatique de tous les nœuds d'administration principaux connectés	a. Cochez la case **Activer la découverte du noeud d'administration**. b. Attendez que la liste des adresses IP découvertes s'affiche. c. Sélectionnez le nœud d'administration principal de la grille dans laquelle ce nœud de stockage de l'appliance sera déployé. d. Cliquez sur **Enregistrer**. e. Attendez que l'état de connexion de la nouvelle adresse IP soit prêt.

4. Dans le champ **Nom du nœud**, indiquez le nom du système que vous souhaitez utiliser pour ce nœud d'appliance, puis cliquez sur **Enregistrer**.

   Le nom qui apparaît ici correspond au nom système du nœud de l'appliance. Les noms de système sont requis pour les opérations StorageGRID internes et ne peuvent pas être modifiés.

5. Dans la section **installation**, vérifiez que l'état actuel est « prêt à démarrer l'installation de `node name` Dans le grid avec le nœud d'administration principal `admin_ip` " Et que le bouton **Start installation** est activé.

   Si le bouton **Start installation** n'est pas activé, vous devrez peut-être modifier la configuration réseau ou les paramètres de port. Pour obtenir des instructions, reportez-vous aux instructions d'entretien de votre appareil.

   > Si vous déployez l'appliance Storage Node en tant que cible de clonage de nœud, arrêtez le processus de déploiement ici et poursuivez la"procédure de clonage de nœud".

6. Dans la page d'accueil du programme d'installation de l'appliance StorageGRID, cliquez sur **Démarrer l'installation**.

   L'état actuel passe à « installation en cours » et la page installation du moniteur s'affiche.

   > Si vous devez accéder manuellement à la page installation du moniteur, cliquez sur **installation du moniteur**.

7. Si votre grid inclut plusieurs nœuds de stockage d'appliance, répétez cette procédure pour chaque appliance.

Si vous devez déployer plusieurs nœuds de stockage d'appliance à la fois, vous pouvez automatiser le processus d'installation à l'aide du `configure-sga.py` Script d'installation de l'appliance.

Déployez le nœud d'appliance des services

Vous pouvez déployer une appliance de services en tant que nœud d'administration principal, nœud d'administration non primaire ou nœud de passerelle. Les appliances SG100 et SG1000 peuvent fonctionner en même temps en tant que nœuds de passerelle et nœuds d'administration (principal ou non primaire).

Déployez l'appliance de services en tant que nœud d'administration principal

Lorsque vous déployez une appliance de services en tant que nœud d'administration principal, utilisez le programme d'installation de l'appliance StorageGRID inclus sur l'appliance pour installer le logiciel StorageGRID ou téléchargez la version du logiciel que vous souhaitez installer. Vous devez installer et configurer le nœud d'administration principal avant d'installer tout autre type de nœud d'appliance. Un nœud d'administration principal peut se connecter au réseau Grid et au réseau d'administration et au réseau client en option, si un ou les deux sont configurés.

Avant de commencer

- L'appliance a été installée dans un rack ou une armoire, connectée à vos réseaux et sous tension.
- Les liens réseau, les adresses IP et le remappage des ports (si nécessaire) ont été configurés pour le serveur à l'aide du programme d'installation de l'appliance StorageGRID.
- Vous avez un ordinateur portable de service avec un "navigateur web pris en charge".
- Vous connaissez l'une des adresses IP attribuées à l'appliance. Vous pouvez utiliser l'adresse IP de n'importe quel réseau StorageGRID connecté.

Description de la tâche

Pour installer StorageGRID sur un nœud d'administration principal de l'appliance :

- Vous utilisez le programme d'installation de l'appliance StorageGRID pour installer le logiciel StorageGRID. Si vous souhaitez installer une autre version du logiciel, vous devez d'abord la télécharger à l'aide du programme d'installation de l'appliance StorageGRID.
- Vous attendez que le logiciel soit installé.
- Lorsque le logiciel a été installé, l'appliance est redémarrée automatiquement.

Étapes

1. Ouvrez un navigateur et saisissez l'adresse IP de l'appliance.
   `https://services_appliance_IP:8443`

   La page d'accueil du programme d'installation de l'appliance StorageGRID s'affiche.

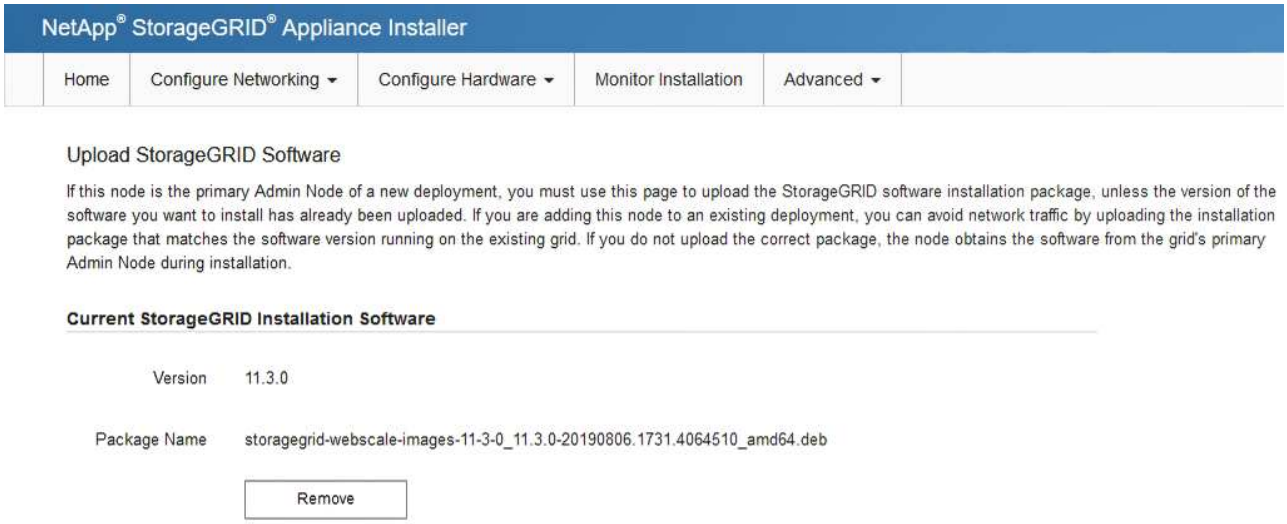
2. Dans la section **ce noeud**, sélectionnez **Administrateur principal**.
3. Dans le champ **Nom de noeud**, entrez le nom que vous souhaitez utiliser pour ce noeud d'appliance, puis cliquez sur **Enregistrer**.

   Le nom de nœud est attribué à ce nœud d'appliance dans le système StorageGRID. Elle s'affiche sur la page Grid Nodes dans Grid Manager.

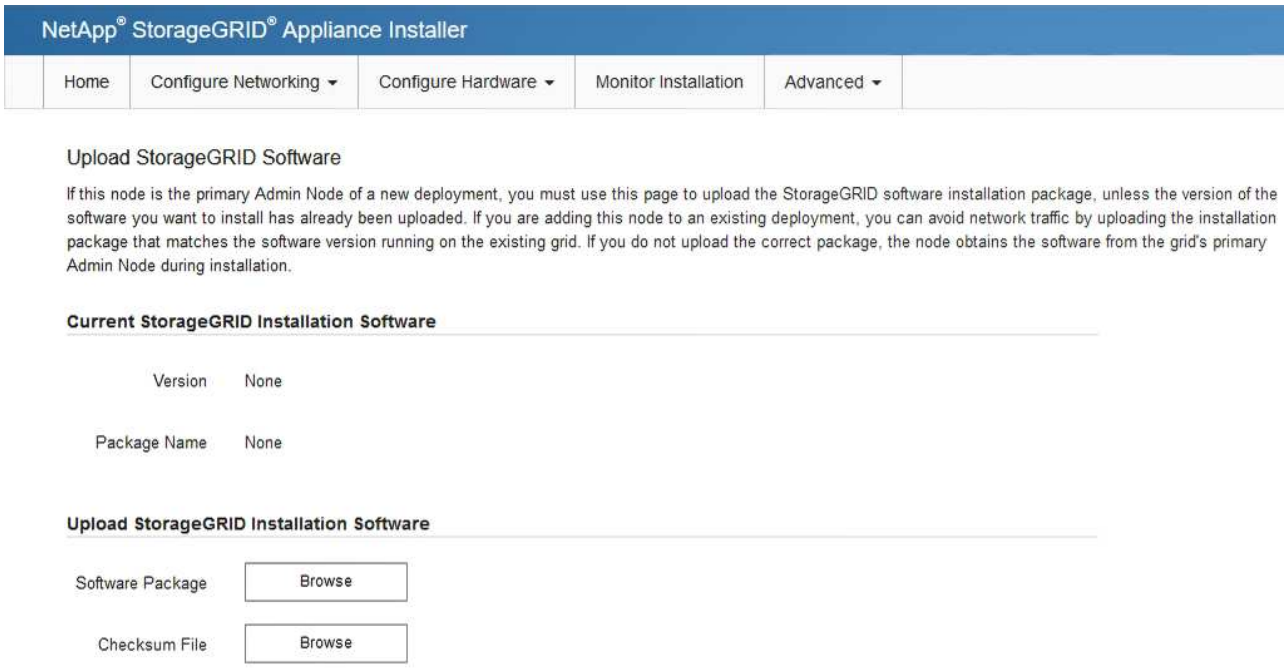
4. Si vous souhaitez installer une autre version du logiciel StorageGRID, procédez comme suit :
   a. Téléchargez l'archive d'installation :

      "Téléchargement NetApp : appliance StorageGRID"

   b. Extrayez l'archive.
   c. Dans le programme d'installation de l'appliance StorageGRID, sélectionnez **Avancé** > **Télécharger le logiciel StorageGRID**.
   d. Cliquez sur **Supprimer** pour supprimer le progiciel actuel.



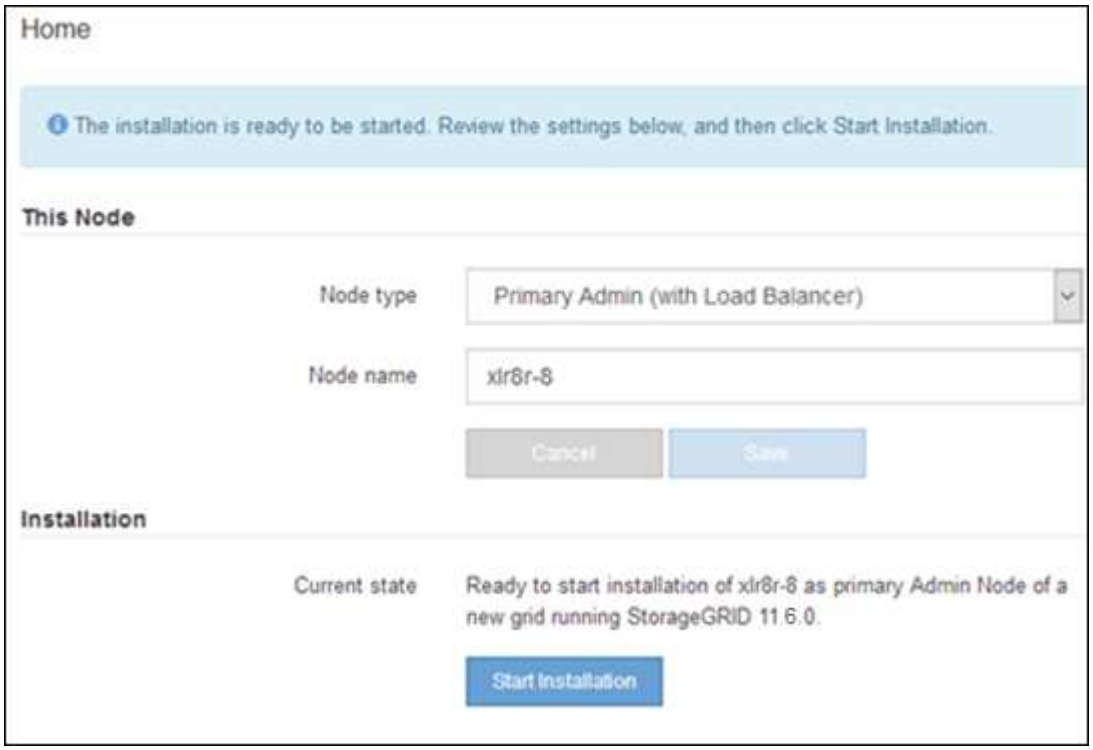
   e. Cliquez sur **Parcourir** pour le progiciel que vous avez téléchargé et extrait, puis cliquez sur **Parcourir** pour le fichier de somme de contrôle.



   f. Sélectionnez **Accueil** pour revenir à la page d'accueil.
5. Confirmez que l'état actuel est « prêt à démarrer l'installation du noeud d'administration principal avec la version x.y du logiciel » et que le bouton **Start installation** est activé.

Si vous déployez l'appliance Admin Node en tant que cible de clonage de nœud, arrêtez le processus de déploiement ici et continuez "procédure de clonage de nœud".

6. Dans la page d'accueil du programme d'installation de l'appliance StorageGRID, cliquez sur **Démarrer l'installation**.



L'état actuel passe à « installation en cours » et la page installation du moniteur s'affiche.

Si vous devez accéder manuellement à la page installation du moniteur, cliquez sur **installation du moniteur** dans la barre de menus.

Déployez une appliance de services en tant que passerelle ou nœud d'administration non primaire

Lorsque vous déployez une appliance de services en tant que nœud de passerelle ou nœud d'administration non primaire, utilisez le programme d'installation de l'appliance StorageGRID inclus sur l'appliance.

Avant de commencer

- L'appliance a été installée dans un rack ou une armoire, connectée à vos réseaux et sous tension.
- Les liens réseau, les adresses IP et le remappage des ports (si nécessaire) ont été configurés pour le serveur à l'aide du programme d'installation de l'appliance StorageGRID.
- Le nœud d'administration principal du système StorageGRID a été déployé.
- Tous les sous-réseaux de réseau Grid répertoriés sur la page de configuration IP du programme d'installation de l'appliance StorageGRID ont été définis dans la liste de sous-réseaux de réseau de grille sur le nœud d'administration principal.
- Vous avez un ordinateur portable de service avec un "navigateur web pris en charge".
- Vous connaissez l'adresse IP attribuée à l'appliance. Vous pouvez utiliser l'adresse IP de n'importe quel réseau StorageGRID connecté.

Description de la tâche

Pour installer StorageGRID sur un nœud d'appliance de services :

- Vous spécifiez ou confirmez l'adresse IP du nœud d'administration principal et le nom du nœud d'appliance.
- Vous démarrez l'installation et attendez que le logiciel soit installé.

  L'installation s'interrompt via les tâches d'installation du nœud de passerelle de l'appliance. Pour reprendre l'installation, connectez-vous au Grid Manager, approuvez tous les nœuds de la grille et terminez le processus d'installation de StorageGRID. L'installation d'un noeud d'administration non primaire ne nécessite pas votre approbation.

> Ne déployez pas les appliances de services SG100 et SG1000 sur le même site. Cela peut entraîner des performances imprévisibles.

> Si vous devez déployer plusieurs nœuds d'appliance à la fois, vous pouvez automatiser le processus d'installation. Voir "Automatisez l'installation et la configuration de l'appliance".

Étapes

1. Ouvrez un navigateur et saisissez l'adresse IP de l'appliance.

   `https://Controller_IP:8443`

   La page d'accueil du programme d'installation de l'appliance StorageGRID s'affiche.

2. Dans la section connexion au noeud d'administration principal, déterminez si vous devez spécifier l'adresse IP du noeud d'administration principal.

   Si vous avez déjà installé d'autres nœuds dans ce centre de données, le programme d'installation de l'appliance StorageGRID peut détecter automatiquement cette adresse IP, en supposant que le nœud d'administration principal, ou au moins un autre nœud de grille avec ADMIN_IP configuré, soit présent sur le même sous-réseau.

3. Si cette adresse IP n'apparaît pas ou si vous devez la modifier, spécifiez l'adresse :

Option	Description
Entrée IP manuelle	a. Décochez la case **Activer la découverte du noeud d'administration**. b. Saisissez l'adresse IP manuellement. c. Cliquez sur **Enregistrer**. d. Attendez que l'état de connexion de la nouvelle adresse IP soit prêt.

Option	Description
Détection automatique de tous les nœuds d'administration principaux connectés	a. Cochez la case **Activer la découverte du noeud d'administration**. b. Attendez que la liste des adresses IP découvertes s'affiche. c. Sélectionnez le nœud d'administration principal de la grille dans laquelle ce nœud de stockage de l'appliance sera déployé. d. Cliquez sur **Enregistrer**. e. Attendez que l'état de connexion de la nouvelle adresse IP soit prêt.

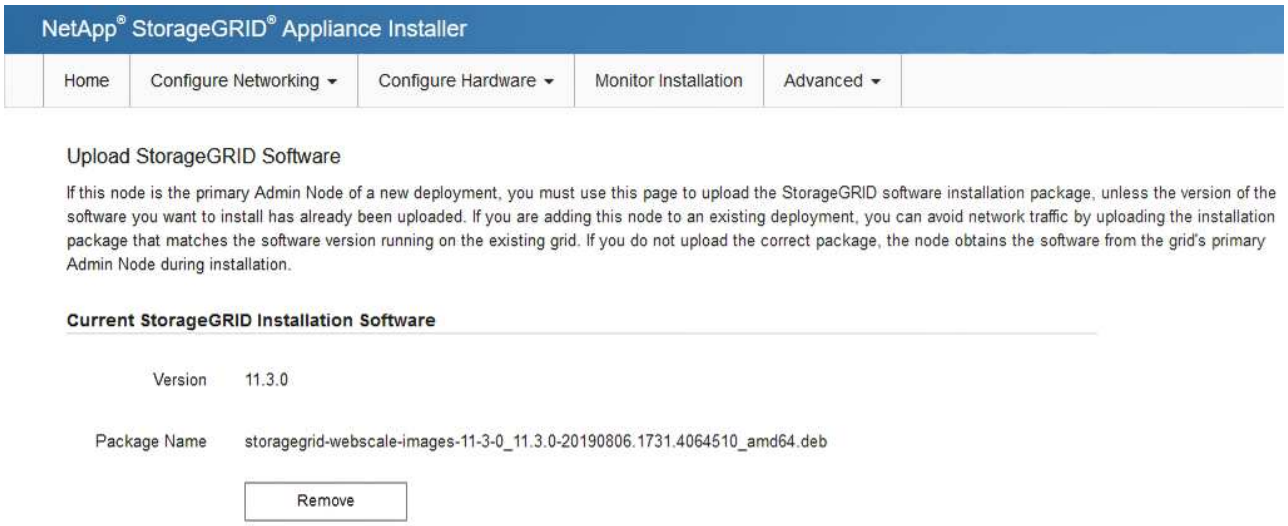
4. Dans le champ **Nom du nœud**, indiquez le nom du système que vous souhaitez utiliser pour ce nœud d'appliance, puis cliquez sur **Enregistrer**.

   Le nom qui apparaît ici correspond au nom système du nœud de l'appliance. Les noms de système sont requis pour les opérations StorageGRID internes et ne peuvent pas être modifiés.

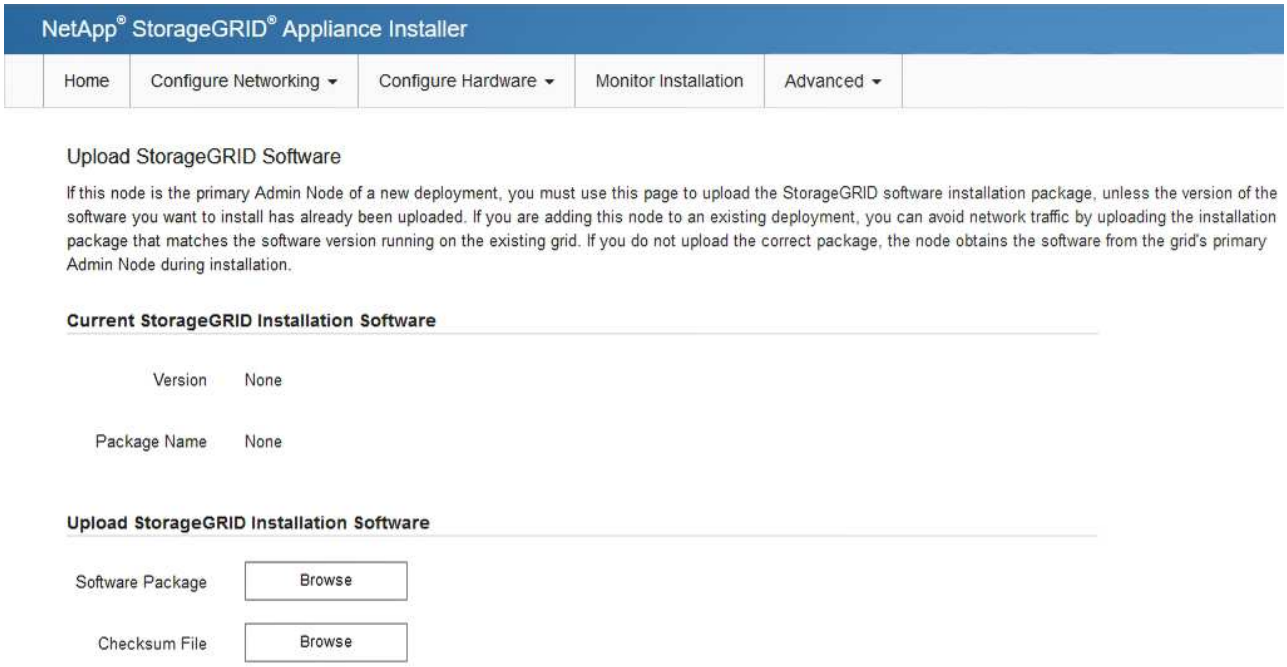
5. Si vous souhaitez installer une autre version du logiciel StorageGRID, procédez comme suit :
   a. Téléchargez l'archive d'installation :

      "Téléchargement NetApp : appliance StorageGRID"

   b. Extrayez l'archive.
   c. Dans le programme d'installation de l'appliance StorageGRID, sélectionnez **Avancé** > **Télécharger le logiciel StorageGRID**.
   d. Cliquez sur **Supprimer** pour supprimer le progiciel actuel.



   e. Cliquez sur **Parcourir** pour le progiciel que vous avez téléchargé et extrait, puis cliquez sur **Parcourir** pour le fichier de somme de contrôle.

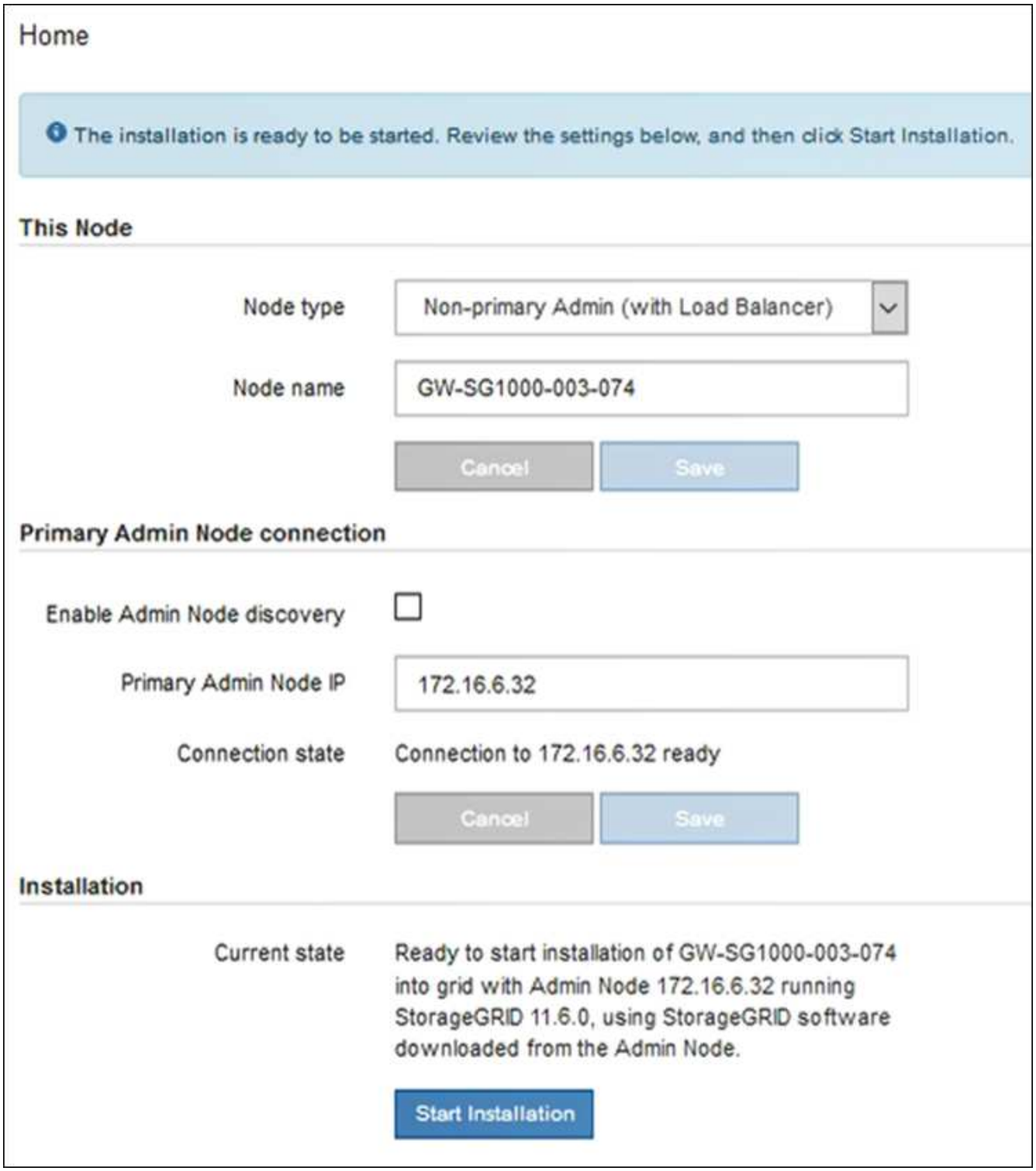


f. Sélectionnez **Accueil** pour revenir à la page d'accueil.

6. Dans la section installation, vérifiez que l'état actuel est « prêt à démarrer l'installation de `node name` Dans le grid avec le nœud d'administration principal `admin_ip` " Et que le bouton **Start installation** est activé.

   Si le bouton **Start installation** n'est pas activé, vous devrez peut-être modifier la configuration réseau ou les paramètres de port. Pour obtenir des instructions, reportez-vous aux instructions d'entretien de votre appareil.

7. Dans la page d'accueil du programme d'installation de l'appliance StorageGRID, cliquez sur **Démarrer l'installation**.



L'état actuel passe à « installation en cours » et la page installation du moniteur s'affiche.

Si vous devez accéder manuellement à la page installation du moniteur, cliquez sur **installation du moniteur** dans la barre de menus.

8. Si votre grid inclut plusieurs nœuds d'appliance, répétez les étapes précédentes pour chaque appliance.

Surveiller l’installation de l’appareil

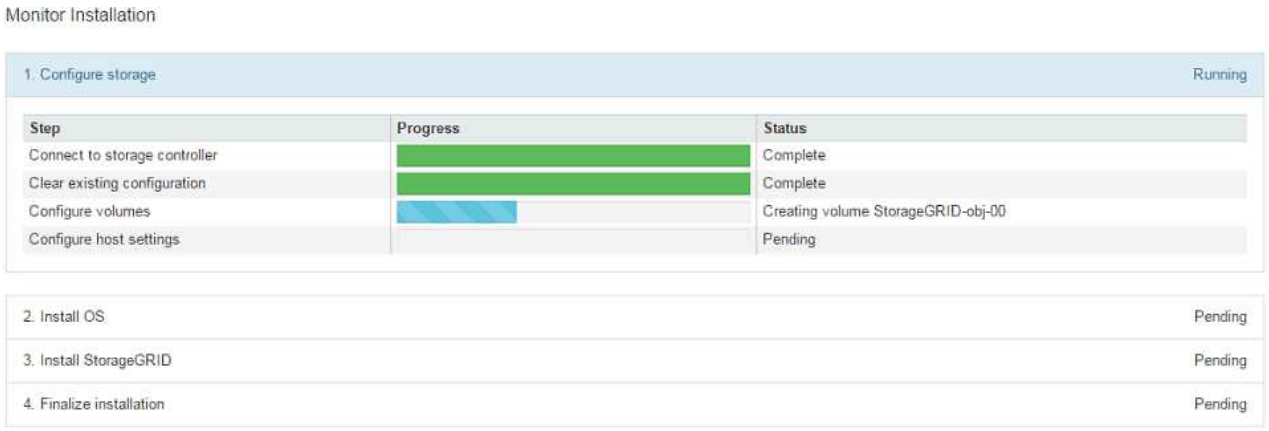
Le programme d’installation de l’appliance StorageGRID indique l’état jusqu’à ce que l’installation soit terminée. Une fois l’installation du logiciel terminée, l’appliance est redémarrée.

Exemple 1. Étapes

Appliance de stockage

1. Pour contrôler la progression de l'installation, cliquez sur **Monitor installation**.

   La page installation du moniteur affiche la progression de l'installation.



   La barre d'état bleue indique la tâche en cours. Les barres d'état vertes indiquent que les tâches ont été effectuées avec succès.

   > Le programme d'installation s'assure que les tâches terminées lors d'une installation précédente ne sont pas réexécutées. Si vous exécutez à nouveau une installation, toutes les tâches qui n'ont pas besoin d'être réexécutées s'affichent avec une barre d'état verte et un état de « `barrét' ».

2. Passez en revue la progression des deux premières étapes d'installation.

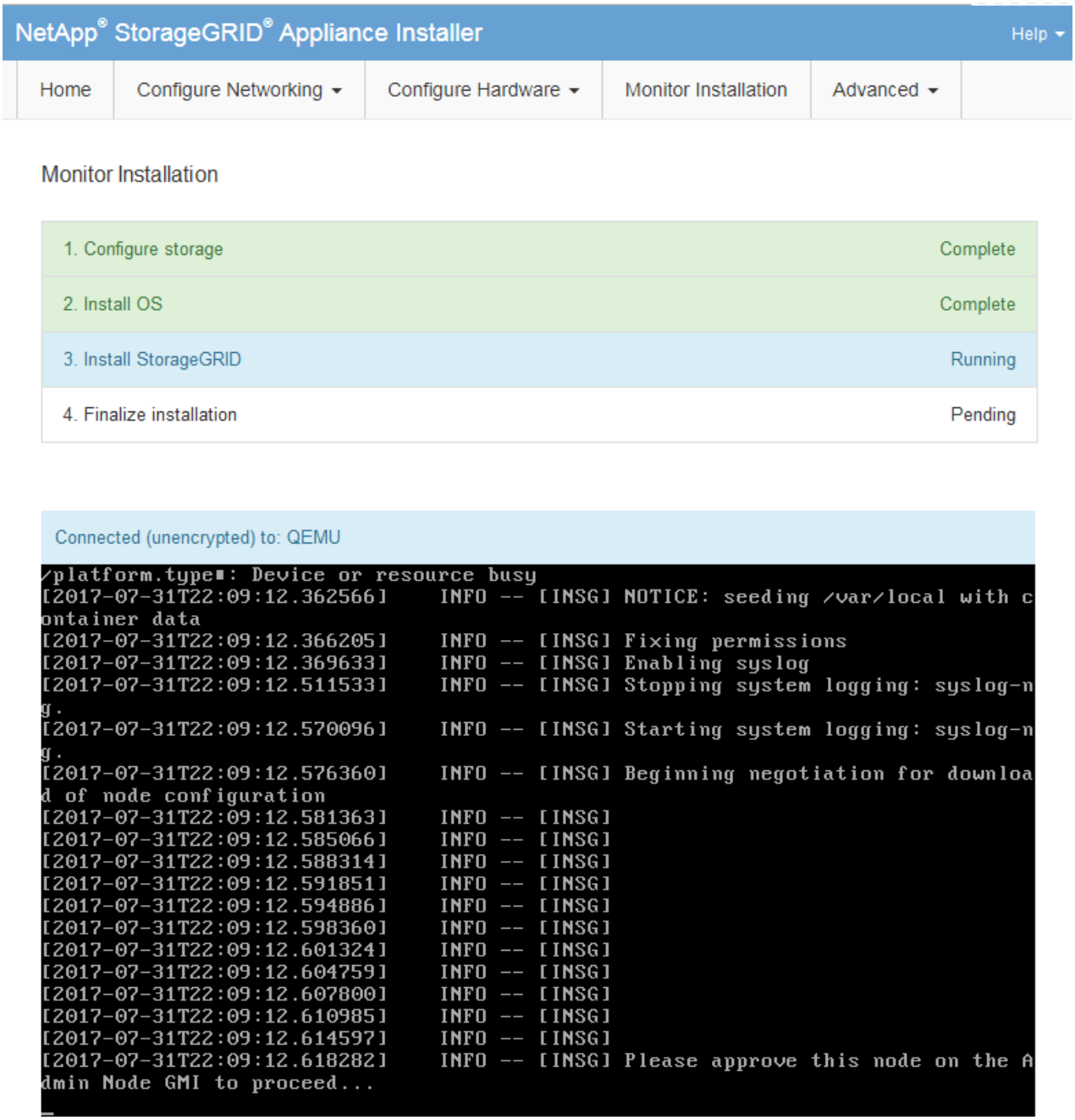
   1. Configurer le stockage

   Au cours de cette étape, le programme d'installation se connecte au contrôleur de stockage, efface toute configuration existante, crée des RAID en fonction du mode RAID configuré, alloue des volumes pour le logiciel StorageGRID et le stockage de données d'objet, et configure les paramètres de l'hôte.

   2. Installez OS

   Au cours de cette étape, le programme d'installation copie l'image du système d'exploitation de base pour StorageGRID sur l'appliance.

3. Continuez à surveiller la progression de l'installation jusqu'à ce que l'étape **installer StorageGRID** s'arrête et qu'un message s'affiche sur la console intégrée, vous invitant à approuver ce nœud sur le nœud d'administration à l'aide du gestionnaire de grille. Passez à l'étape suivante.



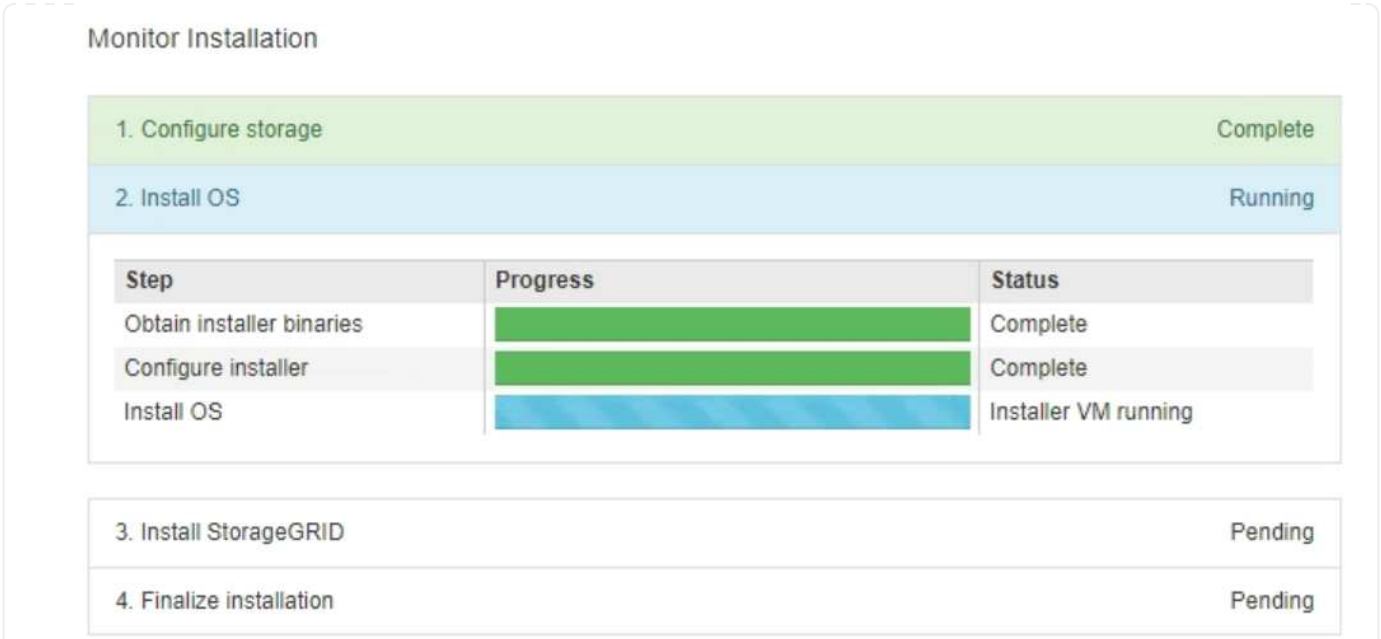
4. Accédez au Grid Manager du nœud administrateur principal, approuvez le nœud de stockage en attente et terminez le processus d'installation de StorageGRID.

   Lorsque vous cliquez sur **Install** dans Grid Manager, l'étape 3 se termine et l'étape 4, **Finalisation installation**, commence. Une fois l'étape 4 terminée, le contrôleur est redémarré.

Appliance de services

1. Pour contrôler la progression de l'installation, cliquez sur **Monitor installation** dans la barre de menus.

   La page installation du moniteur affiche la progression de l'installation.



La barre d'état bleue indique la tâche en cours. Les barres d'état vertes indiquent que les tâches ont été effectuées avec succès.

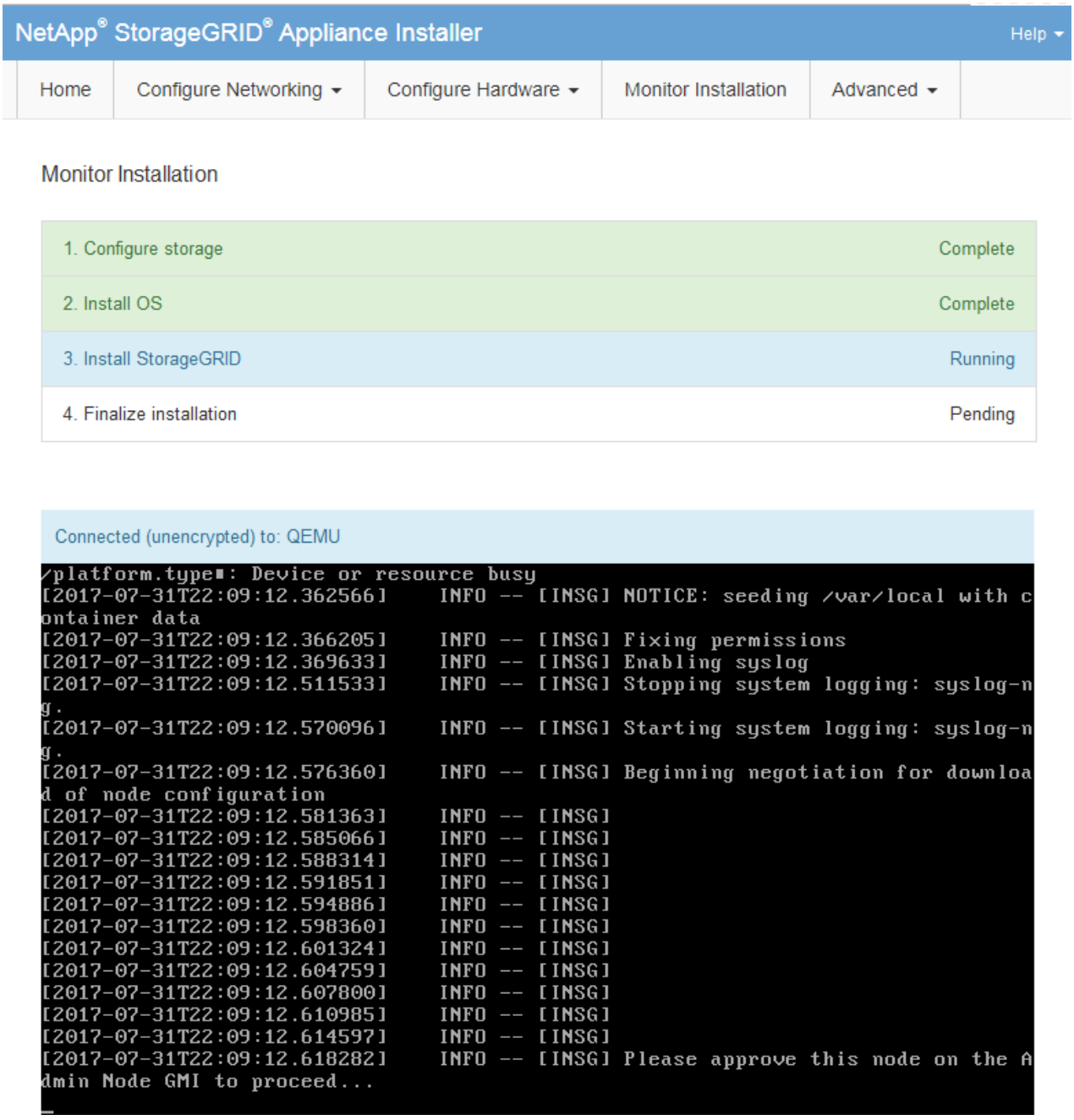
> Le programme d'installation s'assure que les tâches terminées lors d'une installation précédente ne sont pas réexécutées. Si vous exécutez à nouveau une installation, toutes les tâches qui n'ont pas besoin d'être réexécutées s'affichent avec une barre d'état verte et un état de « `barrét' ».

2. Passez en revue l'état d'avancement des deux premières étapes d'installation.
   - **1. Configurer le stockage**

     Au cours de cette étape, le programme d'installation efface toute configuration existante des lecteurs de l'appliance et configure les paramètres de l'hôte.
   - **2. Installez OS**

     Au cours de cette étape, le programme d'installation copie l'image du système d'exploitation de base pour StorageGRID sur l'appliance.
3. Continuez à surveiller la progression de l'installation jusqu'à ce que l'un des processus suivants se produise :
   - Pour tous les nœuds d'appliance à l'exception du nœud d'administration principal, l'étape installer StorageGRID s'interrompt et un message s'affiche sur la console intégrée, vous invitant à approuver ce nœud sur le nœud d'administration à l'aide de Grid Manager. Passez à l'étape suivante.
   - Pour l'installation du nœud d'administration principal de l'appliance, il n'est pas nécessaire d'approuver le nœud. L'appliance est redémarrée. Vous pouvez passer à l'étape suivante.

> Lors de l'installation d'un nœud d'administration principal de l'appliance, une cinquième phase s'affiche (voir l'exemple de capture d'écran montrant quatre phases). Si la cinquième phase est en cours pendant plus de 10 minutes, actualisez manuellement la page Web.



4. Accédez au Grid Manager du nœud administrateur principal, approuvez le nœud de grille en attente et terminez le processus d'installation de StorageGRID.

   Lorsque vous cliquez sur **Install** dans Grid Manager, l'étape 3 se termine et l'étape 4, **Finalisation installation**, commence. Une fois l'étape 4 terminée, l'appareil est redémarré.

Redémarrez l'appliance pendant que le programme d'installation de l'appliance StorageGRID est en cours d'exécution

Vous devrez peut-être redémarrer l'appliance pendant l'exécution du programme d'installation de l'appliance StorageGRID. Par exemple, vous devrez peut-être redémarrer l'appliance si l'installation échoue.

Description de la tâche

Cette procédure s'applique uniquement lorsque le serveur exécute le programme d'installation de l'appliance StorageGRID. Une fois l'installation terminée, cette étape ne fonctionne plus car le programme d'installation de l'appliance StorageGRID n'est plus disponible.

Étapes

1. Dans le programme d'installation de l'appliance StorageGRID, cliquez sur **Avancé** > **redémarrer le contrôleur**, puis sélectionnez l'une des options suivantes :

   - Sélectionnez **Reboot dans StorageGRID** pour redémarrer le contrôleur avec le noeud qui rejoint la grille. Sélectionnez cette option si vous avez terminé de travailler en mode maintenance et que vous êtes prêt à rétablir le fonctionnement normal du nœud.
   - Sélectionnez **redémarrer en mode maintenance** pour redémarrer le contrôleur avec le nœud restant en mode de maintenance. (Cette option n'est disponible que lorsque le contrôleur est en mode de maintenance.) Sélectionnez cette option si des opérations de maintenance supplémentaires doivent être effectuées sur le nœud avant de rejoindre la grille.

   L'appliance est redémarrée.

Dépannage de l'installation matérielle (SGF6112)

Si vous rencontrez des problèmes lors de l'installation, il peut s'avérer utile de consulter les informations de dépannage relatives à la configuration du matériel et aux problèmes de connectivité.

Afficher les codes de démarrage (SGF6112)

Lorsque vous mettez l'appliance sous tension, le contrôleur BMC consigne une série de codes de démarrage. Vous pouvez afficher ces codes sur une console graphique connectée au port de gestion BMC.

Avant de commencer

- Vous savez comment accéder au tableau de bord BMC.
- Si vous souhaitez utiliser Serial-over-LAN (sol), vous avez de l'expérience avec les applications de console IPMI sol.

Étapes

1. Sélectionnez l'une des méthodes suivantes pour afficher les codes de démarrage du contrôleur de l'appliance et rassemblez l'équipement requis.

Méthode	Équipement requis
Console VGA	• Moniteur VGA • Câble VGA
KVM	• Câble RJ-45
Port série	• Câble série DB-9 • Terminal série virtuel
SOL	• Terminal série virtuel

2. Si vous utilisez une console VGA, procédez comme suit :
   a. Connectez un moniteur compatible VGA au port VGA situé à l'arrière de l'appareil.
   b. Afficher les codes affichés sur le moniteur.
3. Si vous utilisez BMC KVM, effectuez les opérations suivantes :
   a. Connectez-vous au port de gestion du contrôleur BMC et connectez-vous à l'interface Web du contrôleur BMC.
   b. Sélectionnez **télécommande**.
   c. Lancez le KVM.
   d. Afficher les codes sur le moniteur virtuel.
4. Si vous utilisez un port série et un terminal, effectuez les opérations suivantes :
   a. Connectez-vous au port USB série situé à l'arrière de l'appareil.
   b. Utiliser les paramètres `115200 8-N-1`.
   c. Afficher les codes imprimés sur le terminal série.
5. Si vous utilisez sol, effectuez les opérations suivantes :
   a. Connectez-vous au sol IPMI à l'aide de l'adresse IP du BMC et des informations d'identification de connexion.

      ```
      ipmitool -I lanplus -H BMC_Port_IP -U admin -P Password sol activate
      ```

   b. Afficher les codes sur le terminal série virtuel.
6. Utilisez le tableau pour rechercher les codes de votre appareil.

Code	Indique
BONJOUR	Le script de démarrage principal a démarré.

Code	Indique
HP	Le système vérifie si le micrologiciel de la carte d'interface réseau (NIC) doit être mis à jour.
RB	Le système redémarre après l'application des mises à jour du firmware.
FP	Les vérifications de mise à jour du micrologiciel du sous-système matériel sont terminées. Les services de communication inter-contrôleurs sont en cours de démarrage.
PC	Le système recherche les données d'installation StorageGRID existantes.
HO	L'appliance StorageGRID est en cours d'exécution.
HAUTE DISPONIBILITÉ	StorageGRID est en cours d'exécution.

Informations associées

"Accéder à l'interface BMC"

Afficher les codes d'erreur (SGF6112)

Si une erreur matérielle se produit lors du démarrage de l'appliance, le contrôleur BMC consigne un code d'erreur. Si nécessaire, vous pouvez afficher ces codes d'erreur à l'aide de l'interface BMC, puis travailler avec le support technique pour résoudre le problème.

Avant de commencer

- Vous savez comment accéder au tableau de bord BMC.

Étapes

1. Dans le tableau de bord BMC, sélectionnez **Code POST BIOS**.
2. Passez en revue les informations affichées pour le code actuel et le code précédent.

   Si l'un des codes d'erreur suivants s'affiche, contactez le support technique pour résoudre le problème.

Code	Indique
0x0E	Microcode introuvable
0x0F	Microcode non chargé
0x50	Erreur d'initialisation de la mémoire. Type de mémoire non valide ou vitesse de mémoire incompatible.
0x51	Erreur d'initialisation de la mémoire. Échec de la lecture du démon du processeur de service.

Code	Indique
0x52	Erreur d’initialisation de la mémoire. La taille de la mémoire n’est pas valide ou les modules de mémoire ne correspondent pas.
0x53	Erreur d’initialisation de la mémoire. Aucune mémoire utilisable détectée.
0x54	Erreur d’initialisation de la mémoire non spécifiée
0x55	Mémoire non installée
0x56	Type de CPU ou vitesse non valide
0x57	Non-concordance du processeur
0x58	Échec de l’autotest de la CPU ou erreur possible du cache de la CPU
0x59	Le micro-code de l’UC est introuvable ou la mise à jour du micro-code a échoué
0x5A	Erreur interne de l’UC
0x5B	La réinitialisation PPI n’est pas disponible
0x5C	Échec de l’autotest du BMC de phase PEI
0xd0	Erreur d’initialisation de l’UC
0xD1	Erreur d’initialisation du pont Nord
0xD2	Erreur d’initialisation du pont Sud
0xd3	Certains protocoles architecturaux ne sont pas disponibles
0xD4	Erreur d’allocation de ressources PCI. Manque de ressources.
0xD5	Pas d’espace pour la ROM optionnelle héritée
0xD6	Aucun périphérique de sortie de console n’a été trouvé
0xD7	Aucun périphérique d’entrée de console n’a été trouvé
0xD8	Mot de passe non valide

Code	Indique
0xD9	Erreur lors du chargement de l'option d'amorçage (erreur Loadimage renvoyée)
0xDA	Échec de l'option de démarrage (erreur StartImage renvoyée)
0xDB	Échec de la mise à jour flash
0xDC	Le protocole de réinitialisation n'est pas disponible
0xDD	Échec de l'autotest du BMC de phase DXE
0xE8	MRC : ERR_NO_MEMORY
0xE9	MRC : ERR_LT_LOCK
0xEA	MRC : ERR_DDR_INIT
0xEB	MRC : ERR_MEM_TEST
0xEC	MRC : SPÉCIFIQUE À ERR_VENDOR
0xED	MRC : ERR_DIMM_COMPAT
0xEE	MRC : COMPATIBILITÉ ERR_MRC
0xEF	MRC : ERR_MRC_STRUCT
0xF0	MRC : ERR_SET_VDD
0xF1	MRC : ERR_IOT_MEM_BUFFER
0xF2	MRC : ERR_RC_INTERNAL
0xF3	MRC : ERR_INVALID_REG_ACCESS
0xF4	MRC : ERR_SET_MC_FREQ
0xF5	MRC : ERR_READ_MC_FREQ
0x70	MRC : ERR_DIMM_CHANNEL
0x74	MRC : ERR_BIST_CHECK

Code	Indique
0xF6	MRC : ERR_SMBUS
0xF7	MRC : ERR_PCU
0xF8	MRC : ERR_NGN
0xF9	MRC : ERR_INTERLEAVE_FAILURE

La configuration matérielle semble se bloquer (SGF6112)

Il se peut que le programme d'installation de l'appliance StorageGRID ne soit pas disponible si des défauts matériels ou des erreurs de câblage empêchent l'appliance de terminer son processus de démarrage.

Étapes

1. Examinez les voyants de l'appareil, ainsi que les codes de démarrage et d'erreur affichés dans le contrôleur BMC.
2. Si vous avez besoin d'aide pour résoudre un problème, contactez le support technique.

Informations associées

- "Afficher les codes de démarrage (SGF6112)"
- "Afficher les codes d'erreur (SGF6112)"

Résolution des problèmes de connexion (SGF6112)

Si vous rencontrez des problèmes de connexion lors de l'installation de l'appliance StorageGRID, vous devez effectuer les actions correctives indiquées.

Connexion à l'appareil impossible

Si vous ne parvenez pas à vous connecter à l'appliance de services, il se peut qu'il y ait un problème de réseau ou que l'installation matérielle n'ait pas été effectuée correctement.

Étapes

1. Essayez d'envoyer une requête ping à l'appareil à l'aide de l'adresse IP de l'appareil :
   `ping appliance_IP`
2. Si vous ne recevez aucune réponse de la commande ping, confirmez que vous utilisez la bonne adresse IP.

   Vous pouvez utiliser l'adresse IP de l'appliance sur le réseau Grid, le réseau Admin ou le réseau client.
3. Si l'adresse IP est correcte, vérifiez le câblage de l'appliance, les émetteurs-récepteurs QSFP ou SFP et la configuration du réseau.
4. Si l'accès physique à l'appareil est disponible, vous pouvez utiliser une connexion directe à l'adresse IP locale de liaison permanente `169.254.0.1` pour vérifier la configuration de la mise en réseau du contrôleur et la mettre à jour si nécessaire. Pour obtenir des instructions détaillées, reportez-vous à l'étape

2 de la section "Accédez au programme d'installation de l'appliance StorageGRID".

Si ce n'est pas le cas, contactez le support technique.

5. Si la commande ping a réussi, ouvrez un navigateur Web.
6. Entrez l'URL du programme d'installation de l'appliance StorageGRID :
`https://appliances_controller_IP:8443`

La page d'accueil s'affiche.

Dépannage de l'installation matérielle (SG6000 ou SG5700)

Si vous rencontrez des problèmes lors de l'installation, il peut s'avérer utile de consulter les informations de dépannage relatives à la configuration du matériel et aux problèmes de connectivité.

Afficher les codes de démarrage (contrôleur SG6000-CN)

Lorsque vous mettez l'appareil sous tension, le contrôleur BMC consigne une série de codes de démarrage pour le contrôleur SG6000-CN. Vous pouvez afficher ces codes de plusieurs façons.

Avant de commencer

- Vous savez comment accéder au tableau de bord BMC.
- Si vous souhaitez utiliser Serial-over-LAN (sol), vous avez de l'expérience avec les applications de console IPMI sol.

Étapes

1. Sélectionnez l'une des méthodes suivantes pour afficher les codes de démarrage du contrôleur de l'appliance et rassemblez l'équipement requis.

Méthode	Équipement requis
Console VGA	• Moniteur VGA • Câble VGA
KVM	• Câble RJ-45
Port série	• Câble série DB-9 • Terminal série virtuel
SOL	• Terminal série virtuel

2. Si vous utilisez une console VGA, procédez comme suit :
   a. Connectez un moniteur compatible VGA au port VGA situé à l'arrière de l'appareil.
   b. Afficher les codes affichés sur le moniteur.
3. Si vous utilisez BMC KVM, effectuez les opérations suivantes :

a. Connectez-vous au port de gestion du contrôleur BMC et connectez-vous à l'interface Web du contrôleur BMC.
b. Sélectionnez **télécommande**.
c. Lancez le KVM.
d. Afficher les codes sur le moniteur virtuel.

4. Si vous utilisez un port série et un terminal, effectuez les opérations suivantes :
   a. Connectez-vous au port série DB-9 situé à l'arrière de l'appareil.
   b. Utiliser les paramètres `115200 8-N-1`.
   c. Afficher les codes imprimés sur le terminal série.
5. Si vous utilisez sol, effectuez les opérations suivantes :
   a. Connectez-vous au sol IPMI à l'aide de l'adresse IP du BMC et des informations d'identification de connexion.

      `ipmitool -I lanplus -H BMC_Port_IP -U admin -P Password sol activate`

      Dans certains cas, le nom d'utilisateur par défaut peut être `root` au lieu de `admin`.

   a. Afficher les codes sur le terminal série virtuel.
6. Utilisez le tableau pour rechercher les codes de votre appareil.

Code	Indique
BONJOUR	Le script de démarrage principal a démarré.
HP	Le système vérifie si le micrologiciel de la carte d'interface réseau (NIC) doit être mis à jour.
RB	Le système redémarre après l'application des mises à jour du firmware.
FP	Les vérifications de mise à jour du micrologiciel du sous-système matériel sont terminées. Les services de communication inter-contrôleurs sont en cours de démarrage.

Code	Indique
IL	Pour un nœud de stockage d'appliance uniquement : Le système est en attente de connectivité avec les contrôleurs de stockage et se synchronise avec le système d'exploitation SANtricity. **Remarque :** si la procédure de démarrage n'est pas en cours au-delà de cette étape, effectuez les opérations suivantes : a. Vérifiez que les quatre câbles d'interconnexion entre le contrôleur SG6000-CN et les deux contrôleurs de stockage sont correctement connectés. b. Si nécessaire, remplacez un ou plusieurs câbles, puis réessayez. c. Si ce n'est pas le cas, contactez le support technique.
PC	Le système recherche les données d'installation StorageGRID existantes.
HO	Le programme d'installation de l'appliance StorageGRID est en cours d'exécution.
HAUTE DISPONIBILITÉ	StorageGRID est en cours d'exécution.

Afficher les codes d'erreur (contrôleur SG6000-CN)

Si une erreur matérielle se produit lors du démarrage du contrôleur SG6000-CN, le contrôleur BMC consigne un code d'erreur. Si nécessaire, vous pouvez afficher ces codes d'erreur à l'aide de l'interface BMC, puis travailler avec le support technique pour résoudre le problème.

Avant de commencer

- Vous savez comment accéder au tableau de bord BMC.

Étapes

1. Dans le tableau de bord BMC, sélectionnez **Code POST BIOS**.
2. Passez en revue les informations affichées pour le code actuel et le code précédent.

   Si l'un des codes d'erreur suivants s'affiche, contactez le support technique pour résoudre le problème.

Code	Indique
0x0E	Microcode introuvable
0x0F	Microcode non chargé
0x50	Erreur d'initialisation de la mémoire. Type de mémoire non valide ou vitesse de mémoire incompatible.

Code	Indique
0x51	Erreur d’initialisation de la mémoire. Échec de la lecture du démon du processeur de service.
0x52	Erreur d’initialisation de la mémoire. La taille de la mémoire n’est pas valide ou les modules de mémoire ne correspondent pas.
0x53	Erreur d’initialisation de la mémoire. Aucune mémoire utilisable détectée.
0x54	Erreur d’initialisation de la mémoire non spécifiée
0x55	Mémoire non installée
0x56	Type de CPU ou vitesse non valide
0x57	Non-concordance du processeur
0x58	Échec de l’autotest de la CPU ou erreur possible du cache de la CPU
0x59	Le micro-code de l’UC est introuvable ou la mise à jour du micro-code a échoué
0x5A	Erreur interne de l’UC
0x5B	La réinitialisation PPI n’est pas disponible
0x5C	Échec de l’autotest du BMC de phase PEI
0xd0	Erreur d’initialisation de l’UC
0xD1	Erreur d’initialisation du pont Nord
0xD2	Erreur d’initialisation du pont Sud
0xd3	Certains protocoles architecturaux ne sont pas disponibles
0xD4	Erreur d’allocation de ressources PCI. Manque de ressources.
0xD5	Pas d’espace pour la ROM optionnelle héritée
0xD6	Aucun périphérique de sortie de console n’a été trouvé
0xD7	Aucun périphérique d’entrée de console n’a été trouvé

Code	Indique
0xD8	Mot de passe non valide
0xD9	Erreur lors du chargement de l’option d’amorçage (erreur Loadimage renvoyée)
0xDA	Échec de l’option de démarrage (erreur StartImage renvoyée)
0xDB	Échec de la mise à jour flash
0xDC	Le protocole de réinitialisation n’est pas disponible
0xDD	Échec de l’autotest du BMC de phase DXE
0xE8	MRC : ERR_NO_MEMORY
0xE9	MRC : ERR_LT_LOCK
0xEA	MRC : ERR_DDR_INIT
0xEB	MRC : ERR_MEM_TEST
0xEC	MRC : SPÉCIFIQUE À ERR_VENDOR
0xED	MRC : ERR_DIMM_COMPAT
0xEE	MRC : COMPATIBILITÉ ERR_MRC
0xEF	MRC : ERR_MRC_STRUCT
0xF0	MRC : ERR_SET_VDD
0xF1	MRC : ERR_IOT_MEM_BUFFER
0xF2	MRC : ERR_RC_INTERNAL
0xF3	MRC : ERR_INVALID_REG_ACCESS
0xF4	MRC : ERR_SET_MC_FREQ
0xF5	MRC : ERR_READ_MC_FREQ
0x70	MRC : ERR_DIMM_CHANNEL

Code	Indique
0x74	MRC : ERR_BIST_CHECK
0xF6	MRC : ERR_SMBUS
0xF7	MRC : ERR_PCU
0xF8	MRC : ERR_NGN
0xF9	MRC : ERR_INTERLEAVE_FAILURE

La configuration matérielle semble suspendue (SG6000 ou SG5700)

Le programme d'installation de l'appliance StorageGRID peut ne pas être disponible si des pannes matérielles ou des erreurs de câblage empêchent les contrôleurs de stockage ou le contrôleur de l'appliance d'effectuer leur démarrage.

Exemple 2. Étapes

SG6000

1. Pour les contrôleurs de stockage, surveiller les codes sur les affichages à sept segments.

   Pendant l'initialisation du matériel pendant la mise sous tension, les deux affichages à sept segments affichent une séquence de codes. Lorsque le matériel démarre correctement, les deux affichages à sept segments s'affichent `99`.

2. Examinez les voyants du contrôleur SG6000-CN ainsi que les codes d'erreur et de démarrage affichés dans le contrôleur BMC.
3. Si vous avez besoin d'aide pour résoudre un problème, contactez le support technique.

SG5700

1. Observez les codes sur les affichages à sept segments.

   Pendant l'initialisation du matériel pendant la mise sous tension, les deux affichages à sept segments affichent une séquence de codes. Lorsque le matériel démarre correctement, les sept segments affichent des codes différents pour chaque contrôleur.

2. Examiner les codes sur l'affichage à sept segments du contrôleur E5700SG.

   > L'installation et le provisionnement prennent du temps. Certaines phases d'installation ne rapportent pas les mises à jour au programme d'installation de l'appliance StorageGRID pendant plusieurs minutes.

   En cas d'erreur, l'affichage à sept segments clignote une séquence, telle QU'IL.

3. Pour comprendre la signification de ces codes, consultez les ressources suivantes :

Contrôleur	Référence
Contrôleur E5700SG	• "Indicateurs d'état sur le contrôleur E5700SG" • « Erreur : erreur lors de la synchronisation avec le logiciel SANtricity OS »
Contrôleur E2800	*E5700 et E2800 System Monitoring Guide* **Remarque :** les codes décrits pour le contrôleur E-Series E5700 ne s'appliquent pas au contrôleur E5700SG de l'appliance.

4. Si ce n'est pas le cas, contactez le support technique.

Informations associées

- "Afficher les indicateurs d'état"
- "Site de documentation sur les systèmes NetApp E-Series"
- "Erreur : erreur de synchronisation avec le logiciel SANtricity OS"
- "Guide de surveillance des systèmes E5700 et E2800"

- "Afficher les codes de démarrage (contrôleur SG6000-CN)"
- "Afficher les codes d'erreur (contrôleur SG6000-CN)"

Résolution des problèmes de connexion (SG6000 ou SG5700)

Si vous rencontrez des problèmes de connexion lors de l'installation de l'appliance StorageGRID, vous devez effectuer les actions correctives indiquées.

Impossible de se connecter à l'appliance SG6000

Si vous ne parvenez pas à vous connecter à l'appliance, il se peut qu'il y ait un problème de réseau ou que l'installation matérielle n'ait pas été effectuée correctement.

Étapes

1. Si vous ne pouvez pas vous connecter à SANtricity System Manager :
   a. Essayez d'envoyer une requête ping à l'appliance en utilisant l'adresse IP de l'un des contrôleurs de stockage du réseau de gestion pour SANtricity System Manager :
   `ping Storage_Controller_IP`
   b. Si vous ne recevez aucune réponse de la commande ping, confirmez que vous utilisez la bonne adresse IP.

      Utilisez l'adresse IP pour le port de gestion 1 de l'un des contrôleurs de stockage.

   c. Si l'adresse IP est correcte, vérifiez le câblage du dispositif et la configuration du réseau.

      Si ce n'est pas le cas, contactez le support technique.

   d. Si la commande ping a réussi, ouvrez un navigateur Web.
   e. Entrez l'URL pour SANtricity System Manager :
   `https://Storage_Controller_IP`

      La page de connexion à SANtricity System Manager s'affiche.

2. Si vous ne parvenez pas à vous connecter au contrôleur SG6000-CN :
   a. Essayez d'envoyer une requête ping à l'appareil à l'aide de l'adresse IP du contrôleur SG6000-CN :
   `ping SG6000-CN_Controller_IP`
   b. Si vous ne recevez aucune réponse de la commande ping, confirmez que vous utilisez la bonne adresse IP.

      Vous pouvez utiliser l'adresse IP de l'appliance sur le réseau Grid, le réseau Admin ou le réseau client.

   c. Si l'adresse IP est correcte, vérifiez le câblage de l'appliance, les émetteurs-récepteurs SFP et la configuration du réseau.
   d. Si l'accès physique au SG6000-CN est disponible, vous pouvez utiliser une connexion directe à l'adresse IP locale de liaison permanente `169.254.0.1` pour vérifier la configuration de la mise en réseau du contrôleur et la mettre à jour si nécessaire. Pour obtenir des instructions détaillées, reportez-vous à l'étape 2 de la section "Accès au programme d'installation de l'appliance StorageGRID".

      Si ce n'est pas le cas, contactez le support technique.

e. Si la commande ping a réussi, ouvrez un navigateur Web.

f. Entrez l'URL du programme d'installation de l'appliance StorageGRID :
`https://SG6000-CN_Controller_IP:8443`

La page d'accueil s'affiche.

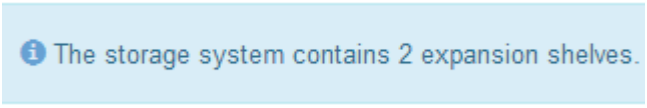
Les tiroirs d'extension SG6060 n'apparaissent pas dans le programme d'installation de l'appliance

Si vous avez installé des tiroirs d'extension pour le SG6060 et qu'ils n'apparaissent pas dans le programme d'installation de l'appliance StorageGRID, vérifiez que ces tiroirs ont été complètement installés et sous tension.

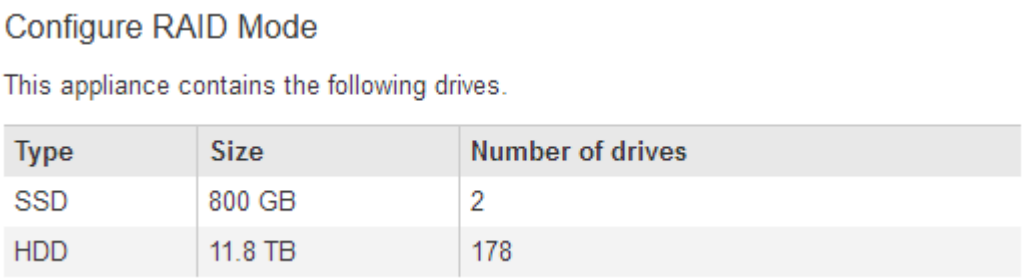
Description de la tâche

Vous pouvez vérifier que les tiroirs d'extension sont connectés à l'appliance en consultant les informations suivantes dans le programme d'installation de l'appliance StorageGRID :

- La page **Home** contient un message sur les tiroirs d'extension.



- La page **Avancé** > **mode RAID** indique par nombre de disques, que l'appliance inclut ou non des tiroirs d'extension. Par exemple, dans la capture d'écran suivante, deux disques SSD et 178 disques durs sont affichés. Un SG6060 avec deux tiroirs d'extension contient 180 disques au total.



Si les pages du programme d'installation de l'appliance StorageGRID n'indiquent pas la présence de tiroirs d'extension, suivez cette procédure.

Étapes

1. Vérifiez que tous les câbles requis ont été correctement connectés. Voir "Cable appliance (SG6000)".
2. Vérifiez que vous avez mis sous tension les tiroirs d'extension. Voir "Branchement des câbles d'alimentation et alimentation (SG6000)".
3. Si vous avez besoin d'aide pour résoudre un problème, contactez le support technique.

Connexion à l'appliance SG5700 impossible

Si vous ne parvenez pas à vous connecter à l'appliance, il se peut qu'il y ait un problème de réseau ou que l'installation matérielle n'ait pas été effectuée correctement.

Étapes

1. Si vous ne pouvez pas vous connecter à SANtricity System Manager :

a. Essayez d'envoyer une commande ping à l'appliance en utilisant l'adresse IP du contrôleur E2800 sur le réseau de gestion pour SANtricity System Manager :
ping *E2800_Controller_IP*

b. Si vous ne recevez aucune réponse de la commande ping, confirmez que vous utilisez la bonne adresse IP.

   Utilisez l'adresse IP du port de gestion 1 du contrôleur E2800.

c. Si l'adresse IP est correcte, vérifiez le câblage du dispositif et la configuration du réseau.

   Si ce n'est pas le cas, contactez le support technique.

d. Si la commande ping a réussi, ouvrez un navigateur Web.

e. Entrez l'URL pour SANtricity System Manager :
https://*E2800_Controller_IP*

   La page de connexion à SANtricity System Manager s'affiche.

2. Si vous ne parvenez pas à vous connecter au contrôleur E5700SG :

   a. Essayez d'envoyer une requête ping à l'appliance à l'aide de l'adresse IP du contrôleur E5700SG :
   ping *E5700SG_Controller_IP*

   b. Si vous ne recevez aucune réponse de la commande ping, confirmez que vous utilisez la bonne adresse IP.

      Vous pouvez utiliser l'adresse IP de l'appliance sur le réseau Grid, le réseau Admin ou le réseau client.

   c. Si l'adresse IP est correcte, vérifiez le câblage de l'appliance, les émetteurs-récepteurs SFP et la configuration du réseau.

      Si ce n'est pas le cas, contactez le support technique.

   d. Si la commande ping a réussi, ouvrez un navigateur Web.

   e. Entrez l'URL du programme d'installation de l'appliance StorageGRID :
   https://*E5700SG_Controller_IP*:8443

      La page d'accueil s'affiche.

Informations associées

"Afficher les indicateurs d'état"

Erreur HE : erreur lors de la synchronisation avec le logiciel SANtricity OS (SG5700)

L'affichage à sept segments sur le contrôleur de calcul indique un code d'erreur SI le programme d'installation de l'appliance StorageGRID ne peut pas se synchroniser avec le logiciel SANtricity OS.

Description de la tâche

Si un code d'erreur HE s'affiche, effectuez cette action corrective.

Étapes

1. Vérifiez l’intégrité des deux câbles d’interconnexion SAS et assurez-vous qu’ils sont correctement connectés.
2. Si nécessaire, remplacez l’un des câbles ou les deux, puis réessayez.
3. Si ce n’est pas le cas, contactez le support technique.

Dépannage de l’installation du matériel (SG100 et SG1000)

Si vous rencontrez des problèmes lors de l’installation, il peut s’avérer utile de consulter les informations de dépannage relatives à la configuration du matériel et aux problèmes de connectivité.

Afficher les codes de démarrage (SG100 et SG1000)

Lorsque vous mettez l’appliance sous tension, le contrôleur BMC consigne une série de codes de démarrage. Vous pouvez afficher ces codes sur une console graphique connectée au port de gestion BMC.

Avant de commencer

- Vous savez comment accéder au tableau de bord BMC.
- Si vous souhaitez utiliser Serial-over-LAN (sol), vous avez de l’expérience avec les applications de console IPMI sol.

Étapes

1. Sélectionnez l’une des méthodes suivantes pour afficher les codes de démarrage du contrôleur de l’appliance et rassemblez l’équipement requis.

Méthode	Équipement requis
Console VGA	• Moniteur VGA • Câble VGA
KVM	• Câble RJ-45
Port série	• Câble série DB-9 • Terminal série virtuel
SOL	• Terminal série virtuel

2. Si vous utilisez une console VGA, procédez comme suit :
   a. Connectez un moniteur compatible VGA au port VGA situé à l’arrière de l’appareil.
   b. Afficher les codes affichés sur le moniteur.
3. Si vous utilisez BMC KVM, effectuez les opérations suivantes :
   a. Connectez-vous au port de gestion du contrôleur BMC et connectez-vous à l’interface Web du contrôleur BMC.
   b. Sélectionnez **télécommande**.

c. Lancez le KVM.

d. Afficher les codes sur le moniteur virtuel.

4. Si vous utilisez un port série et un terminal, effectuez les opérations suivantes :

a. Connectez-vous au port série DB-9 situé à l'arrière de l'appareil.

b. Utiliser les paramètres `115200 8-N-1`.

c. Afficher les codes imprimés sur le terminal série.

5. Si vous utilisez sol, effectuez les opérations suivantes :

a. Connectez-vous au sol IPMI à l'aide de l'adresse IP du BMC et des informations d'identification de connexion.

```
ipmitool -I lanplus -H BMC_Port_IP -U admin -P Password sol activate
```

Dans certains cas, le nom d'utilisateur par défaut peut être `root` au lieu de `admin`.

a. Afficher les codes sur le terminal série virtuel.

6. Utilisez le tableau pour rechercher les codes de votre appareil.

Code	Indique
BONJOUR	Le script de démarrage principal a démarré.
HP	Le système vérifie si le micrologiciel de la carte d'interface réseau (NIC) doit être mis à jour.
RB	Le système redémarre après l'application des mises à jour du firmware.
FP	Les vérifications de mise à jour du micrologiciel du sous-système matériel sont terminées. Les services de communication inter-contrôleurs sont en cours de démarrage.
PC	Le système recherche les données d'installation StorageGRID existantes.
HO	L'appliance StorageGRID est en cours d'exécution.
HAUTE DISPONIBILITÉ	StorageGRID est en cours d'exécution.

Informations associées

"Accéder à l'interface BMC"

Afficher les codes d'erreur (SG100 et SG1000)

Si une erreur matérielle se produit lors du démarrage de l'appliance, le contrôleur BMC consigne un code d'erreur. Si nécessaire, vous pouvez afficher ces codes d'erreur à l'aide de l'interface BMC, puis travailler avec le support technique pour résoudre le problème.

Avant de commencer

- Vous savez comment accéder au tableau de bord BMC.

Étapes

1. Dans le tableau de bord BMC, sélectionnez **Code POST BIOS**.
2. Passez en revue les informations affichées pour le code actuel et le code précédent.

   Si l'un des codes d'erreur suivants s'affiche, contactez le support technique pour résoudre le problème.

Code	Indique
0x0E	Microcode introuvable
0x0F	Microcode non chargé
0x50	Erreur d'initialisation de la mémoire. Type de mémoire non valide ou vitesse de mémoire incompatible.
0x51	Erreur d'initialisation de la mémoire. Échec de la lecture du démon du processeur de service.
0x52	Erreur d'initialisation de la mémoire. La taille de la mémoire n'est pas valide ou les modules de mémoire ne correspondent pas.
0x53	Erreur d'initialisation de la mémoire. Aucune mémoire utilisable détectée.
0x54	Erreur d'initialisation de la mémoire non spécifiée
0x55	Mémoire non installée
0x56	Type de CPU ou vitesse non valide
0x57	Non-concordance du processeur
0x58	Échec de l'autotest de la CPU ou erreur possible du cache de la CPU
0x59	Le micro-code de l'UC est introuvable ou la mise à jour du micro-code a échoué
0x5A	Erreur interne de l'UC
0x5B	La réinitialisation PPI n'est pas disponible
0x5C	Échec de l'autotest du BMC de phase PEI
0xd0	Erreur d'initialisation de l'UC

Code	Indique
0xD1	Erreur d’initialisation du pont Nord
0xD2	Erreur d’initialisation du pont Sud
0xd3	Certains protocoles architecturaux ne sont pas disponibles
0xD4	Erreur d’allocation de ressources PCI. Manque de ressources.
0xD5	Pas d’espace pour la ROM optionnelle héritée
0xD6	Aucun périphérique de sortie de console n’a été trouvé
0xD7	Aucun périphérique d’entrée de console n’a été trouvé
0xD8	Mot de passe non valide
0xD9	Erreur lors du chargement de l’option d’amorçage (erreur Loadimage renvoyée)
0xDA	Échec de l’option de démarrage (erreur StartImage renvoyée)
0xDB	Échec de la mise à jour flash
0xDC	Le protocole de réinitialisation n’est pas disponible
0xDD	Échec de l’autotest du BMC de phase DXE
0xE8	MRC : ERR_NO_MEMORY
0xE9	MRC : ERR_LT_LOCK
0xEA	MRC : ERR_DDR_INIT
0xEB	MRC : ERR_MEM_TEST
0xEC	MRC : SPÉCIFIQUE À ERR_VENDOR
0xED	MRC : ERR_DIMM_COMPAT
0xEE	MRC : COMPATIBILITÉ ERR_MRC
0xEF	MRC : ERR_MRC_STRUCT

Code	Indique
0xF0	MRC : ERR_SET_VDD
0xF1	MRC : ERR_IOT_MEM_BUFFER
0xF2	MRC : ERR_RC_INTERNAL
0xF3	MRC : ERR_INVALID_REG_ACCESS
0xF4	MRC : ERR_SET_MC_FREQ
0xF5	MRC : ERR_READ_MC_FREQ
0x70	MRC : ERR_DIMM_CHANNEL
0x74	MRC : ERR_BIST_CHECK
0xF6	MRC : ERR_SMBUS
0xF7	MRC : ERR_PCU
0xF8	MRC : ERR_NGN
0xF9	MRC : ERR_INTERLEAVE_FAILURE

La configuration matérielle semble suspendue (SG100 et SG1000)

Il se peut que le programme d'installation de l'appliance StorageGRID ne soit pas disponible si des défauts matériels ou des erreurs de câblage empêchent l'appliance de terminer son processus de démarrage.

Étapes

1. Examinez les voyants de l'appareil, ainsi que les codes de démarrage et d'erreur affichés dans le contrôleur BMC.
2. Si vous avez besoin d'aide pour résoudre un problème, contactez le support technique.

Informations associées

- "Afficher les codes de démarrage (SG100 et SG1000)"
- "Afficher les codes d'erreur (SG100 et SG1000)"

Résolution des problèmes de connexion (SG100 et SG1000)

Si vous rencontrez des problèmes de connexion lors de l'installation de l'appliance StorageGRID, vous devez effectuer les actions correctives indiquées.

Connexion à l'appareil impossible

Si vous ne parvenez pas à vous connecter à l'appliance de services, il se peut qu'il y ait un problème de réseau ou que l'installation matérielle n'ait pas été effectuée correctement.

Étapes

1. Essayez d'envoyer une requête ping à l'appareil à l'aide de l'adresse IP de l'appareil :
   `ping services_appliance_IP`
2. Si vous ne recevez aucune réponse de la commande ping, confirmez que vous utilisez la bonne adresse IP.

   Vous pouvez utiliser l'adresse IP de l'appliance sur le réseau Grid, le réseau Admin ou le réseau client.
3. Si l'adresse IP est correcte, vérifiez le câblage de l'appliance, les émetteurs-récepteurs QSFP ou SFP et la configuration du réseau.
4. Si l'accès physique à l'appareil est disponible, vous pouvez utiliser une connexion directe à l'adresse IP locale de liaison permanente `169.254.0.1` pour vérifier la configuration de la mise en réseau du contrôleur et la mettre à jour si nécessaire. Pour obtenir des instructions détaillées, reportez-vous à l'étape 2 de la section "Accédez au programme d'installation de l'appliance StorageGRID".

   Si ce n'est pas le cas, contactez le support technique.
5. Si la commande ping a réussi, ouvrez un navigateur Web.
6. Entrez l'URL du programme d'installation de l'appliance StorageGRID :
   `https://appliances_controller_IP:8443`

   La page d'accueil s'affiche.

Installez Red Hat Enterprise Linux ou CentOS

Installez Red Hat Enterprise Linux ou CentOS: Présentation

L'installation d'un système StorageGRID dans un environnement Red Hat Enterprise Linux (RHEL) ou CentOS Linux comprend trois étapes principales.

1. **Préparation**: Pendant la planification et la préparation, vous effectuez les tâches suivantes :
   - En savoir plus sur les besoins matériels et de stockage pour StorageGRID.
   - Découvrez les détails de "La mise en réseau StorageGRID" vous pouvez ainsi configurer votre réseau de façon appropriée.
   - Identifiez et préparez les serveurs physiques ou virtuels que vous prévoyez d'utiliser pour héberger vos nœuds de grid StorageGRID.
   - Sur les serveurs que vous avez préparés :
     - Installez Linux
     - Configurez le réseau hôte
     - Configurer le stockage de l'hôte
     - Poser le moteur de mise en conteneurs
     - Installez les services d'hôte StorageGRID

2. **Déploiement** : déployez des nœuds de la grille à l'aide de l'interface utilisateur appropriée. Lorsque vous déployez des nœuds grid, ils sont créés dans le cadre du système StorageGRID et connectés à un ou plusieurs réseaux.
   a. Utilisez la ligne de commande Linux et les fichiers de configuration des nœuds pour déployer des nœuds de grille logiciels sur les hôtes que vous avez préparés à l'étape 1.
   b. Utilisez le programme d'installation de l'appliance StorageGRID pour déployer les nœuds d'appliance StorageGRID.

> Les instructions d'installation et d'intégration spécifiques au matériel ne sont pas incluses dans la procédure d'installation de StorageGRID. Pour savoir comment installer les appliances StorageGRID, consultez le "Démarrage rapide pour l'installation du matériel" pour trouver les instructions relatives à votre appareil.

3. **Configuration** : lorsque tous les nœuds ont été déployés, utilisez le gestionnaire de grille pour configurer la grille et terminer l'installation.

Ces instructions recommandent une approche standard de déploiement et de configuration d'un système StorageGRID. Voir également les informations sur les approches alternatives suivantes :

- Utilisez une structure d'orchestration standard comme Ansible, Puppet ou Chef pour installer RHEL ou CentOS, configurer le réseau et le stockage, installer le moteur de conteneur et le service hôte StorageGRID, et déployer des nœuds grid virtuels.
- Automatiser le déploiement et la configuration du système StorageGRID à l'aide d'un script de configuration Python (fourni dans l'archive d'installation).
- Automatisez le déploiement et la configuration des nœuds grid d'appliance avec un script de configuration Python (disponible dans l'archive de l'installation ou depuis le programme d'installation de l'appliance StorageGRID).
- Si vous êtes un développeur avancé de déploiements StorageGRID, utilisez les API REST d'installation pour automatiser l'installation des nœuds grid d'StorageGRID.

Planifiez et préparez-vous pour l'installation de Red Hat ou CentOS

Avant d'installer (Red Hat ou CentOS)

Avant de déployer des nœuds de grid et de configurer StorageGRID, vous devez connaître les étapes et les conditions requises pour effectuer cette procédure.

Les procédures de déploiement et de configuration de StorageGRID supposent que vous connaissez bien l'architecture et le fonctionnement du système StorageGRID.

Vous pouvez déployer un ou plusieurs sites à la fois. Toutefois, tous les sites doivent respecter le minimum requis : disposer d'au moins trois nœuds de stockage.

Avant de démarrer une installation StorageGRID, vous devez :

- Analysez les besoins en calcul, notamment les exigences minimales en termes de CPU et de RAM pour chaque nœud.
- Découvrez comment StorageGRID prend en charge plusieurs réseaux pour faciliter la séparation du trafic, la sécurité et l'administration, et planifiez les réseaux que vous envisagez de connecter à chaque nœud StorageGRID.

Voir le StorageGRID "Instructions de mise en réseau".

- Analysez les exigences de performances et de stockage de chaque type de nœud grid.
- Identifier un ensemble de serveurs (physiques, virtuels ou les deux) qui, dans l'agrégat, fournissent suffisamment de ressources pour prendre en charge le nombre et le type de nœuds StorageGRID que vous prévoyez de déployer.
- Prenez connaissance du "conditions requises pour la migration des nœuds", si vous souhaitez effectuer une maintenance planifiée sur des hôtes physiques sans interruption de service.
- Rassemblez toutes les informations de réseautage à l'avance. À moins que vous n'utilisiez DHCP, rassemblez les adresses IP à attribuer à chaque nœud de grille, ainsi que les adresses IP des serveurs DNS et NTP qui seront utilisés.
- Installez, connectez et configurez tout le matériel requis, y compris les appliances StorageGRID, selon les spécifications.

> Si votre installation StorageGRID n'utilise pas de nœuds de stockage (matériels) StorageGRID, vous devez utiliser un stockage RAID matériel avec un cache d'écriture protégé par batterie (BBWC). StorageGRID ne prend pas en charge l'utilisation de réseaux de stockage virtuels (VSAN), de RAID logiciel ou aucune protection RAID.

> Les instructions d'installation et d'intégration spécifiques au matériel ne sont pas incluses dans la procédure d'installation de StorageGRID. Pour savoir comment installer les appliances StorageGRID, reportez-vous à la section "Installez le matériel de l'appliance".

- Choisissez les outils de déploiement et de configuration que vous souhaitez utiliser.

Matériel requis

Avant d'installer StorageGRID, vous devez rassembler et préparer les ressources nécessaires.

Élément	Remarques
Licence NetApp StorageGRID	Vous devez disposer d'une licence NetApp valide et signée numériquement. **Note**: Une licence de non-production, qui peut être utilisée pour tester et démontrer les grilles de concept, est incluse dans l'archive d'installation de StorageGRID.
Archive de l'installation de StorageGRID	Vous devez "Téléchargez l'archive d'installation de StorageGRID et extrayez les fichiers".

Élément	Remarques
L'ordinateur portable de service	Le système StorageGRID est installé par le biais d'un ordinateur portable de service. L'ordinateur portable de service doit posséder : • Port réseau • Client SSH (par exemple, PuTTY) • "Navigateur Web pris en charge"
Documentation StorageGRID	• "Notes de mise à jour" • "Instructions d'administration de StorageGRID"

Informations associées

"Matrice d'interopérabilité NetApp"

Téléchargez et extrayez les fichiers d'installation de StorageGRID

Vous devez télécharger l'archive d'installation de StorageGRID et extraire les fichiers requis.

Étapes

1. Accédez au "Page de téléchargements NetApp pour StorageGRID".
2. Sélectionnez le bouton pour télécharger la dernière version ou sélectionnez une autre version dans le menu déroulant et sélectionnez **Go**.
3. Connectez-vous avec le nom d'utilisateur et le mot de passe de votre compte NetApp.
4. Si une instruction attention/MustRead apparaît, lisez-la et cochez la case.

   Après l'installation de la version StorageGRID, vous devez appliquer les correctifs requis. Pour plus d'informations, reportez-vous à la section "procédure de correctif dans les instructions de récupération et de maintenance".

5. Lisez le contrat de licence de l'utilisateur final, cochez la case, puis sélectionnez **accepter et continuer**.
6. Dans la colonne **Install StorageGRID**, sélectionnez le fichier .tgz ou .zip pour Red Hat Enterprise Linux ou CentOS.

   Sélectionner `.zip` Fichier si vous exécutez Windows sur l'ordinateur portable de service.

7. Enregistrez et extrayez le fichier d'archive.
8. Choisissez les fichiers dont vous avez besoin dans la liste suivante.

   Les fichiers dont vous avez besoin dépendent de votre topologie de grille planifiée et de la manière dont vous allez déployer votre système StorageGRID.

   Les chemins répertoriés dans la table sont relatifs au répertoire de niveau supérieur installé par l'archive d'installation extraite

Chemin d’accès et nom de fichier	Description
	Fichier texte qui décrit tous les fichiers contenus dans le fichier de téléchargement StorageGRID.
	Licence gratuite qui ne fournit aucun droit d’assistance pour le produit.
	Package RPM pour l’installation des images des nœuds StorageGRID sur vos hôtes RHEL ou CentOS.
	Package RPM pour l’installation du service hôte StorageGRID sur vos hôtes RHEL ou CentOS.
Outil de script de déploiement	Description
	Script Python utilisé pour automatiser la configuration d’un système StorageGRID.
	Script Python utilisé pour automatiser la configuration des appliances StorageGRID.
	Exemple de fichier de configuration à utiliser avec `configure-storagegrid.py` script.
	Exemple de script Python que vous pouvez utiliser pour vous connecter à l’API Grid Management lorsque l’authentification unique est activée. Vous pouvez également utiliser ce script pour le Federate Ping.
	Un fichier de configuration vierge à utiliser avec le `configure-storagegrid.py` script.
	Exemple de rôle et de manuel de vente Ansible pour la configuration des hôtes RHEL ou CentOS pour le déploiement de conteneurs StorageGRID. Vous pouvez personnaliser le rôle ou le PlayBook selon vos besoins.
	Exemple de script Python que vous pouvez utiliser pour vous connecter à l’API de gestion de grille lorsque l’authentification unique (SSO) est activée à l’aide d’Active Directory ou de Ping Federate.

Chemin d'accès et nom de fichier	Description
	Script d'aide appelé par le compagnon `storagegrid-ssoauth-azure.py` Script Python pour effectuer des interactions SSO avec Azure.
	Schémas API pour StorageGRID. **Remarque** : avant d'effectuer une mise à niveau, vous pouvez utiliser ces schémas pour confirmer que tout code que vous avez écrit pour utiliser les API de gestion StorageGRID sera compatible avec la nouvelle version de StorageGRID si vous ne disposez pas d'un environnement StorageGRID non productif pour le test de compatibilité de mise à niveau.

Configuration requise pour le processeur et la RAM

Avant d'installer le logiciel StorageGRID, vérifiez et configurez le matériel afin qu'il soit prêt à prendre en charge le système StorageGRID.

Pour plus d'informations sur les serveurs pris en charge, reportez-vous au "Matrice d'interopérabilité NetApp".

Chaque nœud StorageGRID nécessite au moins :

- Cœurs de processeur : 8 par nœud
- RAM : au moins 24 Go par nœud et 2 à 16 Go de moins que la RAM totale du système, selon la mémoire RAM totale disponible et la quantité de logiciel non StorageGRID exécuté sur le système

Vérifiez que le nombre de nœuds StorageGRID que vous prévoyez d'exécuter sur chaque hôte physique ou virtuel ne dépasse pas le nombre de cœurs de processeur ou la mémoire RAM physique disponible. Si les hôtes ne sont pas dédiés à l'exécution de StorageGRID (non recommandé), veillez à prendre en compte les besoins en ressources des autres applications.

> Surveillez régulièrement l'utilisation de votre processeur et de votre mémoire pour vous assurer que ces ressources continuent de s'adapter à votre charge de travail. Par exemple, doubler l'allocation de la RAM et du processeur pour les nœuds de stockage virtuels fournira des ressources similaires à celles des nœuds d'appliance StorageGRID. En outre, si la quantité de métadonnées par nœud dépasse 500 Go, envisagez d'augmenter la mémoire RAM par nœud à au moins 48 Go. Pour plus d'informations sur la gestion du stockage des métadonnées d'objet, l'augmentation du paramètre espace réservé aux métadonnées et la surveillance de l'utilisation du processeur et de la mémoire, reportez-vous aux instructions de "administration", "contrôle", et "mise à niveau" StorageGRID :

Si le hyperthreading est activé sur les hôtes physiques sous-jacents, vous pouvez fournir 8 cœurs virtuels (4 cœurs physiques) par nœud. Si le hyperthreading n'est pas activé sur les hôtes physiques sous-jacents, vous devez fournir 8 cœurs physiques par nœud.

Si vous utilisez des machines virtuelles en tant qu'hôtes et que vous contrôlez la taille et le nombre de machines virtuelles, nous vous recommandons d'utiliser une seule machine virtuelle pour chaque nœud StorageGRID afin de dimensionner celle-ci en conséquence.

Dans le cas de déploiements en production, vous ne devez pas exécuter plusieurs nœuds de stockage sur le même matériel de stockage physique ou sur le même hôte virtuel. Dans un seul déploiement StorageGRID, chaque nœud de stockage doit se trouver dans son propre domaine de défaillances isolé. Vous pouvez optimiser la durabilité et la disponibilité des données d'objet si vous assurez qu'une seule panne matérielle peut avoir un impact sur un seul nœud de stockage.

Voir aussi "Les besoins en matière de stockage et de performances".

Les besoins en matière de stockage et de performances

Vous devez connaître les exigences de stockage des nœuds StorageGRID afin de fournir un espace suffisant pour prendre en charge la configuration initiale et l'extension future du stockage.

Les nœuds StorageGRID nécessitent trois catégories logiques de stockage :

- **Pool de conteneurs** — stockage de niveau de performances (SAS ou SSD 10 000 tr/min) pour les conteneurs de nœuds, qui sera affecté au pilote de stockage du moteur de conteneur lors de l'installation et de la configuration du moteur de mise en conteneurs sur les hôtes qui prendront en charge vos nœuds StorageGRID.
- **Données système** — stockage de niveau performances (SAS 10 000 tr/min ou SSD) pour le stockage persistant par nœud des données système et des journaux de transactions, que les services hôtes StorageGRID consommeront et mappent vers des nœuds individuels.
- **Données objet** — stockage de niveau performance (SAS 10 000 tr/min ou SSD) et stockage en bloc de niveau capacité (NL-SAS/SATA) pour le stockage persistant des données d'objet et des métadonnées d'objet.

Vous devez utiliser des périphériques de bloc RAID pour toutes les catégories de stockage. Les disques, disques SSD ou JBOD non redondants ne sont pas pris en charge. Vous pouvez utiliser un stockage RAID partagé ou local pour l'une des catégories de stockage. Toutefois, si vous souhaitez utiliser la fonctionnalité de migration de nœuds dans StorageGRID, vous devez stocker les données système et les données d'objet sur un stockage partagé. Pour plus d'informations, voir "Exigences de migration des conteneurs de nœuds".

Exigences en matière de performances

Les performances des volumes utilisés pour les pools de conteneurs, les données système et les métadonnées d'objet ont un impact significatif sur la performance globale du système. Pour ces volumes, il est recommandé d'utiliser un stockage de Tier de performances (SAS 10 000 tr/min ou SSD) pour garantir des performances de disque satisfaisantes en termes de latence, d'opérations d'entrée/sortie par seconde (IOPS) et de débit. Vous pouvez utiliser un stockage de niveau de capacité (NL-SAS/SATA) pour le stockage persistant des données d'objet.

La mise en cache de l'écriture différée est activée sur les volumes utilisés pour le pool de conteneurs, les données système et les données d'objet. Le cache doit se trouver sur un support protégé ou persistant.

Exigences relatives aux hôtes qui utilisent un stockage NetApp ONTAP

Si le nœud StorageGRID utilise le stockage affecté à un système NetApp ONTAP, vérifiez que cette FabricPool règle n'est pas activée pour le volume. La désactivation du Tiering FabricPool pour les volumes utilisés avec des nœuds StorageGRID simplifie la résolution des problèmes et les opérations de stockage.

N'utilisez jamais FabricPool pour transférer automatiquement toutes les données liées à StorageGRID vers StorageGRID. Le Tiering des données StorageGRID vers StorageGRID augmente la complexité opérationnelle et la résolution des problèmes.

Nombre d'hôtes requis

Chaque site StorageGRID requiert au moins trois nœuds de stockage.

Dans un déploiement de production, n'exécutez pas plus d'un nœud de stockage sur un seul hôte physique ou virtuel. L'utilisation d'un hôte dédié pour chaque nœud de stockage fournit un domaine de défaillance isolé.

Les autres types de nœuds, comme les nœuds d'administration ou les nœuds de passerelle, peuvent être déployés sur les mêmes hôtes, ou sur leurs propres hôtes dédiés, si nécessaire.

Nombre de volumes de stockage pour chaque hôte

Le tableau ci-dessous présente le nombre de volumes de stockage (LUN) requis pour chaque hôte et la taille minimale requise pour chaque LUN, en fonction des nœuds à déployer sur cet hôte.

La taille de LUN maximale testée est de 39 To.

Ces nombres sont pour chaque hôte, et non pour l'intégralité de la grille.

Objectif de LUN	Catégorie de stockage	Nombre de LUN	Taille minimale/LUN
Pool de stockage du moteur du conteneur	Pool de conteneurs	1	Nombre total de nœuds × 100 Go
`/var/local` volumétrie	Données système	1 pour chaque nœud sur cet hôte	90 GO
Nœud de stockage	Données d'objet	3 pour chaque nœud de stockage sur cet hôte **Remarque :** Un noeud de stockage logiciel peut avoir 1 à 16 volumes de stockage; au moins 3 volumes de stockage sont recommandés.	12 TO (4 TO/LUN) VOIR Besoins de stockage des nœuds de stockage pour en savoir plus.
Journaux d'audit du nœud d'administration	Données système	1 pour chaque nœud d'administration sur cet hôte	200 GO
Tables des nœuds d'administration	Données système	1 pour chaque nœud d'administration sur cet hôte	200 GO

Selon le niveau d'audit configuré, la taille des entrées utilisateur telles que le nom de clé d'objet S3, Et la quantité de données des journaux d'audit à conserver, il peut être nécessaire d'augmenter la taille de la LUN des journaux d'audit sur chaque nœud d'administration.en général, une grille génère environ 1 Ko de données d'audit par opération S3, Cela signifie qu'un LUN de 200 Go peut prendre en charge 70 millions d'opérations par jour ou 800 opérations par seconde pendant deux à trois jours.

Espace de stockage minimum pour un hôte

Le tableau suivant indique l'espace de stockage minimal requis pour chaque type de nœud. Ce tableau permet de déterminer la quantité minimale de stockage que vous devez fournir à l'hôte dans chaque catégorie de stockage, en fonction des nœuds à déployer sur cet hôte.

Les snapshots de disque ne peuvent pas être utilisés pour restaurer les nœuds de grille. Reportez-vous plutôt au "restauration du nœud grid" procédures pour chaque type de nœud.

Type de nœud	Pool de conteneurs	Données système	Données d'objet
Nœud de stockage	100 GO	90 GO	4,000 GO
Nœud d'administration	100 GO	490 Go (3 LUN)	*non applicable*
Nœud de passerelle	100 GO	90 GO	*non applicable*
Nœud d'archivage	100 GO	90 GO	*non applicable*

Exemple : calcul des besoins en stockage d'un hôte

Supposons que vous prévoyez de déployer trois nœuds sur un même hôte : un nœud de stockage, un nœud d'administration et un nœud de passerelle. Vous devez fournir un minimum de neuf volumes de stockage à l'hôte. Vous aurez besoin d'un minimum de 300 Go de stockage de Tier de performance pour les conteneurs de nœuds, de 670 Go de stockage de Tier de performance pour les données système et les journaux de transactions, et de 12 To de stockage de Tier de capacité pour les données d'objet.

Type de nœud	Objectif de LUN	Nombre de LUN	Taille de la LUN
Nœud de stockage	Pool de stockage du moteur du conteneur	1	300 Go (100 Go/nœud)
Nœud de stockage	`/var/local` volumétrie	1	90 GO
Nœud de stockage	Données d'objet	3	12 TO (4 TO/LUN)
Nœud d'administration	`/var/local` volumétrie	1	90 GO
Nœud d'administration	Journaux d'audit du nœud d'administration	1	200 GO

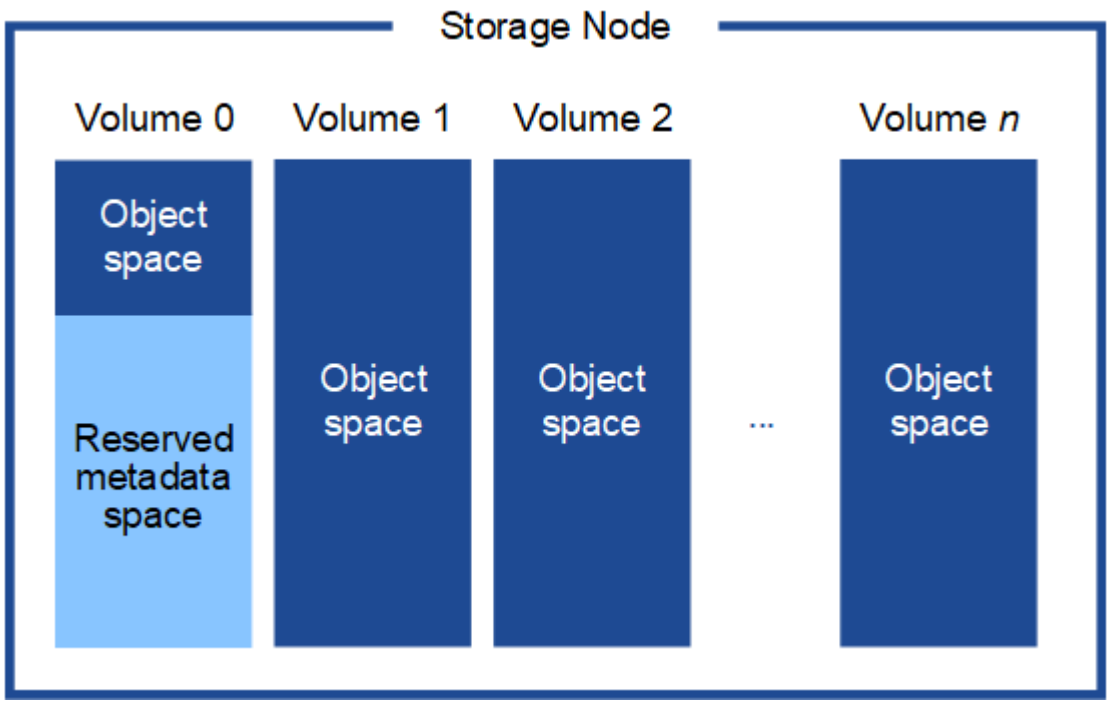
Type de nœud	Objectif de LUN	Nombre de LUN	Taille de la LUN
Nœud d'administration	Tables des nœuds d'administration	1	200 GO
Nœud de passerelle	`/var/local` volumétrie	1	90 GO
Total		**9**	**Pool de conteneurs :** 300 Go **Données système :** 670 Go **Données d'objet :** 12,000 Go

Besoins de stockage des nœuds de stockage

Un nœud de stockage logiciel peut disposer de 1 à 16 volumes de stockage, dont -3 volumes ou plus sont recommandés. Chaque volume de stockage doit être supérieur ou égale à 4 To.

Un nœud de stockage d'appliance peut disposer d'un maximum de 48 volumes de stockage.

Comme illustré dans la figure, StorageGRID réserve l'espace des métadonnées d'objet sur le volume de stockage 0 de chaque nœud de stockage. Tout espace restant sur le volume de stockage 0 et tout autre volume de stockage du nœud de stockage est utilisé exclusivement pour les données d'objet.



Pour assurer la redondance et protéger les métadonnées d'objet contre la perte, StorageGRID stocke trois copies des métadonnées de tous les objets du système sur chaque site. Les trois copies de métadonnées d'objet sont réparties de manière uniforme sur tous les nœuds de stockage de chaque site.

Lorsque vous attribuez de l'espace au volume 0 d'un nouveau nœud de stockage, vous devez vous assurer qu'il y a suffisamment d'espace pour la portion de ce nœud de toutes les métadonnées d'objet.

- Au moins, vous devez affecter au volume 0 au moins 4 To.

> Si vous n'utilisez qu'un seul volume de stockage pour un nœud de stockage et que vous attribuez 4 To ou moins au volume, le nœud de stockage peut entrer l'état de lecture seule au démarrage et ne stocker que les métadonnées de l'objet.

> Si vous attribuez moins de 500 Go au volume 0 (utilisation hors production uniquement), 10 % de la capacité du volume de stockage est réservée aux métadonnées.

- Si vous installez un nouveau système (StorageGRID 11.6 ou supérieur) et que chaque nœud de stockage dispose de 128 Go ou plus de RAM, attribuez 8 To ou plus au volume 0. L'utilisation d'une valeur plus grande pour le volume 0 peut augmenter l'espace autorisé pour les métadonnées sur chaque nœud de stockage.
- Lorsque vous configurez différents nœuds de stockage pour un site, utilisez le même paramètre pour le volume 0 si possible. Si un site contient des nœuds de stockage de différentes tailles, le nœud de stockage avec le plus petit volume 0 déterminera la capacité des métadonnées de ce site.

Pour plus d'informations, rendez-vous sur "Gérer le stockage des métadonnées d'objet".

Exigences de migration des conteneurs de nœuds

La fonction de migration de nœud vous permet de déplacer manuellement un nœud d'un hôte à un autre. En général, les deux hôtes se trouvent dans le même data Center physique.

La migration des nœuds vous permet d'effectuer la maintenance des hôtes physiques sans interrompre les opérations de la grille. Vous déplacez tous les nœuds StorageGRID, un par un, vers un autre hôte avant de mettre l'hôte physique hors ligne. La migration de nœuds ne demande qu'une interruption courte pour chaque nœud et ne doit en aucun cas affecter le fonctionnement ou la disponibilité des services de grid.

Pour utiliser la fonctionnalité de migration de nœuds StorageGRID, votre déploiement doit répondre à des exigences supplémentaires :

- Noms d'interface réseau cohérents entre les hôtes dans un seul data Center physique
- Stockage partagé pour les métadonnées StorageGRID et les volumes de référentiel d'objets accessibles par tous les hôtes dans un seul data Center physique. Vous pouvez, par exemple, utiliser des baies de stockage NetApp E-Series.

Si vous utilisez des hôtes virtuels et que la couche de l'hyperviseur sous-jacent prend en charge la migration des ordinateurs virtuels, vous pouvez utiliser cette fonctionnalité à la place de la fonctionnalité de migration des nœuds de StorageGRID. Dans ce cas, vous pouvez ignorer ces exigences supplémentaires.

Avant d'effectuer la migration ou la maintenance de l'hyperviseur, arrêtez les nœuds selon les besoins. Reportez-vous aux instructions pour "arrêt d'un nœud grid".

VMware Live migration non pris en charge

OpenStack Live migration et VMware Live vMotion entraînent un bond de l'horloge de la machine virtuelle et ne sont pas pris en charge pour les nœuds de grid, quel qu'en soit le type. Bien que les temps d'horloge rares

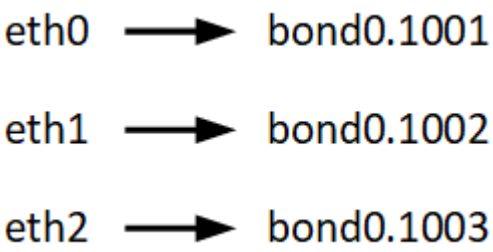
et incorrects peuvent entraîner une perte de données ou des mises à jour de la configuration.

La migration à froid est prise en charge. Dans le cadre d'une migration à froid, vous devez arrêter les nœuds StorageGRID avant de les migrer entre les hôtes. Reportez-vous aux instructions pour "arrêt d'un nœud grid".

Noms d'interface réseau cohérents

Pour déplacer un nœud d'un hôte à un autre, le service d'hôte StorageGRID doit être certain que la connectivité réseau externe du nœud à son emplacement actuel peut être dupliquée au nouvel emplacement. Cette confiance est obtenue grâce à l'utilisation de noms d'interface réseau cohérents dans les hôtes.

Supposons, par exemple, que le nœud StorageGRID exécutant sur Host1 ait été configuré avec les mappages d'interface suivants :



Le côté gauche des flèches correspond aux interfaces traditionnelles affichées à partir d'un conteneur StorageGRID (c'est-à-dire, respectivement, les interfaces réseau Grid, Admin et client). Le côté droit des flèches correspond aux interfaces hôtes réelles fournissant ces réseaux, qui sont trois interfaces VLAN subordonnées à la même liaison d'interface physique.

Supposons maintenant que vous voulez migrer NodeA vers Host2. Si Host2 possède également des interfaces nommées bond0.1001, bond0.1002, et bond0.1003, le système permettra le déplacement, en supposant que les interfaces nommées similaires fourniront la même connectivité sur Host2 que sur Host1. Si Host2 ne possède pas d'interfaces avec les mêmes noms, le déplacement ne sera pas autorisé.

Il existe de nombreuses façons d'obtenir un nom d'interface réseau cohérent sur plusieurs hôtes ; voir "Configuration du réseau hôte" pour quelques exemples.

Stockage partagé

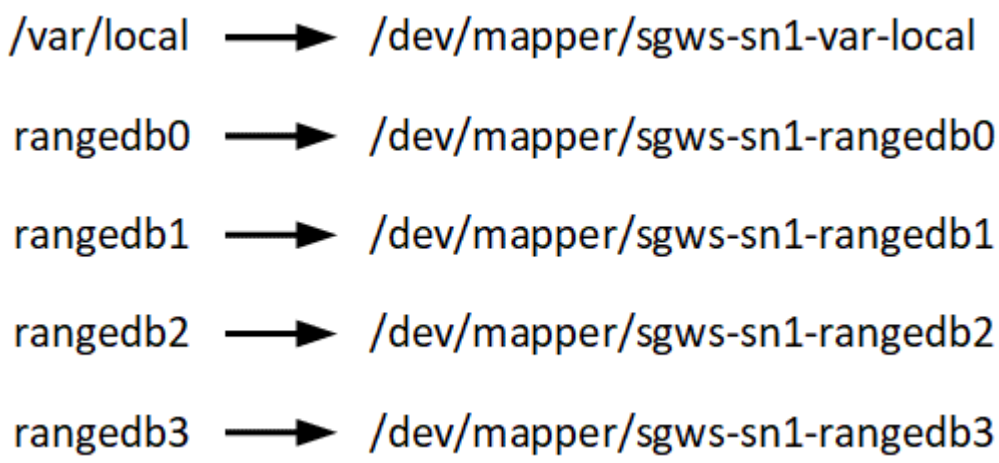
Pour réaliser des migrations de nœuds rapides et sans surcharge, la fonctionnalité de migration de nœuds StorageGRID ne déplace pas physiquement les données du nœud. La migration des nœuds se déroule comme une paire d'opérations d'exportation et d'importation :

1. Lors de l'opération « exportation de nœud », une petite quantité de données d'état permanent est extraite du conteneur de nœud exécuté sur HostA et mise en cache sur le volume de données système de ce nœud. Ensuite, le conteneur de nœud sur HostA est déinstancié.
2. Lors de l'opération « importation de nœud », le conteneur de nœud sur l'hôte B qui utilise la même interface réseau et les mêmes mappages de stockage en bloc qui étaient en vigueur sur l'hôte est instancié. Les données de l'état persistant en cache sont ensuite insérées dans la nouvelle instance.

Compte tenu de ce mode de fonctionnement, toutes les données système et les volumes de stockage objet du nœud doivent être accessibles à la fois à HostA et HostB pour que la migration soit autorisée, et pour fonctionner. En outre, ils doivent avoir été mappés dans le noeud en utilisant des noms qui sont garantis pour faire référence aux mêmes LUN sur HostA et HostB.

L'exemple suivant montre une solution pour le mappage de périphériques de bloc pour un nœud de stockage

StorageGRID, où les chemins d'accès multiples DM sont utilisés sur les hôtes et où le champ alias a été utilisé dans `/etc/multipath.conf` pour fournir des noms de périphériques de bloc cohérents et conviviaux disponibles sur tous les hôtes.



Outils de déploiement

Vous pouvez bénéficier de l'automatisation complète ou partielle de l'installation StorageGRID.

L'automatisation du déploiement peut être utile dans les cas suivants :

- Vous utilisez déjà un framework d'orchestration standard, comme Ansible, Puppet ou Chef, pour déployer et configurer des hôtes physiques ou virtuels.
- Vous prévoyez de déployer plusieurs instances StorageGRID.
- Vous déployez une instance StorageGRID vaste et complexe.

Le service hôte StorageGRID est installé par un package et piloté par des fichiers de configuration qui peuvent être créés de manière interactive lors d'une installation manuelle, ou préparés à l'avance (ou par programmation) pour permettre l'installation automatisée à l'aide des frameworks d'orchestration standard. StorageGRID propose des scripts Python en option permettant d'automatiser la configuration des appliances StorageGRID et l'ensemble du système StorageGRID (la « grille »). Vous pouvez utiliser ces scripts directement, ou vous pouvez les inspecter pour apprendre à utiliser le "API REST d'installation de StorageGRID" vous développez vos connaissances en matière d'outils de déploiement et de configuration du grid.

Si vous souhaitez automatiser tout ou partie de votre déploiement StorageGRID, passez à l'étape suivant "Automatisez l'installation" avant de commencer le processus d'installation.

Préparation des hôtes (Red Hat ou CentOS)

Modification des paramètres à l'échelle de l'hôte lors de l'installation

Sur les systèmes bare Metal, StorageGRID apporte des modifications à l'ensemble de l'hôte `sysctl` paramètres.

Les modifications suivantes sont apportées :

```
# Recommended Cassandra setting: CASSANDRA-3563, CASSANDRA-13008, DataStax
documentation
vm.max_map_count = 1048575

# core file customization
# Note: for cores generated by binaries running inside containers, this
# path is interpreted relative to the container filesystem namespace.
# External cores will go nowhere, unless /var/local/core also exists on
# the host.
kernel.core_pattern = /var/local/core/%e.core.%p

# Set the kernel minimum free memory to the greater of the current value
or
# 512MiB if the host has 48GiB or less of RAM or 1.83GiB if the host has
more than 48GiB of RTAM
vm.min_free_kbytes = 524288

# Enforce current default swappiness value to ensure the VM system has
some
# flexibility to garbage collect behind anonymous mappings. Bump
watermark_scale_factor
# to help avoid OOM conditions in the kernel during memory allocation
bursts. Bump
# dirty_ratio to 90 because we explicitly fsync data that needs to be
persistent, and
# so do not require the dirty_ratio safety net. A low dirty_ratio combined
with a large
# working set (nr_active_pages) can cause us to enter synchronous I/O mode
unnecessarily,
# with deleterious effects on performance.
vm.swappiness = 60
vm.watermark_scale_factor = 200
vm.dirty_ratio = 90

# Turn off slow start after idle
net.ipv4.tcp_slow_start_after_idle = 0

# Tune TCP window settings to improve throughput
net.core.rmem_max = 8388608
net.core.wmem_max = 8388608
net.ipv4.tcp_rmem = 4096 524288 8388608
net.ipv4.tcp_wmem = 4096 262144 8388608
net.core.netdev_max_backlog = 2500

# Turn on MTU probing
net.ipv4.tcp_mtu_probing = 1
```

```
# Be more liberal with firewall connection tracking
net.ipv4.netfilter.ip_conntrack_tcp_be_liberal = 1

# Reduce TCP keepalive time to reasonable levels to terminate dead
connections
net.ipv4.tcp_keepalive_time = 270
net.ipv4.tcp_keepalive_probes = 3
net.ipv4.tcp_keepalive_intvl = 30

# Increase the ARP cache size to tolerate being in a /16 subnet
net.ipv4.neigh.default.gc_thresh1 = 8192
net.ipv4.neigh.default.gc_thresh2 = 32768
net.ipv4.neigh.default.gc_thresh3 = 65536
net.ipv6.neigh.default.gc_thresh1 = 8192
net.ipv6.neigh.default.gc_thresh2 = 32768
net.ipv6.neigh.default.gc_thresh3 = 65536

# Disable IP forwarding, we are not a router
net.ipv4.ip_forward = 0

# Follow security best practices for ignoring broadcast ping requests
net.ipv4.icmp_echo_ignore_broadcasts = 1

# Increase the pending connection and accept backlog to handle larger
connection bursts.
net.core.somaxconn=4096
net.ipv4.tcp_max_syn_backlog=4096
```

Installez Linux

Vous devez installer Linux sur tous les hôtes du grid. Utilisez le "Matrice d'interopérabilité NetApp" pour obtenir une liste des versions prises en charge.

> Assurez-vous que votre système d'exploitation est mis à niveau vers le noyau Linux 4.15 ou supérieur.

Étapes

1. Installez Linux sur tous les hôtes de réseau physiques ou virtuels conformément aux instructions du distributeur ou à la procédure standard.

   > Si vous utilisez le programme d'installation Linux standard, NetApp recommande de sélectionner la configuration du logiciel « nœud de calcul », le cas échéant, ou l'environnement de base « installation minimale ». N'installez aucun environnement de bureau graphique.

2. Assurez-vous que tous les hôtes ont accès aux référentiels de paquets, y compris le canal Extras.

Vous aurez peut-être besoin de ces modules supplémentaires plus tard dans cette procédure d'installation.

3. Si le swap est activé :

   a. Exécutez la commande suivante : `$ sudo swapoff --all`

   b. Supprimez toutes les entrées d'échange de `/etc/fstab` pour conserver les paramètres.

> Si vous ne désactivez pas ces fichiers, les performances peuvent être considérablement réduites.

Configuration du réseau hôte (Red Hat Enterprise Linux ou CentOS)

Une fois l'installation de Linux terminée sur vos hôtes, vous devrez peut-être procéder à une configuration supplémentaire pour préparer un ensemble d'interfaces réseau sur chaque hôte, adapté au mappage vers les nœuds StorageGRID que vous pourrez déployer ultérieurement.

Avant de commencer

- Vous avez passé en revue le "Instructions de mise en réseau d'StorageGRID".
- Vous avez passé en revue les informations sur "exigences de migration des conteneurs de nœuds".
- Si vous utilisez des hôtes virtuels, vous avez lu le Considérations et recommandations relatives au clonage d'adresses MAC avant de configurer le réseau hôte.

> Si vous utilisez des machines virtuelles en tant qu'hôtes, vous devez sélectionner VMXNET 3 comme carte réseau virtuelle. La carte réseau VMware E1000 a provoqué des problèmes de connectivité avec les conteneurs StorageGRID déployés sur certaines distributions de Linux.

Description de la tâche

Les nœuds du grid doivent être capables d'accéder au réseau Grid et, éventuellement, aux réseaux client et Admin. Vous fournissez cet accès en créant des mappages qui associent l'interface physique de l'hôte aux interfaces virtuelles de chaque nœud de la grille. Lors de la création d'interfaces hôtes, utilisez des noms conviviaux pour faciliter le déploiement sur tous les hôtes et pour activer la migration.

Une même interface peut être partagée entre l'hôte et un ou plusieurs nœuds. Par exemple, vous pouvez utiliser la même interface pour l'accès aux hôtes et l'accès au réseau d'administration de nœud afin de faciliter la maintenance des hôtes et des nœuds. Même si une même interface peut être partagée entre l'hôte et les nœuds individuels, toutes doivent avoir des adresses IP différentes. Les adresses IP ne peuvent pas être partagées entre les nœuds ou entre l'hôte et un nœud.

Vous pouvez utiliser la même interface réseau hôte pour fournir l'interface réseau Grid de tous les nœuds StorageGRID de l'hôte ; vous pouvez utiliser une interface réseau hôte différente pour chaque nœud ; ou effectuer un travail entre les deux. Cependant, vous ne fournissez généralement pas la même interface réseau hôte que les interfaces réseau Grid et Admin pour un seul nœud, ou l'interface réseau Grid pour un nœud et l'interface réseau client pour un autre.

Vous pouvez effectuer cette tâche de plusieurs manières. Par exemple, si vos hôtes sont des machines virtuelles et que vous déployez un ou deux nœuds StorageGRID pour chaque hôte, vous pouvez créer le nombre correct d'interfaces réseau dans l'hyperviseur et utiliser un mappage 1-to-1. Si vous déployez plusieurs nœuds sur des hôtes bare Metal pour la production, vous pouvez bénéficier de la prise en charge du VLAN et du LACP de la pile réseau Linux pour la tolérance aux pannes et le partage de bande passante. Les sections suivantes présentent des approches détaillées pour ces deux exemples. Vous n'avez pas besoin

d’utiliser l’un ou l’autre de ces exemples ; vous pouvez utiliser n’importe quelle approche qui répond à vos besoins.

> N’utilisez pas de périphérique de liaison ou de pont directement comme interface réseau du conteneur. Cela pourrait empêcher le démarrage de nœud causé par un problème de noyau avec l’utilisation de MACVLAN avec des périphériques de liaison et de pont dans l’espace de noms de conteneur. Utilisez plutôt un périphérique sans lien, tel qu’un VLAN ou une paire Ethernet virtuelle (Veth). Spécifiez ce périphérique comme interface réseau dans le fichier de configuration de nœud.

Informations associées

"Création de fichiers de configuration de nœud"

Considérations et recommandations relatives au clonage d’adresses MAC

Le clonage d’adresses MAC fait en sorte que le conteneur utilise l’adresse MAC de l’hôte et que l’hôte utilise l’adresse MAC d’une adresse que vous spécifiez ou d’une adresse générée de manière aléatoire. Vous devez utiliser le clonage d’adresses MAC pour éviter l’utilisation de configurations réseau en mode promiscuous.

Activation du clonage MAC

Dans certains environnements, la sécurité peut être améliorée grâce au clonage d’adresses MAC car il vous permet d’utiliser une carte réseau virtuelle dédiée pour le réseau d’administration, le réseau Grid et le réseau client. Le fait d’utiliser le conteneur l’adresse MAC du NIC dédié sur l’hôte vous permet d’éviter d’utiliser des configurations réseau en mode promiscuous.

> Le clonage d’adresses MAC est conçu pour être utilisé avec des installations de serveurs virtuels et peut ne pas fonctionner correctement avec toutes les configurations d’appliances physiques.

> Si un nœud ne démarre pas en raison d’une interface ciblée de clonage MAC occupée, il peut être nécessaire de définir le lien sur « down » avant de démarrer le nœud. En outre, il est possible que l’environnement virtuel puisse empêcher le clonage MAC sur une interface réseau pendant que la liaison est active. Si un nœud ne parvient pas à définir l’adresse MAC et démarre en raison d’une interface en cours d’activité, il est possible que le problème soit résolu en définissant le lien sur « arrêté » avant de démarrer le nœud.

Le clonage d’adresses MAC est désactivé par défaut et doit être défini par des clés de configuration de nœud. Vous devez l’activer lors de l’installation de StorageGRID.

Il existe une clé pour chaque réseau :

- `ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC`
- `GRID_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC`
- `CLIENT_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC`

Le fait de définir la clé sur « true » fait que le conteneur utilise l’adresse MAC de la carte réseau de l’hôte. En outre, l’hôte utilisera ensuite l’adresse MAC du réseau de conteneurs spécifié. Par défaut, l’adresse de conteneur est une adresse générée de manière aléatoire, mais si vous en avez défini une à l’aide de l' `_NETWORK_MAC` clé de configuration de nœud, cette adresse est utilisée à la place. L’hôte et le conteneur

auront toujours des adresses MAC différentes.

> L'activation du clonage MAC sur un hôte virtuel sans activer également le mode promiscuous sur l'hyperviseur peut entraîner la mise en réseau des hôtes Linux à l'aide de l'interface de l'hôte à cesser de fonctionner.

Cas d'utilisation du clonage MAC

Il existe deux cas d'utilisation à prendre en compte pour le clonage MAC :

- Le clonage MAC n'est pas activé : lorsque l' `_CLONE_MAC` Clé dans le fichier de configuration du nœud n'est pas définie ou définie sur « false », l'hôte utilise le MAC de la carte réseau hôte et le conteneur aura un MAC généré par StorageGRID, à moins qu'un MAC ne soit spécifié dans le `_NETWORK_MAC` clé. Si une adresse est définie dans le `_NETWORK_MAC` clé, l'adresse du conteneur sera spécifiée dans le `_NETWORK_MAC` clé. Cette configuration de clés nécessite l'utilisation du mode promiscuous.
- Clonage MAC activé : lorsque le `_CLONE_MAC` La clé du fichier de configuration du nœud est définie sur « true », le conteneur utilise le MAC de la carte réseau de l'hôte et l'hôte utilise un MAC généré par StorageGRID, à moins qu'un MAC ne soit spécifié dans le `_NETWORK_MAC` clé. Si une adresse est définie dans le `_NETWORK_MAC` clé, l'hôte utilise l'adresse spécifiée au lieu d'une adresse générée. Dans cette configuration de clés, vous ne devez pas utiliser le mode promiscuous.

> Si vous ne souhaitez pas utiliser le clonage d'adresses MAC et que vous préférez autoriser toutes les interfaces à recevoir et transmettre des données pour les adresses MAC autres que celles attribuées par l'hyperviseur, Assurez-vous que les propriétés de sécurité au niveau du commutateur virtuel et du groupe de ports sont définies sur **Accept** pour le mode promiscuous, les modifications d'adresse MAC et les transmissions forgées. Les valeurs définies sur le commutateur virtuel peuvent être remplacées par les valeurs au niveau du groupe de ports, de sorte que les paramètres soient les mêmes aux deux endroits.

Pour activer le clonage MAC, reportez-vous à la section "instructions pour la création de fichiers de configuration de nœud".

Exemple de clonage MAC

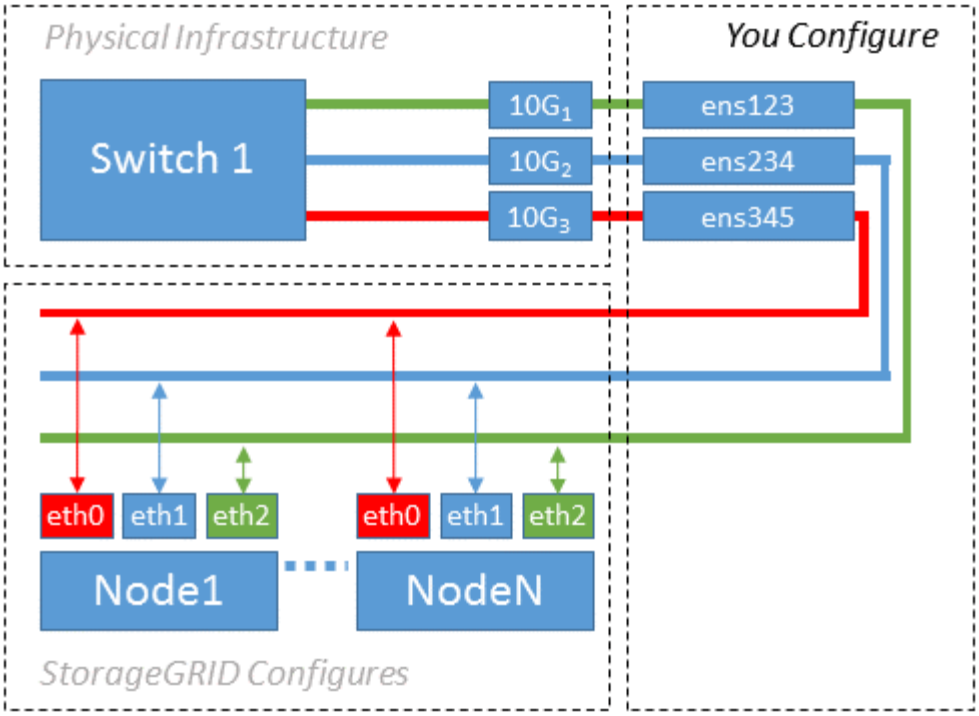
Exemple de clonage MAC activé avec un hôte dont l'adresse MAC est 11:22:33:44:55:66 pour le groupe d'interface 256 et les clés suivantes dans le fichier de configuration de nœud :

- `ADMIN_NETWORK_TARGET = ens256`
- `ADMIN_NETWORK_MAC = b2:9c:02:c2:27:10`
- `ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC = true`

Résultat: L'hôte MAC pour en256 est b2:9c:02:c2:27:10 et l'Admin réseau MAC est 11:22:33:44:55:66

Exemple 1 : mappage 1-à-1 sur des cartes réseau physiques ou virtuelles

L'exemple 1 décrit un mappage d'interface physique simple qui nécessite peu ou pas de configuration côté hôte.



Le système d'exploitation Linux crée le `ensXYZ` interfaces automatiquement lors de l'installation ou du démarrage, ou lorsque les interfaces sont ajoutées à chaud. Aucune configuration n'est nécessaire autre que de s'assurer que les interfaces sont configurées pour s'activer automatiquement après le démarrage. Vous devez déterminer lequel `ensXYZ` Correspond au réseau StorageGRID (Grid, Admin ou client) afin que vous puissiez fournir les mappages corrects plus tard dans le processus de configuration.

Notez que la figure présente plusieurs nœuds StorageGRID. Toutefois, vous utilisez généralement cette configuration pour les machines virtuelles à un seul nœud.

Si le commutateur 1 est un commutateur physique, vous devez configurer les ports connectés aux interfaces 10G1 à 10G3 pour le mode d'accès et les placer sur les VLAN appropriés.

Exemple 2 : liaison LACP avec les VLAN

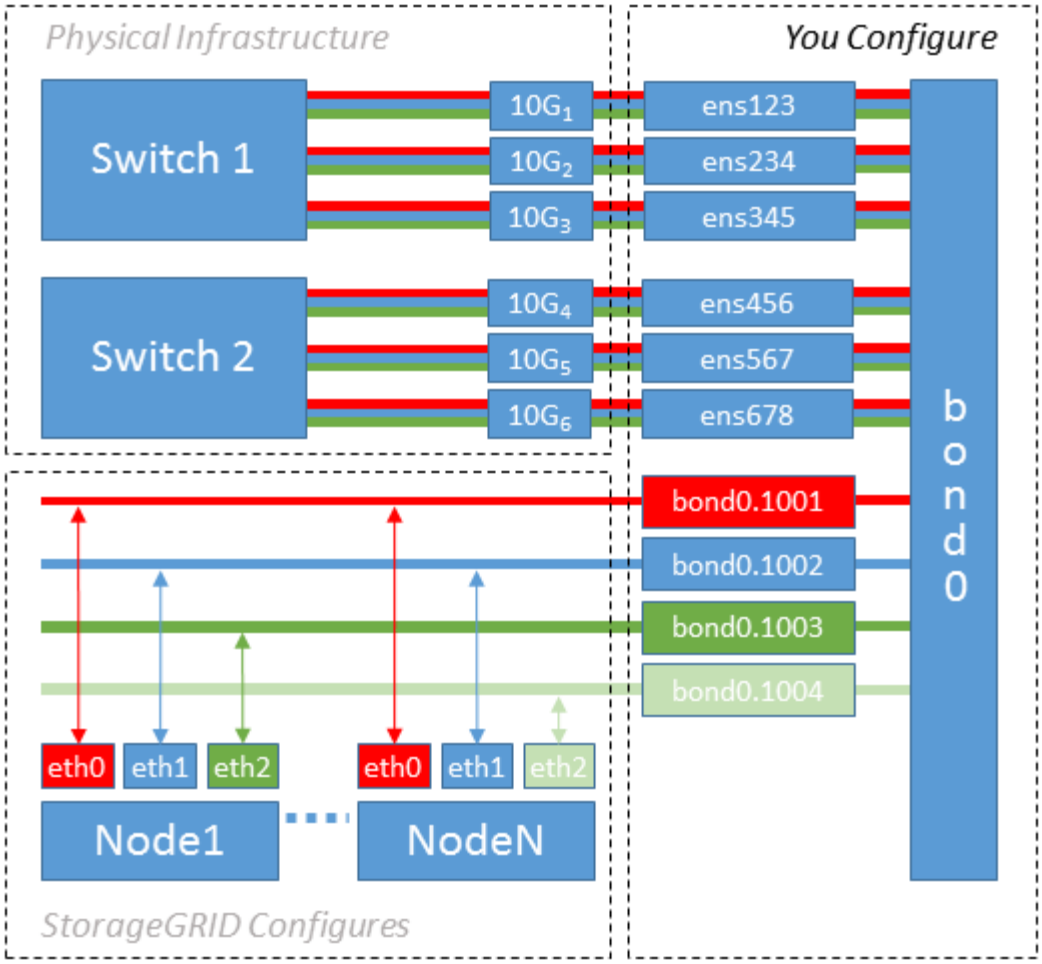
Description de la tâche

L'exemple 2 suppose que vous êtes familier avec les interfaces réseau de liaison et avec la création d'interfaces VLAN sur la distribution Linux que vous utilisez.

L'exemple 2 décrit un schéma générique, flexible et basé sur VLAN qui facilite le partage de toute la bande passante réseau disponible sur tous les nœuds d'un même hôte. Cet exemple s'applique tout particulièrement aux hôtes bare Metal.

Pour comprendre cet exemple, supposons que vous ayez trois sous-réseaux distincts pour les réseaux Grid, Admin et client dans chaque centre de données. Les sous-réseaux se trouvent sur des VLAN distincts (1001, 1002 et 1003) et sont présentés à l'hôte sur un port de jonction lié à LACP (bond0). Vous devez configurer trois interfaces VLAN sur la liaison : bond0.1001, bond0.1002 et bond0.1003.

Si vous avez besoin de VLAN et de sous-réseaux distincts pour les réseaux de nœuds sur le même hôte, vous pouvez ajouter des interfaces VLAN sur la liaison et les mapper sur l'hôte (voir bond0,1004 dans l'illustration).



Étapes

1. Agréger toutes les interfaces réseau physiques qui seront utilisées pour la connectivité réseau StorageGRID en une seule liaison LACP.

   Utilisez le même nom pour la liaison sur chaque hôte. Par exemple : `bond0`.

2. Créez des interfaces VLAN qui utilisent cette liaison comme périphérique physique associé," `using the standard VLAN interface naming convention `physdev-name.VLAN ID`.

   Notez que les étapes 1 et 2 nécessitent une configuration appropriée sur les commutateurs de périphérie qui terminent les autres extrémités des liaisons réseau. Les ports de switch de périphérie doivent également être agrégés dans un canal de port LACP, configuré en tant que jonction et autorisé à passer tous les VLAN requis.

   Des exemples de fichiers de configuration d'interface pour ce schéma de configuration réseau par hôte sont fournis.

Informations associées

"Exemple /etc/sysconfig/network-scripts"

Configurer le stockage de l'hôte

Vous devez allouer des volumes de stockage de blocs à chaque hôte.

Avant de commencer

Vous avez passé en revue les sujets suivants, qui fournissent les informations nécessaires pour accomplir cette tâche :

"Les besoins en matière de stockage et de performances"

"Exigences de migration des conteneurs de nœuds"

Description de la tâche

Lors de l'allocation de volumes de stockage en bloc (LUN) aux hôtes, utilisez les tables de la section « exigences de stockage » pour déterminer les éléments suivants :

- Nombre de volumes requis pour chaque hôte (en fonction du nombre et des types de nœuds à déployer sur cet hôte)
- Catégorie de stockage pour chaque volume (données système ou données objet)
- Taille de chaque volume

Lors du déploiement de nœuds StorageGRID sur l'hôte, vous utiliserez ces informations ainsi que le nom persistant attribué par Linux à chaque volume physique.

> Il n'est pas nécessaire de partitionner, de formater ou de monter ces volumes ; il vous suffit de vous assurer qu'ils sont visibles par les hôtes.

Évitez d'utiliser des fichiers de périphériques spéciaux « bruts » (`/dev/sdb`, par exemple) pendant que vous composez votre liste de noms de volumes. Ces fichiers peuvent être modifiés entre les redémarrages de l'hôte, ce qui peut affecter le fonctionnement correct du système. Si vous utilisez des LUN iSCSI et des chemins d'accès multiples de Device Mapper, envisagez d'utiliser des alias de chemins d'accès multiples dans le `/dev/mapper` Annuaire, en particulier si votre topologie SAN inclut des chemins réseau redondants vers le système de stockage partagé. Vous pouvez également utiliser les liens programmables créés par le système sous `/dev/disk/by-path/` pour les noms de périphériques persistants.

Par exemple :

```
ls -l
$ ls -l /dev/disk/by-path/
total 0
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:00:07.1-ata-2 -> ../../sr0
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:0:0 ->
../../sda
lrwxrwxrwx 1 root root 10 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:0:0-part1
-> ../../sda1
lrwxrwxrwx 1 root root 10 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:0:0-part2
-> ../../sda2
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:1:0 ->
../../sdb
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:2:0 ->
../../sdc
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:3:0 ->
../../sdd
```

Les résultats diffèrent pour chaque installation.

Attribuez des noms conviviaux à chacun de ces volumes de stockage en blocs afin de simplifier l'installation initiale du système StorageGRID et les procédures de maintenance à venir. Si vous utilisez le pilote multipath de device mapper pour obtenir un accès redondant aux volumes de stockage partagés, vous pouvez utiliser le `alias` dans votre `/etc/multipath.conf` fichier.

Par exemple :

```
multipaths {
     multipath {
          wwid 3600a09800059d6df00005df2573c2c30
          alias docker-storage-volume-hostA
     }
     multipath {
          wwid 3600a09800059d6df00005df3573c2c30
          alias sgws-adm1-var-local
     }
     multipath {
          wwid 3600a09800059d6df00005df4573c2c30
          alias sgws-adm1-audit-logs
     }
     multipath {
          wwid 3600a09800059d6df00005df5573c2c30
          alias sgws-adm1-tables
     }
     multipath {
          wwid 3600a09800059d6df00005df6573c2c30
          alias sgws-gw1-var-local
     }
     multipath {
          wwid 3600a09800059d6df00005df7573c2c30
          alias sgws-sn1-var-local
     }
     multipath {
          wwid 3600a09800059d6df00005df7573c2c30
          alias sgws-sn1-rangedb-0
     }
     …
```

Les alias apparaîtront alors en tant que périphériques de bloc dans le `/dev/mapper` répertoire sur l'hôte, ce qui vous permet de spécifier un nom convivial et facile à valider lorsqu'une opération de configuration ou de maintenance requiert la spécification d'un volume de stockage en bloc.

> Si vous configurez un stockage partagé pour prendre en charge la migration des nœuds StorageGRID et que vous utilisez le multipathing du mappeur de périphériques, vous pouvez créer et installer une connexion commune `/etc/multipath.conf` sur tous les hôtes en colocation. Veillez à utiliser un volume de stockage moteur de mise en conteneurs différent sur chaque hôte, L'utilisation d'alias et l'inclusion du nom d'hôte cible dans l'alias pour chaque LUN de volume de stockage de moteur de conteneur rendent cela facile à mémoriser et est recommandé.

Informations associées

"Configurer le volume de stockage du moteur du conteneur"

Configurer le volume de stockage du moteur du conteneur

Avant d'installer le moteur de mise en conteneurs (Docker ou Podman), vous devrez peut-être formater le volume de stockage et le monter.

Description de la tâche

Vous pouvez ignorer ces étapes si vous prévoyez d'utiliser du stockage local pour le volume de stockage Docker ou Podman et disposer d'un espace suffisant disponible sur la partition hôte contenant `/var/lib/docker` Pour Docker et `/var/lib/containers` Pour Podman.

Podman est pris en charge uniquement sur Red Hat Enterprise Linux (RHEL).

Étapes

1. Créer un système de fichiers sur le volume de stockage du moteur de conteneur :

```
sudo mkfs.ext4 container-engine-storage-volume-device
```

2. Monter le volume de stockage du moteur du conteneur :
   - Pour Docker :

```
sudo mkdir -p /var/lib/docker
sudo mount container-storage-volume-device /var/lib/docker
```

   - Pour Podman :

```
sudo mkdir -p /var/lib/containers
sudo mount container-storage-volume-device /var/lib/containers
```

3. Ajoutez une entrée pour conteneur-Storage-volume-device à /etc/fstab.

   Cette étape permet de s'assurer que le volume de stockage se réajuste automatiquement après le redémarrage de l'hôte.

Installez Docker

Le système StorageGRID s'exécute sur Red Hat Enterprise Linux ou CentOS comme un ensemble de conteneurs. Si vous avez choisi d'utiliser le moteur de mise en conteneurs Docker, procédez comme suit pour installer Docker. Sinon, Installez Podman.

Étapes

1. Installez Docker en suivant les instructions de votre distribution Linux.

   Si Docker n'est pas inclus dans votre distribution Linux, vous pouvez le télécharger sur le site Web de Docker.

2. Assurez-vous que Docker a été activé et démarré en exécutant les deux commandes suivantes :

```
sudo systemctl enable docker
```

```
sudo systemctl start docker
```

3. Vérifiez que vous avez installé la version attendue de Docker en saisissant les éléments suivants :

```
sudo docker version
```

Les versions client et serveur doivent être 1.11.0 ou supérieures.

Installez Podman

Le système StorageGRID fonctionne sous Red Hat Enterprise Linux comme un ensemble de conteneurs. Si vous avez choisi d'utiliser le moteur de mise en conteneurs Podman, suivez ces étapes pour installer Podman. Sinon, Installez Docker.

Podman est pris en charge uniquement sur Red Hat Enterprise Linux (RHEL).

Étapes

1. Installez Podman et Podman-Docker en suivant les instructions pour votre distribution Linux.

Vous devez également installer le package Podman-Docker lorsque vous installez Podman.

2. Vérifiez que vous avez installé la version attendue de Podman et Podman-Docker en saisissant les éléments suivants :

```
sudo docker version
```

Le package Podman-Docker vous permet d'utiliser des commandes Docker.

Les versions client et serveur doivent être 3.2.3 ou supérieures.

```
Version: 3.2.3
API Version: 3.2.3
Go Version: go1.15.7
Built: Tue Jul 27 03:29:39 2021
OS/Arch: linux/amd64
```

Installez les services d'hôte StorageGRID

Vous utilisez le package RPM StorageGRID pour installer les services hôte StorageGRID.

Description de la tâche

Ces instructions décrivent l'installation des services hôtes à partir des packages RPM. Vous pouvez également utiliser les métadonnées du référentiel Yum incluses dans l'archive d'installation pour installer les packages RPM à distance. Reportez-vous aux instructions du référentiel Yum pour votre système d'exploitation Linux.

Étapes

1. Copiez les packages RPM StorageGRID sur chacun de vos hôtes, ou mettez-les à disposition sur un stockage partagé.

   Par exemple, placez-les dans le `/tmp` répertoire, afin de pouvoir utiliser la commande exemple à l'étape suivante.

2. Connectez-vous à chaque hôte en tant que root ou en utilisant un compte avec l'autorisation sudo, et exécutez les commandes suivantes dans l'ordre spécifié :

   ```
   sudo yum --nogpgcheck localinstall /tmp/StorageGRID-Webscale-Images-version-SHA.rpm
   ```

   ```
   sudo yum --nogpgcheck localinstall /tmp/StorageGRID-Webscale-Service-version-SHA.rpm
   ```

   Vous devez d'abord installer le package Images et le package Service en second.

   Si vous avez placé les packages dans un répertoire autre que `/tmp`, modifiez la commande pour refléter le chemin que vous avez utilisé.

Déploiement de nœuds de grid virtuel (Red Hat ou CentOS)

Créez des fichiers de configuration de nœuds pour les déploiements Red Hat Enterprise Linux ou CentOS

Les fichiers de configuration des nœuds sont de petits fichiers texte qui fournissent les informations dont le service hôte StorageGRID a besoin pour démarrer un nœud et le connecter à des ressources de stockage bloc et réseau appropriées. Les fichiers de configuration des nœuds sont utilisés pour les nœuds virtuels et ne sont pas utilisés pour les nœuds de l'appliance.

Où placer les fichiers de configuration des nœuds ?

Vous devez placer le fichier de configuration de chaque noeud StorageGRID dans le `/etc/storagegrid/nodes` répertoire de l'hôte sur lequel le nœud va s'exécuter. Par exemple, si vous prévoyez d'exécuter un nœud d'administration, un nœud de passerelle et un nœud de stockage sur HostA, vous devez placer trois fichiers de configuration de nœud dans `/etc/storagegrid/nodes` Sur HostA. Vous pouvez créer les fichiers de configuration directement sur chaque hôte à l'aide d'un éditeur de texte, tel que vim ou nano, ou les créer ailleurs et les déplacer vers chaque hôte.

Comment nommer les fichiers de configuration du nœud ?

Les noms des fichiers de configuration sont importants. Le format est `node-name.conf`, où `node-name` est un nom que vous attribuez au nœud. Ce nom apparaît dans le programme d'installation StorageGRID et sert aux opérations de maintenance de nœud, telles que la migration de nœud.

Les noms de nœud doivent respecter les règles suivantes :

- Doit être unique
- Doit commencer par une lettre
- Peut contenir les caractères A à Z et a à z
- Peut contenir les chiffres 0 à 9
- Peut contenir un ou plusieurs traits d'Union (-)
- Ne doit pas comporter plus de 32 caractères, sans le `.conf` extension

Tous les fichiers dans `/etc/storagegrid/nodes` qui ne suivent pas ces conventions de dénomination ne seront pas analysées par le service hôte.

Si une topologie multisite est planifiée pour votre grille, il se peut qu'un schéma de nommage de nœud type soit :

```
site-nodetype-nodenumber.conf
```

Par exemple, vous pouvez utiliser `dc1-adm1.conf` Pour le premier nœud d'administration dans Data Center 1, et `dc2-sn3.conf` Pour le troisième nœud de stockage dans Data Center 2. Toutefois, vous pouvez utiliser n'importe quel schéma, à condition que tous les noms de nœud suivent les règles d'attribution de nom.

Que contient un fichier de configuration de nœud ?

Les fichiers de configuration contiennent des paires clé/valeur, avec une clé et une valeur par ligne. Pour chaque paire clé/valeur, vous devez respecter les règles suivantes :

- La clé et la valeur doivent être séparées par un signe égal (=) et blanc facultatif.
- Les clés ne peuvent pas contenir d'espace.
- Les valeurs peuvent contenir des espaces intégrés.
- Tout espace blanc de début ou de fin est ignoré.

Certaines clés sont requises pour chaque nœud, tandis que d'autres sont optionnelles ou uniquement nécessaires pour certains types de nœuds.

Le tableau définit les valeurs acceptables pour toutes les clés prises en charge. Dans la colonne du milieu :

R: Requis + BP: Meilleures pratiques + O: Facultatif

Clé	R, BP OU O ?	Valeur
IP_ADMIN	PA	Adresse IPv4 du réseau Grid du nœud d'administration principal de la grille à laquelle ce nœud appartient. Utilisez la même valeur que celle spécifiée pour GRID_NETWORK_IP pour le nœud de grille avec NODE_TYPE = VM_Admin_Node et ADMIN_ROLE = Primary. Si vous omettez ce paramètre, le nœud tente de détecter un nœud d'administration principal à l'aide de mDNS. "Mode de détection des nœuds du grid sur le nœud d'administration principal" **Remarque** : cette valeur est ignorée et peut être interdite sur le noeud d'administration principal.
CONFIG_RÉSEAU_ADMIN	O	DHCP, STATIQUE OU DÉSACTIVÉ
ADMIN_NETWORK_ESL	O	Liste de sous-réseaux séparés par des virgules en notation CIDR à laquelle ce nœud doit communiquer à l'aide de la passerelle Admin Network. Exemple : `172.16.0.0/21,172.17.0.0/21`

PASSERELLE_RÉSEAU_ADMIN	O (**R**)	Adresse IPv4 de la passerelle réseau d'administration locale pour ce nœud. Doit être sur le sous-réseau défini par ADMIN_NETWORK_IP et ADMIN_NETWORK_MASK. Cette valeur est ignorée pour les réseaux configurés par DHCP.
		
		Remarque : ce paramètre est requis si ADMIN_NETWORK_ESL est spécifié.
		
		Exemples :
		
		`1.1.1.1`
		
		`10.224.4.81`

IP_RÉSEAU_ADMIN	O	Adresse IPv4 de ce nœud sur le réseau d'administration. Cette clé n'est requise que lorsque ADMIN_NETWORK_CONFIG = STATIQUE ; ne la spécifiez pas pour d'autres valeurs.
		
		Exemples :
		
		`1.1.1.1`
		
		`10.224.4.81`

Clé	R, BP OU O ?	Valeur
ADMIN_NETWORK_MAC	O	Adresse MAC de l'interface réseau Admin dans le conteneur. Ce champ est facultatif. Si elle est omise, une adresse MAC est générée automatiquement. Doit être composé de 6 paires de chiffres hexadécimaux séparés par deux-points. Exemple : `b2:9c:02:c2:27:10`

ADMIN_NETWORK_MASK	O	Masque de réseau IPv4 pour ce nœud, sur le réseau d'administration. Cette clé n'est requise que lorsque ADMIN_NETWORK_CONFIG = STATIQUE ; ne la spécifiez pas pour d'autres valeurs.
		
		Exemples :
		
		`255.255.255.0`
		
		`255.255.248.0`

MTU_RÉSEAU_ADMIN	O	Unité de transmission maximale (MTU) pour ce nœud sur le réseau Admin. Ne spécifiez pas si ADMIN_NETWORK_CONFIG = DHCP. Si elle est spécifiée, la valeur doit être comprise entre 1280 et 9216. Si omis, 1500 est utilisé.
		
		Si vous souhaitez utiliser des trames jumbo, définissez la valeur MTU sur une valeur adaptée aux trames jumbo, comme 9000. Sinon, conservez la valeur par défaut.
		
		IMPORTANT : la valeur MTU du réseau doit correspondre à la valeur configurée sur le port du commutateur auquel le nœud est connecté. Dans le cas contraire, des problèmes de performances réseau ou une perte de paquets peuvent se produire.
		
		Exemples :
		
		`1500`
		
		`8192`

Clé	R, BP OU O ?	Valeur

CIBLE_RÉSEAU_ADMIN	PA	Nom de l'unité hôte que vous utiliserez pour accéder au réseau d'administration par le nœud StorageGRID. Seuls les noms d'interface réseau sont pris en charge. En général, vous utilisez un nom d'interface différent de celui spécifié pour GRID_NETWORK_TARGET ou CLIENT_NETWORK_TARGET.
		
		Remarque : n'utilisez pas de périphérique de liaison ou de pont comme cible réseau. Configurez un VLAN (ou une autre interface virtuelle) sur le périphérique de liaison, ou utilisez un pont et une paire Ethernet virtuelle (veth).
		
		Meilleure pratique:spécifiez une valeur même si ce nœud ne possède pas d'adresse IP de réseau Admin initialement. Vous pouvez ensuite ajouter une adresse IP de réseau d'administration plus tard, sans avoir à reconfigurer le nœud sur l'hôte.
		
		Exemples :
		
		`bond0.1002`
		
		`ens256`

TYPE_CIBLE_RÉSEAU_ADMIN	O	Interface (Il s'agit de la seule valeur prise en charge.)
ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC	PA	Vrai ou faux Définissez la clé sur « true » pour que le conteneur StorageGRID utilise l'adresse MAC de l'interface hôte cible sur le réseau d'administration. **Meilleure pratique:** dans les réseaux où le mode promiscuous serait nécessaire, utilisez la clé ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC. Pour plus de détails sur le clonage MAC : "Considérations et recommandations relatives au clonage d'adresses MAC (Red Hat Enterprise Linux ou CentOS)" "Considérations et recommandations relatives au clonage d'adresses MAC (Ubuntu ou Debian)"

Clé	R, BP OU O ?	Valeur
RÔLE_ADMINISTRATEUR	**R**	Primaire ou non primaire Cette clé n'est requise que lorsque NODE_TYPE = VM_Admin_Node ; ne la spécifiez pas pour d'autres types de nœuds.

JOURNAUX_AUDIT_BLOC_PÉRIPHÉRIQUE	**R**	Chemin et nom du fichier spécial de périphérique de bloc ce nœud utilisera pour le stockage persistant des journaux d'audit. Cette clé n'est requise que pour les nœuds avec TYPE_NOEUD = VM_Admin_noeud ; ne la spécifiez pas pour d'autres types de noeuds.
		
		Exemples :
		
		`/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0`
		
		`/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd`
		
		`/dev/mapper/sgws-adm1-audit-logs`

Clé	R, BP OU O ?	Valeur

BLOCK_DEVICE_RANGEDB_000
 	
BLOCK_DEVICE_RANGEDB_001
 	
BLOCK_DEVICE_RANGEDB_002
 	
BLOCK_DEVICE_RANGEDB_003
 	
BLOCK_DEVICE_RANGEDB_004
 	
BLOCK_DEVICE_RANGEDB_005
 	
BLOCK_DEVICE_RANGEDB_006
 	
BLOCK_DEVICE_RANGEDB_007
 	
BLOCK_DEVICE_RANGEDB_008
 	
BLOCK_DEVICE_RANGEDB_009
 	
BLOCK_DEVICE_RANGEDB_010
 	
BLOCK_DEVICE_RANGEDB_011
 	
BLOCK_DEVICE_RANGEDB_012
 	
BLOCK_DEVICE_RANGEDB_013
 	
BLOCK_DEVICE_RANGEDB_014
 	
BLOCK_DEVICE_RANGEDB_015
	R	Chemin et nom du fichier spécial de périphérique de bloc ce nœud utilisera pour le stockage objet permanent. Cette clé n'est requise que pour les nœuds avec TYPE_NOEUD = VM_Storage_noeud ; ne la spécifiez pas pour d'autres types de noeuds.
		
		Seul LE BLOC_DEVICE_RANGEDB_000 est requis ; le reste est facultatif. Le dispositif de bloc spécifié pour BLOCK_DEVICE_RANGEDB_000 doit être d'au moins 4 To ; les autres peuvent être plus petits.
		
		Ne laissez pas d'espace. Si vous spécifiez BLOCK_DEVICE_RANGEDB_005, vous devez également spécifier BLOCK_DEVICE_RANGEDB_004.
		
		Remarque : pour la compatibilité avec les déploiements existants, les clés à deux chiffres sont prises en charge pour les nœuds mis à niveau.
		
		Exemples :
		
		`/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0`
		
		`/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd`
		
		`/dev/mapper/sgws-sn1-rangedb-000`

Clé	R, BP OU O ?	Valeur

BLOQUER_LES_TABLES_PÉRIPHÉRIQUES	**R**	Chemin et nom du fichier spécial de l'unité de bloc ce noeud sera utilisé pour le stockage persistant des tables de base de données. Cette clé n'est requise que pour les nœuds avec TYPE_NOEUD = VM_Admin_noeud ; ne la spécifiez pas pour d'autres types de noeuds.
		
		Exemples :
		
		`/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0`
		
		`/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd`
		
		`/dev/mapper/sgws-adm1-tables`

BLOCK_DEVICE_VAR_LOCAL	**R**	Chemin et nom du fichier spécial de périphérique de bloc ce nœud utilisera pour son stockage persistant /var/local.
		
		Exemples :
		
		`/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0`
		
		`/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd`
		
		`/dev/mapper/sgws-sn1-var-local`

CONFIG_RÉSEAU_CLIENT	O	DHCP, STATIQUE OU DÉSACTIVÉ

PASSERELLE_RÉSEAU_CLIENT	O	Adresse IPv4 de la passerelle réseau client locale pour ce nœud, qui doit se trouver sur le sous-réseau défini par CLIENT_NETWORK_IP et CLIENT_NETWORK_MASK. Cette valeur est ignorée pour les réseaux configurés par DHCP.
		
		Exemples :
		
		`1.1.1.1`
		
		`10.224.4.81`

Clé	R, BP OU O ?	Valeur

IP_RÉSEAU_CLIENT	O	Adresse IPv4 de ce nœud sur le réseau client. Cette clé n'est requise que lorsque CLIENT_NETWORK_CONFIG = STATIQUE ; ne la spécifiez pas pour d'autres valeurs.
		
		Exemples :
		
		`1.1.1.1`
		
		`10.224.4.81`

CLIENT_RÉSEAU_MAC	O	Adresse MAC de l'interface réseau client dans le conteneur. Ce champ est facultatif. Si elle est omise, une adresse MAC est générée automatiquement. Doit être composé de 6 paires de chiffres hexadécimaux séparés par deux-points. Exemple : `b2:9c:02:c2:27:20`

MASQUE_RÉSEAU_CLIENT	O	Masque de réseau IPv4 pour ce nœud sur le réseau client. Cette clé n'est requise que lorsque CLIENT_NETWORK_CONFIG = STATIQUE ; ne la spécifiez pas pour d'autres valeurs.
		
		Exemples :
		
		`255.255.255.0`
		
		`255.255.248.0`

Clé	R, BP OU O ?	Valeur

MTU_CLIENT_RÉSEAU	O	Unité de transmission maximale (MTU) pour ce nœud sur le réseau client. Ne spécifiez pas si CLIENT_NETWORK_CONFIG = DHCP. Si elle est spécifiée, la valeur doit être comprise entre 1280 et 9216. Si omis, 1500 est utilisé.
		
		Si vous souhaitez utiliser des trames jumbo, définissez la valeur MTU sur une valeur adaptée aux trames jumbo, comme 9000. Sinon, conservez la valeur par défaut.
		
		IMPORTANT : la valeur MTU du réseau doit correspondre à la valeur configurée sur le port du commutateur auquel le nœud est connecté. Dans le cas contraire, des problèmes de performances réseau ou une perte de paquets peuvent se produire.
		
		Exemples :
		
		`1500`
		
		`8192`

CIBLE_RÉSEAU_CLIENT	PA	Nom du périphérique hôte que vous utiliserez pour accéder au réseau client par le nœud StorageGRID. Seuls les noms d'interface réseau sont pris en charge. En général, vous utilisez un nom d'interface différent de celui spécifié pour GRID_NETWORK_TARGET ou ADMIN_NETWORK_TARGET.
		
		Remarque : n'utilisez pas de périphérique de liaison ou de pont comme cible réseau. Configurez un VLAN (ou une autre interface virtuelle) sur le périphérique de liaison, ou utilisez un pont et une paire Ethernet virtuelle (veth).
		
		Meilleure pratique : Indiquez une valeur même si ce nœud ne possède pas d'adresse IP de réseau client au départ. Vous pouvez ensuite ajouter une adresse IP du réseau client ultérieurement, sans avoir à reconfigurer le nœud sur l'hôte.
		
		Exemples :
		
		`bond0.1003`
		
		`ens423`

TYPE_CIBLE_RÉSEAU_CLIENT	O	Interface (Cette valeur est prise en charge uniquement.)

Clé	R, BP OU O ?	Valeur
CLIENT_RÉSEAU_CIBLE_TYPE_INTERFACE_CLONE_MAC	PA	Vrai ou faux Définissez la clé sur « true » pour que le conteneur StorageGRID utilise l'adresse MAC de l'interface cible hôte sur le réseau client. **Meilleure pratique:** dans les réseaux où le mode promiscuous serait nécessaire, utilisez plutôt la clé CLIENT_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC. Pour plus de détails sur le clonage MAC : "Considérations et recommandations relatives au clonage d'adresses MAC (Red Hat Enterprise Linux ou CentOS)" "Considérations et recommandations relatives au clonage d'adresses MAC (Ubuntu ou Debian)"
CONFIG_RÉSEAU_GRID	PA	STATIQUE ou DHCP (Statique par défaut si non spécifié.)
PASSERELLE_RÉSEAU_GRILLE	**R**	Adresse IPv4 de la passerelle réseau Grid locale pour ce nœud, qui doit se trouver sur le sous-réseau défini par GRID_NETWORK_IP et GRID_NETWORK_MASK. Cette valeur est ignorée pour les réseaux configurés par DHCP. Si le réseau Grid est un sous-réseau unique sans passerelle, utilisez soit l'adresse de passerelle standard pour le sous-réseau (X. Y.1), soit la valeur DE GRID_NETWORK_IP de ce nœud. Ces valeurs simplifient les extensions potentielles du réseau Grid.

IP_RÉSEAU_GRID	**R**	Adresse IPv4 de ce nœud sur le réseau Grid. Cette clé n'est requise que lorsque GRID_NETWORK_CONFIG = STATIQUE ; ne la spécifiez pas pour d'autres valeurs.
		
		Exemples :
		
		`1.1.1.1`
		
		`10.224.4.81`

Clé	R, BP OU O ?	Valeur
GRID_RÉSEAU_MAC	O	Adresse MAC de l'interface réseau de la grille dans le conteneur. Ce champ est facultatif. Si elle est omise, une adresse MAC est générée automatiquement. Doit être composé de 6 paires de chiffres hexadécimaux séparés par deux-points. Exemple : `b2:9c:02:c2:27:30`

GRID_NETWORK_MASK	O	Masque de réseau IPv4 pour ce nœud sur le réseau Grid. Cette clé n'est requise que lorsque GRID_NETWORK_CONFIG = STATIQUE ; ne la spécifiez pas pour d'autres valeurs.
		
		Exemples :
		
		`255.255.255.0`
		
		`255.255.248.0`

GRID_NETWORK_MTU	O	Unité de transmission maximale (MTU) pour ce nœud sur le réseau Grid. Ne spécifiez pas si GRID_NETWORK_CONFIG = DHCP. Si elle est spécifiée, la valeur doit être comprise entre 1280 et 9216. Si omis, 1500 est utilisé. Si vous souhaitez utiliser des trames jumbo, définissez la valeur MTU sur une valeur adaptée aux trames jumbo, comme 9000. Sinon, conservez la valeur par défaut. **IMPORTANT** : la valeur MTU du réseau doit correspondre à la valeur configurée sur le port du commutateur auquel le nœud est connecté. Dans le cas contraire, des problèmes de performances réseau ou une perte de paquets peuvent se produire. **IMPORTANT** : pour des performances réseau optimales, tous les nœuds doivent être configurés avec des valeurs MTU similaires sur leurs interfaces réseau Grid. L'alerte **Grid Network MTU mismatch** est déclenchée en cas de différence importante dans les paramètres MTU pour le réseau Grid sur les nœuds individuels. Les valeurs MTU ne doivent pas nécessairement être identiques pour tous les types de réseau. Exemples : 1500 8192

Clé	R, BP OU O ?	Valeur

CIBLE_RÉSEAU_GRILLE	**R**	Nom de l'unité hôte que vous utiliserez pour accéder au réseau Grid par le nœud StorageGRID. Seuls les noms d'interface réseau sont pris en charge. En général, vous utilisez un nom d'interface différent de celui spécifié pour ADMIN_NETWORK_TARGET ou CLIENT_NETWORK_TARGET.
		
		Remarque : n'utilisez pas de périphérique de liaison ou de pont comme cible réseau. Configurez un VLAN (ou une autre interface virtuelle) sur le périphérique de liaison, ou utilisez un pont et une paire Ethernet virtuelle (veth).
		
		Exemples :
		
		`bond0.1001`
		
		`ens192`

TYPE_CIBLE_RÉSEAU_GRILLE	O	Interface (Il s'agit de la seule valeur prise en charge.)
GRID_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC	**BP**	Vrai ou faux Définissez la valeur de la clé sur « true » pour que le conteneur StorageGRID utilise l'adresse MAC de l'interface cible de l'hôte sur le réseau de la grille. **Meilleure pratique:** dans les réseaux où le mode promiscuous serait nécessaire, utilisez la clé GRID_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC. Pour plus de détails sur le clonage MAC : "Considérations et recommandations relatives au clonage d'adresses MAC (Red Hat Enterprise Linux ou CentOS)" "Considérations et recommandations relatives au clonage d'adresses MAC (Ubuntu ou Debian)"

Clé	R, BP OU O ?	Valeur
INTERFACE_TARGET_nnnn	O	Nom et description facultative d'une interface supplémentaire que vous souhaitez ajouter à ce nœud. Vous pouvez ajouter plusieurs interfaces supplémentaires à chaque nœud. Pour *nnnn*, spécifiez un numéro unique pour chaque entrée INTERFACE_TARGET que vous ajoutez. Pour la valeur, spécifiez le nom de l'interface physique sur l'hôte bare-Metal. Ensuite, si vous le souhaitez, ajoutez une virgule et fournissez une description de l'interface, qui s'affiche sur la page des interfaces VLAN et sur la page des groupes haute disponibilité. Par exemple : `INTERFACE_TARGET_0001=ens256, Trunk` Si vous ajoutez une interface de jonction, vous devez configurer une interface VLAN dans StorageGRID. Si vous ajoutez une interface d'accès, vous pouvez l'ajouter directement à un groupe haute disponibilité ; il n'est pas nécessaire de configurer une interface VLAN.

RAM_MAXIMALE	O	Quantité maximale de RAM que ce nœud est autorisé à consommer. Si cette clé est omise, le nœud n'a aucune restriction de mémoire. Lorsque vous définissez ce champ pour un nœud de niveau production, indiquez une valeur inférieure d'au moins 24 Go et de 16 à 32 Go à la mémoire RAM totale du système.
		
		Remarque : la valeur de la RAM affecte l'espace réservé des métadonnées réelles d'un nœud. Voir la "Description de l'espace réservé aux métadonnées".
		
		Le format de ce champ est `<number><unit>`, où `<unit>` peut être `b`, `k`, `m`, ou `g`.
		
		Exemples :
		
		`24g`
		
		`38654705664b`
		
		Remarque : si vous souhaitez utiliser cette option, vous devez activer la prise en charge du noyau pour les groupes de mémoire.

TYPE_NŒUD	**R**	Type de nœud : VM_Admin_Node VM_Storage_Node VM_Archive_Node VM_API_Gateway

Clé	R, BP OU O ?	Valeur
SCHÉMA DE PORT	O	Permet de remapper tout port utilisé par un nœud pour les communications internes de nœud de grille ou les communications externes. Le remappage des ports est nécessaire si les stratégies de mise en réseau d'entreprise limitent un ou plusieurs ports utilisés par StorageGRID, comme décrit dans "Communications internes sur les nœuds de la grille" ou "Communications externes". **IMPORTANT** : ne mappez pas les ports que vous prévoyez d'utiliser pour configurer les noeuds finaux de l'équilibreur de charge. **Remarque** : si seul PORT_REMAPPAGE est défini, le mappage que vous spécifiez est utilisé pour les communications entrantes et sortantes. Si PORT_REMAPPAGE_INBOUND est également spécifié, PORT_REMAPPAGE s'applique uniquement aux communications sortantes. Le format utilisé est : `<network type>/<protocol>/<default port used by grid node>/<new port>`, où `<network type>` est un grid, un administrateur ou un client. le protocole est tcp ou udp. Par exemple : `PORT_REMAP = client/tcp/18082/443`
PORT_REMAPPAGE_ENTRANT	O	Mappe de nouveau les communications entrantes sur le port spécifié. Si vous spécifiez PORT_REMAP_INBOUND mais que vous ne spécifiez pas de valeur pour PORT_REMAP, les communications sortantes pour le port sont inchangées. **IMPORTANT** : ne mappez pas les ports que vous prévoyez d'utiliser pour configurer les noeuds finaux de l'équilibreur de charge. Le format utilisé est : `<network type>/<protocol:>/<remapped port >/<default port used by grid node>`, où `<network type>` est un grid, un administrateur ou un client. le protocole est tcp ou udp. Par exemple : `PORT_REMAP_INBOUND = grid/tcp/3022/22`

Mode de détection des nœuds du grid sur le nœud d'administration principal

Les nœuds de grid communiquent avec le nœud d'administration principal pour la configuration et la gestion. Chaque nœud de la grille doit connaître l'adresse IP du nœud

d'administration principal sur le réseau Grid.

Pour vous assurer qu'un nœud de grille peut accéder au nœud d'administration principal, vous pouvez effectuer l'une des opérations suivantes lors du déploiement du nœud :

- Vous pouvez utiliser le paramètre ADMIN_IP pour saisir manuellement l'adresse IP du nœud d'administration principal.
- Vous pouvez omettre le paramètre ADMIN_IP pour que le nœud de la grille détecte automatiquement la valeur. La détection automatique est particulièrement utile lorsque le réseau Grid utilise DHCP pour attribuer l'adresse IP au nœud d'administration principal.

La découverte automatique du nœud d'administration principal s'effectue à l'aide d'un système de noms de domaine multicast (mDNS). Lors du premier démarrage du nœud d'administration principal, il publie son adresse IP à l'aide de mDNS. Les autres nœuds du même sous-réseau peuvent alors interroger l'adresse IP et l'acquérir automatiquement. Cependant, comme le trafic IP multicast n'est généralement pas routable entre les sous-réseaux, les nœuds des autres sous-réseaux ne peuvent pas acquérir directement l'adresse IP du nœud Admin principal.

Si vous utilisez la détection automatique :

- Vous devez inclure le paramètre ADMIN_IP pour au moins un nœud de grille sur les sous-réseaux auxquels le nœud d'administration principal n'est pas directement connecté. Ce nœud de grille publie ensuite l'adresse IP du nœud d'administration principal pour les autres nœuds du sous-réseau à détecter avec mDNS.
- Assurez-vous que votre infrastructure réseau prend en charge le trafic IP multicast dans un sous-réseau.

Exemple de fichiers de configuration de nœud

Vous pouvez utiliser les exemples de fichiers de configuration de nœud pour vous aider à configurer les fichiers de configuration de nœud pour votre système StorageGRID. Les exemples montrent les fichiers de configuration des nœuds pour tous les types de nœuds grid.

Pour la plupart des nœuds, vous pouvez ajouter des informations d'adressage réseau de l'administrateur et du client (IP, masque, passerelle, etc.) lorsque vous configurez la grille à l'aide de Grid Manager ou de l'API d'installation. L'exception est le nœud d'administration principal. Si vous souhaitez accéder à l'adresse IP réseau d'administration du nœud d'administration principal pour terminer la configuration de la grille (le réseau de grille n'étant pas routé, par exemple), vous devez configurer la connexion réseau d'administration du nœud d'administration principal dans son fichier de configuration de nœud. Ceci est illustré dans l'exemple.

Dans les exemples, la cible réseau client a été configurée comme une pratique recommandée, même si le réseau client est désactivé par défaut.

Exemple pour le nœud d'administration principal

Exemple de nom de fichier: `/etc/storagegrid/nodes/dc1-adm1.conf`

Exemple de contenu de fichier:

```
NODE_TYPE = VM_Admin_Node
ADMIN_ROLE = Primary
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-adm1-var-local
BLOCK_DEVICE_AUDIT_LOGS = /dev/mapper/dc1-adm1-audit-logs
BLOCK_DEVICE_TABLES = /dev/mapper/dc1-adm1-tables
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.2
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1

ADMIN_NETWORK_CONFIG = STATIC
ADMIN_NETWORK_IP = 192.168.100.2
ADMIN_NETWORK_MASK = 255.255.248.0
ADMIN_NETWORK_GATEWAY = 192.168.100.1
ADMIN_NETWORK_ESL = 192.168.100.0/21,172.16.0.0/21,172.17.0.0/21
```

Exemple de nœud de stockage

Exemple de nom de fichier: `/etc/storagegrid/nodes/dc1-sn1.conf`

Exemple de contenu de fichier:

```
NODE_TYPE = VM_Storage_Node
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-sn1-var-local
BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/dc1-sn1-rangedb-0
BLOCK_DEVICE_RANGEDB_01 = /dev/mapper/dc1-sn1-rangedb-1
BLOCK_DEVICE_RANGEDB_02 = /dev/mapper/dc1-sn1-rangedb-2
BLOCK_DEVICE_RANGEDB_03 = /dev/mapper/dc1-sn1-rangedb-3
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.3
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

Exemple de nœud d'archivage

Exemple de nom de fichier: `/etc/storagegrid/nodes/dc1-arc1.conf`

Exemple de contenu de fichier:

```
NODE_TYPE = VM_Archive_Node
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-arc1-var-local
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.4
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

Exemple pour le nœud de passerelle

Exemple de nom de fichier: `/etc/storagegrid/nodes/dc1-gw1.conf`

Exemple de contenu de fichier:

```
NODE_TYPE = VM_API_Gateway
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-gw1-var-local
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003
GRID_NETWORK_IP = 10.1.0.5
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

Exemple pour un nœud d'administration non primaire

Exemple de nom de fichier: `/etc/storagegrid/nodes/dc1-adm2.conf`

Exemple de contenu de fichier:

```
NODE_TYPE = VM_Admin_Node
ADMIN_ROLE = Non-Primary
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-adm2-var-local
BLOCK_DEVICE_AUDIT_LOGS = /dev/mapper/dc1-adm2-audit-logs
BLOCK_DEVICE_TABLES = /dev/mapper/dc1-adm2-tables
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.6
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

Validation de la configuration StorageGRID

Après avoir créé des fichiers de configuration dans `/etc/storagegrid/nodes` Pour chacun de vos nœuds StorageGRID, vous devez valider le contenu de ces fichiers.

Pour valider le contenu des fichiers de configuration, exécutez la commande suivante sur chaque hôte :

```
sudo storagegrid node validate all
```

Si les fichiers sont corrects, le résultat indique **TRANSMIS** pour chaque fichier de configuration, comme indiqué dans l'exemple.

```
Checking for misnamed node configuration files… PASSED
Checking configuration file for node dc1-adm1… PASSED
Checking configuration file for node dc1-gw1… PASSED
Checking configuration file for node dc1-sn1… PASSED
Checking configuration file for node dc1-sn2… PASSED
Checking configuration file for node dc1-sn3… PASSED
Checking for duplication of unique values between nodes… PASSED
```

Pour une installation automatisée, vous pouvez supprimer cette sortie à l'aide de la `-q` ou `--quiet` dans le `storagegrid` commande (par exemple, `storagegrid --quiet…`). Si vous supprimez la sortie, la commande aura une valeur de sortie non nulle si des avertissements ou des erreurs de configuration ont été détectés.

Si les fichiers de configuration sont incorrects, les problèmes sont affichés comme **AVERTISSEMENT** et **ERREUR**, comme indiqué dans l'exemple. Si des erreurs de configuration sont détectées, vous devez les corriger avant de poursuivre l'installation.

```
Checking for misnamed node configuration files…
  WARNING: ignoring /etc/storagegrid/nodes/dc1-adm1
  WARNING: ignoring /etc/storagegrid/nodes/dc1-sn2.conf.keep
  WARNING: ignoring /etc/storagegrid/nodes/my-file.txt
Checking configuration file for node dc1-adm1…
  ERROR: NODE_TYPE = VM_Foo_Node
         VM_Foo_Node is not a valid node type.  See *.conf.sample
  ERROR: ADMIN_ROLE = Foo
         Foo is not a valid admin role.  See *.conf.sample
  ERROR: BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-gw1-var-local
         /dev/mapper/sgws-gw1-var-local is not a valid block device
Checking configuration file for node dc1-gw1…
  ERROR: GRID_NETWORK_TARGET = bond0.1001
         bond0.1001 is not a valid interface.  See `ip link show`
  ERROR: GRID_NETWORK_IP = 10.1.3
         10.1.3 is not a valid IPv4 address
  ERROR: GRID_NETWORK_MASK = 255.248.255.0
         255.248.255.0 is not a valid IPv4 subnet mask
Checking configuration file for node dc1-sn1…
  ERROR: GRID_NETWORK_GATEWAY = 10.2.0.1
         10.2.0.1 is not on the local subnet
  ERROR: ADMIN_NETWORK_ESL = 192.168.100.0/21,172.16.0foo
         Could not parse subnet list
Checking configuration file for node dc1-sn2… PASSED
Checking configuration file for node dc1-sn3… PASSED
Checking for duplication of unique values between nodes…
  ERROR: GRID_NETWORK_IP = 10.1.0.4
         dc1-sn2 and dc1-sn3 have the same GRID_NETWORK_IP
  ERROR: BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-sn2-var-local
         dc1-sn2 and dc1-sn3 have the same BLOCK_DEVICE_VAR_LOCAL
  ERROR: BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/sgws-sn2-rangedb-0
         dc1-sn2 and dc1-sn3 have the same BLOCK_DEVICE_RANGEDB_00
```

Démarrez le service d'hôte StorageGRID

Pour démarrer vos nœuds StorageGRID et s'assurer qu'ils redémarrent après un redémarrage de l'hôte, vous devez activer et démarrer le service hôte StorageGRID.

Étapes

1. Exécutez les commandes suivantes sur chaque hôte :

```
sudo systemctl enable storagegrid
sudo systemctl start storagegrid
```

2. Exécutez la commande suivante pour vérifier que le déploiement se déroule :

```
sudo storagegrid node status node-name
```

3. Si un nœud renvoie le statut « Not running » ou « Ssured, », exécutez la commande suivante :

```
sudo storagegrid node start node-name
```

4. Si vous avez déjà activé et démarré le service hôte StorageGRID (ou si vous n'êtes pas sûr que le service a été activé et démarré), exécutez également la commande suivante :

```
sudo systemctl reload-or-restart storagegrid
```

Configurer le grid et l'installation complète (Red Hat ou CentOS)

Accédez au Grid Manager

Le gestionnaire de grille permet de définir toutes les informations nécessaires à la configuration du système StorageGRID.

Avant de commencer

Le nœud d'administration principal doit être déployé et avoir terminé la séquence de démarrage initiale.

Étapes

1. Ouvrez votre navigateur Web et accédez à l'une des adresses suivantes :

   `https://primary_admin_node_ip`

   `client_network_ip`

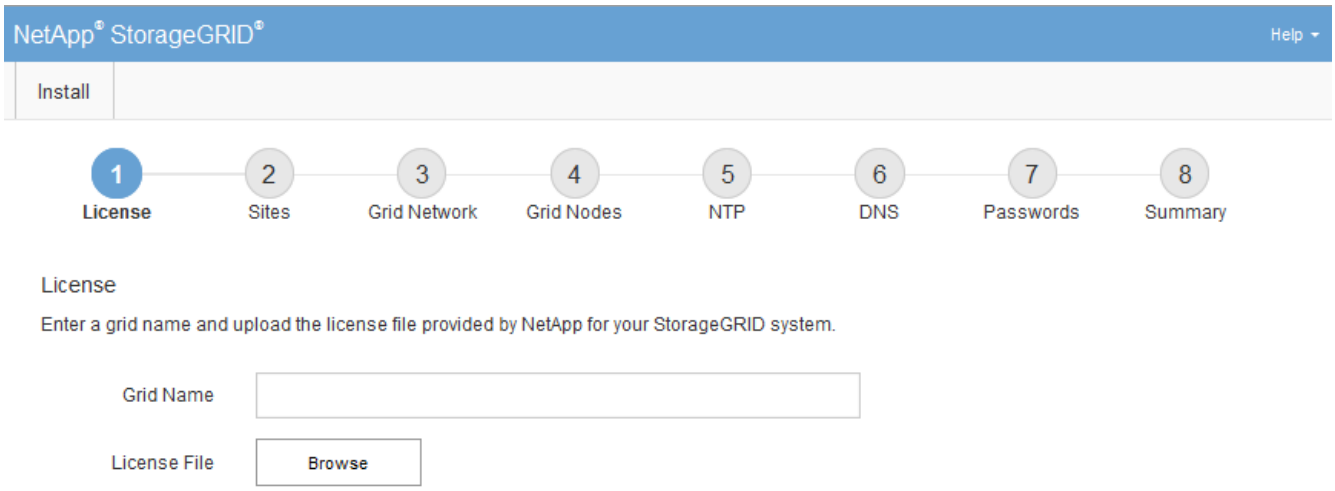
   Vous pouvez également accéder à Grid Manager sur le port 8443 :

   `https://primary_admin_node_ip:8443`

   > Vous pouvez utiliser l'adresse IP du noeud d'administration principal sur le réseau Grid ou sur le réseau Admin, en fonction de votre configuration réseau.

2. Sélectionnez **installer un système StorageGRID**.

   La page utilisée pour configurer un système StorageGRID s'affiche.



Spécifier les informations de licence StorageGRID

Vous devez indiquer le nom de votre système StorageGRID et télécharger le fichier de licence fourni par NetApp.

Étapes

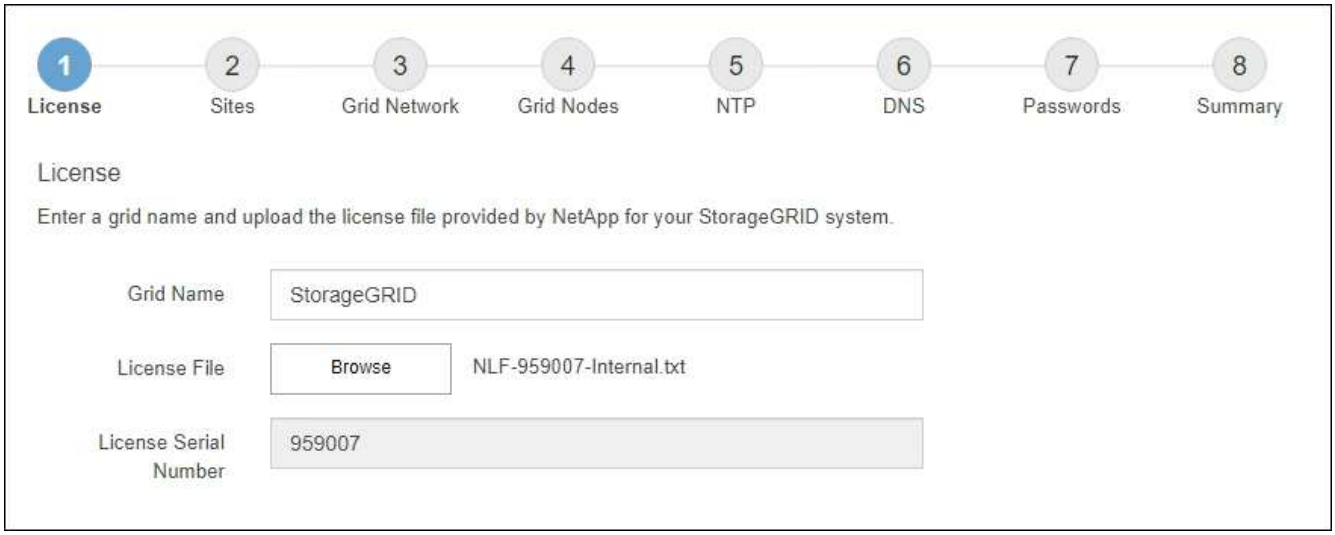
1. Sur la page Licence, entrez un nom significatif pour votre système StorageGRID dans le champ **Nom de la grille**.

   Après l'installation, le nom s'affiche en haut du menu nœuds.

2. Sélectionnez **Browse**, localisez le fichier de licence NetApp (`NLF-unique-id.txt`) Et sélectionnez **Ouvrir**.

   Le fichier de licence est validé et le numéro de série s'affiche.

   > L'archive d'installation de StorageGRID inclut une licence gratuite qui ne fournit aucun droit d'assistance pour le produit. Vous pouvez effectuer une mise à jour vers une licence offrant une assistance après l'installation.



3. Sélectionnez **Suivant**.

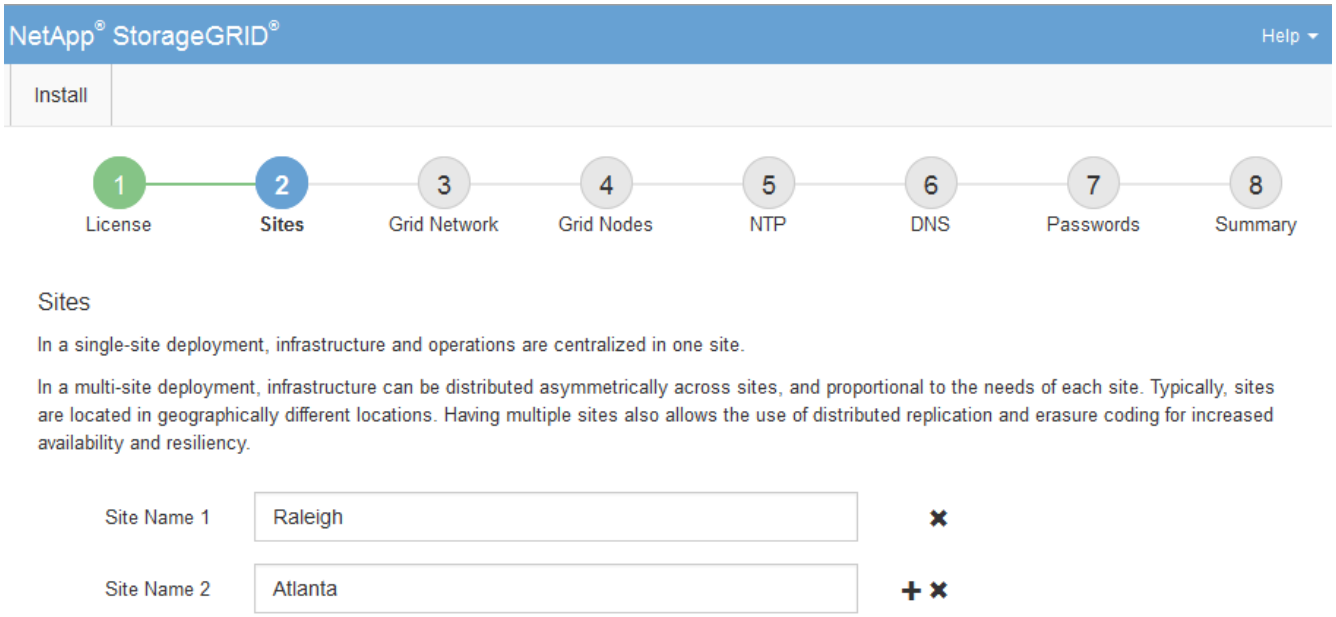
Ajouter des sites

Vous devez créer au moins un site lorsque vous installez StorageGRID. Vous pouvez créer des sites supplémentaires pour augmenter la fiabilité et la capacité de stockage de votre système StorageGRID.

Étapes

1. Sur la page sites, saisissez **Nom du site**.
2. Pour ajouter d'autres sites, cliquez sur le signe plus en regard de la dernière entrée du site et entrez le nom dans la zone de texte Nouveau **Nom du site**.

   Ajoutez autant de sites supplémentaires que nécessaire pour votre topologie de grille. Vous pouvez ajouter jusqu'à 16 sites.



3. Cliquez sur **Suivant**.

Spécifiez les sous-réseaux du réseau de la grille

Vous devez spécifier les sous-réseaux utilisés sur le réseau grille.

Description de la tâche

Les entrées de sous-réseau incluent les sous-réseaux du réseau de la grille pour chaque site de votre système StorageGRID, ainsi que tous les sous-réseaux devant être accessibles via le réseau de la grille.

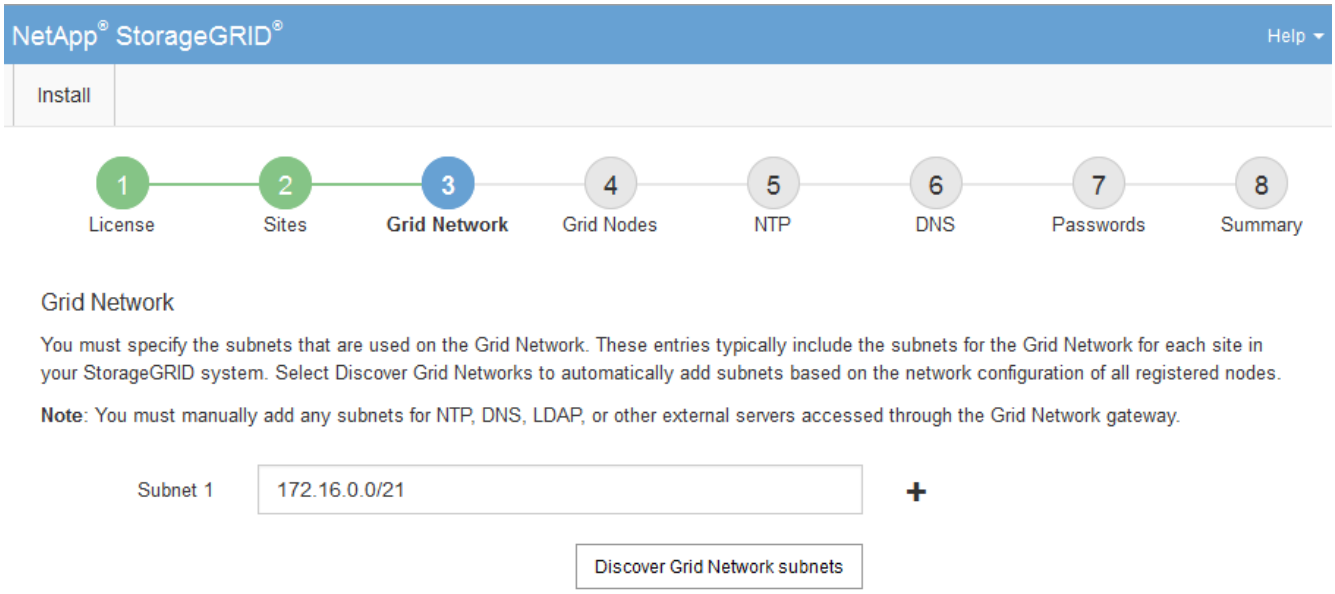
Si vous avez plusieurs sous-réseaux de grille, la passerelle de réseau de grille est requise. Tous les sous-réseaux de la grille spécifiés doivent être accessibles via cette passerelle.

Étapes

1. Spécifiez l'adresse réseau CIDR pour au moins un réseau Grid dans la zone de texte **sous-réseau 1**.
2. Cliquez sur le signe plus à côté de la dernière entrée pour ajouter une entrée réseau supplémentaire.

   Si vous avez déjà déployé au moins un nœud, cliquez sur **détecter les sous-réseaux de réseaux de grille** pour remplir automatiquement la liste de sous-réseaux de réseau de grille avec les sous-réseaux

signalés par les nœuds de grille enregistrés avec le gestionnaire de grille.



3. Cliquez sur **Suivant**.

Approuver les nœuds de la grille en attente

Vous devez approuver chaque nœud de la grille pour pouvoir rejoindre le système StorageGRID.

Avant de commencer

Vous avez déployé l'ensemble des nœuds grid virtuels et d'appliance StorageGRID.

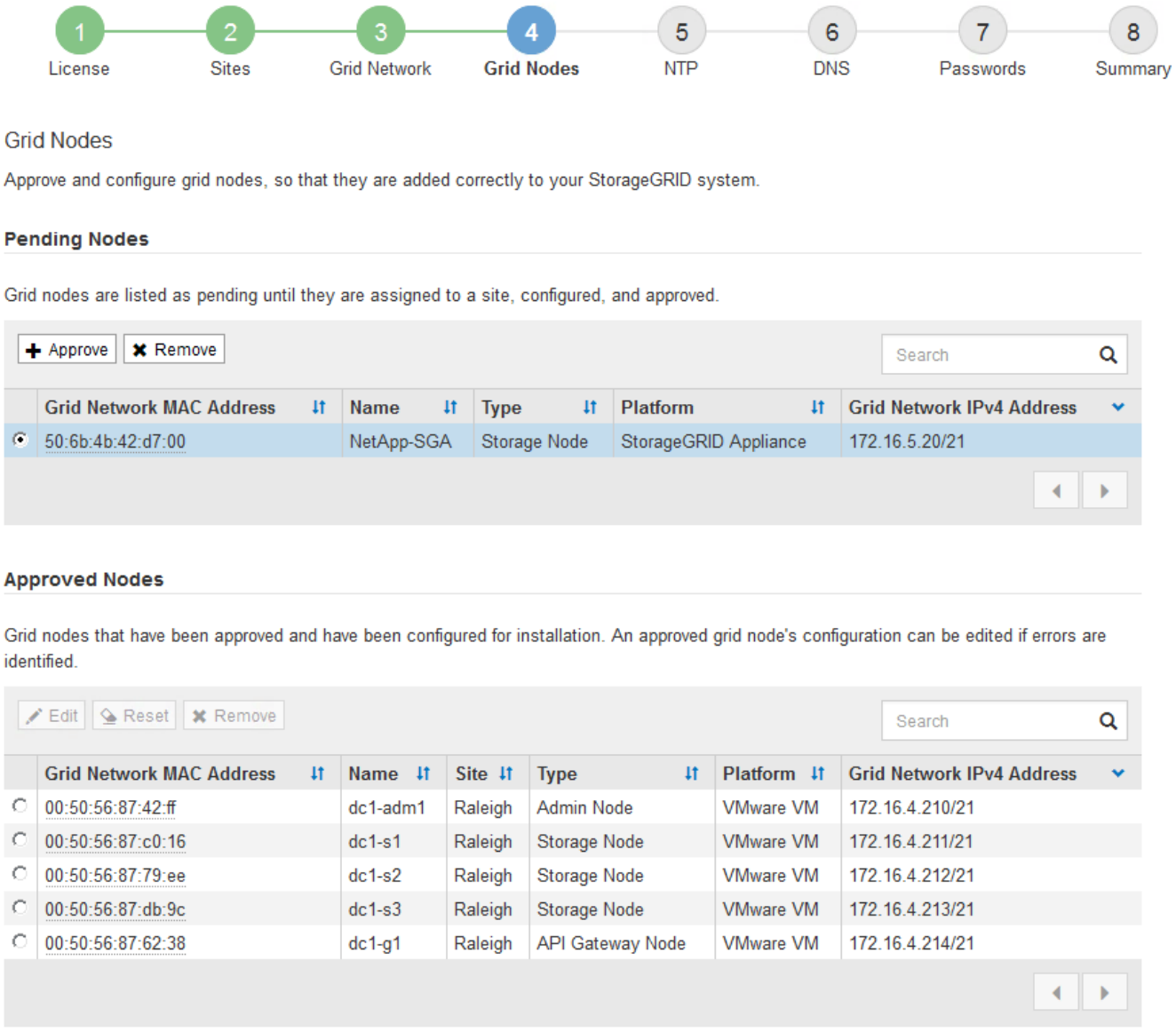
> Il est plus efficace d'effectuer une seule installation de tous les nœuds, au lieu d'installer certains nœuds maintenant et certains nœuds ultérieurement.

Étapes

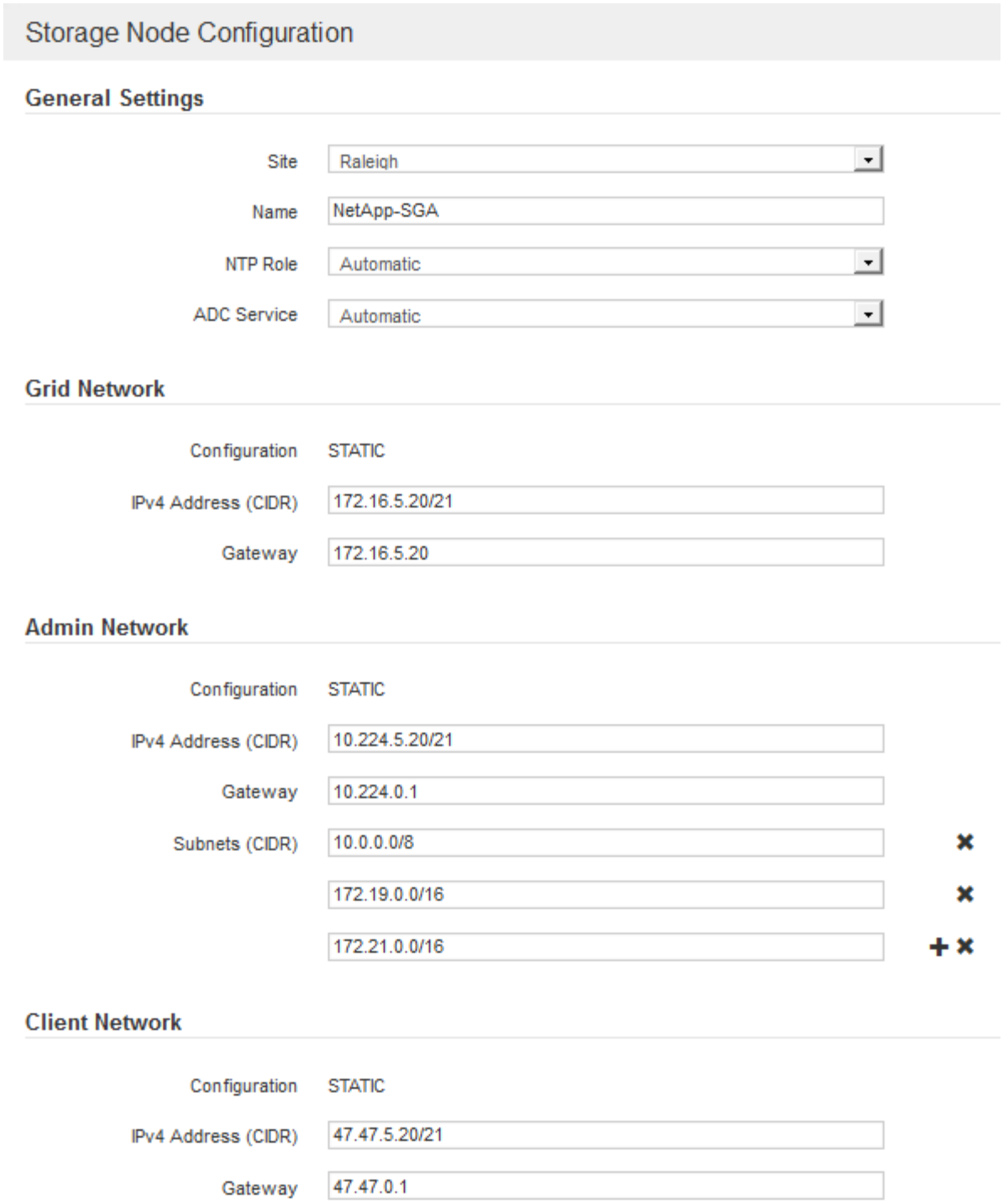
1. Consultez la liste nœuds en attente et vérifiez qu'elle affiche tous les nœuds de la grille que vous avez déployés.

   > Si un nœud de grid n'est pas inclus, vérifiez qu'il a été déployé correctement.

2. Sélectionnez le bouton radio à côté d'un noeud en attente que vous souhaitez approuver.



3. Cliquez sur **approuver**.
4. Dans Paramètres généraux, modifiez les paramètres des propriétés suivantes, si nécessaire :



- **Site** : le nom système du site pour ce noeud de grille.
- **Nom** : le nom du système pour le noeud. Le nom par défaut est le nom que vous avez spécifié lors de la configuration du nœud.

  Les noms de système sont requis pour les opérations StorageGRID internes et ne peuvent pas être modifiés une fois l'installation terminée. Cependant, au cours de cette étape du processus d'installation, vous pouvez modifier les noms de système selon vos besoins.

- **NTP role** : rôle NTP (Network Time Protocol) du noeud de la grille. Les options sont **automatique**, **primaire** et **client**. Si vous sélectionnez **automatique**, le rôle principal est attribué aux nœuds d'administration, aux nœuds de stockage avec services ADC, aux nœuds de passerelle et à tous les

nœuds de grille ayant des adresses IP non statiques. Le rôle client est attribué à tous les autres nœuds de la grille.

> Assurez-vous qu'au moins deux nœuds de chaque site peuvent accéder à au moins quatre sources NTP externes. Si un seul nœud d'un site peut atteindre les sources NTP, des problèmes de synchronisation surviennent en cas de panne de ce nœud. En outre, la désignation de deux nœuds par site en tant que sources NTP principales assure une synchronisation précise si un site est isolé du reste de la grille.

- **Service ADC** (nœuds de stockage uniquement) : sélectionnez **automatique** pour permettre au système de déterminer si le nœud requiert le service contrôleur de domaine administratif (ADC). Le service ADC conserve le suivi de l'emplacement et de la disponibilité des services de réseau. Au moins trois nœuds de stockage de chaque site doivent inclure le service ADC. Vous ne pouvez pas ajouter le service ADC à un nœud après son déploiement.

5. Dans le réseau de grille, modifiez les paramètres des propriétés suivantes si nécessaire :

   - **Adresse IPv4 (CIDR)** : adresse réseau CIDR pour l'interface Grid Network (eth0 dans le conteneur). Par exemple : 192.168.1.234/21
   - **Gateway** : la passerelle réseau Grid. Par exemple : 192.168.0.1

     La passerelle est requise en cas de sous-réseaux de grille multiples.

   > Si vous avez sélectionné DHCP pour la configuration du réseau Grid et que vous modifiez la valeur ici, la nouvelle valeur sera configurée en tant qu'adresse statique sur le nœud. Vous devez vous assurer que l'adresse IP résultante ne se trouve pas dans un pool d'adresses DHCP.

6. Si vous souhaitez configurer le réseau d'administration pour le nœud de la grille, ajoutez ou mettez à jour les paramètres de la section réseau d'administration si nécessaire.

   Entrez les sous-réseaux de destination des routes en dehors de cette interface dans la zone de texte **sous-réseaux (CIDR)**. En cas de sous-réseaux d'administration multiples, la passerelle d'administration est requise.

   > Si vous avez sélectionné DHCP pour la configuration du réseau d'administration et que vous modifiez la valeur ici, la nouvelle valeur sera configurée en tant qu'adresse statique sur le nœud. Vous devez vous assurer que l'adresse IP résultante ne se trouve pas dans un pool d'adresses DHCP.

   Appareils : pour une appliance StorageGRID, si le réseau d'administration n'a pas été configuré lors de l'installation initiale à l'aide du programme d'installation de l'appliance StorageGRID, il ne peut pas être configuré dans cette boîte de dialogue Gestionnaire de grille. Au lieu de cela, vous devez procéder comme suit :

   a. Redémarrez l'appliance : dans le programme d'installation de l'appliance, sélectionnez **Avancé** > **redémarrer**.

      Le redémarrage peut prendre plusieurs minutes.

   b. Sélectionnez **configurer réseau** > **Configuration lien** et activez les réseaux appropriés.
   c. Sélectionnez **configurer réseau** > **Configuration IP** et configurez les réseaux activés.

d. Revenez à la page d'accueil et cliquez sur **Démarrer l'installation**.

e. Dans le Gestionnaire de grille : si le nœud est répertorié dans le tableau nœuds approuvés, supprimez-le.

f. Supprimez le nœud du tableau nœuds en attente.

g. Attendez que le nœud réapparaisse dans la liste nœuds en attente.

h. Confirmez que vous pouvez configurer les réseaux appropriés. Elles doivent déjà être renseignées avec les informations que vous avez fournies sur la page Configuration IP du programme d'installation de l'appliance.

   Pour plus d'informations, reportez-vous aux instructions d'installation de votre modèle d'appareil.

7. Si vous souhaitez configurer le réseau client pour le nœud de grille, ajoutez ou mettez à jour les paramètres dans la section réseau client si nécessaire. Si le réseau client est configuré, la passerelle est requise et devient la passerelle par défaut du noeud après l'installation.

   > Si vous avez sélectionné DHCP pour la configuration du réseau client et que vous modifiez la valeur ici, la nouvelle valeur sera configurée en tant qu'adresse statique sur le nœud. Vous devez vous assurer que l'adresse IP résultante ne se trouve pas dans un pool d'adresses DHCP.

   Appareils : pour une appliance StorageGRID, si le réseau client n'a pas été configuré lors de l'installation initiale à l'aide du programme d'installation de l'appliance StorageGRID, il ne peut pas être configuré dans cette boîte de dialogue Gestionnaire de grille. Au lieu de cela, vous devez procéder comme suit :

   a. Redémarrez l'appliance : dans le programme d'installation de l'appliance, sélectionnez **Avancé** > **redémarrer**.

      Le redémarrage peut prendre plusieurs minutes.

   b. Sélectionnez **configurer réseau** > **Configuration lien** et activez les réseaux appropriés.

   c. Sélectionnez **configurer réseau** > **Configuration IP** et configurez les réseaux activés.

   d. Revenez à la page d'accueil et cliquez sur **Démarrer l'installation**.

   e. Dans le Gestionnaire de grille : si le nœud est répertorié dans le tableau nœuds approuvés, supprimez-le.

   f. Supprimez le nœud du tableau nœuds en attente.

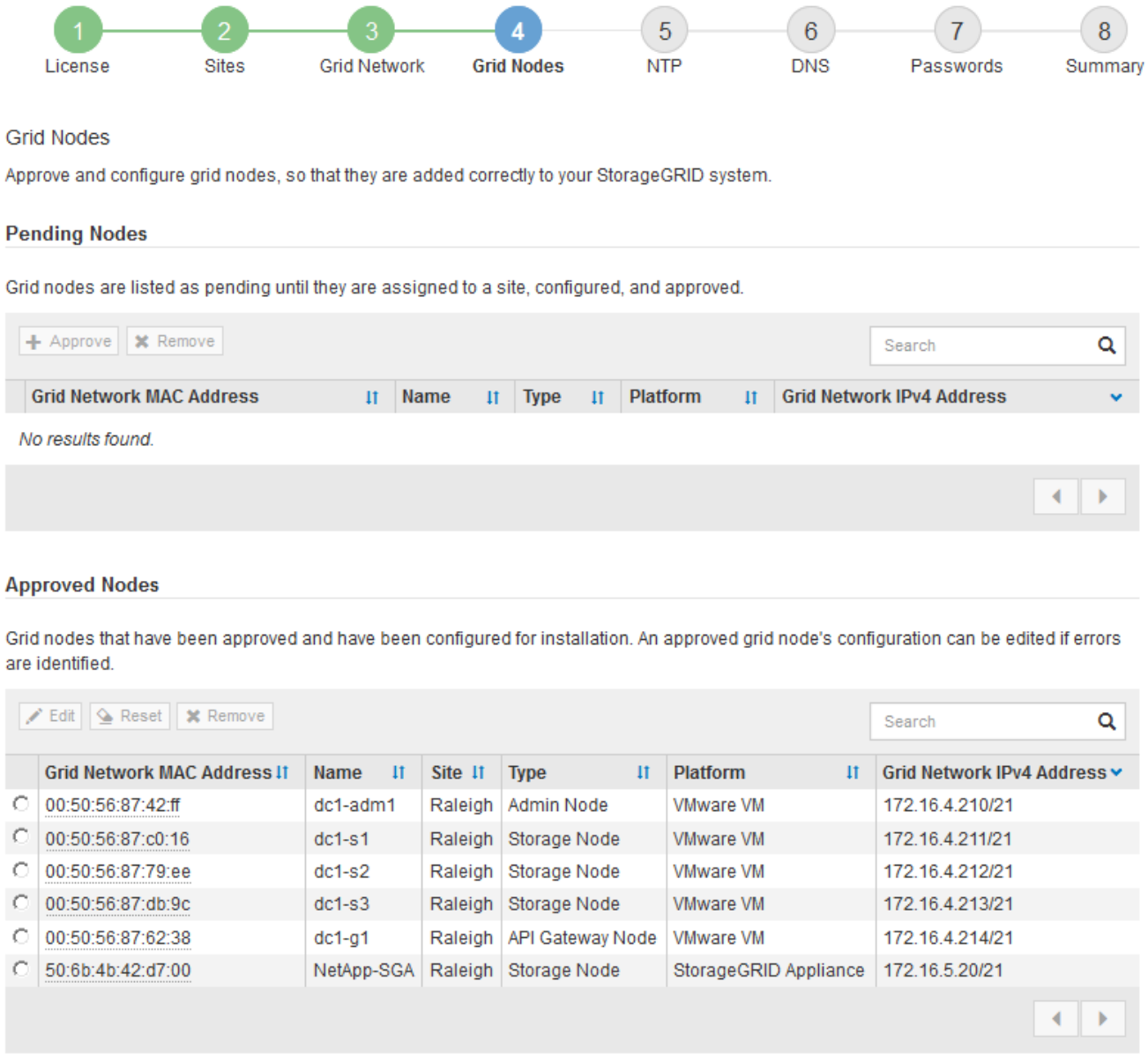
   g. Attendez que le nœud réapparaisse dans la liste nœuds en attente.

   h. Confirmez que vous pouvez configurer les réseaux appropriés. Elles doivent déjà être renseignées avec les informations que vous avez fournies sur la page Configuration IP du programme d'installation de l'appliance.

      Pour plus d'informations, reportez-vous aux instructions d'installation de votre appareil.

8. Cliquez sur **Enregistrer**.

   L'entrée de nœud de la grille passe à la liste nœuds approuvés.



9. Répétez ces étapes pour chaque nœud de grille en attente à approuver.

   Vous devez approuver tous les nœuds que vous souhaitez dans la grille. Cependant, vous pouvez revenir à cette page à tout moment avant de cliquer sur **installer** sur la page Résumé. Vous pouvez modifier les propriétés d'un nœud de grille approuvé en sélectionnant son bouton radio et en cliquant sur **Modifier**.

10. Lorsque vous avez terminé d'approuver les nœuds de la grille, cliquez sur **Suivant**.

Spécifiez les informations sur le serveur Network Time Protocol

Vous devez spécifier les informations de configuration du protocole NTP (Network Time Protocol) pour le système StorageGRID, de sorte que les opérations effectuées sur des serveurs distincts puissent rester synchronisées.

Description de la tâche

Vous devez indiquer des adresses IPv4 pour les serveurs NTP.

Vous devez indiquer des serveurs NTP externes. Les serveurs NTP spécifiés doivent utiliser le protocole NTP.

Vous devez spécifier quatre références de serveur NTP de Stratum 3 ou supérieur pour éviter les problèmes de dérive du temps.

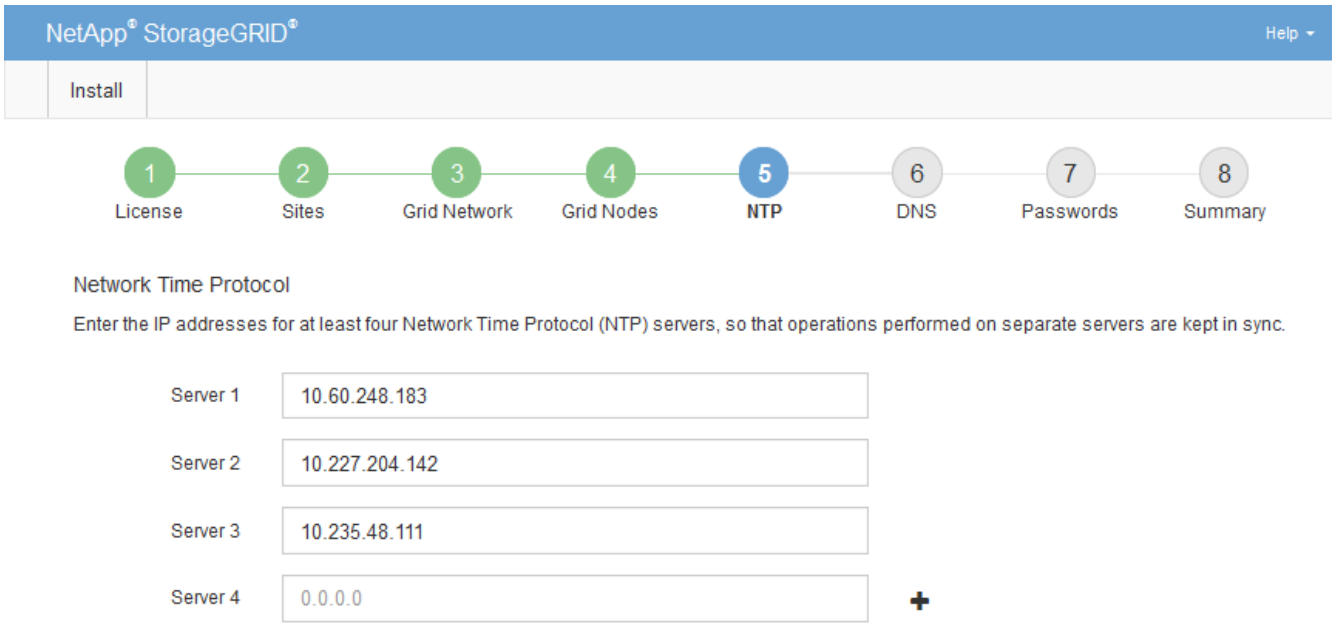
> Lorsque vous spécifiez la source NTP externe pour une installation StorageGRID de niveau production, n'utilisez pas le service heure Windows (W32Time) sur une version de Windows antérieure à Windows Server 2016. Le service de temps des versions antérieures de Windows n'est pas suffisamment précis et n'est pas pris en charge par Microsoft pour une utilisation dans des environnements à haute précision, tels que StorageGRID.
>
> "Limite de prise en charge pour configurer le service de temps Windows pour des environnements de haute précision"

Les serveurs NTP externes sont utilisés par les nœuds auxquels vous avez précédemment attribué des rôles NTP primaires.

> Assurez-vous qu'au moins deux nœuds de chaque site peuvent accéder à au moins quatre sources NTP externes. Si un seul nœud d'un site peut atteindre les sources NTP, des problèmes de synchronisation surviennent en cas de panne de ce nœud. En outre, la désignation de deux nœuds par site en tant que sources NTP principales assure une synchronisation précise si un site est isolé du reste de la grille.

Étapes

1. Spécifiez les adresses IPv4 pour au moins quatre serveurs NTP dans les zones de texte **Server 1** à **Server 4**.
2. Si nécessaire, sélectionnez le signe plus en regard de la dernière entrée pour ajouter des entrées de serveur supplémentaires.



3. Sélectionnez **Suivant**.

Spécifiez les informations du serveur DNS

Vous devez spécifier des informations DNS pour votre système StorageGRID afin de pouvoir accéder aux serveurs externes en utilisant des noms d'hôte au lieu d'adresses IP.

Description de la tâche

Spécification "Informations sur le serveur DNS" Vous permet d'utiliser des noms d'hôte de nom de domaine complet (FQDN) plutôt que des adresses IP pour les notifications par e-mail et AutoSupport.

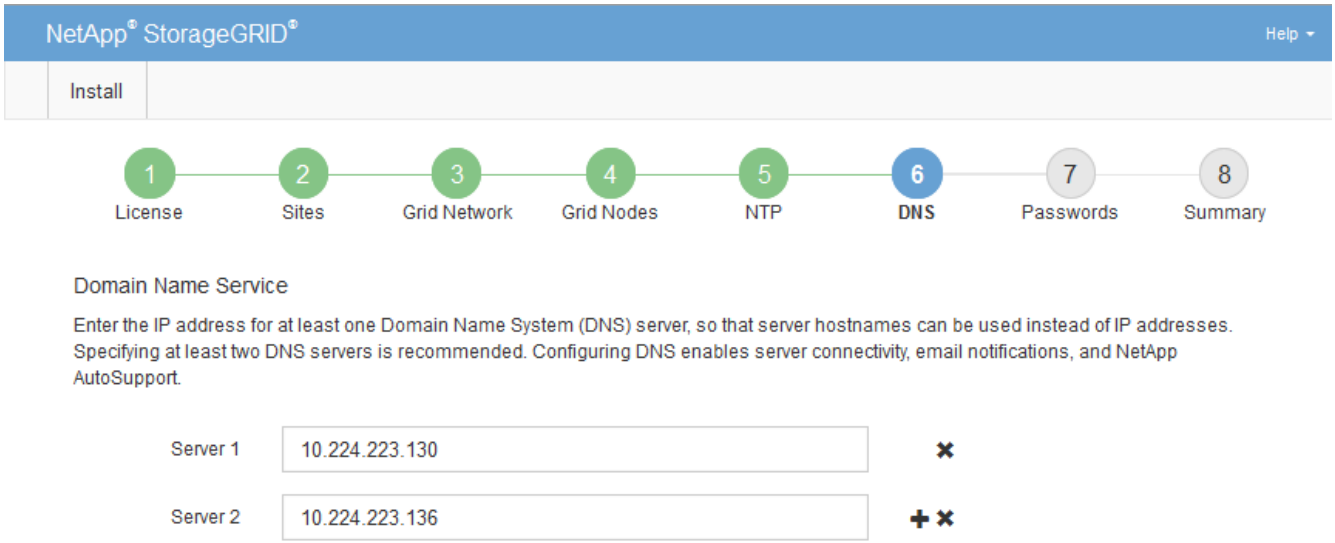
Pour garantir un fonctionnement correct, spécifiez deux ou trois serveurs DNS. Si vous spécifiez plus de trois, il est possible que seulement trois soient utilisés en raison des limitations connues du système d'exploitation sur certaines plates-formes. Si vous avez des restrictions de routage dans votre environnement, vous pouvez le faire "Personnaliser la liste des serveurs DNS" Pour les nœuds individuels (généralement tous les nœuds d'un site) d'utiliser un ensemble différent de trois serveurs DNS.

Si possible, utilisez des serveurs DNS auxquels chaque site peut accéder localement pour vous assurer qu'un site isdébarqué peut résoudre les FQDN pour les destinations externes.

Si les informations du serveur DNS sont omises ou mal configurées, une alarme DNST est déclenchée sur le service SSM de chaque nœud de la grille. L'alarme s'efface lorsque le DNS est configuré correctement et que les nouvelles informations sur le serveur ont atteint tous les nœuds de la grille.

Étapes

1. Spécifiez l'adresse IPv4 pour au moins un serveur DNS dans la zone de texte **Server 1**.
2. Si nécessaire, sélectionnez le signe plus en regard de la dernière entrée pour ajouter des entrées de serveur supplémentaires.



   La meilleure pratique consiste à spécifier au moins deux serveurs DNS. Vous pouvez indiquer jusqu'à six serveurs DNS.

3. Sélectionnez **Suivant**.

Spécifiez les mots de passe système StorageGRID

Dans le cadre de l'installation de votre système StorageGRID, vous devez saisir les mots de passe à utiliser pour sécuriser votre système et effectuer des tâches de maintenance.

Description de la tâche

Utilisez la page installer des mots de passe pour spécifier le mot de passe de provisionnement et le mot de passe utilisateur root de la gestion de grille.

- La phrase secrète de provisionnement est utilisée comme clé de chiffrement et n'est pas stockée par le système StorageGRID.
- Vous devez disposer du mot de passe de provisionnement pour les procédures d'installation, d'extension et de maintenance, y compris le téléchargement du progiciel de restauration. Il est donc important de stocker la phrase secrète de provisionnement dans un emplacement sécurisé.
- Vous pouvez modifier la phrase de passe de provisionnement à partir de Grid Manager si vous en avez la version actuelle.
- Le mot de passe de l'utilisateur root de la gestion de grille peut être modifié à l'aide de Grid Manager.
- La console de ligne de commande générée de manière aléatoire et les mots de passe SSH sont stockés dans le `Passwords.txt` Fichier dans le progiciel de restauration.

Étapes

1. Dans **Provisioning Passphrase**, saisissez la clé de passe de provisionnement qui sera requise pour modifier la topologie de la grille de votre système StorageGRID.

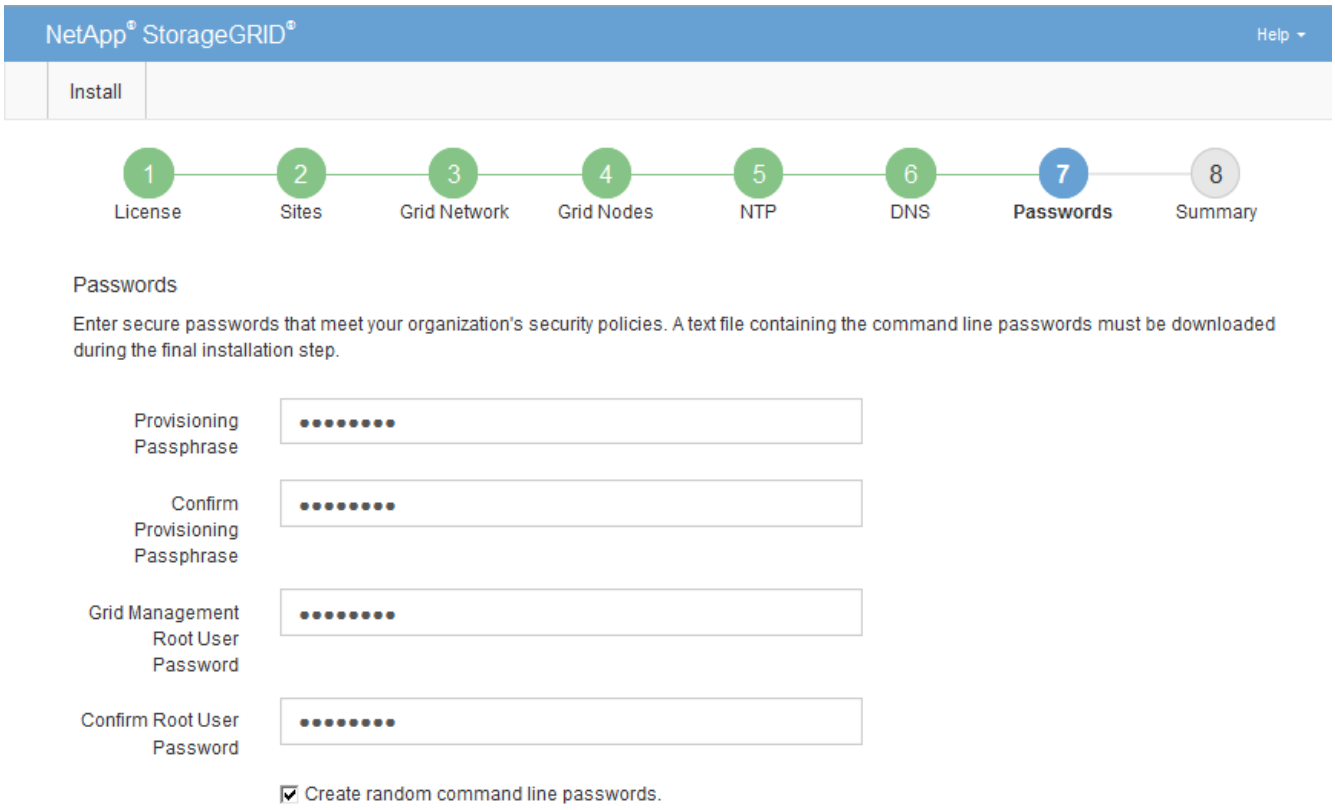
   Stockez la phrase secrète de provisionnement dans un endroit sécurisé.

   > Si une fois l'installation terminée et que vous souhaitez modifier ultérieurement le mot de passe de provisionnement, vous pouvez utiliser le Gestionnaire de grille. Sélectionnez **CONFIGURATION** > **contrôle d'accès**> **mots de passe de grille**.

2. Dans **Confirm Provisioning Passphrase**, saisissez à nouveau la phrase de passe de provisionnement pour la confirmer.
3. Dans **Grid Management Root User Password**, entrez le mot de passe à utiliser pour accéder au gestionnaire de grille en tant qu'utilisateur « root ».

   Stockez le mot de passe en lieu sûr.

4. Dans **confirmer le mot de passe de l'utilisateur racine**, entrez à nouveau le mot de passe de Grid Manager pour le confirmer.



5. Si vous installez une grille à des fins de démonstration de faisabilité ou de démonstration, désactivez éventuellement la case **Créer des mots de passe de ligne de commande aléatoires**.

   Pour les déploiements en production, des mots de passe aléatoires doivent toujours être utilisés pour des raisons de sécurité. Désactivez **Créez des mots de passe de ligne de commande aléatoires** uniquement pour les grilles de démonstration si vous souhaitez utiliser des mots de passe par défaut pour accéder aux nœuds de grille à partir de la ligne de commande à l'aide du compte "`root'" ou "'admin".

   > Vous êtes invité à télécharger le fichier du progiciel de récupération (`sgws-recovery-package-id-revision.zip`) Après avoir cliqué sur **installer** sur la page Résumé. Vous devez "téléchargez ce fichier" pour terminer l'installation. Les mots de passe requis pour accéder au système sont stockés dans le `Passwords.txt` Fichier, contenu dans le fichier du progiciel de récupération.

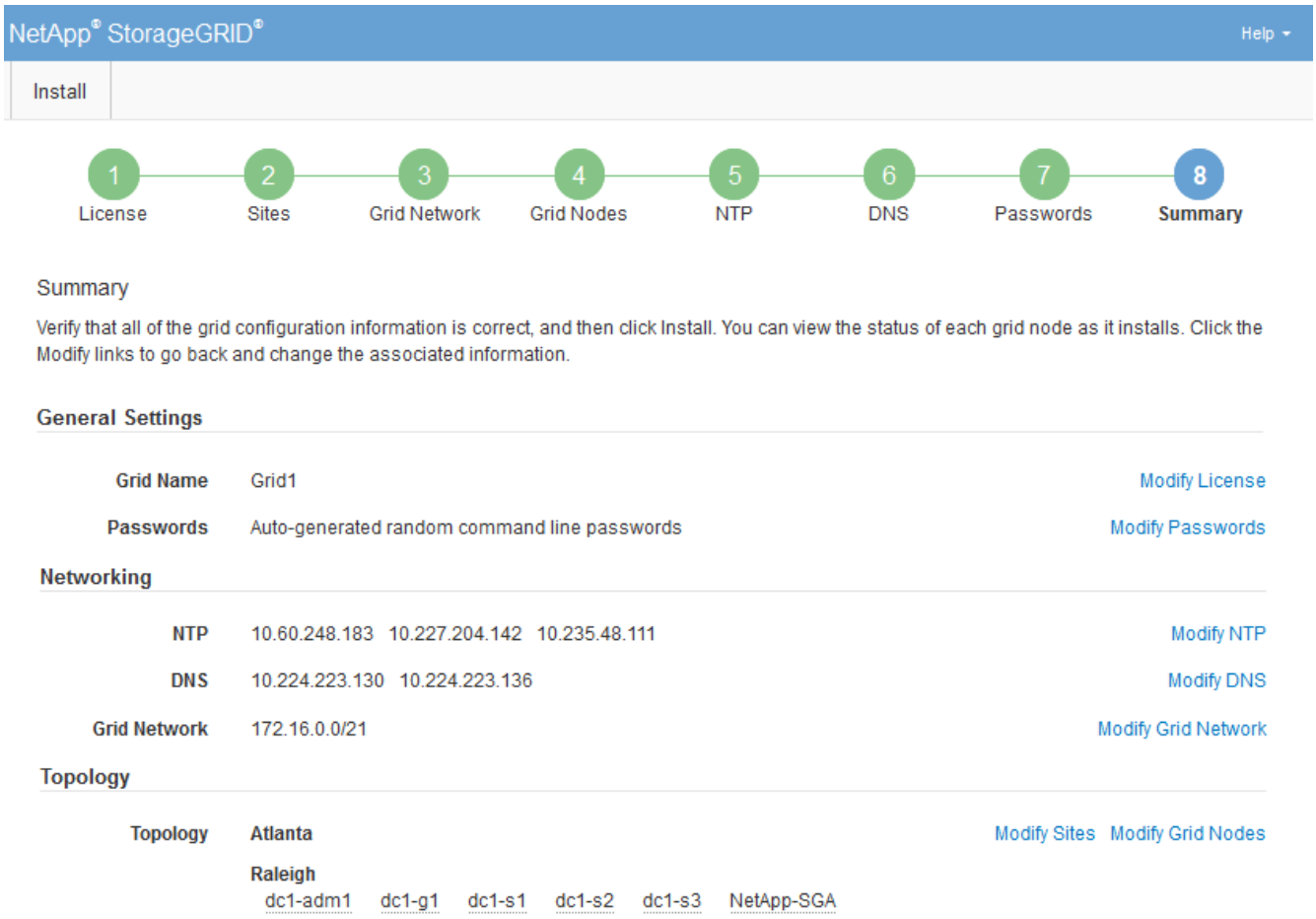
6. Cliquez sur **Suivant**.

Vérifiez votre configuration et terminez l'installation

Vous devez examiner attentivement les informations de configuration que vous avez saisies pour vous assurer que l'installation s'effectue correctement.

Étapes

1. Afficher la page **Résumé**.



2. Vérifiez que toutes les informations de configuration de la grille sont correctes. Utilisez les liens Modifier de la page Résumé pour revenir en arrière et corriger les erreurs.
3. Cliquez sur **installer**.

> Si un nœud est configuré pour utiliser le réseau client, la passerelle par défaut de ce nœud passe du réseau Grid au réseau client lorsque vous cliquez sur **installer**. Si vous perdez la connectivité, vous devez vous assurer que vous accédez au nœud d'administration principal via un sous-réseau accessible. Voir "Instructions de mise en réseau" pour plus d'informations.

4. Cliquez sur **Télécharger le progiciel de récupération**.

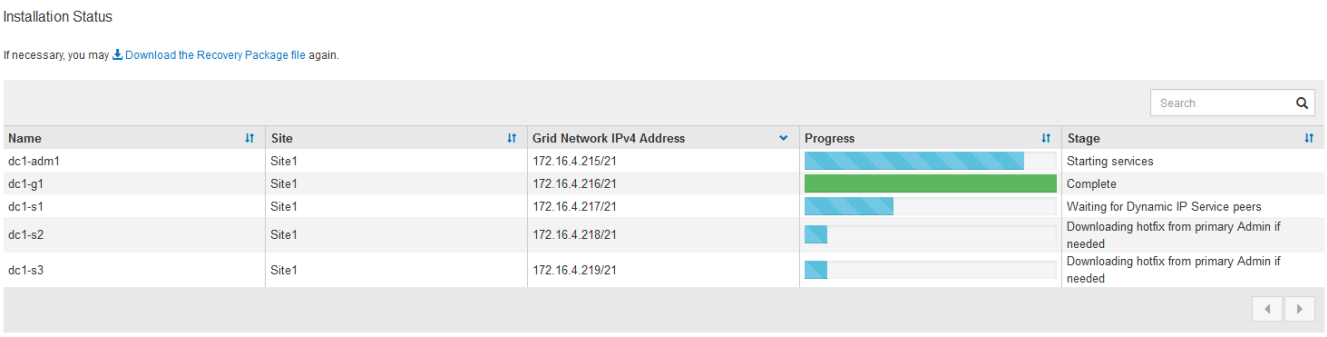
   Lorsque l'installation progresse jusqu'au point où la topologie de la grille est définie, vous êtes invité à télécharger le fichier du progiciel de récupération (`.zip`), et confirmez que vous pouvez accéder avec succès au contenu de ce fichier. Vous devez télécharger le fichier Recovery Package afin de pouvoir restaurer le système StorageGRID en cas de défaillance d'un ou de plusieurs nœuds de la grille. L'installation se poursuit en arrière-plan, mais vous ne pouvez pas terminer l'installation et accéder au système StorageGRID tant que vous n'avez pas téléchargé et vérifié ce fichier.

5. Vérifiez que vous pouvez extraire le contenu du `.zip` enregistrez-le ensuite à deux emplacements distincts, sécurisés et sécurisés.

> Le fichier du progiciel de récupération doit être sécurisé car il contient des clés de cryptage et des mots de passe qui peuvent être utilisés pour obtenir des données du système StorageGRID.

6. Cochez la case **J'ai téléchargé et vérifié le fichier du progiciel de récupération**, puis cliquez sur **Suivant**.

   Si l'installation est toujours en cours, la page d'état s'affiche. Cette page indique la progression de l'installation pour chaque nœud de la grille.



   Lorsque l'étape complète est atteinte pour tous les nœuds de la grille, la page de connexion de Grid Manager s'affiche.

7. Connectez-vous au gestionnaire de grille à l'aide de l'utilisateur « root » et du mot de passe que vous avez spécifié lors de l'installation.

Instructions de post-installation

Une fois le déploiement et la configuration des nœuds de la grille effectués, suivez ces instructions pour l'adressage DHCP et les modifications de configuration réseau.

- Si DHCP était utilisé pour attribuer des adresses IP, configurez une réservation DHCP pour chaque adresse IP sur les réseaux utilisés.

  Vous ne pouvez configurer DHCP que pendant la phase de déploiement. Vous ne pouvez pas configurer DHCP pendant la configuration.

  > Les nœuds redémarrent lors de la modification de leurs adresses IP, ce qui peut entraîner des pannes si une modification d'adresse DHCP affecte plusieurs nœuds simultanément.

- Vous devez utiliser les procédures Modifier IP pour modifier les adresses IP, les masques de sous-réseau et les passerelles par défaut pour un noeud de grille. Voir "Configurez les adresses IP".
- Si vous modifiez la configuration réseau, y compris le routage et les modifications de passerelle, la connectivité client au nœud d'administration principal et à d'autres nœuds de la grille risque d'être perdue. En fonction des modifications de réseau appliquées, vous devrez peut-être rétablir ces connexions.

Automatisation de l'installation (Red Hat Enterprise Linux ou CentOS)

Vous pouvez automatiser l'installation du service hôte StorageGRID et la configuration des nœuds grid.

L'automatisation du déploiement peut être utile dans les cas suivants :

- Vous utilisez déjà un framework d'orchestration standard, comme Ansible, Puppet ou Chef, pour déployer et configurer des hôtes physiques ou virtuels.

- Vous prévoyez de déployer plusieurs instances StorageGRID.
- Vous déployez une instance StorageGRID vaste et complexe.

Le service hôte StorageGRID est installé par un package et piloté par des fichiers de configuration. Vous pouvez créer les fichiers de configuration à l'aide de l'une des méthodes suivantes :

- "Créez les fichiers de configuration" interactivement pendant une installation manuelle.
- Préparez les fichiers de configuration à l'avance (ou par programmation) pour permettre une installation automatisée à l'aide des frameworks d'orchestration standard, comme le décrit dans cet article.

  StorageGRID propose des scripts Python en option permettant d'automatiser la configuration des appliances StorageGRID et de l'ensemble du système StorageGRID (la « grille »). Vous pouvez utiliser ces scripts directement, ou bien les inspecter pour apprendre à utiliser l'API REST d'installation StorageGRID dans les outils de déploiement et de configuration de grid que vous développez vous-même.

Automatisez l'installation et la configuration du service d'hôte StorageGRID

Vous pouvez automatiser l'installation du service hôte StorageGRID à l'aide des frameworks d'orchestration standard tels qu'Ansible, Puppet, Chef, Fabric ou SaltStack.

Le service hôte StorageGRID est fourni en RPM et est piloté par des fichiers de configuration que vous pouvez préparer en avance (ou par programmation) pour activer l'installation automatisée. Si vous utilisez déjà une structure d'orchestration standard pour installer et configurer RHEL ou CentOS, l'ajout d'StorageGRID à vos playbooks ou à vos recettes doit être simple.

Consultez l'exemple de rôle et de PlayBook Ansible dans la `/extras` dossier fourni avec l'archive d'installation. Le PlayBook Ansible présente la façon dont `storagegrid` Le rôle prépare l'hôte et installe StorageGRID sur les serveurs cibles. Vous pouvez personnaliser le rôle ou le PlayBook selon vos besoins.

> Le PlayBook exemple n'inclut pas les étapes requises pour créer des périphériques réseau avant de démarrer le service hôte StorageGRID. Ajoutez ces étapes avant de finaliser et d'utiliser le PlayBook.

Vous pouvez automatiser toutes les étapes pour préparer les hôtes et déployer des nœuds de grille virtuels.

Automatiser la configuration de StorageGRID

Une fois les nœuds grid déployés, vous pouvez automatiser la configuration du système StorageGRID.

Avant de commencer

- Vous connaissez l'emplacement des fichiers suivants à partir de l'archive d'installation.

Nom du fichier	Description
configure-storagegrid.py	Script Python utilisé pour automatiser la configuration
configurez-storagegrid.sample.json	Exemple de fichier de configuration à utiliser avec le script

Nom du fichier	Description
configurez-storagegrid.blank.json	Fichier de configuration vierge à utiliser avec le script

- Vous avez créé un `configure-storagegrid.json` fichier de configuration. Pour créer ce fichier, vous pouvez modifier l'exemple de fichier de configuration (`configure-storagegrid.sample.json`) ou le fichier de configuration vierge (`configure-storagegrid.blank.json`).

Description de la tâche

Vous pouvez utiliser le `configure-storagegrid.py` Script Python et le `configure-storagegrid.json` Fichier de configuration pour automatiser la configuration de votre système StorageGRID.

> Vous pouvez également configurer le système à l'aide de Grid Manager ou de l'API d'installation.

Étapes

1. Connectez-vous à la machine Linux que vous utilisez pour exécuter le script Python.
2. Accédez au répertoire dans lequel vous avez extrait l'archive d'installation.

   Par exemple :

   ```
   cd StorageGRID-Webscale-version/platform
   ```

   où `platform` est `debs`, `rpms`, ou `vsphere`.

3. Exécutez le script Python et utilisez le fichier de configuration que vous avez créé.

   Par exemple :

   ```
   ./configure-storagegrid.py ./configure-storagegrid.json --start-install
   ```

Résultat

Un progiciel de récupération `.zip` le fichier est généré pendant le processus de configuration et il est téléchargé dans le répertoire où vous exécutez le processus d'installation et de configuration. Vous devez sauvegarder le fichier de package de restauration afin de pouvoir restaurer le système StorageGRID en cas de défaillance d'un ou plusieurs nœuds de la grille. Par exemple, copiez-le dans un emplacement sécurisé, sauvegardé sur le réseau et dans un emplacement de stockage cloud sécurisé.

> Le fichier du progiciel de récupération doit être sécurisé car il contient des clés de cryptage et des mots de passe qui peuvent être utilisés pour obtenir des données du système StorageGRID.

Si vous avez indiqué que des mots de passe aléatoires doivent être générés, ouvrez le `Passwords.txt` Fichier et recherche les mots de passe requis pour accéder au système StorageGRID.

```
######################################################################
##### The StorageGRID "recovery package" has been downloaded as: #####
#####           ./sgws-recovery-package-994078-rev1.zip          #####
#####   Safeguard this file as it will be needed in case of a    #####
#####                 StorageGRID node recovery.                 #####
######################################################################
```

Votre système StorageGRID est installé et configuré lorsqu'un message de confirmation s'affiche.

```
StorageGRID has been configured and installed.
```

Informations associées

"Présentation de l'API REST d'installation"

Présentation de l'API REST d'installation

StorageGRID fournit l'API d'installation StorageGRID pour effectuer des tâches d'installation.

L'API utilise la plate-forme swagger open source API pour fournir la documentation de l'API. Swagger permet aux développeurs et aux non-développeurs d'interagir avec l'API dans une interface utilisateur qui illustre la façon dont l'API répond aux paramètres et aux options. Cette documentation suppose que vous êtes familiarisé avec les technologies Web standard et le format de données JSON.

> Toutes les opérations d'API que vous effectuez à l'aide de la page Web API Docs sont des opérations en direct. Veillez à ne pas créer, mettre à jour ou supprimer des données de configuration ou d'autres données par erreur.

Chaque commande de l'API REST inclut l'URL de l'API, une action HTTP, tous les paramètres d'URL requis ou facultatifs et une réponse de l'API attendue.

API d'installation de StorageGRID

L'API d'installation de StorageGRID n'est disponible que lors de la configuration initiale du système StorageGRID et si vous devez effectuer une restauration du nœud d'administration principal. L'API d'installation est accessible via HTTPS depuis le Grid Manager.

Pour accéder à la documentation de l'API, accédez à la page Web d'installation sur le nœud d'administration principal et sélectionnez **aide** > **documentation de l'API** dans la barre de menus.

L'API d'installation de StorageGRID comprend les sections suivantes :

- **Config** — opérations liées à la version du produit et aux versions de l'API. Vous pouvez lister la version du produit ainsi que les versions principales de l'API prises en charge par cette version.
- **Grid** — opérations de configuration au niveau de la grille. Vous pouvez obtenir et mettre à jour les paramètres de la grille, y compris les détails de la grille, les sous-réseaux de la grille, les mots de passe de la grille et les adresses IP des serveurs NTP et DNS.
- **Noeuds** — opérations de configuration au niveau des noeuds. Vous pouvez récupérer une liste de nœuds

de la grille, supprimer un nœud de la grille, configurer un nœud de la grille, afficher un nœud de la grille et réinitialiser la configuration d'un nœud de la grille.

- **Provision** — opérations de provisionnement. Vous pouvez démarrer l'opération de provisionnement et afficher l'état de cette opération.
- **Recovery** — opérations de restauration du noeud d'administration principal. Vous pouvez réinitialiser les informations, télécharger le progiciel de restauration, démarrer la récupération et afficher l'état de l'opération de récupération.
- **Progiciel de récupération** — opérations pour télécharger le progiciel de récupération.
- **Schémas** — schémas API pour les déploiements avancés
- **Sites** — opérations de configuration au niveau du site. Vous pouvez créer, afficher, supprimer et modifier un site.

Par où aller plus loin

Une fois l'installation terminée, effectuez les tâches d'intégration et de configuration requises. Vous pouvez effectuer les tâches facultatives nécessaires.

Tâches requises

- "Créez un compte de locataire" Pour chaque protocole client (Swift ou S3) qui sera utilisé pour stocker des objets sur votre système StorageGRID.
- "Contrôler l'accès au système" en configurant des groupes et des comptes utilisateur. Si vous le souhaitez, vous pouvez "configurer un référentiel d'identité fédéré" (Comme Active Directory ou OpenLDAP), vous pouvez importer des groupes et des utilisateurs d'administration. Ou bien, c'est possible "créer des groupes et des utilisateurs locaux".
- Intégrer et tester le "API S3" ou "API Swift" Applications client que vous utiliserez pour télécharger des objets sur votre système StorageGRID.
- "Configuration des règles de gestion du cycle de vie des informations (ILM) et de la règle ILM" utilisez pour protéger les données d'objet.
- Si votre installation inclut des nœuds de stockage de l'appliance, effectuez les tâches suivantes avec SANtricity OS :
  - Connectez-vous à chaque appliance StorageGRID.
  - Vérifiez la réception des données AutoSupport.

    Voir "Configurer le matériel".
- Examinez et suivez les "Instructions de renforcement du système StorageGRID" pour éliminer les risques de sécurité.
- "Configurez les notifications par e-mail pour les alertes système".
- Si votre système StorageGRID inclut des nœuds d'archivage (obsolètes), configurez la connexion du nœud d'archivage au système de stockage d'archives externe cible.

Tâches facultatives

- "Mettre à jour les adresses IP des nœuds de la grille" S'ils ont changé depuis que vous avez planifié votre déploiement et généré le package de récupération.
- "Configurer le chiffrement du stockage", si nécessaire.

- "Configurer la compression du stockage" pour réduire la taille des objets stockés, si nécessaire.
- "Configurez l'accès au système à des fins d'audit" Par le biais d'un partage de fichiers NFS.

Résoudre les problèmes d'installation

En cas de problème lors de l'installation de votre système StorageGRID, vous pouvez accéder aux fichiers journaux d'installation. Le support technique peut également avoir besoin d'utiliser les fichiers journaux d'installation pour résoudre les problèmes.

Les fichiers journaux d'installation suivants sont disponibles à partir du conteneur qui exécute chaque nœud :

- `/var/local/log/install.log` (disponible sur tous les nœuds de la grille)
- `/var/local/log/gdu-server.log` (Trouvé sur le nœud d'administration principal)

Les fichiers journaux d'installation suivants sont disponibles auprès de l'hôte :

- `/var/log/storagegrid/daemon.log`
- `/var/log/storagegrid/nodes/node-name.log`

Pour savoir comment accéder aux fichiers journaux, reportez-vous à la section "Collecte de fichiers journaux et de données système".

Informations associées

"Dépanner un système StorageGRID"

Exemple /etc/sysconfig/network-scripts

Vous pouvez utiliser ces fichiers d'exemple pour agréger quatre interfaces physiques Linux en une seule liaison LACP, puis établir trois interfaces VLAN qui fixent la liaison pour une utilisation comme interfaces réseau StorageGRID, Admin et client.

Interfaces physiques

Notez que les switchs à l'autre extrémité des liaisons doivent également traiter les quatre ports comme une seule jonction ou un canal de port LACP et doivent passer au moins les trois VLAN référencés avec des balises.

`/etc/sysconfig/network-scripts/ifcfg-ens160`

```
TYPE=Ethernet
NAME=ens160
UUID=011b17dd-642a-4bb9-acae-d71f7e6c8720
DEVICE=ens160
ONBOOT=yes
MASTER=bond0
SLAVE=yes
```

`/etc/sysconfig/network-scripts/ifcfg-ens192`

```
TYPE=Ethernet
NAME=ens192
UUID=e28eb15f-76de-4e5f-9a01-c9200b58d19c
DEVICE=ens192
ONBOOT=yes
MASTER=bond0
SLAVE=yes
```

/etc/sysconfig/network-scripts/ifcfg-ens224

```
TYPE=Ethernet
NAME=ens224
UUID=b0e3d3ef-7472-4cde-902c-ef4f3248044b
DEVICE=ens224
ONBOOT=yes
MASTER=bond0
SLAVE=yes
```

/etc/sysconfig/network-scripts/ifcfg-ens256

```
TYPE=Ethernet
NAME=ens256
UUID=7cf7aabc-3e4b-43d0-809a-1e2378faa4cd
DEVICE=ens256
ONBOOT=yes
MASTER=bond0
SLAVE=yes
```

Interface de liaison

/etc/sysconfig/network-scripts/ifcfg-bond0

```
DEVICE=bond0
TYPE=Bond
BONDING_MASTER=yes
NAME=bond0
ONBOOT=yes
BONDING_OPTS=mode=802.3ad
```

Interfaces VLAN

/etc/sysconfig/network-scripts/ifcfg-bond0.1001

```
VLAN=yes
TYPE=Vlan
DEVICE=bond0.1001
PHYSDEV=bond0
VLAN_ID=1001
REORDER_HDR=0
BOOTPROTO=none
UUID=296435de-8282-413b-8d33-c4dd40fca24a
ONBOOT=yes
```

/etc/sysconfig/network-scripts/ifcfg-bond0.1002

```
VLAN=yes
TYPE=Vlan
DEVICE=bond0.1002
PHYSDEV=bond0
VLAN_ID=1002
REORDER_HDR=0
BOOTPROTO=none
UUID=dbaaec72-0690-491c-973a-57b7dd00c581
ONBOOT=yes
```

/etc/sysconfig/network-scripts/ifcfg-bond0.1003

```
VLAN=yes
TYPE=Vlan
DEVICE=bond0.1003
PHYSDEV=bond0
VLAN_ID=1003
REORDER_HDR=0
BOOTPROTO=none
UUID=d1af4b30-32f5-40b4-8bb9-71a2fbf809a1
ONBOOT=yes
```

Installez Ubuntu ou Debian

Installer Ubuntu ou Debian: Présentation

L'installation d'un système StorageGRID dans un environnement Ubuntu ou Debian comprend trois étapes principales.

1. **Préparation**: Pendant la planification et la préparation, vous effectuez les tâches suivantes :

- En savoir plus sur les besoins matériels et de stockage pour StorageGRID.
- Découvrez les détails de "La mise en réseau StorageGRID" vous pouvez ainsi configurer votre réseau de façon appropriée.
- Identifiez et préparez les serveurs physiques ou virtuels que vous prévoyez d'utiliser pour héberger vos nœuds de grid StorageGRID.
- Sur les serveurs que vous avez préparés :
  - Installez Linux
  - Configurez le réseau hôte
  - Configurer le stockage de l'hôte
  - Installez Docker
  - Installez les services d'hôte StorageGRID

2. **Déploiement** : déployez des nœuds de la grille à l'aide de l'interface utilisateur appropriée. Lorsque vous déployez des nœuds grid, ils sont créés dans le cadre du système StorageGRID et connectés à un ou plusieurs réseaux.
   a. Utilisez les fichiers de configuration de ligne de commande et de nœud Linux pour déployer des nœuds de grille virtuelle sur les hôtes que vous avez préparés à l'étape 1.
   b. Utilisez le programme d'installation de l'appliance StorageGRID pour déployer les nœuds d'appliance StorageGRID.

> Les instructions d'installation et d'intégration spécifiques au matériel ne sont pas incluses dans la procédure d'installation de StorageGRID. Pour savoir comment installer les appliances StorageGRID, consultez le "Démarrage rapide pour l'installation du matériel" pour trouver les instructions relatives à votre appareil.

3. **Configuration** : lorsque tous les nœuds ont été déployés, utilisez le gestionnaire de grille pour configurer la grille et terminer l'installation.

Ces instructions recommandent une approche standard pour le déploiement et la configuration d'un système StorageGRID dans un environnement Ubuntu ou Debian. Voir également les informations sur les approches alternatives suivantes :

- Utilisez une structure d'orchestration standard telle qu'Ansible, Puppet ou Chef pour installer Ubuntu ou Debian, configurer la mise en réseau et le stockage, installer Docker et le service hôte StorageGRID, et déployer des nœuds de grid virtuel.
- Automatiser le déploiement et la configuration du système StorageGRID à l'aide d'un script de configuration Python (fourni dans l'archive d'installation).
- Automatisez le déploiement et la configuration des nœuds grid d'appliance avec un script de configuration Python (disponible dans l'archive de l'installation ou depuis le programme d'installation de l'appliance StorageGRID).
- Si vous êtes un développeur avancé de déploiements StorageGRID, utilisez les API REST d'installation pour automatiser l'installation des nœuds grid d'StorageGRID.

Planifier et préparer l'installation d'Ubuntu ou de Debian

Avant d'installer (Ubuntu ou Debian)

Avant de déployer des nœuds de grid et de configurer StorageGRID, vous devez

connaître les étapes et les conditions requises pour effectuer cette procédure.

Les procédures de déploiement et de configuration de StorageGRID supposent que vous connaissez bien l'architecture et le fonctionnement du système StorageGRID.

Vous pouvez déployer un ou plusieurs sites à la fois. Toutefois, tous les sites doivent respecter le minimum requis : disposer d'au moins trois nœuds de stockage.

Avant de démarrer une installation StorageGRID, vous devez :

- Analysez les besoins en calcul, notamment les exigences minimales en termes de CPU et de RAM pour chaque nœud.
- Découvrez comment StorageGRID prend en charge plusieurs réseaux pour faciliter la séparation du trafic, la sécurité et l'administration, et planifiez les réseaux que vous envisagez de connecter à chaque nœud StorageGRID.

  Voir le StorageGRID "Instructions de mise en réseau".

- Analysez les exigences de performances et de stockage de chaque type de nœud grid.
- Identifier un ensemble de serveurs (physiques, virtuels ou les deux) qui, dans l'agrégat, fournissent suffisamment de ressources pour prendre en charge le nombre et le type de nœuds StorageGRID que vous prévoyez de déployer.
- Prenez connaissance du "conditions requises pour la migration des nœuds", si vous souhaitez effectuer une maintenance planifiée sur des hôtes physiques sans interruption de service.
- Rassemblez toutes les informations de réseautage à l'avance. À moins que vous n'utilisiez DHCP, rassemblez les adresses IP à attribuer à chaque nœud de grille, ainsi que les adresses IP des serveurs DNS et NTP qui seront utilisés.
- Installez, connectez et configurez tout le matériel requis, y compris les appliances StorageGRID, selon les spécifications.

  > Si votre installation StorageGRID n'utilise pas de nœuds de stockage (matériels) StorageGRID, vous devez utiliser un stockage RAID matériel avec un cache d'écriture protégé par batterie (BBWC). StorageGRID ne prend pas en charge l'utilisation de réseaux de stockage virtuels (VSAN), de RAID logiciel ou aucune protection RAID.

  > Les instructions d'installation et d'intégration spécifiques au matériel ne sont pas incluses dans la procédure d'installation de StorageGRID. Pour savoir comment installer les appliances StorageGRID, reportez-vous à la section "Installez le matériel de l'appliance".

- Choisissez les outils de déploiement et de configuration que vous souhaitez utiliser.

Matériel requis

Avant d'installer StorageGRID, vous devez rassembler et préparer les ressources nécessaires.

Élément	Remarques
Licence NetApp StorageGRID	Vous devez disposer d'une licence NetApp valide et signée numériquement. **Note**: Une licence de non-production, qui peut être utilisée pour tester et démontrer les grilles de concept, est incluse dans l'archive d'installation de StorageGRID.
Archive de l'installation de StorageGRID	Vous devez "Téléchargez l'archive d'installation de StorageGRID et extrayez les fichiers".
L'ordinateur portable de service	Le système StorageGRID est installé par le biais d'un ordinateur portable de service. L'ordinateur portable de service doit posséder : • Port réseau • Client SSH (par exemple, PuTTY) • "Navigateur Web pris en charge"
Documentation StorageGRID	• "Notes de mise à jour" • "Instructions d'administration de StorageGRID"

Informations associées

"Matrice d'interopérabilité NetApp"

Téléchargez et extrayez les fichiers d'installation de StorageGRID

Vous devez télécharger l'archive d'installation de StorageGRID et extraire les fichiers requis.

Étapes

1. Accédez au "Page de téléchargements NetApp pour StorageGRID".
2. Sélectionnez le bouton pour télécharger la dernière version ou sélectionnez une autre version dans le menu déroulant et sélectionnez **Go**.
3. Connectez-vous avec le nom d'utilisateur et le mot de passe de votre compte NetApp.
4. Si une instruction attention/MustRead apparaît, lisez-la et cochez la case.

   Après l'installation de la version StorageGRID, vous devez appliquer les correctifs requis. Pour plus d'informations, reportez-vous à la section "procédure de correctif dans les instructions de récupération et de maintenance"

5. Lisez le contrat de licence de l'utilisateur final, cochez la case, puis sélectionnez **accepter et continuer**.

   La page des téléchargements de la version sélectionnée s'affiche. La page contient trois colonnes :

6. Dans la colonne **Install StorageGRID**, sélectionnez le fichier .tgz ou .zip pour Ubuntu ou Debian.

   Sélectionner `.zip` Fichier si vous exécutez Windows sur l'ordinateur portable de service.

7. Enregistrez et extrayez le fichier d'archive.
8. Choisissez les fichiers dont vous avez besoin dans la liste suivante.

   L'ensemble de fichiers dont vous avez besoin dépend de votre topologie de grille planifiée et de la manière dont vous allez déployer votre grille StorageGRID.

   Les chemins répertoriés dans la table sont relatifs au répertoire de niveau supérieur installé par l'archive d'installation extraite.

Chemin d'accès et nom de fichier	Description
	Fichier texte qui décrit tous les fichiers contenus dans le fichier de téléchargement StorageGRID.
	Un fichier de licence NetApp hors production que vous pouvez utiliser pour tester et réaliser des démonstrations de faisabilité.
	DEB paquet pour installer les images de noeud StorageGRID sur des hôtes Ubuntu ou Debian.
	Somme de contrôle MD5 pour le fichier `/debs/storagegrid-webscale-images-version-SHA.deb`.
	Paquet DEB pour l'installation du service hôte StorageGRID sur des hôtes Ubuntu ou Debian.
Outil de script de déploiement	Description
	Script Python utilisé pour automatiser la configuration d'un système StorageGRID.
	Script Python utilisé pour automatiser la configuration des appliances StorageGRID.
	Exemple de script Python que vous pouvez utiliser pour vous connecter à l'API Grid Management lorsque l'authentification unique est activée. Vous pouvez également utiliser ce script pour le Federate Ping.
	Exemple de fichier de configuration à utiliser avec `configure-storagegrid.py` script.

Chemin d'accès et nom de fichier	Description
	Un fichier de configuration vierge à utiliser avec le `configure-storagegrid.py` script.
	Exemple de rôle et de manuel de vente Ansible pour la configuration des hôtes Ubuntu ou Debian pour le déploiement de conteneurs StorageGRID. Vous pouvez personnaliser le rôle ou le PlayBook selon vos besoins.
	Exemple de script Python que vous pouvez utiliser pour vous connecter à l'API de gestion de grille lorsque l'authentification unique (SSO) est activée à l'aide d'Active Directory ou de Ping Federate.
	Script d'aide appelé par le compagnon `storagegrid-ssoauth-azure.py` Script Python pour effectuer des interactions SSO avec Azure.
	Schémas API pour StorageGRID. **Remarque** : avant d'effectuer une mise à niveau, vous pouvez utiliser ces schémas pour confirmer que tout code que vous avez écrit pour utiliser les API de gestion StorageGRID sera compatible avec la nouvelle version de StorageGRID si vous ne disposez pas d'un environnement StorageGRID non productif pour le test de compatibilité de mise à niveau.

Configuration requise pour le processeur et la RAM

Avant d'installer le logiciel StorageGRID, vérifiez et configurez le matériel afin qu'il soit prêt à prendre en charge le système StorageGRID.

Pour plus d'informations sur les serveurs pris en charge, reportez-vous au "Matrice d'interopérabilité NetApp".

Chaque nœud StorageGRID nécessite au moins :

- Cœurs de processeur : 8 par nœud
- RAM : au moins 24 Go par nœud et 2 à 16 Go de moins que la RAM totale du système, selon la mémoire RAM totale disponible et la quantité de logiciel non StorageGRID exécuté sur le système

Vérifiez que le nombre de nœuds StorageGRID que vous prévoyez d'exécuter sur chaque hôte physique ou virtuel ne dépasse pas le nombre de cœurs de processeur ou la mémoire RAM physique disponible. Si les hôtes ne sont pas dédiés à l'exécution de StorageGRID (non recommandé), veillez à prendre en compte les besoins en ressources des autres applications.

Surveillez régulièrement l'utilisation de votre processeur et de votre mémoire pour vous assurer que ces ressources continuent de s'adapter à votre charge de travail. Par exemple, doubler l'allocation de la RAM et du processeur pour les nœuds de stockage virtuels fournira des ressources similaires à celles des nœuds d'appliance StorageGRID. En outre, si la quantité de métadonnées par nœud dépasse 500 Go, envisagez d'augmenter la mémoire RAM par nœud à au moins 48 Go. Pour plus d'informations sur la gestion du stockage des métadonnées d'objet, l'augmentation du paramètre espace réservé aux métadonnées et la surveillance de l'utilisation du processeur et de la mémoire, reportez-vous aux instructions de "administration", "contrôle", et "mise à niveau" StorageGRID :

Si le hyperthreading est activé sur les hôtes physiques sous-jacents, vous pouvez fournir 8 cœurs virtuels (4 cœurs physiques) par nœud. Si le hyperthreading n'est pas activé sur les hôtes physiques sous-jacents, vous devez fournir 8 cœurs physiques par nœud.

Si vous utilisez des machines virtuelles en tant qu'hôtes et que vous contrôlez la taille et le nombre de machines virtuelles, nous vous recommandons d'utiliser une seule machine virtuelle pour chaque nœud StorageGRID afin de dimensionner celle-ci en conséquence.

Dans le cas de déploiements en production, vous ne devez pas exécuter plusieurs nœuds de stockage sur le même matériel de stockage physique ou sur le même hôte virtuel. Dans un seul déploiement StorageGRID, chaque nœud de stockage doit se trouver dans son propre domaine de défaillances isolé. Vous pouvez optimiser la durabilité et la disponibilité des données d'objet si vous assurez qu'une seule panne matérielle peut avoir un impact sur un seul nœud de stockage.

Voir aussi "Les besoins en matière de stockage et de performances".

Les besoins en matière de stockage et de performances

Vous devez connaître les exigences de stockage des nœuds StorageGRID afin de fournir un espace suffisant pour prendre en charge la configuration initiale et l'extension future du stockage.

Les nœuds StorageGRID nécessitent trois catégories logiques de stockage :

- **Pool de conteneurs** — stockage de niveau performances (SAS 10 000 tr/min ou SSD) pour les conteneurs de nœuds, qui sera attribué au pilote de stockage Docker lors de l'installation et de la configuration de Docker sur les hôtes qui prendront en charge vos nœuds StorageGRID.
- **Données système** — stockage de niveau performances (SAS 10 000 tr/min ou SSD) pour le stockage persistant par nœud des données système et des journaux de transactions, que les services hôtes StorageGRID consommeront et mappent vers des nœuds individuels.
- **Données objet** — stockage de niveau performance (SAS 10 000 tr/min ou SSD) et stockage en bloc de niveau capacité (NL-SAS/SATA) pour le stockage persistant des données d'objet et des métadonnées d'objet.

Vous devez utiliser des périphériques de bloc RAID pour toutes les catégories de stockage. Les disques, disques SSD ou JBOD non redondants ne sont pas pris en charge. Vous pouvez utiliser un stockage RAID partagé ou local pour l'une des catégories de stockage. Toutefois, si vous souhaitez utiliser la fonctionnalité de migration de nœuds dans StorageGRID, vous devez stocker les données système et les données d'objet sur un stockage partagé. Pour plus d'informations, voir "Exigences de migration des conteneurs de nœuds".

Exigences en matière de performances

Les performances des volumes utilisés pour les pools de conteneurs, les données système et les métadonnées d'objet ont un impact significatif sur la performance globale du système. Pour ces volumes, il est recommandé d'utiliser un stockage de Tier de performances (SAS 10 000 tr/min ou SSD) pour garantir des performances de disque satisfaisantes en termes de latence, d'opérations d'entrée/sortie par seconde (IOPS) et de débit. Vous pouvez utiliser un stockage de niveau de capacité (NL-SAS/SATA) pour le stockage persistant des données d'objet.

La mise en cache de l'écriture différée est activée sur les volumes utilisés pour le pool de conteneurs, les données système et les données d'objet. Le cache doit se trouver sur un support protégé ou persistant.

Exigences relatives aux hôtes qui utilisent un stockage NetApp ONTAP

Si le nœud StorageGRID utilise le stockage affecté à un système NetApp ONTAP, vérifiez que cette FabricPool règle n'est pas activée pour le volume. La désactivation du Tiering FabricPool pour les volumes utilisés avec des nœuds StorageGRID simplifie la résolution des problèmes et les opérations de stockage.

> ⓘ N'utilisez jamais FabricPool pour transférer automatiquement toutes les données liées à StorageGRID vers StorageGRID. Le Tiering des données StorageGRID vers StorageGRID augmente la complexité opérationnelle et la résolution des problèmes.

Nombre d'hôtes requis

Chaque site StorageGRID requiert au moins trois nœuds de stockage.

> ⓘ Dans un déploiement de production, n'exécutez pas plus d'un nœud de stockage sur un seul hôte physique ou virtuel. L'utilisation d'un hôte dédié pour chaque nœud de stockage fournit un domaine de défaillance isolé.

Les autres types de nœuds, comme les nœuds d'administration ou les nœuds de passerelle, peuvent être déployés sur les mêmes hôtes, ou sur leurs propres hôtes dédiés, si nécessaire.

Nombre de volumes de stockage pour chaque hôte

Le tableau ci-dessous présente le nombre de volumes de stockage (LUN) requis pour chaque hôte et la taille minimale requise pour chaque LUN, en fonction des nœuds à déployer sur cet hôte.

La taille de LUN maximale testée est de 39 To.

> ⓘ Ces nombres sont pour chaque hôte, et non pour l'intégralité de la grille.

Objectif de LUN	Catégorie de stockage	Nombre de LUN	Taille minimale/LUN
Pool de stockage du moteur du conteneur	Pool de conteneurs	1	Nombre total de nœuds × 100 Go
`/var/local` volumétrie	Données système	1 pour chaque nœud sur cet hôte	90 GO

Objectif de LUN	Catégorie de stockage	Nombre de LUN	Taille minimale/LUN
Nœud de stockage	Données d'objet	3 pour chaque nœud de stockage sur cet hôte **Remarque :** Un noeud de stockage logiciel peut avoir 1 à 16 volumes de stockage; au moins 3 volumes de stockage sont recommandés.	12 To (4 To/LUN) consultez la section exigences de stockage des nœuds de stockage pour en savoir plus.
Journaux d'audit du nœud d'administration	Données système	1 pour chaque nœud d'administration sur cet hôte	200 GO
Tables des nœuds d'administration	Données système	1 pour chaque nœud d'administration sur cet hôte	200 GO

Selon le niveau d'audit configuré, la taille des entrées utilisateur telles que le nom de clé d'objet S3, Et la quantité de données des journaux d'audit à conserver, il peut être nécessaire d'augmenter la taille de la LUN des journaux d'audit sur chaque nœud d'administration.en général, une grille génère environ 1 Ko de données d'audit par opération S3, Cela signifie qu'un LUN de 200 Go peut prendre en charge 70 millions d'opérations par jour ou 800 opérations par seconde pendant deux à trois jours.

Espace de stockage minimum pour un hôte

Le tableau suivant indique l'espace de stockage minimal requis pour chaque type de nœud. Ce tableau permet de déterminer la quantité minimale de stockage que vous devez fournir à l'hôte dans chaque catégorie de stockage, en fonction des nœuds à déployer sur cet hôte.

Les snapshots de disque ne peuvent pas être utilisés pour restaurer les nœuds de grille. Reportez-vous plutôt au "restauration du nœud grid" procédures pour chaque type de nœud.

Type de nœud	Pool de conteneurs	Données système	Données d'objet
Nœud de stockage	100 GO	90 GO	4,000 GO
Nœud d'administration	100 GO	490 Go (3 LUN)	*non applicable*
Nœud de passerelle	100 GO	90 GO	*non applicable*
Nœud d'archivage	100 GO	90 GO	*non applicable*

Exemple : calcul des besoins en stockage d'un hôte

Supposons que vous prévoyez de déployer trois nœuds sur un même hôte : un nœud de stockage, un nœud d'administration et un nœud de passerelle. Vous devez fournir un minimum de neuf volumes de stockage à

l'hôte. Vous aurez besoin d'un minimum de 300 Go de stockage de Tier de performance pour les conteneurs de nœuds, de 670 Go de stockage de Tier de performance pour les données système et les journaux de transactions, et de 12 To de stockage de Tier de capacité pour les données d'objet.

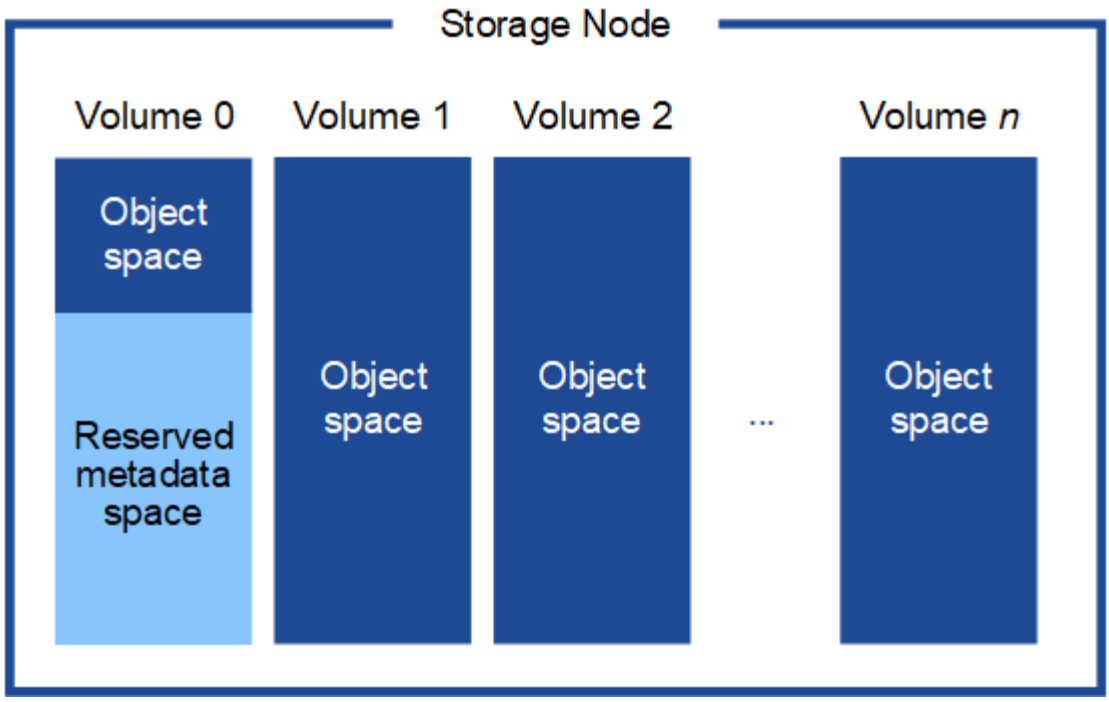
Type de nœud	Objectif de LUN	Nombre de LUN	Taille de la LUN
Nœud de stockage	Pool de stockage Docker	1	300 Go (100 Go/nœud)
Nœud de stockage	`/var/local` volumétrie	1	90 GO
Nœud de stockage	Données d'objet	3	12 TO (4 TO/LUN)
Nœud d'administration	`/var/local` volumétrie	1	90 GO
Nœud d'administration	Journaux d'audit du nœud d'administration	1	200 GO
Nœud d'administration	Tables des nœuds d'administration	1	200 GO
Nœud de passerelle	`/var/local` volumétrie	1	90 GO
Total		**9**	**Pool de conteneurs :** 300 Go **Données système :** 670 Go **Données d'objet :** 12,000 Go

Besoins de stockage des nœuds de stockage

Un nœud de stockage logiciel peut disposer de 1 à 16 volumes de stockage, dont -3 volumes ou plus sont recommandés. Chaque volume de stockage doit être supérieur ou égale à 4 To.

Un nœud de stockage d'appliance peut disposer d'un maximum de 48 volumes de stockage.

Comme illustré dans la figure, StorageGRID réserve l'espace des métadonnées d'objet sur le volume de stockage 0 de chaque nœud de stockage. Tout espace restant sur le volume de stockage 0 et tout autre volume de stockage du nœud de stockage est utilisé exclusivement pour les données d'objet.



Pour assurer la redondance et protéger les métadonnées d'objet contre la perte, StorageGRID stocke trois copies des métadonnées de tous les objets du système sur chaque site. Les trois copies de métadonnées d'objet sont réparties de manière uniforme sur tous les nœuds de stockage de chaque site.

Lorsque vous attribuez de l'espace au volume 0 d'un nouveau nœud de stockage, vous devez vous assurer qu'il y a suffisamment d'espace pour la portion de ce nœud de toutes les métadonnées d'objet.

- Au moins, vous devez affecter au volume 0 au moins 4 To.

> Si vous n'utilisez qu'un seul volume de stockage pour un nœud de stockage et que vous attribuez 4 To ou moins au volume, le nœud de stockage peut entrer l'état de lecture seule au démarrage et ne stocker que les métadonnées de l'objet.

> Si vous attribuez moins de 500 Go au volume 0 (utilisation hors production uniquement), 10 % de la capacité du volume de stockage est réservée aux métadonnées.

- Si vous installez un nouveau système (StorageGRID 11.6 ou supérieur) et que chaque nœud de stockage dispose de 128 Go ou plus de RAM, attribuez 8 To ou plus au volume 0. L'utilisation d'une valeur plus grande pour le volume 0 peut augmenter l'espace autorisé pour les métadonnées sur chaque nœud de stockage.
- Lorsque vous configurez différents nœuds de stockage pour un site, utilisez le même paramètre pour le volume 0 si possible. Si un site contient des nœuds de stockage de différentes tailles, le nœud de stockage avec le plus petit volume 0 déterminera la capacité des métadonnées de ce site.

Pour plus d'informations, rendez-vous sur "Gérer le stockage des métadonnées d'objet".

Exigences de migration des conteneurs de nœuds

La fonction de migration de nœud vous permet de déplacer manuellement un nœud d'un hôte à un autre. En général, les deux hôtes se trouvent dans le même data Center physique.

La migration des nœuds vous permet d'effectuer la maintenance des hôtes physiques sans interrompre les opérations de la grille. Vous déplacez tous les nœuds StorageGRID, un par un, vers un autre hôte avant de mettre l'hôte physique hors ligne. La migration de nœuds ne demande qu'une interruption courte pour chaque nœud et ne doit en aucun cas affecter le fonctionnement ou la disponibilité des services de grid.

Pour utiliser la fonctionnalité de migration de nœuds StorageGRID, votre déploiement doit répondre à des exigences supplémentaires :

- Noms d'interface réseau cohérents entre les hôtes dans un seul data Center physique
- Stockage partagé pour les métadonnées StorageGRID et les volumes de référentiel d'objets accessibles par tous les hôtes dans un seul data Center physique. Vous pouvez, par exemple, utiliser des baies de stockage NetApp E-Series.

Si vous utilisez des hôtes virtuels et que la couche de l'hyperviseur sous-jacent prend en charge la migration des ordinateurs virtuels, vous pouvez utiliser cette fonctionnalité à la place de la fonctionnalité de migration des nœuds de StorageGRID. Dans ce cas, vous pouvez ignorer ces exigences supplémentaires.

Avant d'effectuer la migration ou la maintenance de l'hyperviseur, arrêtez les nœuds selon les besoins. Reportez-vous aux instructions pour "arrêt d'un nœud grid".

VMware Live migration non pris en charge

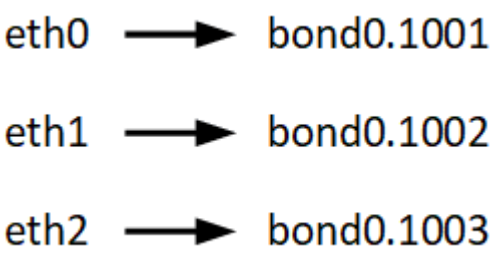
OpenStack Live migration et VMware Live vMotion entraînent un bond de l'horloge de la machine virtuelle et ne sont pas pris en charge pour les nœuds de grid, quel qu'en soit le type. Bien que les temps d'horloge rares et incorrects peuvent entraîner une perte de données ou des mises à jour de la configuration.

La migration à froid est prise en charge. Dans le cadre d'une migration à froid, vous devez arrêter les nœuds StorageGRID avant de les migrer entre les hôtes. Reportez-vous aux instructions pour "arrêt d'un nœud grid".

Noms d'interface réseau cohérents

Pour déplacer un nœud d'un hôte à un autre, le service d'hôte StorageGRID doit être certain que la connectivité réseau externe du nœud à son emplacement actuel peut être dupliquée au nouvel emplacement. Cette confiance est obtenue grâce à l'utilisation de noms d'interface réseau cohérents dans les hôtes.

Supposons, par exemple, que le nœud StorageGRID exécutant sur Host1 ait été configuré avec les mappages d'interface suivants :



Le côté gauche des flèches correspond aux interfaces traditionnelles affichées à partir d'un conteneur StorageGRID (c'est-à-dire, respectivement, les interfaces réseau Grid, Admin et client). Le côté droit des flèches correspond aux interfaces hôtes réelles fournissant ces réseaux, qui sont trois interfaces VLAN subordonnées à la même liaison d'interface physique.

Supposons maintenant que vous voulez migrer NodeA vers Host2. Si Host2 possède également des interfaces nommées bond0.1001, bond0.1002, et bond0.1003, le système permettra le déplacement, en supposant que

les interfaces nommées similaires fourniront la même connectivité sur Host2 que sur Host1. Si Host2 ne possède pas d'interfaces avec les mêmes noms, le déplacement ne sera pas autorisé.

Il existe de nombreuses façons d'obtenir un nom d'interface réseau cohérent sur plusieurs hôtes ; voir "Configurez le réseau hôte" pour quelques exemples.

Stockage partagé

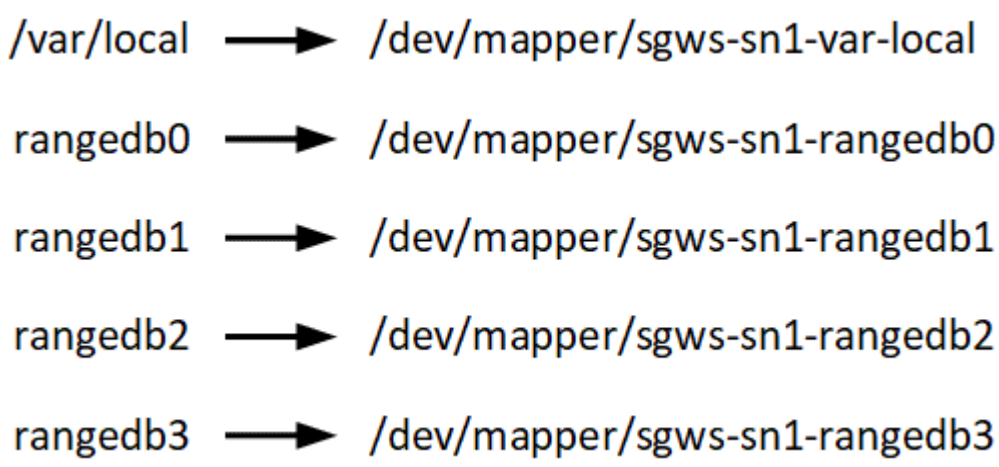
Pour réaliser des migrations de nœuds rapides et sans surcharge, la fonctionnalité de migration de nœuds StorageGRID ne déplace pas physiquement les données du nœud. La migration des nœuds se déroule comme une paire d'opérations d'exportation et d'importation :

Étapes

1. Lors de l'opération « exportation de nœud », une petite quantité de données d'état permanent est extraite du conteneur de nœud exécuté sur HostA et mise en cache sur le volume de données système de ce nœud. Ensuite, le conteneur de nœud sur HostA est déinstancié.
2. Lors de l'opération « importation de nœud », le conteneur de nœud sur l'hôte B qui utilise la même interface réseau et les mêmes mappages de stockage en bloc qui étaient en vigueur sur l'hôte est instancié. Les données de l'état persistant en cache sont ensuite insérées dans la nouvelle instance.

Compte tenu de ce mode de fonctionnement, toutes les données système et les volumes de stockage objet du nœud doivent être accessibles à la fois à HostA et HostB pour que la migration soit autorisée, et pour fonctionner. En outre, ils doivent avoir été mappés dans le noeud en utilisant des noms qui sont garantis pour faire référence aux mêmes LUN sur HostA et HostB.

L'exemple suivant montre une solution pour le mappage de périphériques de bloc pour un nœud de stockage StorageGRID, où les chemins d'accès multiples DM sont utilisés sur les hôtes et où le champ alias a été utilisé dans `/etc/multipath.conf` pour fournir des noms de périphériques de bloc cohérents et conviviaux disponibles sur tous les hôtes.



Outils de déploiement

Vous pouvez bénéficier de l'automatisation complète ou partielle de l'installation StorageGRID.

L'automatisation du déploiement peut être utile dans les cas suivants :

- Vous utilisez déjà un framework d'orchestration standard, comme Ansible, Puppet ou Chef, pour déployer et configurer des hôtes physiques ou virtuels.

- Vous prévoyez de déployer plusieurs instances StorageGRID.
- Vous déployez une instance StorageGRID vaste et complexe.

Le service hôte StorageGRID est installé par un package et piloté par des fichiers de configuration qui peuvent être créés de manière interactive lors d'une installation manuelle, ou préparés à l'avance (ou par programmation) pour permettre l'installation automatisée à l'aide des frameworks d'orchestration standard. StorageGRID propose des scripts Python en option permettant d'automatiser la configuration des appliances StorageGRID et l'ensemble du système StorageGRID (la « grille »). Vous pouvez utiliser ces scripts directement, ou bien les inspecter pour apprendre à utiliser l'API REST d'installation StorageGRID dans les outils de déploiement et de configuration de grid que vous développez vous-même.

Si vous souhaitez automatiser tout ou partie de votre déploiement StorageGRID, passez à l'étape suivant "Automatisez l'installation" avant de commencer le processus d'installation.

Préparer les hôtes (Ubuntu ou Debian)

Modification des paramètres à l'échelle de l'hôte lors de l'installation

Sur les systèmes bare Metal, StorageGRID apporte des modifications à l'ensemble de l'hôte `sysctl` paramètres.

Les modifications suivantes sont apportées :

```
# Recommended Cassandra setting: CASSANDRA-3563, CASSANDRA-13008, DataStax
documentation
vm.max_map_count = 1048575

# core file customization
# Note: for cores generated by binaries running inside containers, this
# path is interpreted relative to the container filesystem namespace.
# External cores will go nowhere, unless /var/local/core also exists on
# the host.
kernel.core_pattern = /var/local/core/%e.core.%p

# Set the kernel minimum free memory to the greater of the current value
or
# 512MiB if the host has 48GiB or less of RAM or 1.83GiB if the host has
more than 48GiB of RTAM
vm.min_free_kbytes = 524288

# Enforce current default swappiness value to ensure the VM system has
some
# flexibility to garbage collect behind anonymous mappings. Bump
watermark_scale_factor
# to help avoid OOM conditions in the kernel during memory allocation
bursts. Bump
# dirty_ratio to 90 because we explicitly fsync data that needs to be
persistent, and
```

```
# so do not require the dirty_ratio safety net. A low dirty_ratio combined
with a large
# working set (nr_active_pages) can cause us to enter synchronous I/O mode
unnecessarily,
# with deleterious effects on performance.
vm.swappiness = 60
vm.watermark_scale_factor = 200
vm.dirty_ratio = 90

# Turn off slow start after idle
net.ipv4.tcp_slow_start_after_idle = 0

# Tune TCP window settings to improve throughput
net.core.rmem_max = 8388608
net.core.wmem_max = 8388608
net.ipv4.tcp_rmem = 4096 524288 8388608
net.ipv4.tcp_wmem = 4096 262144 8388608
net.core.netdev_max_backlog = 2500

# Turn on MTU probing
net.ipv4.tcp_mtu_probing = 1

# Be more liberal with firewall connection tracking
net.ipv4.netfilter.ip_conntrack_tcp_be_liberal = 1

# Reduce TCP keepalive time to reasonable levels to terminate dead
connections
net.ipv4.tcp_keepalive_time = 270
net.ipv4.tcp_keepalive_probes = 3
net.ipv4.tcp_keepalive_intvl = 30

# Increase the ARP cache size to tolerate being in a /16 subnet
net.ipv4.neigh.default.gc_thresh1 = 8192
net.ipv4.neigh.default.gc_thresh2 = 32768
net.ipv4.neigh.default.gc_thresh3 = 65536
net.ipv6.neigh.default.gc_thresh1 = 8192
net.ipv6.neigh.default.gc_thresh2 = 32768
net.ipv6.neigh.default.gc_thresh3 = 65536

# Disable IP forwarding, we are not a router
net.ipv4.ip_forward = 0

# Follow security best practices for ignoring broadcast ping requests
net.ipv4.icmp_echo_ignore_broadcasts = 1

# Increase the pending connection and accept backlog to handle larger
connection bursts.
```

```
net.core.somaxconn=4096
net.ipv4.tcp_max_syn_backlog=4096
```

Installez Linux

Vous devez installer Linux sur tous les hôtes du grid. Utilisez le "Matrice d'interopérabilité NetApp (IMT)" pour obtenir une liste des versions prises en charge.

> Assurez-vous que votre système d'exploitation est mis à niveau vers le noyau Linux 4.15 ou supérieur.

Étapes

1. Installez Linux sur tous les hôtes de réseau physiques ou virtuels conformément aux instructions du distributeur ou à la procédure standard.

   > N'installez aucun environnement de bureau graphique. Lors de l'installation d'Ubuntu, vous devez sélectionner **utilitaires système standard**. La sélection de **OpenSSH Server** est recommandée pour activer l'accès ssh à vos hôtes Ubuntu. Toutes les autres options peuvent rester désactivées.

2. Assurez-vous que tous les hôtes ont accès aux référentiels de paquets Ubuntu ou Debian.
3. Si le swap est activé :
   a. Exécutez la commande suivante : `$ sudo swapoff --all`
   b. Supprimez toutes les entrées d'échange de `/etc/fstab` pour conserver les paramètres.

      > Si vous ne désactivez pas ces fichiers, les performances peuvent être considérablement réduites.

Comprendre l'installation du profil AppArmor

Si vous travaillez dans un environnement Ubuntu déployé automatiquement et que vous utilisez le système de contrôle d'accès obligatoire AppArmor, il est possible que les profils AppArmor associés aux paquets que vous installez sur le système de base soient bloqués par les paquets correspondants installés avec StorageGRID.

Par défaut, les profils AppArmor sont installés pour les packages que vous installez sur le système d'exploitation de base. Lorsque vous exécutez ces packages à partir du conteneur système StorageGRID, les profils AppArmor sont bloqués. Les paquets de base DHCP, MySQL, NTP et tcdump sont en conflit avec AppArmor, et d'autres paquets de base peuvent également entrer en conflit.

Vous avez le choix entre deux options pour gérer les profils AppArmor :

- Désactivez les profils individuels pour les packages installés sur le système de base qui se chevauchent avec les packages du conteneur système StorageGRID. Lorsque vous désactivez des profils individuels, une entrée apparaît dans les fichiers journaux StorageGRID indiquant qu'AppArmor est activé.

  Utiliser les commandes suivantes :

```
sudo ln -s /etc/apparmor.d/<profile.name> /etc/apparmor.d/disable/
sudo apparmor_parser -R /etc/apparmor.d/<profile.name>
```

Exemple:

```
sudo ln -s /etc/apparmor.d/bin.ping /etc/apparmor.d/disable/
sudo apparmor_parser -R /etc/apparmor.d/bin.ping
```

- Désactivez AppArmor. Pour Ubuntu 9.10 ou version ultérieure, suivez les instructions dans la communauté en ligne Ubuntu: "Désactivez AppArmor". Il est possible que la désactivation complète d'AppArmor ne soit pas possible sur les versions Ubuntu plus récentes.

  Une fois AppArmor désactivé, aucune entrée indiquant qu'AppArmor est activé ne s'affiche dans les fichiers journaux de StorageGRID.

Configurer le réseau hôte (Ubuntu ou Debian)

Une fois l'installation de Linux terminée sur vos hôtes, vous devrez peut-être procéder à une configuration supplémentaire pour préparer un ensemble d'interfaces réseau sur chaque hôte, adapté au mappage vers les nœuds StorageGRID que vous pourrez déployer ultérieurement.

Avant de commencer

- Vous avez passé en revue le "Instructions de mise en réseau d'StorageGRID".
- Vous avez passé en revue les informations sur "exigences de migration des conteneurs de nœuds".
- Si vous utilisez des hôtes virtuels, vous avez lu le Considérations et recommandations relatives au clonage d'adresses MAC avant de configurer le réseau hôte.

> Si vous utilisez des machines virtuelles en tant qu'hôtes, vous devez sélectionner VMXNET 3 comme carte réseau virtuelle. La carte réseau VMware E1000 a provoqué des problèmes de connectivité avec les conteneurs StorageGRID déployés sur certaines distributions de Linux.

Description de la tâche

Les nœuds du grid doivent être capables d'accéder au réseau Grid et, éventuellement, aux réseaux client et Admin. Vous fournissez cet accès en créant des mappages qui associent l'interface physique de l'hôte aux interfaces virtuelles de chaque nœud de la grille. Lors de la création d'interfaces hôtes, utilisez des noms conviviaux pour faciliter le déploiement sur tous les hôtes et pour activer la migration.

Une même interface peut être partagée entre l'hôte et un ou plusieurs nœuds. Par exemple, vous pouvez utiliser la même interface pour l'accès aux hôtes et l'accès au réseau d'administration de nœud afin de faciliter la maintenance des hôtes et des nœuds. Même si une même interface peut être partagée entre l'hôte et les nœuds individuels, toutes doivent avoir des adresses IP différentes. Les adresses IP ne peuvent pas être partagées entre les nœuds ou entre l'hôte et un nœud.

Vous pouvez utiliser la même interface réseau hôte pour fournir l'interface réseau Grid de tous les nœuds StorageGRID de l'hôte ; vous pouvez utiliser une interface réseau hôte différente pour chaque nœud ; ou effectuer un travail entre les deux. Cependant, vous ne fournissez généralement pas la même interface réseau

hôte que les interfaces réseau Grid et Admin pour un seul nœud, ou l'interface réseau Grid pour un nœud et l'interface réseau client pour un autre.

Vous pouvez effectuer cette tâche de plusieurs manières. Par exemple, si vos hôtes sont des machines virtuelles et que vous déployez un ou deux nœuds StorageGRID pour chaque hôte, vous pouvez créer le nombre correct d'interfaces réseau dans l'hyperviseur et utiliser un mappage 1-to-1. Si vous déployez plusieurs nœuds sur des hôtes bare Metal pour la production, vous pouvez bénéficier de la prise en charge du VLAN et du LACP de la pile réseau Linux pour la tolérance aux pannes et le partage de bande passante. Les sections suivantes présentent des approches détaillées pour ces deux exemples. Vous n'avez pas besoin d'utiliser l'un ou l'autre de ces exemples ; vous pouvez utiliser n'importe quelle approche qui répond à vos besoins.

> N'utilisez pas de périphérique de liaison ou de pont directement comme interface réseau du conteneur. Cela pourrait empêcher le démarrage de nœud causé par un problème de noyau avec l'utilisation de MACVLAN avec des périphériques de liaison et de pont dans l'espace de noms de conteneur. Utilisez plutôt un périphérique sans lien, tel qu'un VLAN ou une paire Ethernet virtuelle (Veth). Spécifiez ce périphérique comme interface réseau dans le fichier de configuration de nœud.

Considérations et recommandations relatives au clonage d'adresses MAC

Le clonage d'adresses MAC fait en sorte que le conteneur utilise l'adresse MAC de l'hôte et que l'hôte utilise l'adresse MAC d'une adresse que vous spécifiez ou d'une adresse générée de manière aléatoire. Vous devez utiliser le clonage d'adresses MAC pour éviter l'utilisation de configurations réseau en mode promiscuous.

Activation du clonage MAC

Dans certains environnements, la sécurité peut être améliorée grâce au clonage d'adresses MAC car il vous permet d'utiliser une carte réseau virtuelle dédiée pour le réseau d'administration, le réseau Grid et le réseau client. Le fait d'utiliser le conteneur l'adresse MAC du NIC dédié sur l'hôte vous permet d'éviter d'utiliser des configurations réseau en mode promiscuous.

> Le clonage d'adresses MAC est conçu pour être utilisé avec des installations de serveurs virtuels et peut ne pas fonctionner correctement avec toutes les configurations d'appliances physiques.

> Si un nœud ne démarre pas en raison d'une interface ciblée de clonage MAC occupée, il peut être nécessaire de définir le lien sur « down » avant de démarrer le nœud. En outre, il est possible que l'environnement virtuel puisse empêcher le clonage MAC sur une interface réseau pendant que la liaison est active. Si un nœud ne parvient pas à définir l'adresse MAC et démarre en raison d'une interface en cours d'activité, il est possible que le problème soit résolu en définissant le lien sur « arrêté » avant de démarrer le nœud.

Le clonage d'adresses MAC est désactivé par défaut et doit être défini par des clés de configuration de nœud. Vous devez l'activer lors de l'installation de StorageGRID.

Il existe une clé pour chaque réseau :

- `ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC`
- `GRID_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC`

- `CLIENT_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC`

Le fait de définir la clé sur « true » fait que le conteneur utilise l'adresse MAC de la carte réseau de l'hôte. En outre, l'hôte utilisera ensuite l'adresse MAC du réseau de conteneurs spécifié. Par défaut, l'adresse de conteneur est une adresse générée de manière aléatoire, mais si vous en avez défini une à l'aide de l' `_NETWORK_MAC` clé de configuration de nœud, cette adresse est utilisée à la place. L'hôte et le conteneur auront toujours des adresses MAC différentes.

> L'activation du clonage MAC sur un hôte virtuel sans activer également le mode promiscuous sur l'hyperviseur peut entraîner la mise en réseau des hôtes Linux à l'aide de l'interface de l'hôte à cesser de fonctionner.

Cas d'utilisation du clonage MAC

Il existe deux cas d'utilisation à prendre en compte pour le clonage MAC :

- Le clonage MAC n'est pas activé : lorsque l' `_CLONE_MAC` Clé dans le fichier de configuration du nœud n'est pas définie ou définie sur « false », l'hôte utilise le MAC de la carte réseau hôte et le conteneur aura un MAC généré par StorageGRID, à moins qu'un MAC ne soit spécifié dans le `_NETWORK_MAC` clé. Si une adresse est définie dans le `_NETWORK_MAC` clé, l'adresse du conteneur sera spécifiée dans le `_NETWORK_MAC` clé. Cette configuration de clés nécessite l'utilisation du mode promiscuous.
- Clonage MAC activé : lorsque le `_CLONE_MAC` La clé du fichier de configuration du nœud est définie sur « true », le conteneur utilise le MAC de la carte réseau de l'hôte et l'hôte utilise un MAC généré par StorageGRID, à moins qu'un MAC ne soit spécifié dans le `_NETWORK_MAC` clé. Si une adresse est définie dans le `_NETWORK_MAC` clé, l'hôte utilise l'adresse spécifiée au lieu d'une adresse générée. Dans cette configuration de clés, vous ne devez pas utiliser le mode promiscuous.

> Si vous ne souhaitez pas utiliser le clonage d'adresses MAC et que vous préférez autoriser toutes les interfaces à recevoir et transmettre des données pour les adresses MAC autres que celles attribuées par l'hyperviseur, Assurez-vous que les propriétés de sécurité au niveau du commutateur virtuel et du groupe de ports sont définies sur **Accept** pour le mode promiscuous, les modifications d'adresse MAC et les transmissions forgées. Les valeurs définies sur le commutateur virtuel peuvent être remplacées par les valeurs au niveau du groupe de ports, de sorte que les paramètres soient les mêmes aux deux endroits.

Pour activer le clonage MAC, reportez-vous à la section "instructions pour la création de fichiers de configuration de nœud".

Exemple de clonage MAC

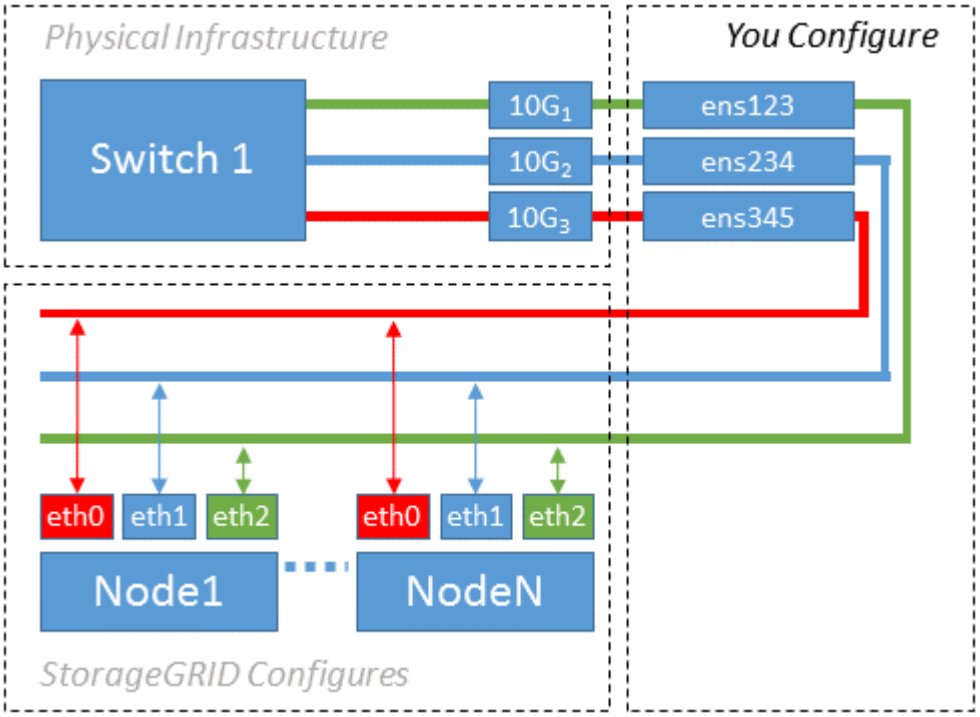
Exemple de clonage MAC activé avec un hôte dont l'adresse MAC est 11:22:33:44:55:66 pour le groupe d'interface 256 et les clés suivantes dans le fichier de configuration de nœud :

- `ADMIN_NETWORK_TARGET = ens256`
- `ADMIN_NETWORK_MAC = b2:9c:02:c2:27:10`
- `ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC = true`

Résultat : le MAC hôte pour en256 est b2:9c:02:c2:27:10 et le MAC réseau Admin est 11:22:33:44:55:66

Exemple 1 : mappage 1-à-1 sur des cartes réseau physiques ou virtuelles

L'exemple 1 décrit un mappage d'interface physique simple qui nécessite peu ou pas de configuration côté hôte.



Le système d'exploitation Linux crée automatiquement les interfaces enXYZ lors de l'installation ou du démarrage, ou lorsque les interfaces sont ajoutées à chaud. Aucune configuration n'est nécessaire autre que de s'assurer que les interfaces sont configurées pour s'activer automatiquement après le démarrage. Vous devez déterminer quel enXYZ correspond au réseau StorageGRID (grille, administrateur ou client) afin que vous puissiez fournir les mappages corrects plus tard dans le processus de configuration.

Notez que la figure présente plusieurs nœuds StorageGRID. Toutefois, vous utilisez généralement cette configuration pour les machines virtuelles à un seul nœud.

Si le commutateur 1 est un commutateur physique, vous devez configurer les ports connectés aux interfaces $10G_1$ à $10G_3$ pour le mode d'accès, et les placer sur les VLAN appropriés.

Exemple 2 : liaison LACP avec les VLAN

L'exemple 2 suppose que vous êtes familier avec les interfaces réseau de liaison et avec la création d'interfaces VLAN sur la distribution Linux que vous utilisez.

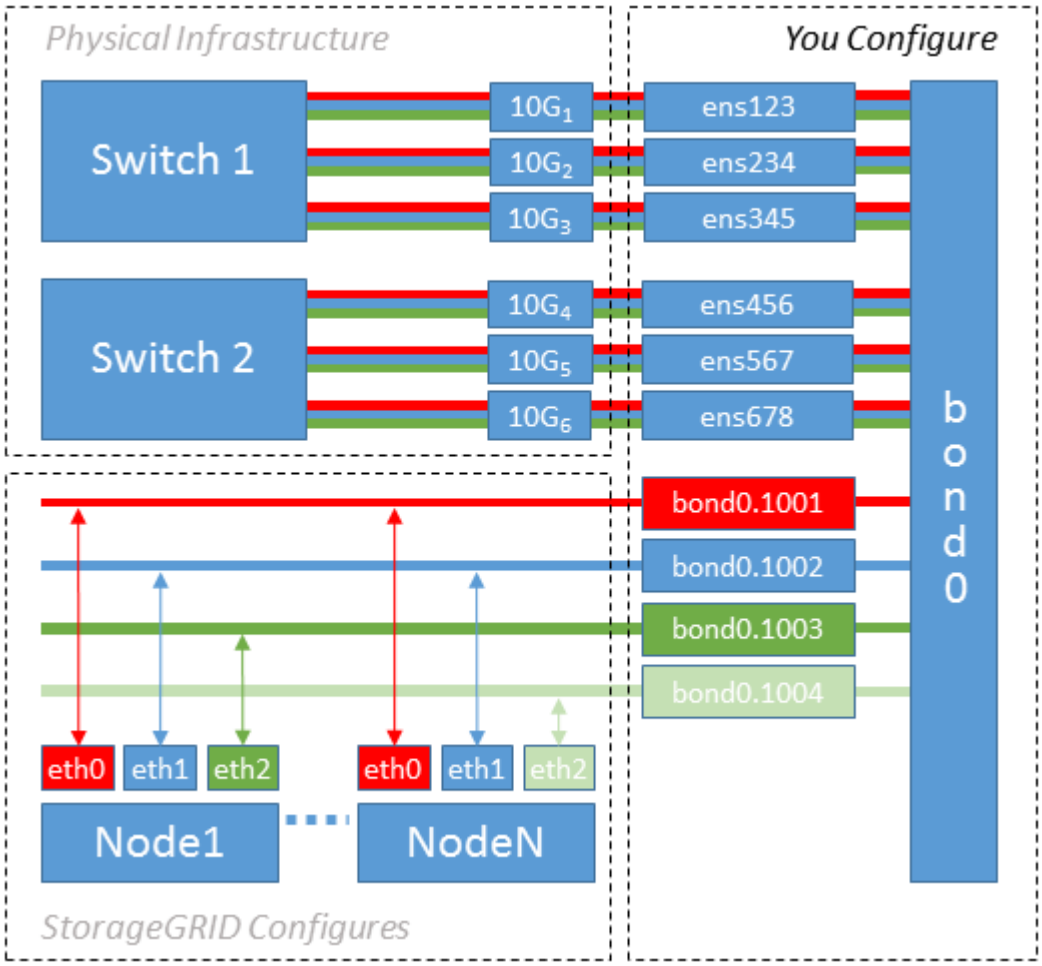
Description de la tâche

L'exemple 2 décrit un schéma générique, flexible et basé sur VLAN qui facilite le partage de toute la bande passante réseau disponible sur tous les nœuds d'un même hôte. Cet exemple s'applique tout particulièrement aux hôtes bare Metal.

Pour comprendre cet exemple, supposons que vous ayez trois sous-réseaux distincts pour les réseaux Grid, Admin et client dans chaque centre de données. Les sous-réseaux se trouvent sur des VLAN distincts (1001, 1002 et 1003) et sont présentés à l'hôte sur un port de jonction lié à LACP (bond0). Vous devez configurer trois interfaces VLAN sur la liaison : bond0.1001, bond0.1002 et bond0.1003.

Si vous avez besoin de VLAN et de sous-réseaux distincts pour les réseaux de nœuds sur le même hôte, vous

pouvez ajouter des interfaces VLAN sur la liaison et les mapper sur l'hôte (voir bond0,1004 dans l'illustration).



Étapes

1. Agréger toutes les interfaces réseau physiques qui seront utilisées pour la connectivité réseau StorageGRID en une seule liaison LACP.

   Utilisez le même nom pour le lien sur chaque hôte, par exemple bond0.

2. Créez des interfaces VLAN qui utilisent cette liaison comme périphérique physique associé," `using the standard VLAN interface naming convention `physdev-name.VLAN ID`.

   Notez que les étapes 1 et 2 nécessitent une configuration appropriée sur les commutateurs de périphérie qui terminent les autres extrémités des liaisons réseau. Les ports de switch de périphérie doivent également être agrégés dans un canal de port LACP, configuré en tant que jonction et autorisé à passer tous les VLAN requis.

   Des exemples de fichiers de configuration d'interface pour ce schéma de configuration réseau par hôte sont fournis.

Informations associées

"Exemple /etc/network/interfaces"

Vous devez allouer des volumes de stockage de blocs à chaque hôte.

Avant de commencer

Vous avez passé en revue les sujets suivants, qui fournissent les informations nécessaires pour accomplir cette tâche :

"Les besoins en matière de stockage et de performances"

"Exigences de migration des conteneurs de nœuds"

Description de la tâche

Lors de l'allocation de volumes de stockage en bloc (LUN) aux hôtes, utilisez les tables de la section « exigences de stockage » pour déterminer les éléments suivants :

- Nombre de volumes requis pour chaque hôte (en fonction du nombre et des types de nœuds à déployer sur cet hôte)
- Catégorie de stockage pour chaque volume (données système ou données objet)
- Taille de chaque volume

Lors du déploiement de nœuds StorageGRID sur l'hôte, vous utiliserez ces informations ainsi que le nom persistant attribué par Linux à chaque volume physique.

> Il n'est pas nécessaire de partitionner, de formater ou de monter ces volumes ; il vous suffit de vous assurer qu'ils sont visibles par les hôtes.

Évitez d'utiliser des fichiers de périphériques spéciaux « bruts » (`/dev/sdb`, par exemple) pendant que vous composez votre liste de noms de volumes. Ces fichiers peuvent être modifiés entre les redémarrages de l'hôte, ce qui peut affecter le fonctionnement correct du système. Si vous utilisez des LUN iSCSI et des chemins d'accès multiples de Device Mapper, envisagez d'utiliser des alias de chemins d'accès multiples dans le `/dev/mapper` Annuaire, en particulier si votre topologie SAN inclut des chemins réseau redondants vers le système de stockage partagé. Vous pouvez également utiliser les liens programmables créés par le système sous `/dev/disk/by-path/` pour les noms de périphériques persistants.

Par exemple :

```
ls -l
$ ls -l /dev/disk/by-path/
total 0
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:00:07.1-ata-2 -> ../../sr0
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:0:0 ->
../../sda
lrwxrwxrwx 1 root root 10 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:0:0-part1
-> ../../sda1
lrwxrwxrwx 1 root root 10 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:0:0-part2
-> ../../sda2
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:1:0 ->
../../sdb
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:2:0 ->
../../sdc
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:3:0 ->
../../sdd
```

Les résultats diffèrent pour chaque installation.

Attribuez des noms conviviaux à chacun de ces volumes de stockage en blocs afin de simplifier l'installation initiale du système StorageGRID et les procédures de maintenance à venir. Si vous utilisez le pilote multipath de device mapper pour obtenir un accès redondant aux volumes de stockage partagés, vous pouvez utiliser le `alias` dans votre `/etc/multipath.conf` fichier.

Par exemple :

```
multipaths {
     multipath {
          wwid 3600a09800059d6df00005df2573c2c30
          alias docker-storage-volume-hostA
     }
     multipath {
          wwid 3600a09800059d6df00005df3573c2c30
          alias sgws-adm1-var-local
     }
     multipath {
          wwid 3600a09800059d6df00005df4573c2c30
          alias sgws-adm1-audit-logs
     }
     multipath {
          wwid 3600a09800059d6df00005df5573c2c30
          alias sgws-adm1-tables
     }
     multipath {
          wwid 3600a09800059d6df00005df6573c2c30
          alias sgws-gw1-var-local
     }
     multipath {
          wwid 3600a09800059d6df00005df7573c2c30
          alias sgws-sn1-var-local
     }
     multipath {
          wwid 3600a09800059d6df00005df7573c2c30
          alias sgws-sn1-rangedb-0
     }
     …
```

Les alias apparaîtront alors en tant que périphériques de bloc dans le `/dev/mapper` répertoire sur l'hôte, ce qui vous permet de spécifier un nom convivial et facile à valider lorsqu'une opération de configuration ou de maintenance requiert la spécification d'un volume de stockage en bloc.

> Si vous configurez un stockage partagé pour prendre en charge la migration des nœuds StorageGRID et que vous utilisez le multipathing du mappeur de périphériques, vous pouvez créer et installer une connexion commune `/etc/multipath.conf` sur tous les hôtes en colocation. Il vous suffit d'utiliser un volume de stockage Docker différent sur chaque hôte. L'utilisation des alias et l'inclusion du nom d'hôte cible dans l'alias de chaque LUN de volume de stockage Docker rendent cela facile à mémoriser et est recommandé.

Informations associées

"Les besoins en matière de stockage et de performances"

"Exigences de migration des conteneurs de nœuds"

Configurer le volume de stockage Docker

Avant d'installer Docker, il se peut que vous deviez formater le volume de stockage Docker et le monter sur `/var/lib/docker`.

Description de la tâche

Vous pouvez ignorer ces étapes si vous prévoyez d'utiliser le stockage local pour le volume de stockage Docker et disposer d'un espace suffisant sur la partition hôte contenant `/var/lib`.

Étapes

1. Créez un système de fichiers sur le volume de stockage Docker :

```
sudo mkfs.ext4 docker-storage-volume-device
```

2. Montez le volume de stockage Docker :

```
sudo mkdir -p /var/lib/docker
sudo mount docker-storage-volume-device /var/lib/docker
```

3. Ajoutez une entrée pour docker-Storage-volume-device au fichier /etc/fstab.

   Cette étape permet de s'assurer que le volume de stockage se réajuste automatiquement après le redémarrage de l'hôte.

Installez Docker

Le système StorageGRID s'exécute sous Linux comme un ensemble de conteneurs Docker. Avant de pouvoir installer StorageGRID, vous devez installer Docker.

Étapes

1. Installez Docker en suivant les instructions de votre distribution Linux.

   Si Docker n'est pas inclus dans votre distribution Linux, vous pouvez le télécharger sur le site Web de Docker.

2. Assurez-vous que Docker a été activé et démarré en exécutant les deux commandes suivantes :

```
sudo systemctl enable docker
```

```
sudo systemctl start docker
```

3. Vérifiez que vous avez installé la version attendue de Docker en saisissant les éléments suivants :

```
sudo docker version
```

Les versions client et serveur doivent être 1.11.0 ou supérieures.

Informations associées

"Configurer le stockage de l'hôte"

Installez les services d'hôte StorageGRID

Vous utilisez le package StorageGRID DEB pour installer les services hôte StorageGRID.

Description de la tâche

Ces instructions décrivent comment installer les services hôte à partir des packages DEB. Vous pouvez également utiliser les métadonnées du référentiel APT incluses dans l'archive d'installation pour installer les packages DEB à distance. Consultez les instructions du référentiel APT pour votre système d'exploitation Linux.

Étapes

1. Copiez les packages StorageGRID DEB sur chacun de vos hôtes ou mettez-les à disposition sur un stockage partagé.

   Par exemple, placez-les dans le `/tmp` répertoire, afin de pouvoir utiliser la commande exemple à l'étape suivante.

2. Connectez-vous à chaque hôte en tant que root ou en utilisant un compte avec l'autorisation sudo, et exécutez les commandes suivantes.

   Vous devez installer le `images` le paquet en premier, et le `service` deuxième forfait. Si vous avez placé les packages dans un répertoire autre que `/tmp`, modifiez la commande pour refléter le chemin que vous avez utilisé.

```
sudo dpkg --install /tmp/storagegrid-webscale-images-version-SHA.deb
```

```
sudo dpkg --install /tmp/storagegrid-webscale-service-version-SHA.deb
```

> Python 2.7 doit déjà être installé avant que les modules StorageGRID ne puissent être installés. Le `sudo dpkg --install /tmp/storagegrid-webscale-images-version-SHA.deb` la commande échoue jusqu'à ce que vous l'ayez fait.

Déploiement de nœuds de grid virtuel (Ubuntu ou Debian)

Créez des fichiers de configuration de nœuds pour les déploiements Ubuntu ou Debian

Les fichiers de configuration des nœuds sont de petits fichiers texte qui fournissent les informations dont le service hôte StorageGRID a besoin pour démarrer un nœud et le connecter à des ressources de stockage bloc et réseau appropriées. Les fichiers de

configuration des nœuds sont utilisés pour les nœuds virtuels et ne sont pas utilisés pour les nœuds de l'appliance.

Où placer les fichiers de configuration des nœuds ?

Vous devez placer le fichier de configuration de chaque noeud StorageGRID dans le `/etc/storagegrid/nodes` répertoire de l'hôte sur lequel le nœud va s'exécuter. Par exemple, si vous prévoyez d'exécuter un nœud d'administration, un nœud de passerelle et un nœud de stockage sur HostA, vous devez placer trois fichiers de configuration de nœud dans `/etc/storagegrid/nodes` Sur HostA. Vous pouvez créer les fichiers de configuration directement sur chaque hôte à l'aide d'un éditeur de texte, tel que vim ou nano, ou les créer ailleurs et les déplacer vers chaque hôte.

Comment nommer les fichiers de configuration du nœud ?

Les noms des fichiers de configuration sont importants. Le format est `node-name.conf`, où `node-name` est un nom que vous attribuez au nœud. Ce nom apparaît dans le programme d'installation StorageGRID et sert aux opérations de maintenance de nœud, telles que la migration de nœud.

Les noms de nœud doivent respecter les règles suivantes :

- Doit être unique
- Doit commencer par une lettre
- Peut contenir les caractères A à Z et a à z
- Peut contenir les chiffres 0 à 9
- Peut contenir un ou plusieurs traits d'Union (-)
- Ne doit pas comporter plus de 32 caractères, sans le `.conf` extension

Tous les fichiers dans `/etc/storagegrid/nodes` qui ne suivent pas ces conventions de dénomination ne seront pas analysées par le service hôte.

Si une topologie multisite est planifiée pour votre grille, il se peut qu'un schéma de nommage de nœud type soit :

```
site-nodetype-nodenumber.conf
```

Par exemple, vous pouvez utiliser `dc1-adm1.conf` Pour le premier nœud d'administration dans Data Center 1, et `dc2-sn3.conf` Pour le troisième nœud de stockage dans Data Center 2. Toutefois, vous pouvez utiliser n'importe quel schéma, à condition que tous les noms de nœud suivent les règles d'attribution de nom.

Que contient un fichier de configuration de nœud ?

Les fichiers de configuration contiennent des paires clé/valeur, avec une clé et une valeur par ligne. Pour chaque paire clé/valeur, vous devez respecter les règles suivantes :

- La clé et la valeur doivent être séparées par un signe égal (=) et blanc facultatif.
- Les clés ne peuvent pas contenir d'espace.
- Les valeurs peuvent contenir des espaces intégrés.
- Tout espace blanc de début ou de fin est ignoré.

Certaines clés sont requises pour chaque nœud, tandis que d'autres sont optionnelles ou uniquement nécessaires pour certains types de nœuds.

Le tableau définit les valeurs acceptables pour toutes les clés prises en charge. Dans la colonne du milieu :

R: Requis + BP: Meilleures pratiques + O: Facultatif

Clé	R, BP OU O ?	Valeur
IP_ADMIN	PA	Adresse IPv4 du réseau Grid du nœud d'administration principal de la grille à laquelle ce nœud appartient. Utilisez la même valeur que celle spécifiée pour GRID_NETWORK_IP pour le nœud de grille avec NODE_TYPE = VM_Admin_Node et ADMIN_ROLE = Primary. Si vous omettez ce paramètre, le nœud tente de détecter un nœud d'administration principal à l'aide de mDNS. "Mode de détection des nœuds du grid sur le nœud d'administration principal" **Remarque** : cette valeur est ignorée et peut être interdite sur le noeud d'administration principal.
CONFIG_RÉSEAU_ADMIN	O	DHCP, STATIQUE OU DÉSACTIVÉ
ADMIN_NETWORK_ESL	O	Liste de sous-réseaux séparés par des virgules en notation CIDR à laquelle ce nœud doit communiquer à l'aide de la passerelle Admin Network. Exemple : `172.16.0.0/21,172.17.0.0/21`

PASSERELLE_RÉSEAU_ADMIN	O (**R**)	Adresse IPv4 de la passerelle réseau d'administration locale pour ce nœud. Doit être sur le sous-réseau défini par ADMIN_NETWORK_IP et ADMIN_NETWORK_MASK. Cette valeur est ignorée pour les réseaux configurés par DHCP.
		
		Remarque : ce paramètre est requis si ADMIN_NETWORK_ESL est spécifié.
		
		Exemples :
		
		`1.1.1.1`
		
		`10.224.4.81`

Clé	R, BP OU O ?	Valeur

IP_RÉSEAU_ADMIN	O	Adresse IPv4 de ce nœud sur le réseau d'administration. Cette clé n'est requise que lorsque ADMIN_NETWORK_CONFIG = STATIQUE ; ne la spécifiez pas pour d'autres valeurs.
		
		Exemples :
		
		`1.1.1.1`
		
		`10.224.4.81`

ADMIN_NETWORK_MAC	O	Adresse MAC de l'interface réseau Admin dans le conteneur. Ce champ est facultatif. Si elle est omise, une adresse MAC est générée automatiquement. Doit être composé de 6 paires de chiffres hexadécimaux séparés par deux-points. Exemple : `b2:9c:02:c2:27:10`

ADMIN_NETWORK_MASK	O	Masque de réseau IPv4 pour ce nœud, sur le réseau d'administration. Cette clé n'est requise que lorsque ADMIN_NETWORK_CONFIG = STATIQUE ; ne la spécifiez pas pour d'autres valeurs.
		
		Exemples :
		
		`255.255.255.0`
		
		`255.255.248.0`

Clé	R, BP OU O ?	Valeur

MTU_RÉSEAU_ADMIN	O	Unité de transmission maximale (MTU) pour ce nœud sur le réseau Admin. Ne spécifiez pas si ADMIN_NETWORK_CONFIG = DHCP. Si elle est spécifiée, la valeur doit être comprise entre 1280 et 9216. Si omis, 1500 est utilisé.
		
		Si vous souhaitez utiliser des trames jumbo, définissez la valeur MTU sur une valeur adaptée aux trames jumbo, comme 9000. Sinon, conservez la valeur par défaut.
		
		IMPORTANT : la valeur MTU du réseau doit correspondre à la valeur configurée sur le port du commutateur auquel le nœud est connecté. Dans le cas contraire, des problèmes de performances réseau ou une perte de paquets peuvent se produire.
		
		Exemples :
		
		`1500`
		
		`8192`

CIBLE_RÉSEAU_ADMIN	PA	Nom de l'unité hôte que vous utiliserez pour accéder au réseau d'administration par le nœud StorageGRID. Seuls les noms d'interface réseau sont pris en charge. En général, vous utilisez un nom d'interface différent de celui spécifié pour GRID_NETWORK_TARGET ou CLIENT_NETWORK_TARGET.
		
		Remarque : n'utilisez pas de périphérique de liaison ou de pont comme cible réseau. Configurez un VLAN (ou une autre interface virtuelle) sur le périphérique de liaison, ou utilisez un pont et une paire Ethernet virtuelle (veth).
		
		Meilleure pratique:spécifiez une valeur même si ce nœud ne possède pas d'adresse IP de réseau Admin initialement. Vous pouvez ensuite ajouter une adresse IP de réseau d'administration plus tard, sans avoir à reconfigurer le nœud sur l'hôte.
		
		Exemples :
		
		`bond0.1002`
		
		`ens256`

TYPE_CIBLE_RÉSEAU_ADMIN	O	Interface (Il s'agit de la seule valeur prise en charge.)

Clé	R, BP OU O ?	Valeur
ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC	PA	Vrai ou faux Définissez la clé sur « true » pour que le conteneur StorageGRID utilise l'adresse MAC de l'interface hôte cible sur le réseau d'administration. **Meilleure pratique:** dans les réseaux où le mode promiscuous serait nécessaire, utilisez la clé ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC. Pour plus de détails sur le clonage MAC : "Considérations et recommandations relatives au clonage d'adresses MAC (Red Hat Enterprise Linux ou CentOS)" "Considérations et recommandations relatives au clonage d'adresses MAC (Ubuntu ou Debian)"
RÔLE_ADMINISTRATEUR	**R**	Primaire ou non primaire Cette clé n'est requise que lorsque NODE_TYPE = VM_Admin_Node ; ne la spécifiez pas pour d'autres types de nœuds.

JOURNAUX_AUDIT_BLOC_PÉRIPHÉRIQUE	**R**	Chemin et nom du fichier spécial de périphérique de bloc ce nœud utilisera pour le stockage persistant des journaux d'audit. Cette clé n'est requise que pour les nœuds avec TYPE_NOEUD = VM_Admin_noeud ; ne la spécifiez pas pour d'autres types de noeuds.
		
		Exemples :
		
		`/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0`
		
		`/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd`
		
		`/dev/mapper/sgws-adm1-audit-logs`

Clé	R, BP OU O ?	Valeur

BLOCK_DEVICE_RANGEDB_000
 	
BLOCK_DEVICE_RANGEDB_001
 	
BLOCK_DEVICE_RANGEDB_002
 	
BLOCK_DEVICE_RANGEDB_003
 	
BLOCK_DEVICE_RANGEDB_004
 	
BLOCK_DEVICE_RANGEDB_005
 	
BLOCK_DEVICE_RANGEDB_006
 	
BLOCK_DEVICE_RANGEDB_007
 	
BLOCK_DEVICE_RANGEDB_008
 	
BLOCK_DEVICE_RANGEDB_009
 	
BLOCK_DEVICE_RANGEDB_010
 	
BLOCK_DEVICE_RANGEDB_011
 	
BLOCK_DEVICE_RANGEDB_012
 	
BLOCK_DEVICE_RANGEDB_013
 	
BLOCK_DEVICE_RANGEDB_014
 	
BLOCK_DEVICE_RANGEDB_015
	R	Chemin et nom du fichier spécial de périphérique de bloc ce nœud utilisera pour le stockage objet permanent. Cette clé n'est requise que pour les nœuds avec TYPE_NOEUD = VM_Storage_noeud ; ne la spécifiez pas pour d'autres types de noeuds.
		
		Seul LE BLOC_DEVICE_RANGEDB_000 est requis ; le reste est facultatif. Le dispositif de bloc spécifié pour BLOCK_DEVICE_RANGEDB_000 doit être d'au moins 4 To ; les autres peuvent être plus petits.
		
		Ne laissez pas d'espace. Si vous spécifiez BLOCK_DEVICE_RANGEDB_005, vous devez également spécifier BLOCK_DEVICE_RANGEDB_004.
		
		Remarque : pour la compatibilité avec les déploiements existants, les clés à deux chiffres sont prises en charge pour les nœuds mis à niveau.
		
		Exemples :
		
		`/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0`
		
		`/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd`
		
		`/dev/mapper/sgws-sn1-rangedb-000`

Clé	R, BP OU O ?	Valeur

BLOQUER_LES_TABLES_PÉRIPHÉRIQUES	**R**	Chemin et nom du fichier spécial de l'unité de bloc ce noeud sera utilisé pour le stockage persistant des tables de base de données. Cette clé n'est requise que pour les nœuds avec TYPE_NOEUD = VM_Admin_noeud ; ne la spécifiez pas pour d'autres types de noeuds.
		
		Exemples :
		
		`/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0`
		
		`/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd`
		
		`/dev/mapper/sgws-adm1-tables`

BLOCK_DEVICE_VAR_LOCAL	**R**	Chemin et nom du fichier spécial de périphérique de bloc ce nœud utilisera pour son stockage persistant /var/local.
		
		Exemples :
		
		`/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0`
		
		`/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd`
		
		`/dev/mapper/sgws-sn1-var-local`

CONFIG_RÉSEAU_CLIENT	O	DHCP, STATIQUE OU DÉSACTIVÉ

PASSERELLE_RÉSEAU_CLIENT	O	Adresse IPv4 de la passerelle réseau client locale pour ce nœud, qui doit se trouver sur le sous-réseau défini par CLIENT_NETWORK_IP et CLIENT_NETWORK_MASK. Cette valeur est ignorée pour les réseaux configurés par DHCP.
		
		Exemples :
		
		`1.1.1.1`
		
		`10.224.4.81`

Clé	R, BP OU O ?	Valeur

IP_RÉSEAU_CLIENT	O	Adresse IPv4 de ce nœud sur le réseau client. Cette clé n'est requise que lorsque CLIENT_NETWORK_CONFIG = STATIQUE ; ne la spécifiez pas pour d'autres valeurs.
		
		Exemples :
		
		`1.1.1.1`
		
		`10.224.4.81`

CLIENT_RÉSEAU_MAC	O	Adresse MAC de l'interface réseau client dans le conteneur. Ce champ est facultatif. Si elle est omise, une adresse MAC est générée automatiquement. Doit être composé de 6 paires de chiffres hexadécimaux séparés par deux-points. Exemple : `b2:9c:02:c2:27:20`

MASQUE_RÉSEAU_CLIENT	O	Masque de réseau IPv4 pour ce nœud sur le réseau client. Cette clé n'est requise que lorsque CLIENT_NETWORK_CONFIG = STATIQUE ; ne la spécifiez pas pour d'autres valeurs.
		
		Exemples :
		
		`255.255.255.0`
		
		`255.255.248.0`

Clé	R, BP OU O ?	Valeur

MTU_CLIENT_RÉSEAU	O	Unité de transmission maximale (MTU) pour ce nœud sur le réseau client. Ne spécifiez pas si CLIENT_NETWORK_CONFIG = DHCP. Si elle est spécifiée, la valeur doit être comprise entre 1280 et 9216. Si omis, 1500 est utilisé.
		
		Si vous souhaitez utiliser des trames jumbo, définissez la valeur MTU sur une valeur adaptée aux trames jumbo, comme 9000. Sinon, conservez la valeur par défaut.
		
		IMPORTANT : la valeur MTU du réseau doit correspondre à la valeur configurée sur le port du commutateur auquel le nœud est connecté. Dans le cas contraire, des problèmes de performances réseau ou une perte de paquets peuvent se produire.
		
		Exemples :
		
		`1500`
		
		`8192`

CIBLE_RÉSEAU_CLIENT	PA	Nom du périphérique hôte que vous utiliserez pour accéder au réseau client par le nœud StorageGRID. Seuls les noms d'interface réseau sont pris en charge. En général, vous utilisez un nom d'interface différent de celui spécifié pour GRID_NETWORK_TARGET ou ADMIN_NETWORK_TARGET.
		
		Remarque : n'utilisez pas de périphérique de liaison ou de pont comme cible réseau. Configurez un VLAN (ou une autre interface virtuelle) sur le périphérique de liaison, ou utilisez un pont et une paire Ethernet virtuelle (veth).
		
		Meilleure pratique : Indiquez une valeur même si ce nœud ne possède pas d'adresse IP de réseau client au départ. Vous pouvez ensuite ajouter une adresse IP du réseau client ultérieurement, sans avoir à reconfigurer le nœud sur l'hôte.
		
		Exemples :
		
		`bond0.1003`
		
		`ens423`

TYPE_CIBLE_RÉSEAU_CLIENT	O	Interface (Cette valeur est prise en charge uniquement.)

Clé	R, BP OU O ?	Valeur
CLIENT_RÉSEAU_CIBLE_TYPE_INTERFACE_CLONE_MAC	PA	Vrai ou faux Définissez la clé sur « true » pour que le conteneur StorageGRID utilise l'adresse MAC de l'interface cible hôte sur le réseau client. **Meilleure pratique:** dans les réseaux où le mode promiscuous serait nécessaire, utilisez plutôt la clé CLIENT_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC. Pour plus de détails sur le clonage MAC : "Considérations et recommandations relatives au clonage d'adresses MAC (Red Hat Enterprise Linux ou CentOS)" "Considérations et recommandations relatives au clonage d'adresses MAC (Ubuntu ou Debian)"
CONFIG_RÉSEAU_GRID	PA	STATIQUE ou DHCP (Statique par défaut si non spécifié.)
PASSERELLE_RÉSEAU_GRILLE	**R**	Adresse IPv4 de la passerelle réseau Grid locale pour ce nœud, qui doit se trouver sur le sous-réseau défini par GRID_NETWORK_IP et GRID_NETWORK_MASK. Cette valeur est ignorée pour les réseaux configurés par DHCP. Si le réseau Grid est un sous-réseau unique sans passerelle, utilisez soit l'adresse de passerelle standard pour le sous-réseau (X. Y.1), soit la valeur DE GRID_NETWORK_IP de ce nœud. Ces valeurs simplifient les extensions potentielles du réseau Grid.

IP_RÉSEAU_GRID	**R**	Adresse IPv4 de ce nœud sur le réseau Grid. Cette clé n'est requise que lorsque GRID_NETWORK_CONFIG = STATIQUE ; ne la spécifiez pas pour d'autres valeurs.
		
		Exemples :
		
		`1.1.1.1`
		
		`10.224.4.81`

Clé	R, BP OU O ?	Valeur
GRID_RÉSEAU_MAC	O	Adresse MAC de l'interface réseau de la grille dans le conteneur. Ce champ est facultatif. Si elle est omise, une adresse MAC est générée automatiquement. Doit être composé de 6 paires de chiffres hexadécimaux séparés par deux-points. Exemple : `b2:9c:02:c2:27:30`

GRID_NETWORK_MASK	O	Masque de réseau IPv4 pour ce nœud sur le réseau Grid. Cette clé n'est requise que lorsque GRID_NETWORK_CONFIG = STATIQUE ; ne la spécifiez pas pour d'autres valeurs.
		
		Exemples :
		
		`255.255.255.0`
		
		`255.255.248.0`

GRID_NETWORK_MTU	O	Unité de transmission maximale (MTU) pour ce nœud sur le réseau Grid. Ne spécifiez pas si GRID_NETWORK_CONFIG = DHCP. Si elle est spécifiée, la valeur doit être comprise entre 1280 et 9216. Si omis, 1500 est utilisé. Si vous souhaitez utiliser des trames jumbo, définissez la valeur MTU sur une valeur adaptée aux trames jumbo, comme 9000. Sinon, conservez la valeur par défaut. **IMPORTANT** : la valeur MTU du réseau doit correspondre à la valeur configurée sur le port du commutateur auquel le nœud est connecté. Dans le cas contraire, des problèmes de performances réseau ou une perte de paquets peuvent se produire. **IMPORTANT** : pour des performances réseau optimales, tous les nœuds doivent être configurés avec des valeurs MTU similaires sur leurs interfaces réseau Grid. L'alerte **Grid Network MTU mismatch** est déclenchée en cas de différence importante dans les paramètres MTU pour le réseau Grid sur les nœuds individuels. Les valeurs MTU ne doivent pas nécessairement être identiques pour tous les types de réseau. Exemples : 1500 8192

Clé	R, BP OU O ?	Valeur

CIBLE_RÉSEAU_GRILLE	**R**	Nom de l'unité hôte que vous utiliserez pour accéder au réseau Grid par le nœud StorageGRID. Seuls les noms d'interface réseau sont pris en charge. En général, vous utilisez un nom d'interface différent de celui spécifié pour ADMIN_NETWORK_TARGET ou CLIENT_NETWORK_TARGET.
		
		Remarque : n'utilisez pas de périphérique de liaison ou de pont comme cible réseau. Configurez un VLAN (ou une autre interface virtuelle) sur le périphérique de liaison, ou utilisez un pont et une paire Ethernet virtuelle (veth).
		
		Exemples :
		
		`bond0.1001`
		
		`ens192`

TYPE_CIBLE_RÉSEAU_GRILLE	O	Interface (Il s'agit de la seule valeur prise en charge.)
GRID_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC	**BP**	Vrai ou faux Définissez la valeur de la clé sur « true » pour que le conteneur StorageGRID utilise l'adresse MAC de l'interface cible de l'hôte sur le réseau de la grille. **Meilleure pratique:** dans les réseaux où le mode promiscuous serait nécessaire, utilisez la clé GRID_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC. Pour plus de détails sur le clonage MAC : "Considérations et recommandations relatives au clonage d'adresses MAC (Red Hat Enterprise Linux ou CentOS)" "Considérations et recommandations relatives au clonage d'adresses MAC (Ubuntu ou Debian)"

Clé	R, BP OU O ?	Valeur
INTERFACE_TARGET_nnnn	O	Nom et description facultative d'une interface supplémentaire que vous souhaitez ajouter à ce nœud. Vous pouvez ajouter plusieurs interfaces supplémentaires à chaque nœud. Pour *nnnn*, spécifiez un numéro unique pour chaque entrée INTERFACE_TARGET que vous ajoutez. Pour la valeur, spécifiez le nom de l'interface physique sur l'hôte bare-Metal. Ensuite, si vous le souhaitez, ajoutez une virgule et fournissez une description de l'interface, qui s'affiche sur la page des interfaces VLAN et sur la page des groupes haute disponibilité. Par exemple : `INTERFACE_TARGET_0001=ens256, Trunk` Si vous ajoutez une interface de jonction, vous devez configurer une interface VLAN dans StorageGRID. Si vous ajoutez une interface d'accès, vous pouvez l'ajouter directement à un groupe haute disponibilité ; il n'est pas nécessaire de configurer une interface VLAN.

RAM_MAXIMALE	O	Quantité maximale de RAM que ce nœud est autorisé à consommer. Si cette clé est omise, le nœud n'a aucune restriction de mémoire. Lorsque vous définissez ce champ pour un nœud de niveau production, indiquez une valeur inférieure d'au moins 24 Go et de 16 à 32 Go à la mémoire RAM totale du système.
		
		Remarque : la valeur de la RAM affecte l'espace réservé des métadonnées réelles d'un nœud. Voir la "Description de l'espace réservé aux métadonnées".
		
		Le format de ce champ est `<number><unit>`, où `<unit>` peut être `b`, `k`, `m`, ou `g`.
		
		Exemples :
		
		`24g`
		
		`38654705664b`
		
		Remarque : si vous souhaitez utiliser cette option, vous devez activer la prise en charge du noyau pour les groupes de mémoire.

TYPE_NŒUD	**R**	Type de nœud : VM_Admin_Node VM_Storage_Node VM_Archive_Node VM_API_Gateway

Clé	R, BP OU O ?	Valeur
SCHÉMA DE PORT	O	Permet de remapper tout port utilisé par un nœud pour les communications internes de nœud de grille ou les communications externes. Le remappage des ports est nécessaire si les stratégies de mise en réseau d'entreprise limitent un ou plusieurs ports utilisés par StorageGRID, comme décrit dans "Communications internes sur les nœuds de la grille" ou "Communications externes". **IMPORTANT** : ne mappez pas les ports que vous prévoyez d'utiliser pour configurer les noeuds finaux de l'équilibreur de charge. **Remarque** : si seul PORT_REMAPPAGE est défini, le mappage que vous spécifiez est utilisé pour les communications entrantes et sortantes. Si PORT_REMAPPAGE_INBOUND est également spécifié, PORT_REMAPPAGE s'applique uniquement aux communications sortantes. Le format utilisé est : `<network type>/<protocol>/<default port used by grid node>/<new port>`, où `<network type>` est un grid, un administrateur ou un client. le protocole est tcp ou udp. Par exemple : `PORT_REMAP = client/tcp/18082/443`
PORT_REMAPPAGE_ENTRANT	O	Mappe de nouveau les communications entrantes sur le port spécifié. Si vous spécifiez PORT_REMAP_INBOUND mais que vous ne spécifiez pas de valeur pour PORT_REMAP, les communications sortantes pour le port sont inchangées. **IMPORTANT** : ne mappez pas les ports que vous prévoyez d'utiliser pour configurer les noeuds finaux de l'équilibreur de charge. Le format utilisé est : `<network type>/<protocol:>/<remapped port >/<default port used by grid node>`, où `<network type>` est un grid, un administrateur ou un client. le protocole est tcp ou udp. Par exemple : `PORT_REMAP_INBOUND = grid/tcp/3022/22`

Mode de détection des nœuds du grid sur le nœud d'administration principal

Les nœuds de grid communiquent avec le nœud d'administration principal pour la configuration et la gestion. Chaque nœud de la grille doit connaître l'adresse IP du nœud

d’administration principal sur le réseau Grid.

Pour vous assurer qu’un nœud de grille peut accéder au nœud d’administration principal, vous pouvez effectuer l’une des opérations suivantes lors du déploiement du nœud :

- Vous pouvez utiliser le paramètre ADMIN_IP pour saisir manuellement l’adresse IP du nœud d’administration principal.
- Vous pouvez omettre le paramètre ADMIN_IP pour que le nœud de la grille détecte automatiquement la valeur. La détection automatique est particulièrement utile lorsque le réseau Grid utilise DHCP pour attribuer l’adresse IP au nœud d’administration principal.

La découverte automatique du nœud d’administration principal s’effectue à l’aide d’un système de noms de domaine multicast (mDNS). Lors du premier démarrage du nœud d’administration principal, il publie son adresse IP à l’aide de mDNS. Les autres nœuds du même sous-réseau peuvent alors interroger l’adresse IP et l’acquérir automatiquement. Cependant, comme le trafic IP multicast n’est généralement pas routable entre les sous-réseaux, les nœuds des autres sous-réseaux ne peuvent pas acquérir directement l’adresse IP du nœud Admin principal.

Si vous utilisez la détection automatique :

- Vous devez inclure le paramètre ADMIN_IP pour au moins un nœud de grille sur les sous-réseaux auxquels le nœud d’administration principal n’est pas directement connecté. Ce nœud de grille publie ensuite l’adresse IP du nœud d’administration principal pour les autres nœuds du sous-réseau à détecter avec mDNS.
- Assurez-vous que votre infrastructure réseau prend en charge le trafic IP multicast dans un sous-réseau.

Exemple de fichiers de configuration de nœud

Vous pouvez utiliser les exemples de fichiers de configuration de nœud pour vous aider à configurer les fichiers de configuration de nœud pour votre système StorageGRID. Les exemples montrent les fichiers de configuration des nœuds pour tous les types de nœuds grid.

Pour la plupart des nœuds, vous pouvez ajouter des informations d’adressage réseau de l’administrateur et du client (IP, masque, passerelle, etc.) lorsque vous configurez la grille à l’aide de Grid Manager ou de l’API d’installation. L’exception est le nœud d’administration principal. Si vous souhaitez accéder à l’adresse IP réseau d’administration du nœud d’administration principal pour terminer la configuration de la grille (le réseau de grille n’étant pas routé, par exemple), vous devez configurer la connexion réseau d’administration du nœud d’administration principal dans son fichier de configuration de nœud. Ceci est illustré dans l’exemple.

Dans les exemples, la cible réseau client a été configurée comme une pratique recommandée, même si le réseau client est désactivé par défaut.

Exemple pour le nœud d’administration principal

Exemple de nom de fichier: `/etc/storagegrid/nodes/dc1-adm1.conf`

Exemple de contenu de fichier:

```
NODE_TYPE = VM_Admin_Node
ADMIN_ROLE = Primary
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-adm1-var-local
BLOCK_DEVICE_AUDIT_LOGS = /dev/mapper/dc1-adm1-audit-logs
BLOCK_DEVICE_TABLES = /dev/mapper/dc1-adm1-tables
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.2
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1

ADMIN_NETWORK_CONFIG = STATIC
ADMIN_NETWORK_IP = 192.168.100.2
ADMIN_NETWORK_MASK = 255.255.248.0
ADMIN_NETWORK_GATEWAY = 192.168.100.1
ADMIN_NETWORK_ESL = 192.168.100.0/21,172.16.0.0/21,172.17.0.0/21
```

Exemple de nœud de stockage

Exemple de nom de fichier: `/etc/storagegrid/nodes/dc1-sn1.conf`

Exemple de contenu de fichier:

```
NODE_TYPE = VM_Storage_Node
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-sn1-var-local
BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/dc1-sn1-rangedb-0
BLOCK_DEVICE_RANGEDB_01 = /dev/mapper/dc1-sn1-rangedb-1
BLOCK_DEVICE_RANGEDB_02 = /dev/mapper/dc1-sn1-rangedb-2
BLOCK_DEVICE_RANGEDB_03 = /dev/mapper/dc1-sn1-rangedb-3
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.3
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

Exemple de nœud d'archivage

Exemple de nom de fichier: `/etc/storagegrid/nodes/dc1-arc1.conf`

Exemple de contenu de fichier:

```
NODE_TYPE = VM_Archive_Node
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-arc1-var-local
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.4
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

Exemple pour le nœud de passerelle

Exemple de nom de fichier: `/etc/storagegrid/nodes/dc1-gw1.conf`

Exemple de contenu de fichier:

```
NODE_TYPE = VM_API_Gateway
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-gw1-var-local
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003
GRID_NETWORK_IP = 10.1.0.5
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

Exemple pour un nœud d'administration non primaire

Exemple de nom de fichier: `/etc/storagegrid/nodes/dc1-adm2.conf`

Exemple de contenu de fichier:

```
NODE_TYPE = VM_Admin_Node
ADMIN_ROLE = Non-Primary
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-adm2-var-local
BLOCK_DEVICE_AUDIT_LOGS = /dev/mapper/dc1-adm2-audit-logs
BLOCK_DEVICE_TABLES = /dev/mapper/dc1-adm2-tables
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.6
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

Validation de la configuration StorageGRID

Après avoir créé des fichiers de configuration dans `/etc/storagegrid/nodes` Pour chacun de vos nœuds StorageGRID, vous devez valider le contenu de ces fichiers.

Pour valider le contenu des fichiers de configuration, exécutez la commande suivante sur chaque hôte :

```
sudo storagegrid node validate all
```

Si les fichiers sont corrects, le résultat indique **TRANSMIS** pour chaque fichier de configuration, comme indiqué dans l'exemple.

```
Checking for misnamed node configuration files… PASSED
Checking configuration file for node dc1-adm1… PASSED
Checking configuration file for node dc1-gw1… PASSED
Checking configuration file for node dc1-sn1… PASSED
Checking configuration file for node dc1-sn2… PASSED
Checking configuration file for node dc1-sn3… PASSED
Checking for duplication of unique values between nodes… PASSED
```

Pour une installation automatisée, vous pouvez supprimer cette sortie à l'aide de la `-q` ou `--quiet` dans le `storagegrid` commande (par exemple, `storagegrid --quiet…`). Si vous supprimez la sortie, la commande aura une valeur de sortie non nulle si des avertissements ou des erreurs de configuration ont été détectés.

Si les fichiers de configuration sont incorrects, les problèmes sont affichés comme **AVERTISSEMENT** et **ERREUR**, comme indiqué dans l'exemple. Si des erreurs de configuration sont détectées, vous devez les corriger avant de poursuivre l'installation.

```
Checking for misnamed node configuration files…
  WARNING: ignoring /etc/storagegrid/nodes/dc1-adm1
  WARNING: ignoring /etc/storagegrid/nodes/dc1-sn2.conf.keep
  WARNING: ignoring /etc/storagegrid/nodes/my-file.txt
Checking configuration file for node dc1-adm1…
  ERROR: NODE_TYPE = VM_Foo_Node
         VM_Foo_Node is not a valid node type.  See *.conf.sample
  ERROR: ADMIN_ROLE = Foo
         Foo is not a valid admin role.  See *.conf.sample
  ERROR: BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-gw1-var-local
         /dev/mapper/sgws-gw1-var-local is not a valid block device
Checking configuration file for node dc1-gw1…
  ERROR: GRID_NETWORK_TARGET = bond0.1001
         bond0.1001 is not a valid interface.  See `ip link show`
  ERROR: GRID_NETWORK_IP = 10.1.3
         10.1.3 is not a valid IPv4 address
  ERROR: GRID_NETWORK_MASK = 255.248.255.0
         255.248.255.0 is not a valid IPv4 subnet mask
Checking configuration file for node dc1-sn1…
  ERROR: GRID_NETWORK_GATEWAY = 10.2.0.1
         10.2.0.1 is not on the local subnet
  ERROR: ADMIN_NETWORK_ESL = 192.168.100.0/21,172.16.0foo
         Could not parse subnet list
Checking configuration file for node dc1-sn2… PASSED
Checking configuration file for node dc1-sn3… PASSED
Checking for duplication of unique values between nodes…
  ERROR: GRID_NETWORK_IP = 10.1.0.4
         dc1-sn2 and dc1-sn3 have the same GRID_NETWORK_IP
  ERROR: BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-sn2-var-local
         dc1-sn2 and dc1-sn3 have the same BLOCK_DEVICE_VAR_LOCAL
  ERROR: BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/sgws-sn2-rangedb-0
         dc1-sn2 and dc1-sn3 have the same BLOCK_DEVICE_RANGEDB_00
```

Démarrez le service d'hôte StorageGRID

Pour démarrer vos nœuds StorageGRID et s'assurer qu'ils redémarrent après un redémarrage de l'hôte, vous devez activer et démarrer le service hôte StorageGRID.

Étapes

1. Exécutez les commandes suivantes sur chaque hôte :

```
sudo systemctl enable storagegrid
sudo systemctl start storagegrid
```

2. Exécutez la commande suivante pour vérifier que le déploiement se déroule :

```
sudo storagegrid node status node-name
```

3. Si un nœud renvoie le statut « Not running » ou « Ssured, », exécutez la commande suivante :

```
sudo storagegrid node start node-name
```

4. Si vous avez déjà activé et démarré le service hôte StorageGRID (ou si vous n'êtes pas sûr que le service a été activé et démarré), exécutez également la commande suivante :

```
sudo systemctl reload-or-restart storagegrid
```

Configurer la grille et l'installation complète (Ubuntu ou Debian)

Accédez au Grid Manager

Le gestionnaire de grille permet de définir toutes les informations nécessaires à la configuration du système StorageGRID.

Avant de commencer

Le nœud d'administration principal doit être déployé et avoir terminé la séquence de démarrage initiale.

Étapes

1. Ouvrez votre navigateur Web et accédez à l'une des adresses suivantes :

   `https://primary_admin_node_ip`

   `client_network_ip`

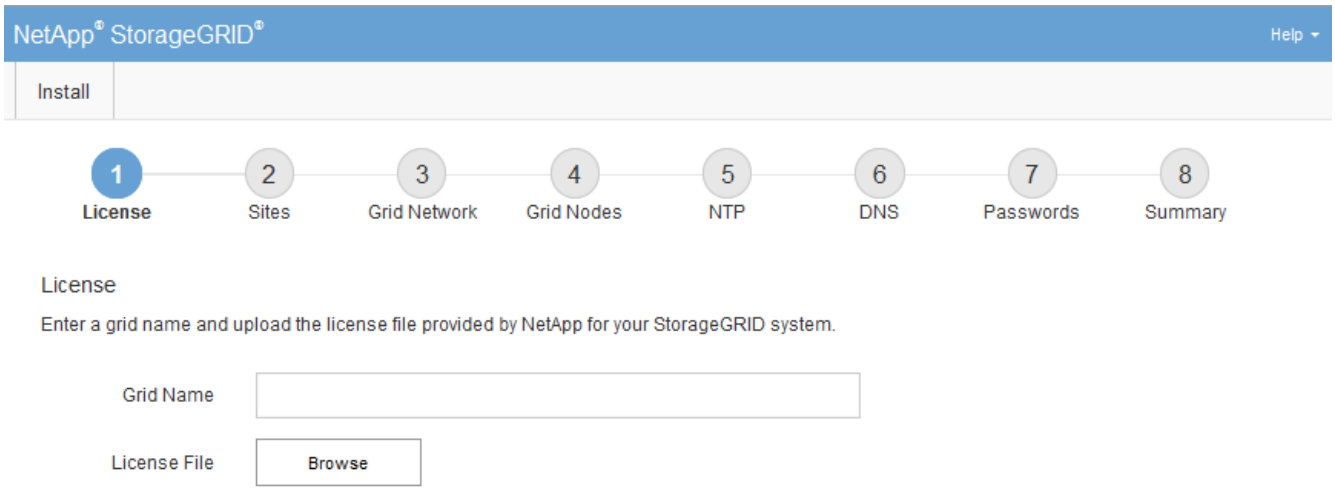
   Vous pouvez également accéder à Grid Manager sur le port 8443 :

   `https://primary_admin_node_ip:8443`

   > Vous pouvez utiliser l'adresse IP du noeud d'administration principal sur le réseau Grid ou sur le réseau Admin, en fonction de votre configuration réseau.

2. Sélectionnez **installer un système StorageGRID**.

   La page utilisée pour configurer un système StorageGRID s'affiche.



Spécifier les informations de licence StorageGRID

Vous devez indiquer le nom de votre système StorageGRID et télécharger le fichier de licence fourni par NetApp.

Étapes

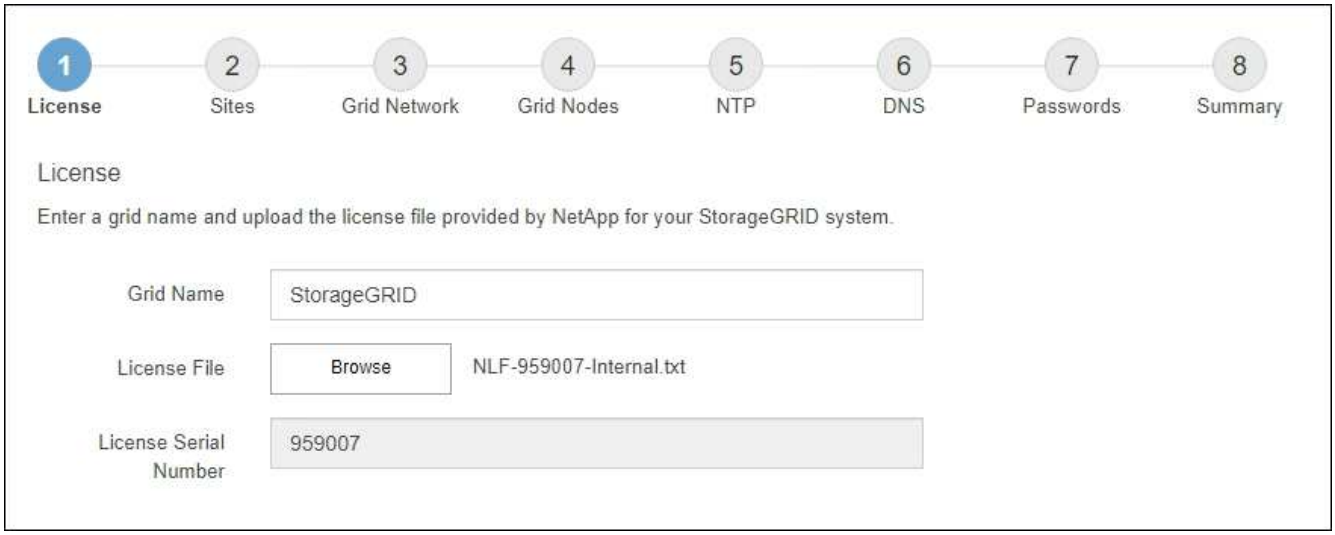
1. Sur la page Licence, entrez un nom significatif pour votre système StorageGRID dans le champ **Nom de la grille**.

   Après l'installation, le nom s'affiche en haut du menu nœuds.

2. Sélectionnez **Browse**, localisez le fichier de licence NetApp (`NLF-unique-id.txt`) Et sélectionnez **Ouvrir**.

   Le fichier de licence est validé et le numéro de série s'affiche.

   > L'archive d'installation de StorageGRID inclut une licence gratuite qui ne fournit aucun droit d'assistance pour le produit. Vous pouvez effectuer une mise à jour vers une licence offrant une assistance après l'installation.



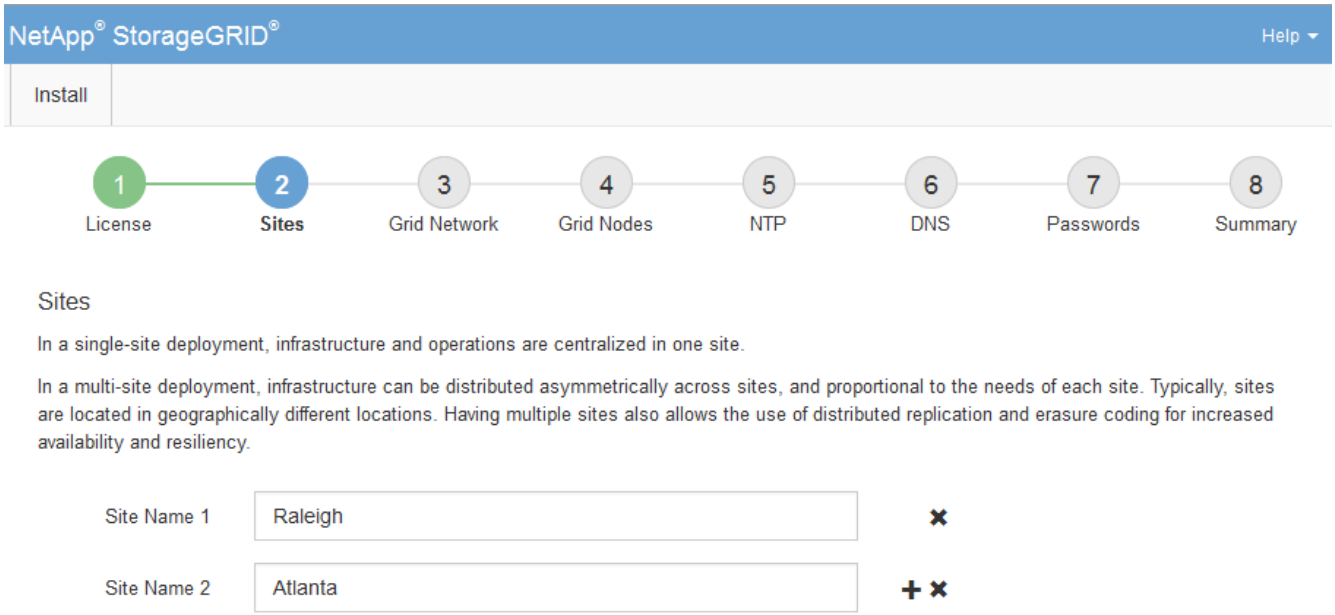
3. Sélectionnez **Suivant**.

Ajouter des sites

Vous devez créer au moins un site lorsque vous installez StorageGRID. Vous pouvez créer des sites supplémentaires pour augmenter la fiabilité et la capacité de stockage de votre système StorageGRID.

1. Sur la page sites, saisissez **Nom du site**.
2. Pour ajouter d'autres sites, cliquez sur le signe plus en regard de la dernière entrée du site et entrez le nom dans la zone de texte Nouveau **Nom du site**.

   Ajoutez autant de sites supplémentaires que nécessaire pour votre topologie de grille. Vous pouvez ajouter jusqu'à 16 sites.



3. Cliquez sur **Suivant**.

Spécifiez les sous-réseaux du réseau de la grille

Vous devez spécifier les sous-réseaux utilisés sur le réseau grille.

Description de la tâche

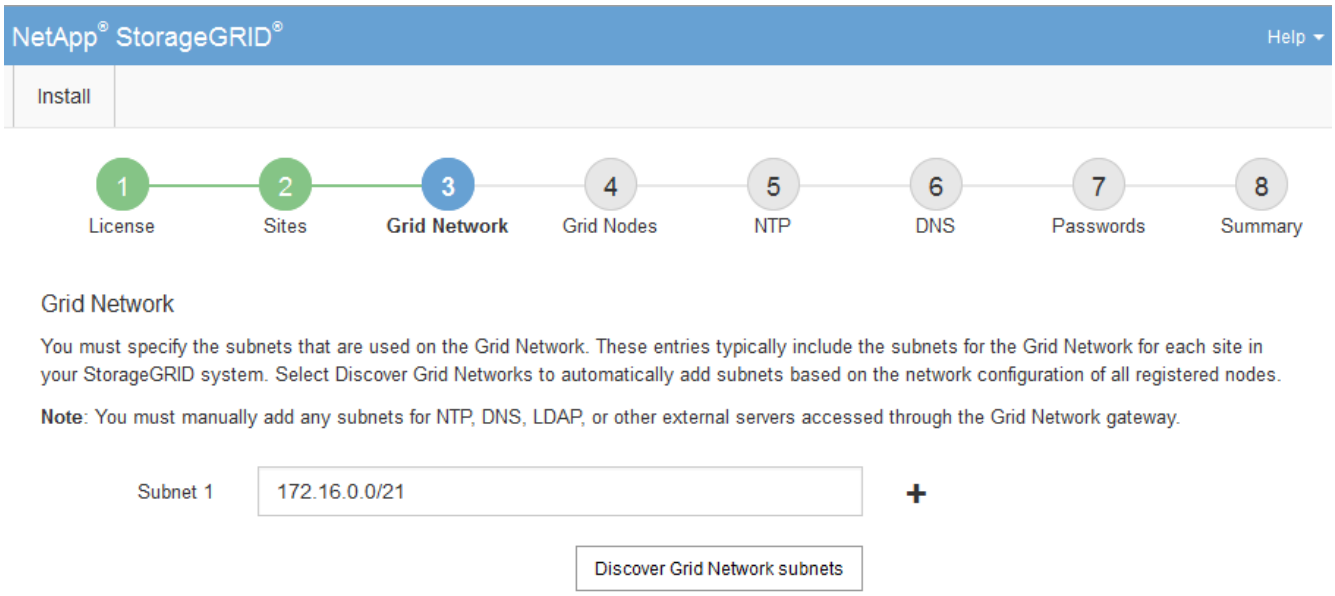
Les entrées de sous-réseau incluent les sous-réseaux du réseau de la grille pour chaque site de votre système StorageGRID, ainsi que tous les sous-réseaux devant être accessibles via le réseau de la grille.

Si vous avez plusieurs sous-réseaux de grille, la passerelle de réseau de grille est requise. Tous les sous-réseaux de la grille spécifiés doivent être accessibles via cette passerelle.

Étapes

1. Spécifiez l'adresse réseau CIDR pour au moins un réseau Grid dans la zone de texte **sous-réseau 1**.
2. Cliquez sur le signe plus à côté de la dernière entrée pour ajouter une entrée réseau supplémentaire.

   Si vous avez déjà déployé au moins un nœud, cliquez sur **détecter les sous-réseaux de réseaux de grille** pour remplir automatiquement la liste de sous-réseaux de réseau de grille avec les sous-réseaux signalés par les nœuds de grille enregistrés avec le gestionnaire de grille.



3. Cliquez sur **Suivant**.

Approuver les nœuds de la grille en attente

Vous devez approuver chaque nœud de la grille pour pouvoir rejoindre le système StorageGRID.

Avant de commencer

Vous avez déployé l'ensemble des nœuds grid virtuels et d'appliance StorageGRID.

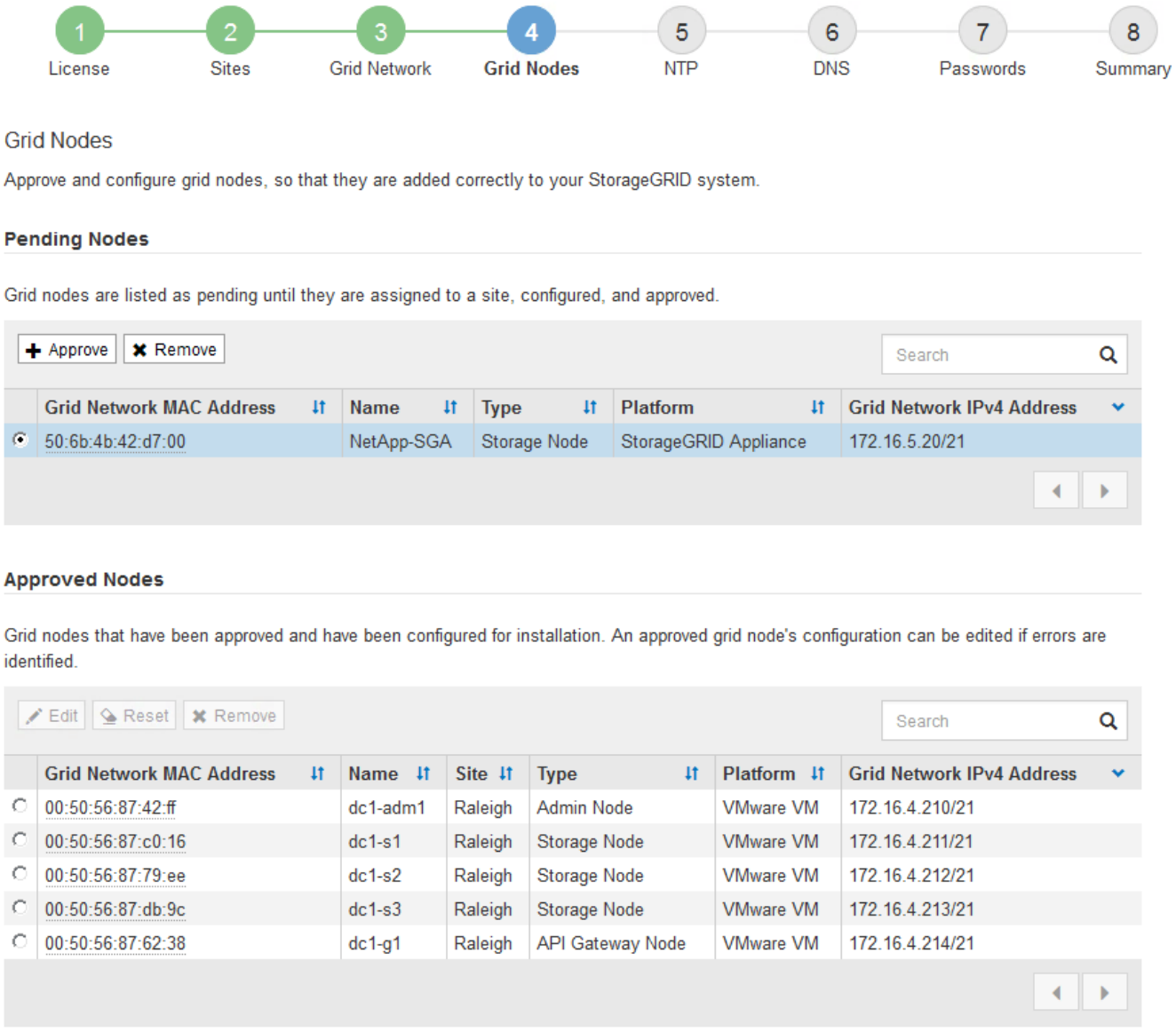
> Il est plus efficace d'effectuer une seule installation de tous les nœuds, au lieu d'installer certains nœuds maintenant et certains nœuds ultérieurement.

Étapes

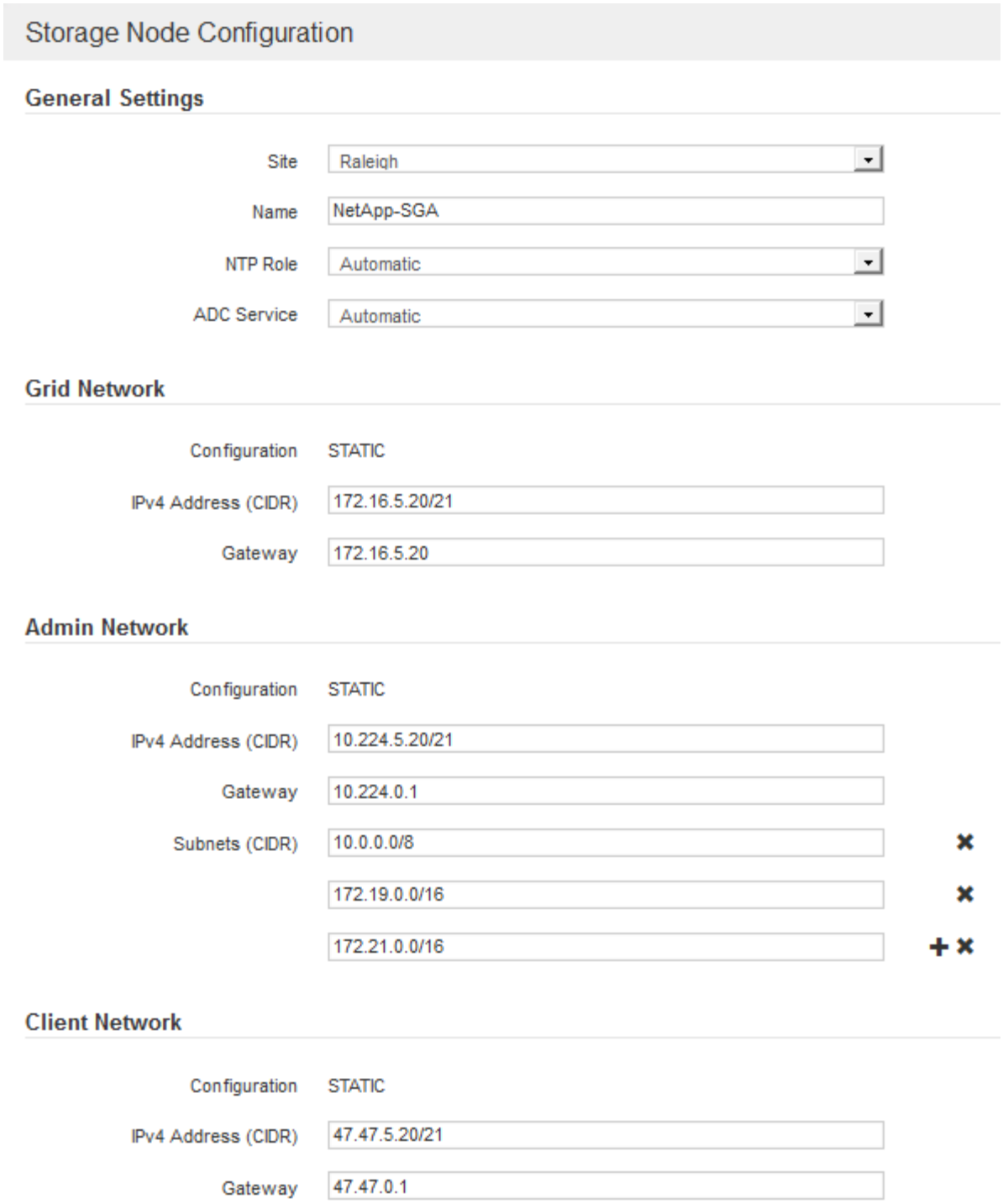
1. Consultez la liste nœuds en attente et vérifiez qu'elle affiche tous les nœuds de la grille que vous avez déployés.

   > Si un nœud de grid n'est pas inclus, vérifiez qu'il a été déployé correctement.

2. Sélectionnez le bouton radio à côté d'un noeud en attente que vous souhaitez approuver.



3. Cliquez sur **approuver**.
4. Dans Paramètres généraux, modifiez les paramètres des propriétés suivantes, si nécessaire :



- **Site** : le nom système du site pour ce noeud de grille.
- **Nom** : le nom du système pour le noeud. Le nom par défaut est le nom que vous avez spécifié lors de la configuration du nœud.

  Les noms de système sont requis pour les opérations StorageGRID internes et ne peuvent pas être modifiés une fois l'installation terminée. Cependant, au cours de cette étape du processus d'installation, vous pouvez modifier les noms de système selon vos besoins.

- **NTP role** : rôle NTP (Network Time Protocol) du noeud de la grille. Les options sont **automatique**, **primaire** et **client**. Si vous sélectionnez **automatique**, le rôle principal est attribué aux nœuds d'administration, aux nœuds de stockage avec services ADC, aux nœuds de passerelle et à tous les

nœuds de grille ayant des adresses IP non statiques. Le rôle client est attribué à tous les autres nœuds de la grille.

> Assurez-vous qu'au moins deux nœuds de chaque site peuvent accéder à au moins quatre sources NTP externes. Si un seul nœud d'un site peut atteindre les sources NTP, des problèmes de synchronisation surviennent en cas de panne de ce nœud. En outre, la désignation de deux nœuds par site en tant que sources NTP principales assure une synchronisation précise si un site est isolé du reste de la grille.

- **Service ADC** (nœuds de stockage uniquement) : sélectionnez **automatique** pour permettre au système de déterminer si le nœud requiert le service contrôleur de domaine administratif (ADC). Le service ADC conserve le suivi de l'emplacement et de la disponibilité des services de réseau. Au moins trois nœuds de stockage de chaque site doivent inclure le service ADC. Vous ne pouvez pas ajouter le service ADC à un nœud après son déploiement.

5. Dans le réseau de grille, modifiez les paramètres des propriétés suivantes si nécessaire :

   - **Adresse IPv4 (CIDR)** : adresse réseau CIDR pour l'interface Grid Network (eth0 dans le conteneur). Par exemple : 192.168.1.234/21
   - **Gateway** : la passerelle réseau Grid. Par exemple : 192.168.0.1

     La passerelle est requise en cas de sous-réseaux de grille multiples.

   > Si vous avez sélectionné DHCP pour la configuration du réseau Grid et que vous modifiez la valeur ici, la nouvelle valeur sera configurée en tant qu'adresse statique sur le nœud. Vous devez vous assurer que l'adresse IP résultante ne se trouve pas dans un pool d'adresses DHCP.

6. Si vous souhaitez configurer le réseau d'administration pour le nœud de la grille, ajoutez ou mettez à jour les paramètres de la section réseau d'administration si nécessaire.

   Entrez les sous-réseaux de destination des routes en dehors de cette interface dans la zone de texte **sous-réseaux (CIDR)**. En cas de sous-réseaux d'administration multiples, la passerelle d'administration est requise.

   > Si vous avez sélectionné DHCP pour la configuration du réseau d'administration et que vous modifiez la valeur ici, la nouvelle valeur sera configurée en tant qu'adresse statique sur le nœud. Vous devez vous assurer que l'adresse IP résultante ne se trouve pas dans un pool d'adresses DHCP.

   Appareils : pour une appliance StorageGRID, si le réseau d'administration n'a pas été configuré lors de l'installation initiale à l'aide du programme d'installation de l'appliance StorageGRID, il ne peut pas être configuré dans cette boîte de dialogue Gestionnaire de grille. Au lieu de cela, vous devez procéder comme suit :

   a. Redémarrez l'appliance : dans le programme d'installation de l'appliance, sélectionnez **Avancé** > **redémarrer**.

      Le redémarrage peut prendre plusieurs minutes.

   b. Sélectionnez **configurer réseau** > **Configuration lien** et activez les réseaux appropriés.
   c. Sélectionnez **configurer réseau** > **Configuration IP** et configurez les réseaux activés.

d. Revenez à la page d'accueil et cliquez sur **Démarrer l'installation**.

e. Dans le Gestionnaire de grille : si le nœud est répertorié dans le tableau nœuds approuvés, supprimez-le.

f. Supprimez le nœud du tableau nœuds en attente.

g. Attendez que le nœud réapparaisse dans la liste nœuds en attente.

h. Confirmez que vous pouvez configurer les réseaux appropriés. Elles doivent déjà être renseignées avec les informations que vous avez fournies sur la page Configuration IP du programme d'installation de l'appliance.

   Pour plus d'informations, reportez-vous au "Démarrage rapide pour l'installation du matériel" pour trouver les instructions relatives à votre appareil.

7. Si vous souhaitez configurer le réseau client pour le nœud de grille, ajoutez ou mettez à jour les paramètres dans la section réseau client si nécessaire. Si le réseau client est configuré, la passerelle est requise et devient la passerelle par défaut du noeud après l'installation.

   > ⓘ Si vous avez sélectionné DHCP pour la configuration du réseau client et que vous modifiez la valeur ici, la nouvelle valeur sera configurée en tant qu'adresse statique sur le nœud. Vous devez vous assurer que l'adresse IP résultante ne se trouve pas dans un pool d'adresses DHCP.

   Appareils : pour une appliance StorageGRID, si le réseau client n'a pas été configuré lors de l'installation initiale à l'aide du programme d'installation de l'appliance StorageGRID, il ne peut pas être configuré dans cette boîte de dialogue Gestionnaire de grille. Au lieu de cela, vous devez procéder comme suit :

   a. Redémarrez l'appliance : dans le programme d'installation de l'appliance, sélectionnez **Avancé** > **redémarrer**.

      Le redémarrage peut prendre plusieurs minutes.

   b. Sélectionnez **configurer réseau** > **Configuration lien** et activez les réseaux appropriés.

   c. Sélectionnez **configurer réseau** > **Configuration IP** et configurez les réseaux activés.

   d. Revenez à la page d'accueil et cliquez sur **Démarrer l'installation**.

   e. Dans le Gestionnaire de grille : si le nœud est répertorié dans le tableau nœuds approuvés, supprimez-le.

   f. Supprimez le nœud du tableau nœuds en attente.

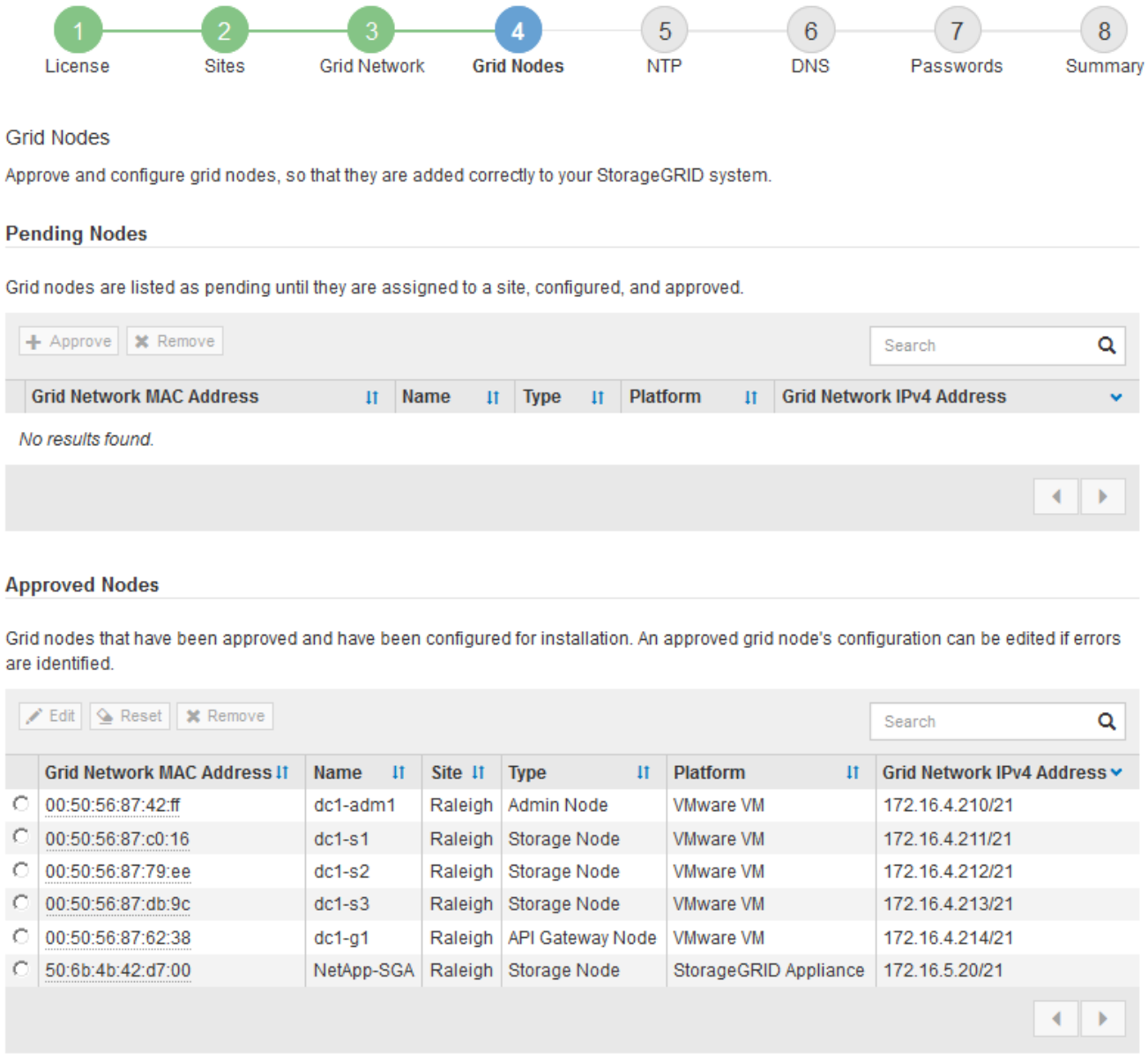
   g. Attendez que le nœud réapparaisse dans la liste nœuds en attente.

   h. Confirmez que vous pouvez configurer les réseaux appropriés. Elles doivent déjà être renseignées avec les informations que vous avez fournies sur la page Configuration IP du programme d'installation de l'appliance.

      Pour savoir comment installer les appliances StorageGRID, consultez le "Démarrage rapide pour l'installation du matériel" pour trouver les instructions relatives à votre appareil.

8. Cliquez sur **Enregistrer**.

   L'entrée de nœud de la grille passe à la liste nœuds approuvés.



9. Répétez ces étapes pour chaque nœud de grille en attente à approuver.

   Vous devez approuver tous les nœuds que vous souhaitez dans la grille. Cependant, vous pouvez revenir à cette page à tout moment avant de cliquer sur **installer** sur la page Résumé. Vous pouvez modifier les propriétés d'un nœud de grille approuvé en sélectionnant son bouton radio et en cliquant sur **Modifier**.

10. Lorsque vous avez terminé d'approuver les nœuds de la grille, cliquez sur **Suivant**.

Spécifiez les informations sur le serveur Network Time Protocol

Vous devez spécifier les informations de configuration du protocole NTP (Network Time Protocol) pour le système StorageGRID, de sorte que les opérations effectuées sur des serveurs distincts puissent rester synchronisées.

Description de la tâche

Vous devez indiquer des adresses IPv4 pour les serveurs NTP.

Vous devez indiquer des serveurs NTP externes. Les serveurs NTP spécifiés doivent utiliser le protocole NTP.

Vous devez spécifier quatre références de serveur NTP de Stratum 3 ou supérieur pour éviter les problèmes de dérive du temps.

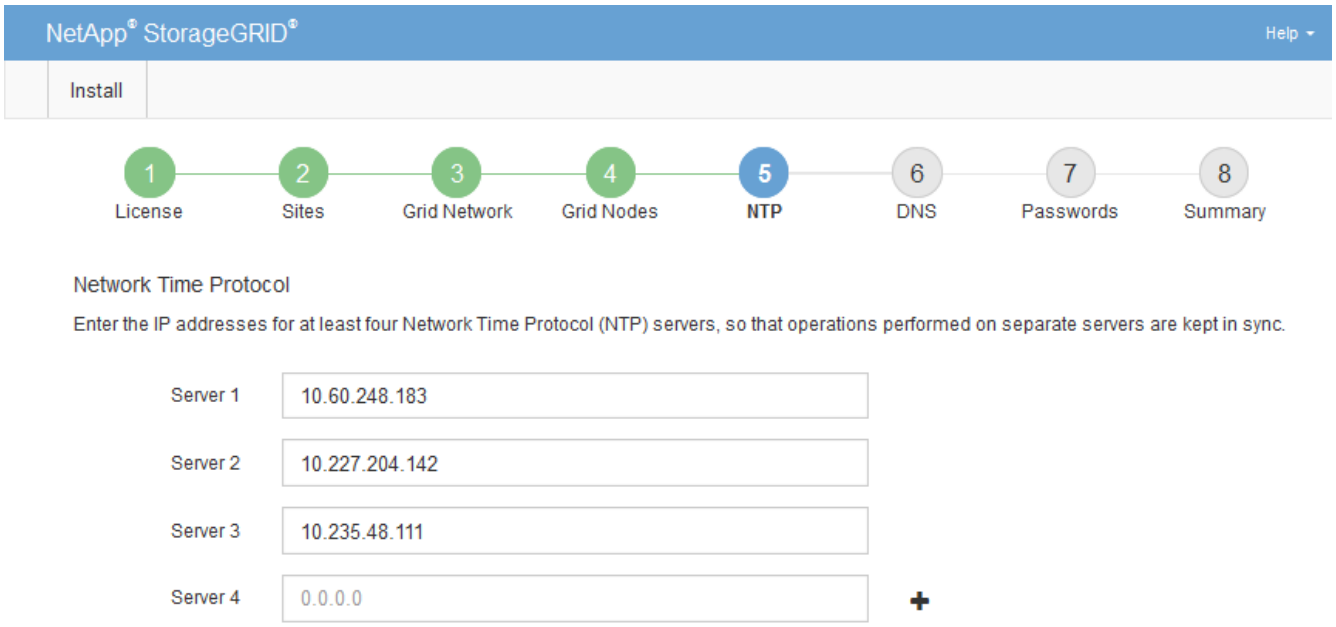
> Lorsque vous spécifiez la source NTP externe pour une installation StorageGRID de niveau production, n'utilisez pas le service heure Windows (W32Time) sur une version de Windows antérieure à Windows Server 2016. Le service de temps des versions antérieures de Windows n'est pas suffisamment précis et n'est pas pris en charge par Microsoft pour une utilisation dans des environnements à haute précision, tels que StorageGRID.
>
> "Limite de prise en charge pour configurer le service de temps Windows pour des environnements de haute précision"

Les serveurs NTP externes sont utilisés par les nœuds auxquels vous avez précédemment attribué des rôles NTP primaires.

> Assurez-vous qu'au moins deux nœuds de chaque site peuvent accéder à au moins quatre sources NTP externes. Si un seul nœud d'un site peut atteindre les sources NTP, des problèmes de synchronisation surviennent en cas de panne de ce nœud. En outre, la désignation de deux nœuds par site en tant que sources NTP principales assure une synchronisation précise si un site est isolé du reste de la grille.

Étapes

1. Spécifiez les adresses IPv4 pour au moins quatre serveurs NTP dans les zones de texte **Server 1** à **Server 4**.
2. Si nécessaire, sélectionnez le signe plus en regard de la dernière entrée pour ajouter des entrées de serveur supplémentaires.



3. Sélectionnez **Suivant**.

Informations associées

"Instructions de mise en réseau"

Spécifiez les informations du serveur DNS

Vous devez spécifier des informations DNS pour votre système StorageGRID afin de pouvoir accéder aux serveurs externes en utilisant des noms d'hôte au lieu d'adresses IP.

Description de la tâche

Spécification "Informations sur le serveur DNS" Vous permet d'utiliser des noms d'hôte de nom de domaine complet (FQDN) plutôt que des adresses IP pour les notifications par e-mail et AutoSupport.

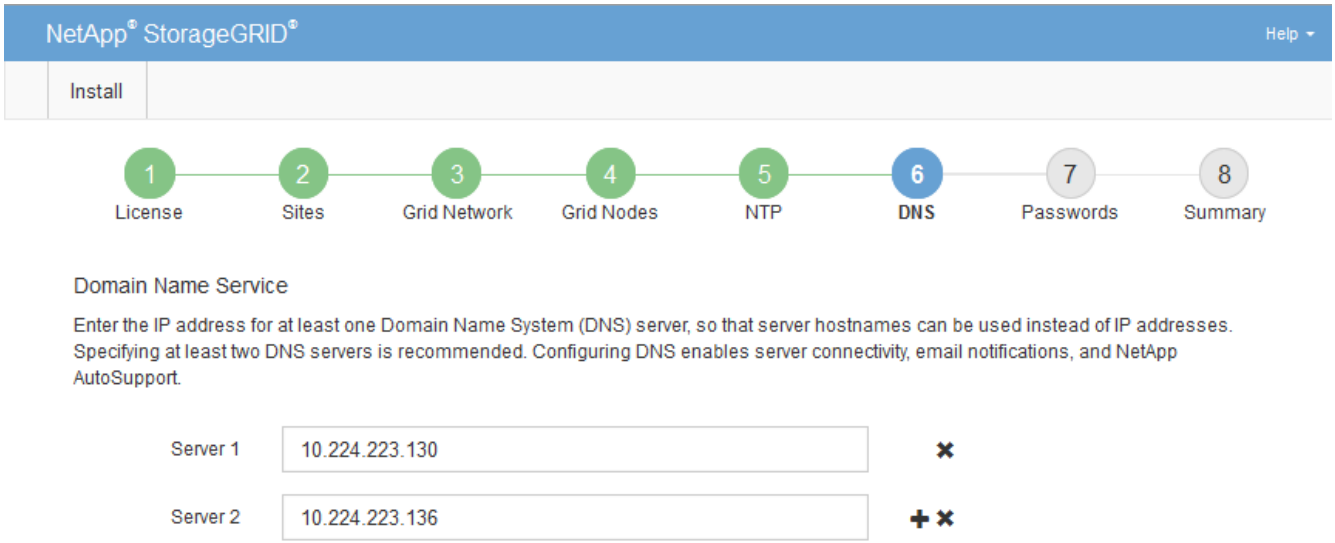
Pour garantir un fonctionnement correct, spécifiez deux ou trois serveurs DNS. Si vous spécifiez plus de trois, il est possible que seulement trois soient utilisés en raison des limitations connues du système d'exploitation sur certaines plates-formes. Si vous avez des restrictions de routage dans votre environnement, vous pouvez le faire "Personnaliser la liste des serveurs DNS" Pour les nœuds individuels (généralement tous les nœuds d'un site) d'utiliser un ensemble différent de trois serveurs DNS.

Si possible, utilisez des serveurs DNS auxquels chaque site peut accéder localement pour vous assurer qu'un site isdébarqué peut résoudre les FQDN pour les destinations externes.

Si les informations du serveur DNS sont omises ou mal configurées, une alarme DNST est déclenchée sur le service SSM de chaque nœud de la grille. L'alarme s'efface lorsque le DNS est configuré correctement et que les nouvelles informations sur le serveur ont atteint tous les nœuds de la grille.

Étapes

1. Spécifiez l'adresse IPv4 pour au moins un serveur DNS dans la zone de texte **Server 1**.
2. Si nécessaire, sélectionnez le signe plus en regard de la dernière entrée pour ajouter des entrées de serveur supplémentaires.



   La meilleure pratique consiste à spécifier au moins deux serveurs DNS. Vous pouvez indiquer jusqu'à six serveurs DNS.

3. Sélectionnez **Suivant**.

Spécifiez les mots de passe système StorageGRID

Dans le cadre de l'installation de votre système StorageGRID, vous devez saisir les mots de passe à utiliser pour sécuriser votre système et effectuer des tâches de maintenance.

Description de la tâche

Utilisez la page installer des mots de passe pour spécifier le mot de passe de provisionnement et le mot de passe utilisateur root de la gestion de grille.

- La phrase secrète de provisionnement est utilisée comme clé de chiffrement et n'est pas stockée par le système StorageGRID.
- Vous devez disposer du mot de passe de provisionnement pour les procédures d'installation, d'extension et de maintenance, y compris le téléchargement du progiciel de restauration. Il est donc important de stocker la phrase secrète de provisionnement dans un emplacement sécurisé.
- Vous pouvez modifier la phrase de passe de provisionnement à partir de Grid Manager si vous en avez la version actuelle.
- Le mot de passe de l'utilisateur root de la gestion de grille peut être modifié à l'aide de Grid Manager.
- La console de ligne de commande générée de manière aléatoire et les mots de passe SSH sont stockés dans le `Passwords.txt` Fichier dans le progiciel de restauration.

Étapes

1. Dans **Provisioning Passphrase**, saisissez la clé de passe de provisionnement qui sera requise pour modifier la topologie de la grille de votre système StorageGRID.

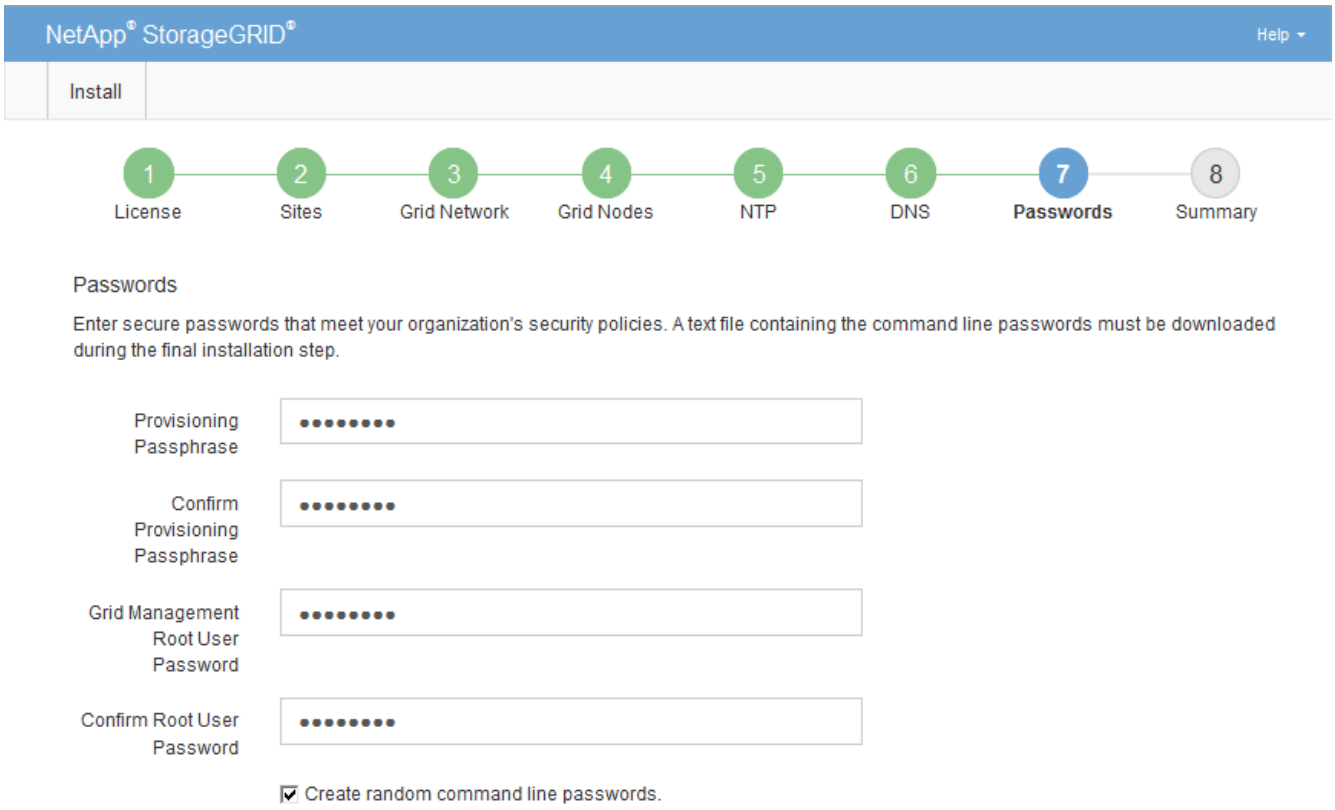
   Stockez la phrase secrète de provisionnement dans un endroit sécurisé.

   > Si une fois l'installation terminée et que vous souhaitez modifier ultérieurement le mot de passe de provisionnement, vous pouvez utiliser le Gestionnaire de grille. Sélectionnez **CONFIGURATION** > **contrôle d'accès**> **mots de passe de grille**.

2. Dans **Confirm Provisioning Passphrase**, saisissez à nouveau la phrase de passe de provisionnement pour la confirmer.
3. Dans **Grid Management Root User Password**, entrez le mot de passe à utiliser pour accéder au gestionnaire de grille en tant qu'utilisateur « root ».

   Stockez le mot de passe en lieu sûr.

4. Dans **confirmer le mot de passe de l'utilisateur racine**, entrez à nouveau le mot de passe de Grid Manager pour le confirmer.



5. Si vous installez une grille à des fins de démonstration de faisabilité ou de démonstration, désactivez éventuellement la case **Créer des mots de passe de ligne de commande aléatoires**.

   Pour les déploiements en production, des mots de passe aléatoires doivent toujours être utilisés pour des raisons de sécurité. Désactivez **Créez des mots de passe de ligne de commande aléatoires** uniquement pour les grilles de démonstration si vous souhaitez utiliser des mots de passe par défaut pour accéder aux nœuds de grille à partir de la ligne de commande à l'aide du compte "`root'" ou "'admin".

   > Vous êtes invité à télécharger le fichier du progiciel de récupération (`sgws-recovery-package-id-revision.zip`) Après avoir cliqué sur **installer** sur la page Résumé. Vous devez "téléchargez ce fichier" pour terminer l'installation. Les mots de passe requis pour accéder au système sont stockés dans le `Passwords.txt` Fichier, contenu dans le fichier du progiciel de récupération.

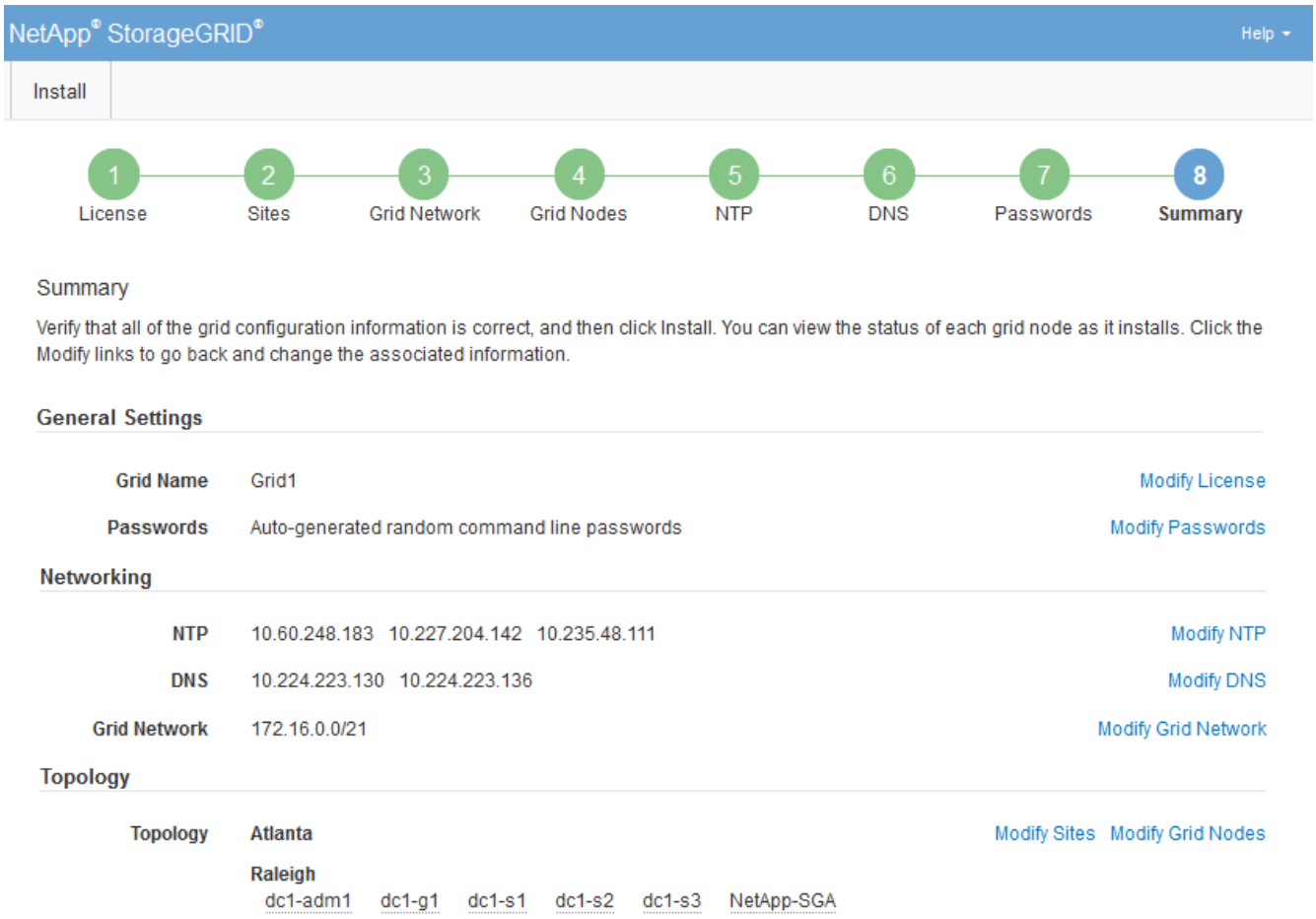
6. Cliquez sur **Suivant**.

Vérifiez votre configuration et terminez l'installation

Vous devez examiner attentivement les informations de configuration que vous avez saisies pour vous assurer que l'installation s'effectue correctement.

Étapes

1. Afficher la page **Résumé**.



2. Vérifiez que toutes les informations de configuration de la grille sont correctes. Utilisez les liens Modifier de la page Résumé pour revenir en arrière et corriger les erreurs.
3. Cliquez sur **installer**.

> Si un nœud est configuré pour utiliser le réseau client, la passerelle par défaut de ce nœud passe du réseau Grid au réseau client lorsque vous cliquez sur **installer**. Si vous perdez la connectivité, vous devez vous assurer que vous accédez au nœud d'administration principal via un sous-réseau accessible. Voir "Instructions de mise en réseau" pour plus d'informations.

4. Cliquez sur **Télécharger le progiciel de récupération**.

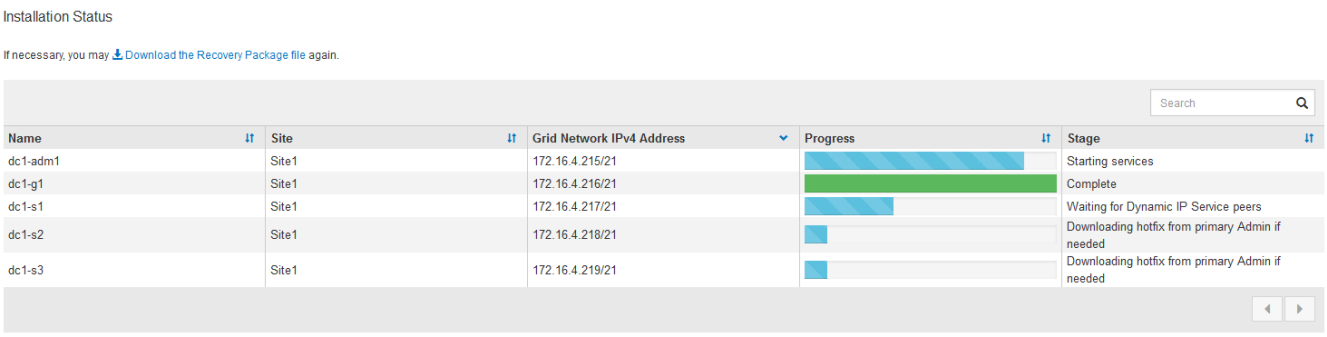
   Lorsque l'installation progresse jusqu'au point où la topologie de la grille est définie, vous êtes invité à télécharger le fichier du progiciel de récupération (`.zip`), et confirmez que vous pouvez accéder avec succès au contenu de ce fichier. Vous devez télécharger le fichier Recovery Package afin de pouvoir restaurer le système StorageGRID en cas de défaillance d'un ou de plusieurs nœuds de la grille. L'installation se poursuit en arrière-plan, mais vous ne pouvez pas terminer l'installation et accéder au système StorageGRID tant que vous n'avez pas téléchargé et vérifié ce fichier.

5. Vérifiez que vous pouvez extraire le contenu du `.zip` enregistrez-le ensuite à deux emplacements distincts, sécurisés et sécurisés.

> Le fichier du progiciel de récupération doit être sécurisé car il contient des clés de cryptage et des mots de passe qui peuvent être utilisés pour obtenir des données du système StorageGRID.

6. Cochez la case **J'ai téléchargé et vérifié le fichier du progiciel de récupération**, puis cliquez sur **Suivant**.

   Si l'installation est toujours en cours, la page d'état s'affiche. Cette page indique la progression de l'installation pour chaque nœud de la grille.



   Lorsque l'étape complète est atteinte pour tous les nœuds de la grille, la page de connexion de Grid Manager s'affiche.

7. Connectez-vous au gestionnaire de grille à l'aide de l'utilisateur « root » et du mot de passe que vous avez spécifié lors de l'installation.

Instructions de post-installation

Une fois le déploiement et la configuration des nœuds de la grille effectués, suivez ces instructions pour l'adressage DHCP et les modifications de configuration réseau.

- Si DHCP était utilisé pour attribuer des adresses IP, configurez une réservation DHCP pour chaque adresse IP sur les réseaux utilisés.

  Vous ne pouvez configurer DHCP que pendant la phase de déploiement. Vous ne pouvez pas configurer DHCP pendant la configuration.

  > Les nœuds redémarrent lors de la modification de leurs adresses IP, ce qui peut entraîner des pannes si une modification d'adresse DHCP affecte plusieurs nœuds simultanément.

- Vous devez utiliser les procédures Modifier IP pour modifier les adresses IP, les masques de sous-réseau et les passerelles par défaut pour un noeud de grille. Voir "Configurez les adresses IP".
- Si vous modifiez la configuration réseau, y compris le routage et les modifications de passerelle, la connectivité client au nœud d'administration principal et à d'autres nœuds de la grille risque d'être perdue. En fonction des modifications de réseau appliquées, vous devrez peut-être rétablir ces connexions.

Automatisation de l'installation (Ubuntu ou Debian)

Vous pouvez automatiser l'installation du service hôte StorageGRID et la configuration des nœuds grid.

Description de la tâche

L'automatisation du déploiement peut être utile dans les cas suivants :

- Vous utilisez déjà un framework d'orchestration standard, comme Ansible, Puppet ou Chef, pour déployer et configurer des hôtes physiques ou virtuels.

- Vous prévoyez de déployer plusieurs instances StorageGRID.
- Vous déployez une instance StorageGRID vaste et complexe.

Le service hôte StorageGRID est installé par un package et piloté par des fichiers de configuration qui peuvent être créés de manière interactive lors d'une installation manuelle, ou préparés à l'avance (ou par programmation) pour permettre l'installation automatisée à l'aide des frameworks d'orchestration standard. StorageGRID propose des scripts Python en option permettant d'automatiser la configuration des appliances StorageGRID et l'ensemble du système StorageGRID (la « grille »). Vous pouvez utiliser ces scripts directement, ou bien les inspecter pour apprendre à utiliser l'API REST d'installation StorageGRID dans les outils de déploiement et de configuration de grid que vous développez vous-même.

Automatisez l'installation et la configuration du service d'hôte StorageGRID

Vous pouvez automatiser l'installation du service hôte StorageGRID à l'aide des frameworks d'orchestration standard tels qu'Ansible, Puppet, Chef, Fabric ou SaltStack.

Le service hôte StorageGRID est fourni dans un DEO et est piloté par des fichiers de configuration prêts à l'avance (ou par programmation) pour permettre une installation automatisée. Si vous utilisez déjà une infrastructure d'orchestration standard pour installer et configurer Ubuntu ou Debian, l'ajout de StorageGRID à vos playbooks ou à vos recettes doit être simple.

Vous pouvez automatiser ces tâches :

1. Installation de Linux
2. Configuration de Linux
3. Configuration des interfaces réseau de l'hôte pour répondre aux exigences StorageGRID
4. Configuration du stockage de l'hôte pour répondre aux exigences StorageGRID
5. Installation de Docker
6. Installation du service hôte StorageGRID
7. Création de fichiers de configuration de nœud StorageGRID dans `/etc/storagegrid/nodes`
8. Validation des fichiers de configuration de nœuds StorageGRID
9. Démarrage du service hôte StorageGRID

Exemple de rôle et de PlayBook Ansible

Exemple de rôle et de manuel de vente Ansible sont fournis avec l'archive d'installation dans le dossier /extras. Le PlayBook Ansible présente la façon dont `storagegrid` Le rôle prépare les hôtes et installe StorageGRID sur les serveurs cibles. Vous pouvez personnaliser le rôle ou le PlayBook selon vos besoins.

Automatiser la configuration de StorageGRID

Une fois les nœuds grid déployés, vous pouvez automatiser la configuration du système StorageGRID.

Avant de commencer

- Vous connaissez l'emplacement des fichiers suivants à partir de l'archive d'installation.

Nom du fichier	Description
configure-storagegrid.py	Script Python utilisé pour automatiser la configuration

Nom du fichier	Description
configurez-storagegrid.sample.json	Exemple de fichier de configuration à utiliser avec le script
configurez-storagegrid.blank.json	Fichier de configuration vierge à utiliser avec le script

- Vous avez créé un `configure-storagegrid.json` fichier de configuration. Pour créer ce fichier, vous pouvez modifier l'exemple de fichier de configuration (`configure-storagegrid.sample.json`) ou le fichier de configuration vierge (`configure-storagegrid.blank.json`).

Description de la tâche

Vous pouvez utiliser le `configure-storagegrid.py` Script Python et le `configure-storagegrid.json` Fichier de configuration pour automatiser la configuration de votre système StorageGRID.

> Vous pouvez également configurer le système à l'aide de Grid Manager ou de l'API d'installation.

Étapes

1. Connectez-vous à la machine Linux que vous utilisez pour exécuter le script Python.
2. Accédez au répertoire dans lequel vous avez extrait l'archive d'installation.

   Par exemple :

   ```
   cd StorageGRID-Webscale-version/platform
   ```

   où `platform` est `debs`, `rpms`, ou `vsphere`.

3. Exécutez le script Python et utilisez le fichier de configuration que vous avez créé.

   Par exemple :

   ```
   ./configure-storagegrid.py ./configure-storagegrid.json --start-install
   ```

Résultat

Un progiciel de récupération `.zip` le fichier est généré pendant le processus de configuration et il est téléchargé dans le répertoire où vous exécutez le processus d'installation et de configuration. Vous devez sauvegarder le fichier de package de restauration afin de pouvoir restaurer le système StorageGRID en cas de défaillance d'un ou plusieurs nœuds de la grille. Par exemple, copiez-le dans un emplacement sécurisé, sauvegardé sur le réseau et dans un emplacement de stockage cloud sécurisé.

> Le fichier du progiciel de récupération doit être sécurisé car il contient des clés de cryptage et des mots de passe qui peuvent être utilisés pour obtenir des données du système StorageGRID.

Si vous avez indiqué que des mots de passe aléatoires doivent être générés, ouvrez le `Passwords.txt` Fichier et recherche les mots de passe requis pour accéder au système StorageGRID.

```
######################################################################
##### The StorageGRID "recovery package" has been downloaded as: #####
#####           ./sgws-recovery-package-994078-rev1.zip          #####
#####   Safeguard this file as it will be needed in case of a    #####
#####                 StorageGRID node recovery.                 #####
######################################################################
```

Votre système StorageGRID est installé et configuré lorsqu'un message de confirmation s'affiche.

```
StorageGRID has been configured and installed.
```

Informations associées

"Présentation de l'API REST d'installation"

Présentation de l'API REST d'installation

StorageGRID fournit l'API d'installation StorageGRID pour effectuer des tâches d'installation.

L'API utilise la plate-forme swagger open source API pour fournir la documentation de l'API. Swagger permet aux développeurs et aux non-développeurs d'interagir avec l'API dans une interface utilisateur qui illustre la façon dont l'API répond aux paramètres et aux options. Cette documentation suppose que vous êtes familiarisé avec les technologies Web standard et le format de données JSON.

> Toutes les opérations d'API que vous effectuez à l'aide de la page Web API Docs sont des opérations en direct. Veillez à ne pas créer, mettre à jour ou supprimer des données de configuration ou d'autres données par erreur.

Chaque commande de l'API REST inclut l'URL de l'API, une action HTTP, tous les paramètres d'URL requis ou facultatifs et une réponse de l'API attendue.

API d'installation de StorageGRID

L'API d'installation de StorageGRID n'est disponible que lors de la configuration initiale du système StorageGRID et si vous devez effectuer une restauration du nœud d'administration principal. L'API d'installation est accessible via HTTPS depuis le Grid Manager.

Pour accéder à la documentation de l'API, accédez à la page Web d'installation sur le nœud d'administration principal et sélectionnez **aide** > **documentation de l'API** dans la barre de menus.

L'API d'installation de StorageGRID comprend les sections suivantes :

- **Config** — opérations liées à la version du produit et aux versions de l'API. Vous pouvez lister la version du produit ainsi que les versions principales de l'API prises en charge par cette version.
- **Grid** — opérations de configuration au niveau de la grille. Vous pouvez obtenir et mettre à jour les paramètres de la grille, y compris les détails de la grille, les sous-réseaux de la grille, les mots de passe de la grille et les adresses IP des serveurs NTP et DNS.
- **Noeuds** — opérations de configuration au niveau des noeuds. Vous pouvez récupérer une liste de nœuds

de la grille, supprimer un nœud de la grille, configurer un nœud de la grille, afficher un nœud de la grille et réinitialiser la configuration d'un nœud de la grille.

- **Provision** — opérations de provisionnement. Vous pouvez démarrer l'opération de provisionnement et afficher l'état de cette opération.
- **Recovery** — opérations de restauration du noeud d'administration principal. Vous pouvez réinitialiser les informations, télécharger le progiciel de restauration, démarrer la récupération et afficher l'état de l'opération de récupération.
- **Progiciel de récupération** — opérations pour télécharger le progiciel de récupération.
- **Schémas** — schémas API pour les déploiements avancés
- **Sites** — opérations de configuration au niveau du site. Vous pouvez créer, afficher, supprimer et modifier un site.

Informations associées

"Automatisation de l'installation"

Par où aller plus loin

Une fois l'installation terminée, effectuez les tâches d'intégration et de configuration requises. Vous pouvez effectuer les tâches facultatives nécessaires.

Tâches requises

- "Créez un compte de locataire" Pour chaque protocole client (Swift ou S3) qui sera utilisé pour stocker des objets sur votre système StorageGRID.
- "Contrôler l'accès au système" en configurant des groupes et des comptes utilisateur. Si vous le souhaitez, vous pouvez "configurer un référentiel d'identité fédéré" (Comme Active Directory ou OpenLDAP), vous pouvez importer des groupes et des utilisateurs d'administration. Ou bien, c'est possible "créer des groupes et des utilisateurs locaux".
- Intégrer et tester le "API S3" ou "API Swift" Applications client que vous utiliserez pour télécharger des objets sur votre système StorageGRID.
- "Configuration des règles de gestion du cycle de vie des informations (ILM) et de la règle ILM" utilisez pour protéger les données d'objet.
- Si votre installation inclut des nœuds de stockage de l'appliance, effectuez les tâches suivantes avec SANtricity OS :
  - Connectez-vous à chaque appliance StorageGRID.
  - Vérifiez la réception des données AutoSupport.

    Voir "Configurer le matériel".
- Examinez et suivez les "Instructions de renforcement du système StorageGRID" pour éliminer les risques de sécurité.
- "Configurez les notifications par e-mail pour les alertes système".
- Si votre système StorageGRID inclut des nœuds d'archivage (obsolètes), configurez la connexion du nœud d'archivage au système de stockage d'archives externe cible.

Tâches facultatives

- "Mettre à jour les adresses IP des nœuds de la grille" S'ils ont changé depuis que vous avez planifié votre déploiement et généré le package de récupération.
- "Configurer le chiffrement du stockage", si nécessaire.
- "Configurer la compression du stockage" pour réduire la taille des objets stockés, si nécessaire.
- "Configurez l'accès au système à des fins d'audit" Par le biais d'un partage de fichiers NFS.

Résoudre les problèmes d'installation

En cas de problème lors de l'installation de votre système StorageGRID, vous pouvez accéder aux fichiers journaux d'installation. Le support technique peut également avoir besoin d'utiliser les fichiers journaux d'installation pour résoudre les problèmes.

Les fichiers journaux d'installation suivants sont disponibles à partir du conteneur qui exécute chaque nœud :

- `/var/local/log/install.log` (disponible sur tous les nœuds de la grille)
- `/var/local/log/gdu-server.log` (Trouvé sur le nœud d'administration principal)

Les fichiers journaux d'installation suivants sont disponibles auprès de l'hôte :

- `/var/log/storagegrid/daemon.log`
- `/var/log/storagegrid/nodes/<node-name>.log`

Pour savoir comment accéder aux fichiers journaux, reportez-vous à la section "Collecte de fichiers journaux et de données système".

Informations associées

"Dépanner un système StorageGRID"

Exemple /etc/network/interfaces

Le `/etc/network/interfaces` Le fichier comprend trois sections qui définissent les interfaces physiques, l'interface de liaison et les interfaces VLAN. Vous pouvez combiner ces trois exemples de sections dans un seul fichier, qui agrège quatre interfaces physiques Linux en une seule liaison LACP, puis établir trois interfaces VLAN qui soudent le lien pour une utilisation en tant qu'interfaces réseau StorageGRID, Admin et client.

Interfaces physiques

Notez que les switchs à l'autre extrémité des liaisons doivent également traiter les quatre ports comme une seule jonction ou un canal de port LACP et doivent passer au moins les trois VLAN référencés avec des balises.

```
# loopback interface
auto lo
iface lo inet loopback

# ens160 interface
auto ens160
iface ens160 inet manual
    bond-master bond0
    bond-primary en160

# ens192 interface
auto ens192
iface ens192 inet manual
    bond-master bond0

# ens224 interface
auto ens224
iface ens224 inet manual
    bond-master bond0

# ens256 interface
auto ens256
iface ens256 inet manual
    bond-master bond0
```

Interface de liaison

```
# bond0 interface
auto bond0
iface bond0 inet manual
    bond-mode 4
    bond-miimon 100
    bond-slaves ens160 ens192 end224 ens256
```

Interfaces VLAN

```
# 1001 vlan
auto bond0.1001
iface bond0.1001 inet manual
vlan-raw-device bond0

# 1002 vlan
auto bond0.1002
iface bond0.1002 inet manual
vlan-raw-device bond0

# 1003 vlan
auto bond0.1003
iface bond0.1003 inet manual
vlan-raw-device bond0
```

Installez VMware

Installer VMware : présentation

L'installation d'un système StorageGRID dans un environnement VMware comprend trois étapes principales.

1. **Préparation**: Pendant la planification et la préparation, vous effectuez les tâches suivantes :
   - En savoir plus sur les exigences en matière de performances, de stockage et de matériel, de logiciels et de machines virtuelles pour StorageGRID.
   - Découvrez les détails de "La mise en réseau StorageGRID" vous pouvez ainsi configurer votre réseau de façon appropriée.
   - Identifiez et préparez les serveurs physiques que vous prévoyez d'utiliser pour héberger vos nœuds de grid StorageGRID.
   - Sur les serveurs que vous avez préparés :
     - Installation de l'hyperviseur VMware vSphere
     - Configurer les hôtes ESX
     - Installer et configurer VMware vSphere et vCenter
2. **Déploiement** : déployez des nœuds de grille à l'aide du client Web VMware vSphere. Lorsque vous déployez des nœuds grid, ils sont créés dans le cadre du système StorageGRID et connectés à un ou plusieurs réseaux.
   a. Utilisez le client Web VMware vSphere, un fichier .vmdk et un ensemble de modèles de fichiers .ovf pour déployer les nœuds basés sur logiciel en tant que machines virtuelles (VM) sur les serveurs que vous avez préparés à l'étape 1.
   b. Utilisez le programme d'installation de l'appliance StorageGRID pour déployer les nœuds d'appliance StorageGRID.

> Les instructions d'installation et d'intégration spécifiques au matériel ne sont pas incluses dans la procédure d'installation de StorageGRID. Pour savoir comment installer les appliances StorageGRID, consultez le "Démarrage rapide pour l'installation du matériel" pour trouver les instructions relatives à votre appareil.

3. **Configuration** : lorsque tous les nœuds ont été déployés, utilisez le gestionnaire de grille pour configurer la grille et terminer l'installation.

Ces instructions recommandent une approche standard de déploiement et de configuration d'un système StorageGRID dans un environnement VMware. Voir également les informations sur les approches alternatives suivantes :

- Utilisez le script deploy-vsphere-ovftool.sh Bash (disponible dans l'archive d'installation) pour déployer des nœuds grid dans VMware vSphere.
- Automatiser le déploiement et la configuration du système StorageGRID à l'aide d'un script de configuration Python (fourni dans l'archive d'installation).
- Automatisez le déploiement et la configuration des nœuds grid d'appliance avec un script de configuration Python (disponible dans l'archive de l'installation ou depuis le programme d'installation de l'appliance StorageGRID).
- Si vous êtes un développeur avancé de déploiements StorageGRID, utilisez les API REST d'installation pour automatiser l'installation des nœuds grid d'StorageGRID.

Planification et préparation de l'installation VMware

Avant d'installer (VMware)

Avant de déployer des nœuds grid et de configurer la grille de StorageGRID, vous devez connaître les étapes et les conditions requises pour terminer la procédure.

Les procédures de déploiement et de configuration de StorageGRID supposent que vous connaissez bien l'architecture et les fonctionnalités opérationnelles du système StorageGRID.

Vous pouvez déployer un ou plusieurs sites à la fois. Toutefois, tous les sites doivent respecter le minimum requis : disposer d'au moins trois nœuds de stockage.

Avant de démarrer la procédure de déploiement de nœuds et de configuration grid, vous devez :

- Planification du déploiement StorageGRID
- Installez, connectez et configurez tout le matériel requis, y compris les appliances StorageGRID, selon les spécifications.

> Si votre installation StorageGRID n'utilise pas de nœuds de stockage (matériels) StorageGRID, vous devez utiliser un stockage RAID matériel avec un cache d'écriture protégé par batterie (BBWC). StorageGRID ne prend pas en charge l'utilisation de réseaux de stockage virtuels (VSAN), de RAID logiciel ou aucune protection RAID.

> Les instructions d'installation et d'intégration spécifiques au matériel ne sont pas incluses dans la procédure d'installation de StorageGRID. Pour savoir comment installer les appliances StorageGRID, reportez-vous à la section "Installez le matériel de l'appliance".

- Prenez connaissance du "options réseau disponibles et mise en œuvre de chaque option réseau sur les nœuds grid".
- Rassemblez toutes les informations de réseautage à l'avance. À moins que vous n'utilisiez DHCP, rassemblez les adresses IP à attribuer à chaque nœud de grille, ainsi que les adresses IP des serveurs DNS et NTP qui seront utilisés.
- Choisissez les outils de déploiement et de configuration que vous souhaitez utiliser.

Matériel requis

Avant d'installer StorageGRID, vous devez rassembler et préparer les ressources nécessaires.

Élément	Remarques
Licence NetApp StorageGRID	Vous devez disposer d'une licence NetApp valide et signée numériquement. **Remarque** : l'archive d'installation de StorageGRID inclut une licence gratuite qui ne fournit aucun droit de support pour le produit.
Archive de l'installation de StorageGRID	Vous devez "Téléchargez l'archive d'installation de StorageGRID et extrayez les fichiers".
Le logiciel et la documentation VMware	Lors de l'installation, vous utilisez le client Web VMware vSphere pour déployer des nœuds grid virtuels sur des machines virtuelles. Pour les versions prises en charge, reportez-vous à la section "Matrice d'interopérabilité NetApp".
L'ordinateur portable de service	Le système StorageGRID est installé par le biais d'un ordinateur portable de service. L'ordinateur portable de service doit posséder : • Port réseau • Client SSH (par exemple, PuTTY) • "Navigateur Web pris en charge"
Documentation StorageGRID	• "Notes de mise à jour" • "Instructions d'administration de StorageGRID"

Téléchargez et extrayez les fichiers d'installation de StorageGRID

Vous devez télécharger les archives d'installation de StorageGRID et extraire les fichiers.

Étapes

1. Accédez au "Page de téléchargements NetApp pour StorageGRID".
2. Sélectionnez le bouton pour télécharger la dernière version ou sélectionnez une autre version dans le menu déroulant et sélectionnez **Go**.
3. Connectez-vous avec le nom d'utilisateur et le mot de passe de votre compte NetApp.

4. Si une instruction attention/MustRead apparaît, lisez-la et cochez la case.

> Après l'installation de la version StorageGRID, vous devez appliquer les correctifs requis. Pour plus d'informations, reportez-vous à la section "procédure de correctif dans les instructions de récupération et de maintenance"

5. Lisez le contrat de licence de l'utilisateur final, cochez la case, puis sélectionnez **accepter et continuer**.
6. Dans la colonne **Install StorageGRID**, sélectionnez le fichier .tgz ou .zip pour VMware.

> Utilisez le `.zip` Fichier si vous exécutez Windows sur l'ordinateur portable de service.

7. Enregistrez et extrayez le fichier d'archive.
8. Choisissez les fichiers dont vous avez besoin dans la liste suivante.

   Les fichiers dont vous avez besoin dépendent de votre topologie de grille planifiée et de la manière dont vous allez déployer votre système StorageGRID.

> Les chemins répertoriés dans la table sont relatifs au répertoire de niveau supérieur installé par l'archive d'installation extraite.

Chemin d'accès et nom de fichier	Description
	Fichier texte qui décrit tous les fichiers contenus dans le fichier de téléchargement StorageGRID.
	Licence gratuite qui ne fournit aucun droit d'assistance pour le produit.
	Fichier de disque de machine virtuelle utilisé comme modèle pour créer des machines virtuelles de nœud de grille.
	Fichier modèle du format Open Virtualization (`.ovf`) et fichier manifeste (`.mf`) Pour le déploiement du nœud d'administration principal.
	Le fichier de modèle (`.ovf`) et fichier manifeste (`.mf`) Pour le déploiement de nœuds d'administration non primaires.
	Le fichier de modèle (`.ovf`) et fichier manifeste (`.mf`) Pour le déploiement des nœuds d'archivage.
	Le fichier de modèle (`.ovf`) et fichier manifeste (`.mf`) Pour le déploiement des nœuds de passerelle.

Chemin d'accès et nom de fichier	Description
	Le fichier de modèle (`.ovf`) et fichier manifeste (`.mf`) Pour le déploiement de nœuds de stockage basés sur des machines virtuelles.
Outil de script de déploiement	Description
	Script de shell de Bash utilisé pour automatiser le déploiement de nœuds de grille virtuels.
	Exemple de fichier de configuration à utiliser avec `deploy-vsphere-ovftool.sh` script.
	Script Python utilisé pour automatiser la configuration d'un système StorageGRID.
	Script Python utilisé pour automatiser la configuration des appliances StorageGRID.
	Exemple de script Python que vous pouvez utiliser pour vous connecter à l'API de gestion de grille lorsque l'authentification unique (SSO) est activée. Vous pouvez également utiliser ce script pour le Federate Ping.
	Exemple de fichier de configuration à utiliser avec `configure-storagegrid.py` script.
	Un fichier de configuration vierge à utiliser avec le `configure-storagegrid.py` script.
	Exemple de script Python que vous pouvez utiliser pour vous connecter à l'API de gestion de grille lorsque l'authentification unique (SSO) est activée à l'aide d'Active Directory ou de Ping Federate.
	Script d'aide appelé par le compagnon `storagegrid-ssoauth-azure.py` Script Python pour effectuer des interactions SSO avec Azure.

Chemin d'accès et nom de fichier	Description
	Schémas API pour StorageGRID. **Remarque** : avant d'effectuer une mise à niveau, vous pouvez utiliser ces schémas pour confirmer que tout code que vous avez écrit pour utiliser les API de gestion StorageGRID sera compatible avec la nouvelle version de StorageGRID si vous ne disposez pas d'un environnement StorageGRID non productif pour le test de compatibilité de mise à niveau.

Configuration logicielle requise

Vous pouvez utiliser une machine virtuelle pour héberger tout type de nœud grid StorageGRID. Une machine virtuelle est requise pour chaque nœud de grid installé sur le serveur VMware.

Hyperviseur VMware vSphere

Vous devez installer VMware vSphere Hypervisor sur un serveur physique préparé. Avant d'installer le logiciel VMware, le matériel doit être configuré correctement (y compris les versions du micrologiciel et les paramètres du BIOS).

- Configurez la mise en réseau dans l'hyperviseur pour prendre en charge la mise en réseau du système StorageGRID que vous installez.

  "Instructions de mise en réseau"

- Assurez-vous que le datastore est suffisamment grand pour les machines virtuelles et les disques virtuels requis pour héberger les nœuds de la grille.
- Si vous créez plusieurs datastores, nommez chacun d'entre eux afin de pouvoir facilement identifier les datastores à utiliser pour chaque nœud de la grille lorsque vous créez des machines virtuelles.

Configuration requise de l'hôte ESX

> Vous devez configurer correctement le protocole NTP (Network Time Protocol) sur chaque hôte ESX. Si l'heure de l'hôte est incorrecte, des effets négatifs, y compris la perte de données, peuvent survenir.

Configuration requise pour VMware

Vous devez installer et configurer VMware vSphere et vCenter avant de déployer les nœuds grid StorageGRID.

Pour connaître les versions prises en charge des logiciels VMware vSphere Hypervisor et VMware vCenter Server, reportez-vous au "Matrice d'interopérabilité NetApp".

Pour connaître les étapes d'installation de ces produits VMware, reportez-vous à la documentation VMware.

Configuration requise pour le processeur et la RAM

Avant d'installer le logiciel StorageGRID, vérifiez et configurez le matériel afin qu'il soit prêt à prendre en charge le système StorageGRID.

Pour plus d'informations sur les serveurs pris en charge, reportez-vous au "Matrice d'interopérabilité NetApp".

Chaque nœud StorageGRID nécessite au moins :

- Cœurs de processeur : 8 par nœud
- RAM : au moins 24 Go par nœud et 2 à 16 Go de moins que la RAM totale du système, selon la mémoire RAM totale disponible et la quantité de logiciel non StorageGRID exécuté sur le système

Vérifiez que le nombre de nœuds StorageGRID que vous prévoyez d'exécuter sur chaque hôte physique ou virtuel ne dépasse pas le nombre de cœurs de processeur ou la mémoire RAM physique disponible. Si les hôtes ne sont pas dédiés à l'exécution de StorageGRID (non recommandé), veillez à prendre en compte les besoins en ressources des autres applications.

> Surveillez régulièrement l'utilisation de votre processeur et de votre mémoire pour vous assurer que ces ressources continuent de s'adapter à votre charge de travail. Par exemple, doubler l'allocation de la RAM et du processeur pour les nœuds de stockage virtuels fournira des ressources similaires à celles des nœuds d'appliance StorageGRID. En outre, si la quantité de métadonnées par nœud dépasse 500 Go, envisagez d'augmenter la mémoire RAM par nœud à au moins 48 Go. Pour plus d'informations sur la gestion du stockage des métadonnées d'objet, l'augmentation du paramètre espace réservé aux métadonnées et la surveillance de l'utilisation du processeur et de la mémoire, reportez-vous aux instructions de "administration", "contrôle", et "mise à niveau" StorageGRID :

Si le hyperthreading est activé sur les hôtes physiques sous-jacents, vous pouvez fournir 8 cœurs virtuels (4 cœurs physiques) par nœud. Si le hyperthreading n'est pas activé sur les hôtes physiques sous-jacents, vous devez fournir 8 cœurs physiques par nœud.

Si vous utilisez des machines virtuelles en tant qu'hôtes et que vous contrôlez la taille et le nombre de machines virtuelles, nous vous recommandons d'utiliser une seule machine virtuelle pour chaque nœud StorageGRID afin de dimensionner celle-ci en conséquence.

Dans le cas de déploiements en production, vous ne devez pas exécuter plusieurs nœuds de stockage sur le même matériel de stockage physique ou sur le même hôte virtuel. Dans un seul déploiement StorageGRID, chaque nœud de stockage doit se trouver dans son propre domaine de défaillances isolé. Vous pouvez optimiser la durabilité et la disponibilité des données d'objet si vous assurez qu'une seule panne matérielle peut avoir un impact sur un seul nœud de stockage.

Voir aussi "Les besoins en matière de stockage et de performances".

Les besoins en matière de stockage et de performances

Vous devez connaître les besoins en performances et en stockage des nœuds StorageGRID hébergés par des machines virtuelles, afin que vous puissiez disposer d'un espace suffisant pour prendre en charge la configuration initiale et l'extension future du stockage.

Exigences en matière de performances

Les performances du volume du système d'exploitation et du premier volume de stockage ont un impact significatif sur les performances globales du système. Assurez-vous que ces baies offrent les performances appropriées en termes de latence, d'opérations d'entrée/sortie par seconde (IOPS) et de débit.

Tous les nœuds StorageGRID nécessitent que le lecteur du système d'exploitation et tous les volumes de stockage aient une mise en cache à écriture différée activée. Le cache doit se trouver sur un support protégé ou persistant.

Ainsi que les machines virtuelles qui utilisent le stockage NetApp ONTAP

Si vous déployez un nœud StorageGRID en tant que machine virtuelle avec un stockage affecté à un système NetApp ONTAP, vous avez confirmé que cette FabricPool règle n'est pas activée pour le volume. Par exemple, si un nœud StorageGRID s'exécute en tant que machine virtuelle sur un hôte VMware, assurez-vous que la règle de hiérarchisation FabricPool n'est pas activée pour le volume qui sauvegarde le datastore du nœud. La désactivation du Tiering FabricPool pour les volumes utilisés avec des nœuds StorageGRID simplifie la résolution des problèmes et les opérations de stockage.

> N'utilisez jamais FabricPool pour transférer automatiquement toutes les données liées à StorageGRID vers StorageGRID. Le Tiering des données StorageGRID vers StorageGRID augmente la complexité opérationnelle et la résolution des problèmes.

Nombre de machines virtuelles requises

Chaque site StorageGRID requiert au moins trois nœuds de stockage.

> Dans un déploiement de production, n'exécutez pas plus d'un nœud de stockage sur un seul serveur de machine virtuelle. L'utilisation d'un hôte de machine virtuelle dédié pour chaque nœud de stockage fournit un domaine de panne isolé.

D'autres types de nœuds, comme les nœuds d'administration ou les nœuds de passerelle, peuvent être déployés sur le même hôte de machine virtuelle, ou sur leurs propres hôtes de machine virtuelle dédiée. Toutefois, si vous avez plusieurs nœuds du même type (deux nœuds de passerelle, par exemple), n'installez pas toutes les instances sur le même hôte de machine virtuelle.

Besoins en stockage par type de nœud

Dans un environnement de production, les machines virtuelles pour les nœuds grid StorageGRID doivent répondre à des exigences différentes, selon les types de nœuds.

> Les snapshots de disque ne peuvent pas être utilisés pour restaurer les nœuds de grille. Reportez-vous plutôt au "restauration du nœud grid" procédures pour chaque type de nœud.

Type de nœud	Stockage
Nœud d'administration	LUN DE 100 GO POUR OS LUN de 200 Go pour les tables de nœuds d'administration LUN de 200 Go pour le journal d'audit du nœud d'administration

Type de nœud	Stockage
Nœud de stockage	LUN DE 100 GO POUR OS 3 LUN pour chaque nœud de stockage sur cet hôte **Remarque** : un nœud de stockage peut avoir 1 à 16 LUN de stockage ; au moins 3 LUN de stockage sont recommandées. Taille minimale par LUN : 4 To Taille de la LUN testée maximale : 39 To.
Nœud de passerelle	LUN DE 100 GO POUR OS
Nœud d'archivage	LUN DE 100 GO POUR OS

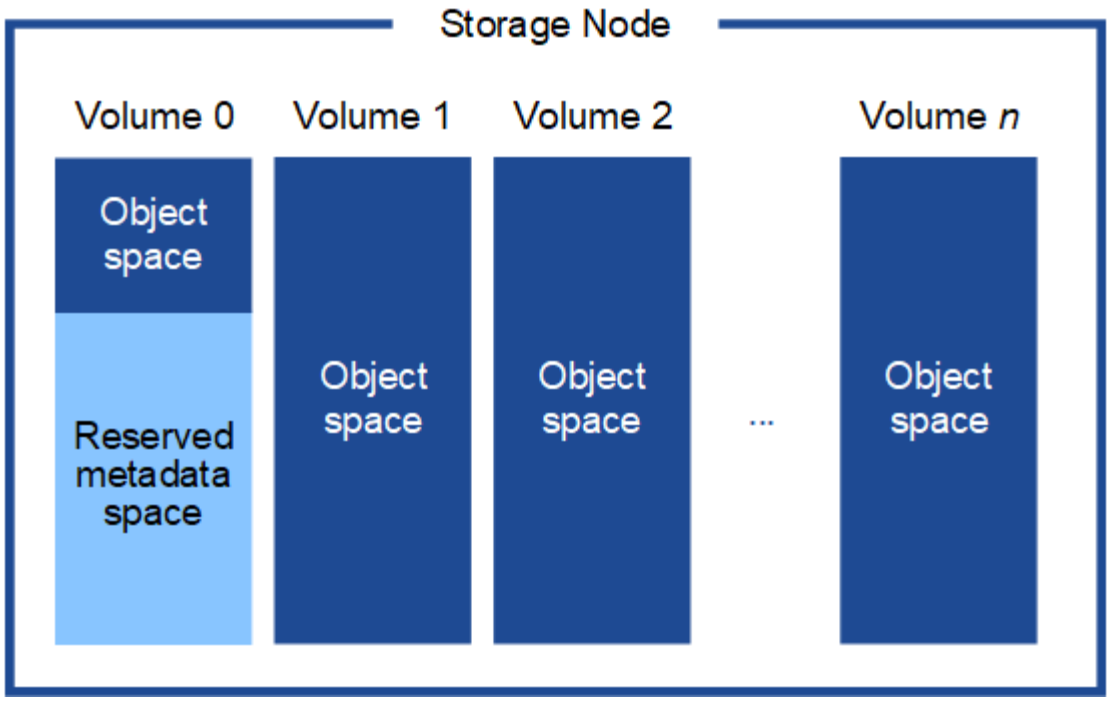
Selon le niveau d'audit configuré, la taille des entrées utilisateur telles que le nom de clé d'objet S3, Et la quantité de données des journaux d'audit à conserver, il peut être nécessaire d'augmenter la taille de la LUN des journaux d'audit sur chaque nœud d'administration.en général, une grille génère environ 1 Ko de données d'audit par opération S3, Cela signifie qu'un LUN de 200 Go peut prendre en charge 70 millions d'opérations par jour ou 800 opérations par seconde pendant deux à trois jours.

Besoins de stockage des nœuds de stockage

Un nœud de stockage logiciel peut disposer de 1 à 16 volumes de stockage, dont -3 volumes ou plus sont recommandés. Chaque volume de stockage doit être supérieur ou égale à 4 To.

Un nœud de stockage d'appliance peut disposer d'un maximum de 48 volumes de stockage.

Comme illustré dans la figure, StorageGRID réserve l'espace des métadonnées d'objet sur le volume de stockage 0 de chaque nœud de stockage. Tout espace restant sur le volume de stockage 0 et tout autre volume de stockage du nœud de stockage est utilisé exclusivement pour les données d'objet.



Pour assurer la redondance et protéger les métadonnées d'objet contre la perte, StorageGRID stocke trois copies des métadonnées de tous les objets du système sur chaque site. Les trois copies de métadonnées d'objet sont réparties de manière uniforme sur tous les nœuds de stockage de chaque site.

Lorsque vous attribuez de l'espace au volume 0 d'un nouveau nœud de stockage, vous devez vous assurer qu'il y a suffisamment d'espace pour la portion de ce nœud de toutes les métadonnées d'objet.

- Au moins, vous devez affecter au volume 0 au moins 4 To.

> Si vous n'utilisez qu'un seul volume de stockage pour un nœud de stockage et que vous attribuez 4 To ou moins au volume, le nœud de stockage peut entrer l'état de lecture seule au démarrage et ne stocker que les métadonnées de l'objet.

> Si vous attribuez moins de 500 Go au volume 0 (utilisation hors production uniquement), 10 % de la capacité du volume de stockage est réservée aux métadonnées.

- Si vous installez un nouveau système (StorageGRID 11.6 ou supérieur) et que chaque nœud de stockage dispose de 128 Go ou plus de RAM, attribuez 8 To ou plus au volume 0. L'utilisation d'une valeur plus grande pour le volume 0 peut augmenter l'espace autorisé pour les métadonnées sur chaque nœud de stockage.
- Lorsque vous configurez différents nœuds de stockage pour un site, utilisez le même paramètre pour le volume 0 si possible. Si un site contient des nœuds de stockage de différentes tailles, le nœud de stockage avec le plus petit volume 0 déterminera la capacité des métadonnées de ce site.

Pour plus d'informations, rendez-vous sur "Gérer le stockage des métadonnées d'objet".

Déploiement de nœuds grid de machine virtuelle (VMware)

Collecte d'informations sur votre environnement de déploiement

Avant de déployer les nœuds de la grille, vous devez collecter des informations sur la

configuration de votre réseau et l'environnement VMware.

> Il est plus efficace d'effectuer une seule installation de tous les nœuds, au lieu d'installer certains nœuds maintenant et certains nœuds ultérieurement.

Informations sur VMware

Vous devez accéder à l'environnement de déploiement et collecter des informations sur l'environnement VMware, les réseaux créés pour les réseaux Grid, Admin et client, ainsi que les types de volume de stockage que vous envisagez d'utiliser pour les nœuds de stockage.

Vous devez collecter des informations sur votre environnement VMware, notamment :

- Nom d'utilisateur et mot de passe d'un compte VMware vSphere disposant des autorisations appropriées pour terminer le déploiement.
- Informations sur l'hôte, le datastore et la configuration réseau pour chaque machine virtuelle de nœud de grid StorageGRID.

> VMware Live vMotion provoque l'augmentation de l'horloge de la machine virtuelle et n'est pas pris en charge pour les nœuds grid d'aucun type. Bien que les temps d'horloge rares et incorrects peuvent entraîner une perte de données ou des mises à jour de la configuration.

Informations sur le réseau

Vous devez collecter des informations sur le réseau VMware créé pour le réseau StorageGRID Grid Network (obligatoire), notamment :

- Nom du réseau.
- Si vous n'utilisez pas DHCP, les détails de mise en réseau requis pour chaque nœud de grille (adresse IP, passerelle et masque réseau).
- Si vous n'utilisez pas DHCP, l'adresse IP du nœud d'administration principal sur le réseau Grid. Pour plus d'informations, reportez-vous à la section « découverte des nœuds de grille du nœud d'administration principal ».

Informations sur le réseau d'administration

Pour les nœuds qui seront connectés au réseau d'administration StorageGRID facultatif, vous devez collecter des informations sur le réseau VMware créé pour ce réseau, notamment :

- Nom du réseau.
- Méthode utilisée pour attribuer des adresses IP, statiques ou DHCP.
- Si vous utilisez des adresses IP statiques, les informations de mise en réseau requises pour chaque nœud de la grille (adresse IP, passerelle, masque de réseau).
- La liste des sous-réseaux externes (ESL) pour le réseau Admin.

Informations sur le réseau client

Pour les nœuds qui seront connectés au réseau client StorageGRID en option, vous devez collecter des informations sur le réseau VMware créé pour ce réseau, notamment :

- Nom du réseau.

- Méthode utilisée pour attribuer des adresses IP, statiques ou DHCP.
- Si vous utilisez des adresses IP statiques, les informations de mise en réseau requises pour chaque nœud de la grille (adresse IP, passerelle, masque de réseau).

Informations sur les interfaces supplémentaires

Vous pouvez éventuellement ajouter une jonction ou des interfaces d'accès à la machine virtuelle dans vCenter après l'installation du nœud. Par exemple, vous pouvez ajouter une interface de jonction à un noeud d'administration ou de passerelle, de sorte que vous pouvez utiliser des interfaces VLAN pour isoler le trafic appartenant à différentes applications ou locataires. Vous pouvez également ajouter une interface d'accès à utiliser au sein d'un groupe de haute disponibilité (HA).

Les interfaces que vous ajoutez s'affichent sur la page des interfaces VLAN et sur la page HA Groups de la grille Manager.

- Si vous ajoutez une interface de jonction, configurez une ou plusieurs interfaces VLAN pour chaque nouvelle interface parent. Voir "Configurez les interfaces VLAN".
- Si vous ajoutez une interface d'accès, vous devez l'ajouter directement aux groupes haute disponibilité. Voir "configurez les groupes haute disponibilité".

Volumes de stockage pour les nœuds de stockage virtuels

Vous devez collecter les informations suivantes pour les nœuds de stockage basés sur des machines virtuelles :

- Le nombre et la taille des volumes de stockage (LUN de stockage) que vous envisagez d'ajouter. Voir « exigences en matière de stockage et de performances ».

Informations de configuration de la grille

Vous devez collecter des informations pour configurer votre grille :

- Licence Grid
- Adresses IP du serveur NTP (Network Time Protocol)
- Adresses IP du serveur DNS

Informations associées

"Mode de détection des nœuds du grid sur le nœud d'administration principal"

"Les besoins en matière de stockage et de performances"

Mode de détection des nœuds du grid sur le nœud d'administration principal

Les nœuds de grid communiquent avec le nœud d'administration principal pour la configuration et la gestion. Chaque nœud de la grille doit connaître l'adresse IP du nœud d'administration principal sur le réseau Grid.

Pour vous assurer qu'un nœud de grille peut accéder au nœud d'administration principal, vous pouvez effectuer l'une des opérations suivantes lors du déploiement du nœud :

- Vous pouvez utiliser le paramètre ADMIN_IP pour saisir manuellement l'adresse IP du nœud d'administration principal.

- Vous pouvez omettre le paramètre ADMIN_IP pour que le nœud de la grille détecte automatiquement la valeur. La détection automatique est particulièrement utile lorsque le réseau Grid utilise DHCP pour attribuer l'adresse IP au nœud d'administration principal.

La découverte automatique du nœud d'administration principal s'effectue à l'aide d'un système de noms de domaine multicast (mDNS). Lors du premier démarrage du nœud d'administration principal, il publie son adresse IP à l'aide de mDNS. Les autres nœuds du même sous-réseau peuvent alors interroger l'adresse IP et l'acquérir automatiquement. Cependant, comme le trafic IP multicast n'est généralement pas routable entre les sous-réseaux, les nœuds des autres sous-réseaux ne peuvent pas acquérir directement l'adresse IP du nœud Admin principal.

Si vous utilisez la détection automatique :

- Vous devez inclure le paramètre ADMIN_IP pour au moins un nœud de grille sur les sous-réseaux auxquels le nœud d'administration principal n'est pas directement connecté. Ce nœud de grille publie ensuite l'adresse IP du nœud d'administration principal pour les autres nœuds du sous-réseau à détecter avec mDNS.
- Assurez-vous que votre infrastructure réseau prend en charge le trafic IP multicast dans un sous-réseau.

Déployez un nœud StorageGRID en tant que serveur virtuel

Vous utilisez le client Web VMware vSphere pour déployer chaque nœud de grid en tant que machine virtuelle. Pendant le déploiement, chaque nœud de grid est créé et connecté à un ou plusieurs réseaux StorageGRID.

Si vous devez déployer des nœuds de stockage StorageGRID, reportez-vous à la section "Déployez le nœud de stockage de l'appliance".

Vous pouvez également remapper les ports du nœud ou augmenter les paramètres de processeur ou de mémoire du nœud avant de le mettre sous tension.

Avant de commencer

- Vous avez passé en revue la procédure à suivre "planification et préparation de l'installation"Et vous comprenez la configuration requise pour les logiciels, le processeur et la RAM, ainsi que pour le stockage et les performances.
- Vous connaissez déjà l'hyperviseur VMware vSphere et êtes déjà familiarisé avec le déploiement de serveurs virtuels dans cet environnement.

Le `open-vm-tools` Package, une implémentation open source similaire à VMware Tools, est inclus avec la machine virtuelle StorageGRID. Vous n'avez pas besoin d'installer VMware Tools manuellement.

- Vous avez téléchargé et extrait la version correcte de l'archive d'installation StorageGRID pour VMware.

Si vous déployez le nouveau nœud dans le cadre d'une opération d'extension ou de restauration, vous devez utiliser la version d'StorageGRID en cours d'exécution sur la grille.

- Vous disposez du disque d'ordinateur virtuel StorageGRID (`.vmdk`) fichier :

```
NetApp-SG-version-SHA.vmdk
```

- Vous avez le `.ovf` et `.mf` fichiers pour chaque type de nœud de la grille que vous déployez :

Nom du fichier	Description
vsphere-primary-admin.ovf vsphere-primary-admin.mf	Fichier modèle et fichier manifeste pour le nœud d'administration principal.
vsphere-non-primary-admin.ovf vsphere-non-primary-admin.mf	Fichier modèle et fichier manifeste pour un nœud d'administration non primaire.
vsphere-archive.ovf vsphere-archive.mf	Fichier de modèle et fichier manifeste pour un nœud d'archivage.
vsphere-gateway.ovf vsphere-gateway.mf	Fichier modèle et fichier manifeste pour un nœud passerelle.
vsphere-storage.ovf vsphere-storage.mf	Fichier modèle et fichier manifeste pour un noeud de stockage.

- Le `.vdmk`, `.ovf`, et `.mf` les fichiers se trouvent tous dans le même répertoire.
- Vous disposez d'un plan pour réduire les domaines d'échec. Par exemple, vous ne devez pas déployer tous les nœuds de passerelle sur un serveur de machine virtuelle unique.

> Dans un déploiement de production, n'exécutez pas plus d'un nœud de stockage sur un seul serveur de machine virtuelle. L'utilisation d'un hôte de machine virtuelle dédié pour chaque nœud de stockage fournit un domaine de panne isolé.

- Si vous déployez un nœud dans le cadre d'une opération d'extension ou de restauration, vous disposez de la "Instructions d'extension d'un système StorageGRID" ou le "instructions de récupération et de maintenance".
- Si vous déployez un nœud StorageGRID en tant que machine virtuelle avec un stockage affecté à un système NetApp ONTAP, vous avez confirmé que cette FabricPool règle n'est pas activée pour le volume. Par exemple, si un nœud StorageGRID s'exécute en tant que machine virtuelle sur un hôte VMware, assurez-vous que la règle de hiérarchisation FabricPool n'est pas activée pour le volume qui sauvegarde le datastore du nœud. La désactivation du Tiering FabricPool pour les volumes utilisés avec des nœuds StorageGRID simplifie la résolution des problèmes et les opérations de stockage.

> N'utilisez jamais FabricPool pour transférer automatiquement toutes les données liées à StorageGRID vers StorageGRID. Le Tiering des données StorageGRID vers StorageGRID augmente la complexité opérationnelle et la résolution des problèmes.

Description de la tâche

Suivez ces instructions pour déployer au départ des nœuds VMware, ajouter un nouveau nœud VMware dans une extension ou remplacer un nœud VMware dans le cadre d'une opération de restauration. Sauf indication contraire dans les étapes, la procédure de déploiement des nœuds est la même pour tous les types de

nœuds, y compris les nœuds d'administration, les nœuds de stockage, les nœuds de passerelle et les nœuds d'archivage.

Si vous installez un nouveau système StorageGRID :

- Vous devez déployer le nœud d'administration principal avant de déployer un autre nœud de la grille.
- Vous devez vous assurer que chaque machine virtuelle peut se connecter au noeud d'administration principal via le réseau Grid.
- Vous devez déployer tous les nœuds de la grille avant de configurer la grille.

Si vous effectuez une opération d'extension ou de reprise :

- Vous devez vous assurer que la nouvelle machine virtuelle peut se connecter au nœud d'administration principal via le réseau Grid.

Si vous devez remmapper l'un des ports du nœud, ne mettez pas le nouveau nœud sous tension tant que la configuration du remap des ports n'est pas terminée.

Étapes

1. À l'aide de vCenter, déployez un modèle OVF.

   Si vous spécifiez une URL, pointez vers un dossier contenant les fichiers suivants. Sinon, sélectionnez chacun de ces fichiers dans un répertoire local.

   ```
   NetApp-SG-version-SHA.vmdk
   vsphere-node.ovf
   vsphere-node.mf
   ```

   Par exemple, s'il s'agit du premier nœud que vous déployez, utilisez ces fichiers pour déployer le nœud d'administration principal de votre système StorageGRID :

   ```
   NetApp-SG-version-SHA.vmdk
   sphere-primary-admin.ovf
   sphere-primary-admin.mf
   ```

2. Fournissez un nom pour la machine virtuelle.

   La pratique standard consiste à utiliser le même nom pour la machine virtuelle et le nœud de grille.

3. Placez la machine virtuelle dans le pool de ressources ou vApp approprié.
4. Si vous déployez le nœud d'administration principal, lisez et acceptez le contrat de licence de l'utilisateur final.

   Selon votre version de vCenter, l'ordre des étapes varie en fonction de l'acceptation du contrat de licence de l'utilisateur final, en précisant le nom de la machine virtuelle et en sélectionnant un datastore.

5. Sélectionnez le stockage de la machine virtuelle.

   Si vous déployez un nœud dans le cadre de l'opération de restauration, suivez les instructions de la section étape de restauration du stockage pour ajouter de nouveaux disques virtuels, reconnectez-les à

partir du nœud de grille défaillant, ou les deux.

Lors du déploiement d'un nœud de stockage, utilisez au moins 3 volumes de stockage, chaque volume de stockage étant de 4 To ou plus. Vous devez affecter au moins 4 To au volume 0.

> Le fichier .ovf de nœud de stockage définit plusieurs VMDK pour le stockage. À moins que ces VMDK ne répondent à vos besoins de stockage, vous devez les supprimer et attribuer des VMDK ou des RDM appropriés pour le stockage avant de mettre le nœud sous tension. Les VMDK sont plus fréquemment utilisés dans les environnements VMware et sont plus faciles à gérer, tandis que les RDM peuvent fournir de meilleures performances pour les charges de travail utilisant des objets de plus grande taille (par exemple, plus de 100 Mo).

> Certaines installations StorageGRID peuvent utiliser des volumes de stockage plus grands et plus actifs que les charges de travail virtualisées standard. Vous devrez peut-être régler certains paramètres de l'hyperviseur, par exemple `MaxAddressableSpaceTB`, pour obtenir des performances optimales. Si vous rencontrez des problèmes de performances médiocres, contactez votre support de virtualisation pour déterminer si votre environnement peut bénéficier du réglage de la configuration propre aux charges de travail.

6. Sélectionnez réseaux.

   Déterminez les réseaux StorageGRID que le nœud utilisera en sélectionnant un réseau de destination pour chaque réseau source.

   - Le réseau Grid est requis. Vous devez sélectionner un réseau de destination dans l'environnement vSphere.
   - Si vous utilisez le réseau Admin, sélectionnez un autre réseau de destination dans l'environnement vSphere. Si vous n'utilisez pas le réseau d'administration, sélectionnez la même destination que celle que vous avez sélectionnée pour le réseau en grille.
   - Si vous utilisez le réseau client, sélectionnez un autre réseau de destination dans l'environnement vSphere. Si vous n'utilisez pas le réseau client, sélectionnez la destination que vous avez sélectionnée pour le réseau Grid.

7. Sous **Personnaliser le modèle**, configurez les propriétés du nœud StorageGRID requises.

   a. Entrez le **Nom du noeud**.

      > Si vous récupérez un nœud de la grille, vous devez entrer le nom du nœud que vous récupérez.

   b. Dans la section **Grid Network (eth0)**, sélectionnez STATIQUE ou DHCP pour la configuration **Grid network IP**.

      - Si vous sélectionnez STATIQUE, saisissez l'adresse IP * réseau Grid*, **masque réseau Grid**, **passerelle réseau Grid** et **MTU réseau Grid**.
      - Si vous sélectionnez DHCP, l'adresse IP * réseau Grid*, **masque de réseau Grid** et **passerelle réseau Grid** sont automatiquement affectées.

   c. Dans le champ **IP d'administration principale**, entrez l'adresse IP du noeud d'administration principal pour le réseau de grille.

      > Cette étape ne s'applique pas si le nœud que vous déployez est le nœud d'administration principal.

Si vous omettez l'adresse IP du nœud d'administration principal, l'adresse IP est automatiquement découverte si le nœud d'administration principal, ou au moins un autre nœud de la grille avec ADMIN_IP configuré, est présent sur le même sous-réseau. Cependant, il est recommandé de définir ici l'adresse IP du nœud d'administration principal.

a. Dans la section **Admin Network (eth1)**, sélectionnez STATIQUE, DHCP ou DÉSACTIVÉ pour la configuration **Admin network IP**.
   - Si vous ne souhaitez pas utiliser le réseau d'administration, sélectionnez DÉSACTIVÉ et entrez **0.0.0.0** pour l'adresse IP du réseau d'administration. Vous pouvez laisser les autres champs vides.
   - Si vous sélectionnez STATIQUE, saisissez l'adresse IP* du réseau **Admin, *masque réseau Admin**, **passerelle réseau Admin** et **MTU du réseau Admin**.
   - Si vous sélectionnez STATIQUE, entrez la liste **réseau d'administration externe de sous-réseau**. Vous devez également configurer une passerelle.
   - Si vous sélectionnez DHCP, l'adresse IP **réseau Admin**, **masque réseau Admin** et **passerelle réseau Admin** sont automatiquement affectées.

b. Dans la section **réseau client (eth2)**, sélectionnez STATIQUE, DHCP ou DÉSACTIVÉ pour la configuration **IP réseau client**.
   - Si vous ne souhaitez pas utiliser le réseau client, sélectionnez DÉSACTIVÉ et entrez **0.0.0.0** pour l'adresse IP du réseau client. Vous pouvez laisser les autres champs vides.
   - Si vous sélectionnez STATIQUE, entrez l'adresse IP * du réseau client*, **masque de réseau client**, **passerelle de réseau client** et **MTU du réseau client**.
   - Si vous sélectionnez DHCP, l'adresse IP * du réseau client*, **masque de réseau client** et **passerelle réseau client** sont automatiquement affectées.

8. Vérifiez la configuration de l'ordinateur virtuel et apportez les modifications nécessaires.
9. Lorsque vous êtes prêt à terminer, sélectionnez **Finish** pour lancer le téléchargement de la machine virtuelle.
10. si vous avez déployé ce nœud dans le cadre d'une opération de restauration et qu'il ne s'agit pas d'une restauration de nœud complet, effectuez les opérations suivantes une fois le déploiement terminé :

    a. Cliquez avec le bouton droit de la souris sur la machine virtuelle et sélectionnez **Modifier les paramètres**.

    b. Sélectionnez chaque disque dur virtuel par défaut qui a été désigné pour le stockage, puis sélectionnez **Supprimer**.

    c. En fonction de vos conditions de restauration des données, ajoutez de nouveaux disques virtuels en fonction de vos besoins de stockage, reconnectez tous les disques durs virtuels conservés sur le nœud de grille défaillant précédemment retiré, ou les deux.

    Notez les consignes importantes suivantes :

    - Si vous ajoutez de nouveaux disques, vous devez utiliser le même type de périphérique de stockage que celui utilisé avant la restauration du noeud.
    - Le fichier .ovf de nœud de stockage définit plusieurs VMDK pour le stockage. À moins que ces VMDK ne répondent à vos besoins de stockage, vous devez les supprimer et attribuer des VMDK ou des RDM appropriés pour le stockage avant de mettre le nœud sous tension. Les VMDK sont plus fréquemment utilisés dans les environnements VMware et sont plus faciles à gérer, tandis que les RDM peuvent fournir de meilleures performances pour les charges de travail utilisant des objets de plus grande taille (par exemple, plus de 100 Mo).

11. Si vous devez remappage les ports utilisés par ce nœud, effectuez les étapes suivantes.

Vous devrez peut-être remapper un port si les règles de réseau de votre entreprise limitent l'accès à un ou plusieurs ports utilisés par StorageGRID. Voir la "instructions de mise en réseau" Pour les ports utilisés par StorageGRID.

> Ne mappez pas les ports utilisés dans les terminaux d'équilibrage de charge.

a. Sélectionnez la nouvelle VM.
b. Dans l'onglet configurer, sélectionnez **Paramètres** > **Options vApp**. L'emplacement de **vApp Options** dépend de la version de vCenter.
c. Dans le tableau **Propriétés**, localisez PORT_REMAPPAGE_INBOUND et PORT_REMAPPAGE.
d. Pour mapper symétriquement les communications entrantes et sortantes d'un port, sélectionnez **PORT_REMAPPAGE**.

> Si seul PORT_REMAPPAGE est défini, le mappage que vous spécifiez s'applique aux communications entrantes et sortantes. Si PORT_REMAPPAGE_INBOUND est également spécifié, PORT_REMAPPAGE s'applique uniquement aux communications sortantes.

   i. Faites défiler l'écran jusqu'en haut du tableau et sélectionnez **Modifier**.
   ii. Dans l'onglet Type, sélectionnez **configurable par l'utilisateur**, puis **Enregistrer**.
   iii. Sélectionnez **définir la valeur**.
   iv. Saisissez le mappage de port :

```
<network type>/<protocol>/<default port used by grid node>/<new port>
```

   `<network type>` est un grid, un administrateur ou un client, et `<protocol>` est tcp ou udp.

   Par exemple, pour remappage le trafic ssh du port 22 vers le port 3022, entrez :

```
client/tcp/22/3022
```

   i. Sélectionnez **OK**.

e. Pour spécifier le port utilisé pour les communications entrantes vers le nœud, sélectionnez **PORT_REMAPPAGE_INBOUND**.

> Si vous spécifiez PORT_REMAP_INBOUND et que vous n'indiquez pas de valeur pour PORT_REMAP, les communications sortantes pour le port sont inchangées.

   i. Faites défiler l'écran jusqu'en haut du tableau et sélectionnez **Modifier**.
   ii. Dans l'onglet Type, sélectionnez **configurable par l'utilisateur**, puis **Enregistrer**.
   iii. Sélectionnez **définir la valeur**.
   iv. Saisissez le mappage de port :

```
<network type>/<protocol>/<remapped inbound port>/<default inbound port
used by grid node>
```

   `<network type>` est un grid, un administrateur ou un client, et `<protocol>` est tcp ou udp.

Par exemple, pour remappage le trafic SSH entrant envoyé au port 3022 afin qu'il soit reçu au port 22 par le nœud de grille, entrez ce qui suit :

```
client/tcp/3022/22
```

i. Sélectionnez **OK**

12. Pour augmenter les valeurs par défaut du CPU ou de la mémoire du nœud :
    a. Cliquez avec le bouton droit de la souris sur la machine virtuelle et sélectionnez **Modifier les paramètres**.
    b. Modifiez le nombre de CPU ou la quantité de mémoire nécessaire.

       Définissez la **réserve de mémoire** sur la même taille que la **mémoire** allouée à la machine virtuelle.

    c. Sélectionnez **OK**.
13. Mise sous tension de la machine virtuelle

Une fois que vous avez terminé

Si vous avez déployé ce nœud dans le cadre d'une procédure d'extension ou de restauration, revenez à ces instructions pour terminer la procédure.

Configuration du grid et installation complète (VMware)

Accédez au Grid Manager

Le gestionnaire de grille permet de définir toutes les informations nécessaires à la configuration du système StorageGRID.

Avant de commencer

Le nœud d'administration principal doit être déployé et avoir terminé la séquence de démarrage initiale.

Étapes

1. Ouvrez votre navigateur Web et accédez à l'une des adresses suivantes :

   `https://primary_admin_node_ip`

   `https://client_network_ip`

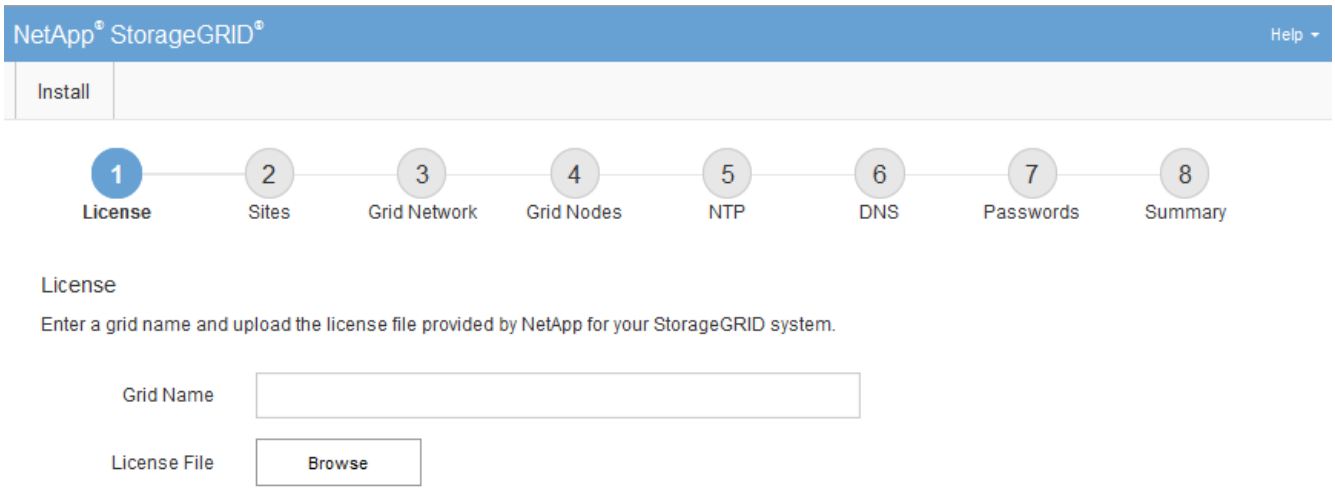
   Vous pouvez également accéder à Grid Manager sur le port 8443 :

   `https://primary_admin_node_ip:8443`

   > Vous pouvez utiliser l'adresse IP du noeud d'administration principal sur le réseau Grid ou sur le réseau Admin, en fonction de votre configuration réseau. Vous devrez peut-être utiliser l'option Security/Advanced de votre navigateur pour accéder à un certificat non approuvé.

2. Sélectionnez **installer un système StorageGRID**.

   La page utilisée pour configurer une grille StorageGRID s'affiche.



Spécifier les informations de licence StorageGRID

Vous devez indiquer le nom de votre système StorageGRID et télécharger le fichier de licence fourni par NetApp.

Étapes

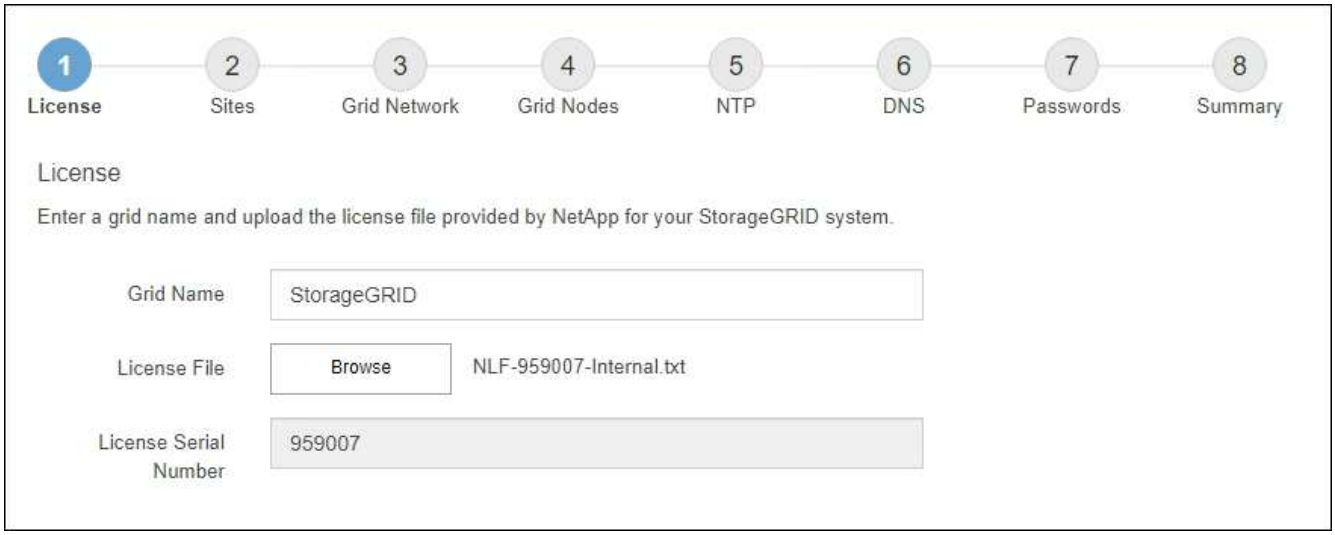
1. Sur la page Licence, entrez un nom significatif pour votre système StorageGRID dans le champ **Nom de la grille**.

   Après l'installation, le nom s'affiche en haut du menu nœuds.

2. Sélectionnez **Browse**, localisez le fichier de licence NetApp (`NLF-unique-id.txt`) Et sélectionnez **Ouvrir**.

   Le fichier de licence est validé et le numéro de série s'affiche.

   > L'archive d'installation de StorageGRID inclut une licence gratuite qui ne fournit aucun droit d'assistance pour le produit. Vous pouvez effectuer une mise à jour vers une licence offrant une assistance après l'installation.



3. Sélectionnez **Suivant**.

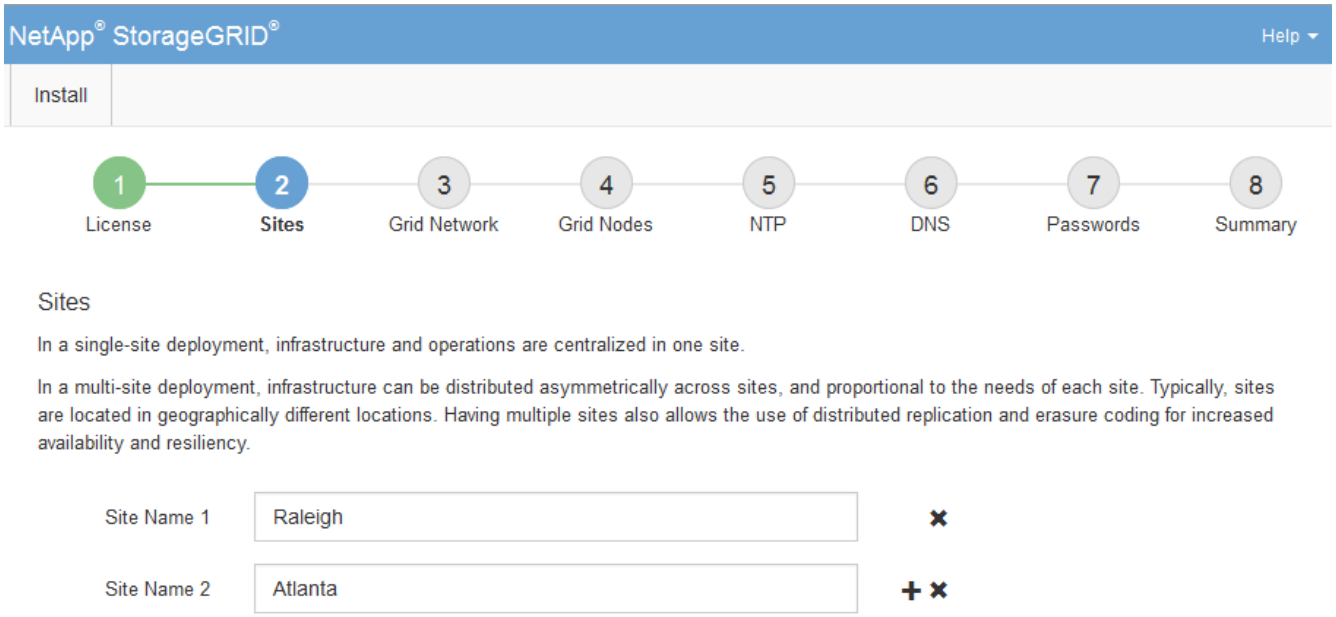
Ajouter des sites

Vous devez créer au moins un site lorsque vous installez StorageGRID. Vous pouvez créer des sites supplémentaires pour augmenter la fiabilité et la capacité de stockage de votre système StorageGRID.

Étapes

1. Sur la page sites, saisissez **Nom du site**.
2. Pour ajouter d'autres sites, cliquez sur le signe plus en regard de la dernière entrée du site et entrez le nom dans la zone de texte Nouveau **Nom du site**.

   Ajoutez autant de sites supplémentaires que nécessaire pour votre topologie de grille. Vous pouvez ajouter jusqu'à 16 sites.



3. Cliquez sur **Suivant**.

Spécifiez les sous-réseaux du réseau de la grille

Vous devez spécifier les sous-réseaux utilisés sur le réseau grille.

Description de la tâche

Les entrées de sous-réseau incluent les sous-réseaux du réseau de la grille pour chaque site de votre système StorageGRID, ainsi que tous les sous-réseaux devant être accessibles via le réseau de la grille.

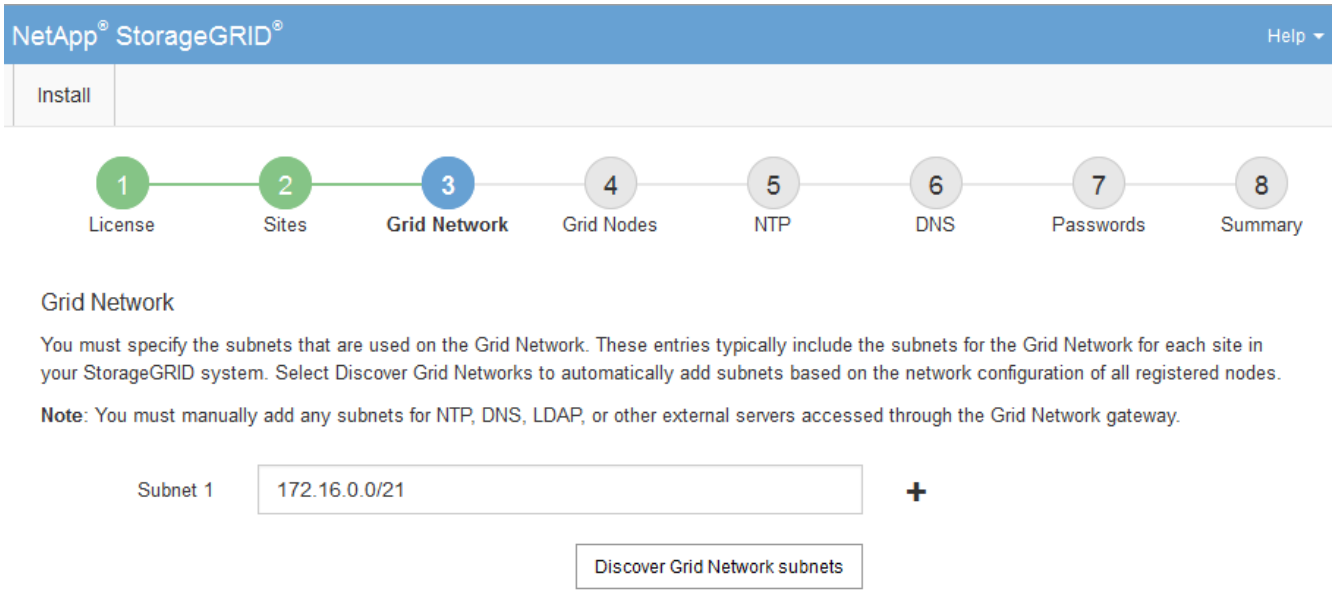
Si vous avez plusieurs sous-réseaux de grille, la passerelle de réseau de grille est requise. Tous les sous-réseaux de la grille spécifiés doivent être accessibles via cette passerelle.

Étapes

1. Spécifiez l'adresse réseau CIDR pour au moins un réseau Grid dans la zone de texte **sous-réseau 1**.
2. Cliquez sur le signe plus à côté de la dernière entrée pour ajouter une entrée réseau supplémentaire.

   Si vous avez déjà déployé au moins un nœud, cliquez sur **détecter les sous-réseaux de réseaux de grille** pour remplir automatiquement la liste de sous-réseaux de réseau de grille avec les sous-réseaux

signalés par les nœuds de grille enregistrés avec le gestionnaire de grille.



3. Cliquez sur **Suivant**.

Approuver les nœuds de la grille en attente

Vous devez approuver chaque nœud de la grille pour pouvoir rejoindre le système StorageGRID.

Avant de commencer

Vous avez déployé l'ensemble des nœuds grid virtuels et d'appliance StorageGRID.

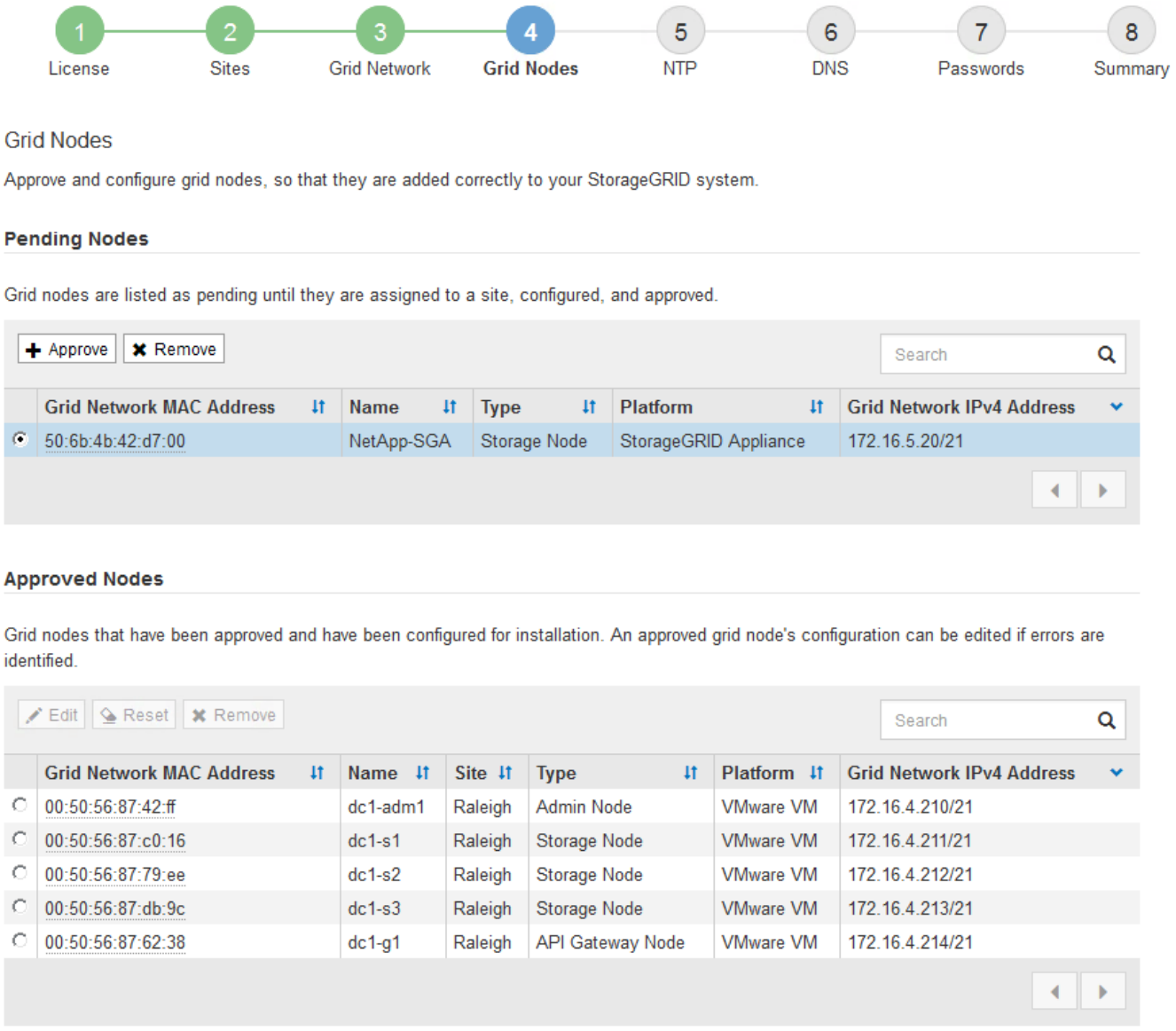
> Il est plus efficace d'effectuer une seule installation de tous les nœuds, au lieu d'installer certains nœuds maintenant et certains nœuds ultérieurement.

Étapes

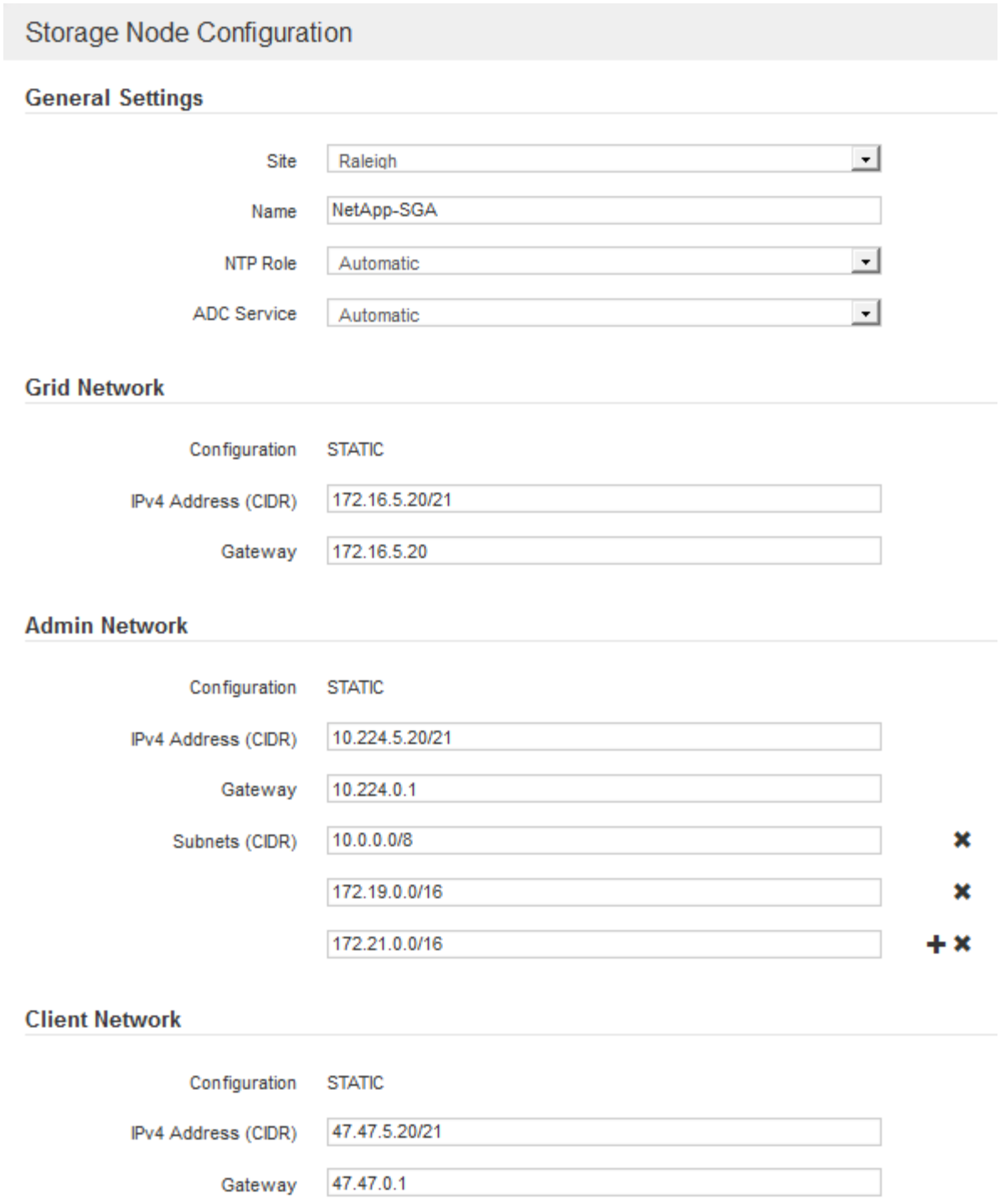
1. Consultez la liste nœuds en attente et vérifiez qu'elle affiche tous les nœuds de la grille que vous avez déployés.

   > Si un nœud de grid n'est pas inclus, vérifiez qu'il a été déployé correctement.

2. Sélectionnez le bouton radio à côté d'un noeud en attente que vous souhaitez approuver.



3. Cliquez sur **approuver**.
4. Dans Paramètres généraux, modifiez les paramètres des propriétés suivantes, si nécessaire :



- **Site** : le nom système du site pour ce noeud de grille.
- **Nom** : le nom du système pour le noeud. Le nom par défaut est le nom que vous avez spécifié lors de la configuration du nœud.

  Les noms de système sont requis pour les opérations StorageGRID internes et ne peuvent pas être modifiés une fois l'installation terminée. Cependant, au cours de cette étape du processus d'installation, vous pouvez modifier les noms de système selon vos besoins.

> Pour un noeud VMware, vous pouvez changer le nom ici, mais cette action ne changera pas le nom de la machine virtuelle dans vSphere.

- **NTP role** : rôle NTP (Network Time Protocol) du noeud de la grille. Les options sont **automatique**, **primaire** et **client**. Si vous sélectionnez **automatique**, le rôle principal est attribué aux nœuds d'administration, aux nœuds de stockage avec services ADC, aux nœuds de passerelle et à tous les nœuds de grille ayant des adresses IP non statiques. Le rôle client est attribué à tous les autres nœuds de la grille.

  > Assurez-vous qu'au moins deux nœuds de chaque site peuvent accéder à au moins quatre sources NTP externes. Si un seul nœud d'un site peut atteindre les sources NTP, des problèmes de synchronisation surviennent en cas de panne de ce nœud. En outre, la désignation de deux nœuds par site en tant que sources NTP principales assure une synchronisation précise si un site est isolé du reste de la grille.

- **Service ADC** (nœuds de stockage uniquement) : sélectionnez **automatique** pour permettre au système de déterminer si le nœud requiert le service contrôleur de domaine administratif (ADC). Le service ADC conserve le suivi de l'emplacement et de la disponibilité des services de réseau. Au moins trois nœuds de stockage de chaque site doivent inclure le service ADC. Vous ne pouvez pas ajouter le service ADC à un nœud après son déploiement.

5. Dans le réseau de grille, modifiez les paramètres des propriétés suivantes si nécessaire :

   - **Adresse IPv4 (CIDR)** : adresse réseau CIDR pour l'interface Grid Network (eth0 dans le conteneur). Par exemple : 192.168.1.234/21
   - **Gateway** : la passerelle réseau Grid. Par exemple : 192.168.0.1

     > La passerelle est requise en cas de sous-réseaux de grille multiples.

   > Si vous avez sélectionné DHCP pour la configuration du réseau Grid et que vous modifiez la valeur ici, la nouvelle valeur sera configurée en tant qu'adresse statique sur le nœud. Vous devez vous assurer que l'adresse IP résultante ne se trouve pas dans un pool d'adresses DHCP.

6. Si vous souhaitez configurer le réseau d'administration pour le nœud de la grille, ajoutez ou mettez à jour les paramètres de la section réseau d'administration si nécessaire.

   Entrez les sous-réseaux de destination des routes en dehors de cette interface dans la zone de texte **sous-réseaux (CIDR)**. En cas de sous-réseaux d'administration multiples, la passerelle d'administration est requise.

   > Si vous avez sélectionné DHCP pour la configuration du réseau d'administration et que vous modifiez la valeur ici, la nouvelle valeur sera configurée en tant qu'adresse statique sur le nœud. Vous devez vous assurer que l'adresse IP résultante ne se trouve pas dans un pool d'adresses DHCP.

   Appareils : pour une appliance StorageGRID, si le réseau d'administration n'a pas été configuré lors de l'installation initiale à l'aide du programme d'installation de l'appliance StorageGRID, il ne peut pas être configuré dans cette boîte de dialogue Gestionnaire de grille. Au lieu de cela, vous devez procéder comme suit :

   a. Redémarrez l'appliance : dans le programme d'installation de l'appliance, sélectionnez **Avancé** > **redémarrer**.

      Le redémarrage peut prendre plusieurs minutes.

b. Sélectionnez **configurer réseau** > **Configuration lien** et activez les réseaux appropriés.

c. Sélectionnez **configurer réseau** > **Configuration IP** et configurez les réseaux activés.

d. Revenez à la page d'accueil et cliquez sur **Démarrer l'installation**.

e. Dans le Gestionnaire de grille : si le nœud est répertorié dans le tableau nœuds approuvés, supprimez-le.

f. Supprimez le nœud du tableau nœuds en attente.

g. Attendez que le nœud réapparaisse dans la liste nœuds en attente.

h. Confirmez que vous pouvez configurer les réseaux appropriés. Elles doivent déjà être renseignées avec les informations que vous avez fournies sur la page Configuration IP du programme d'installation de l'appliance.

   Pour plus d'informations, reportez-vous au "Démarrage rapide pour l'installation du matériel" pour trouver les instructions relatives à votre appareil.

7. Si vous souhaitez configurer le réseau client pour le nœud de grille, ajoutez ou mettez à jour les paramètres dans la section réseau client si nécessaire. Si le réseau client est configuré, la passerelle est requise et devient la passerelle par défaut du noeud après l'installation.

   > Si vous avez sélectionné DHCP pour la configuration du réseau client et que vous modifiez la valeur ici, la nouvelle valeur sera configurée en tant qu'adresse statique sur le nœud. Vous devez vous assurer que l'adresse IP résultante ne se trouve pas dans un pool d'adresses DHCP.

   Appareils : pour une appliance StorageGRID, si le réseau client n'a pas été configuré lors de l'installation initiale à l'aide du programme d'installation de l'appliance StorageGRID, il ne peut pas être configuré dans cette boîte de dialogue Gestionnaire de grille. Au lieu de cela, vous devez procéder comme suit :

   a. Redémarrez l'appliance : dans le programme d'installation de l'appliance, sélectionnez **Avancé** > **redémarrer**.

      Le redémarrage peut prendre plusieurs minutes.

   b. Sélectionnez **configurer réseau** > **Configuration lien** et activez les réseaux appropriés.

   c. Sélectionnez **configurer réseau** > **Configuration IP** et configurez les réseaux activés.

   d. Revenez à la page d'accueil et cliquez sur **Démarrer l'installation**.

   e. Dans le Gestionnaire de grille : si le nœud est répertorié dans le tableau nœuds approuvés, supprimez-le.

   f. Supprimez le nœud du tableau nœuds en attente.

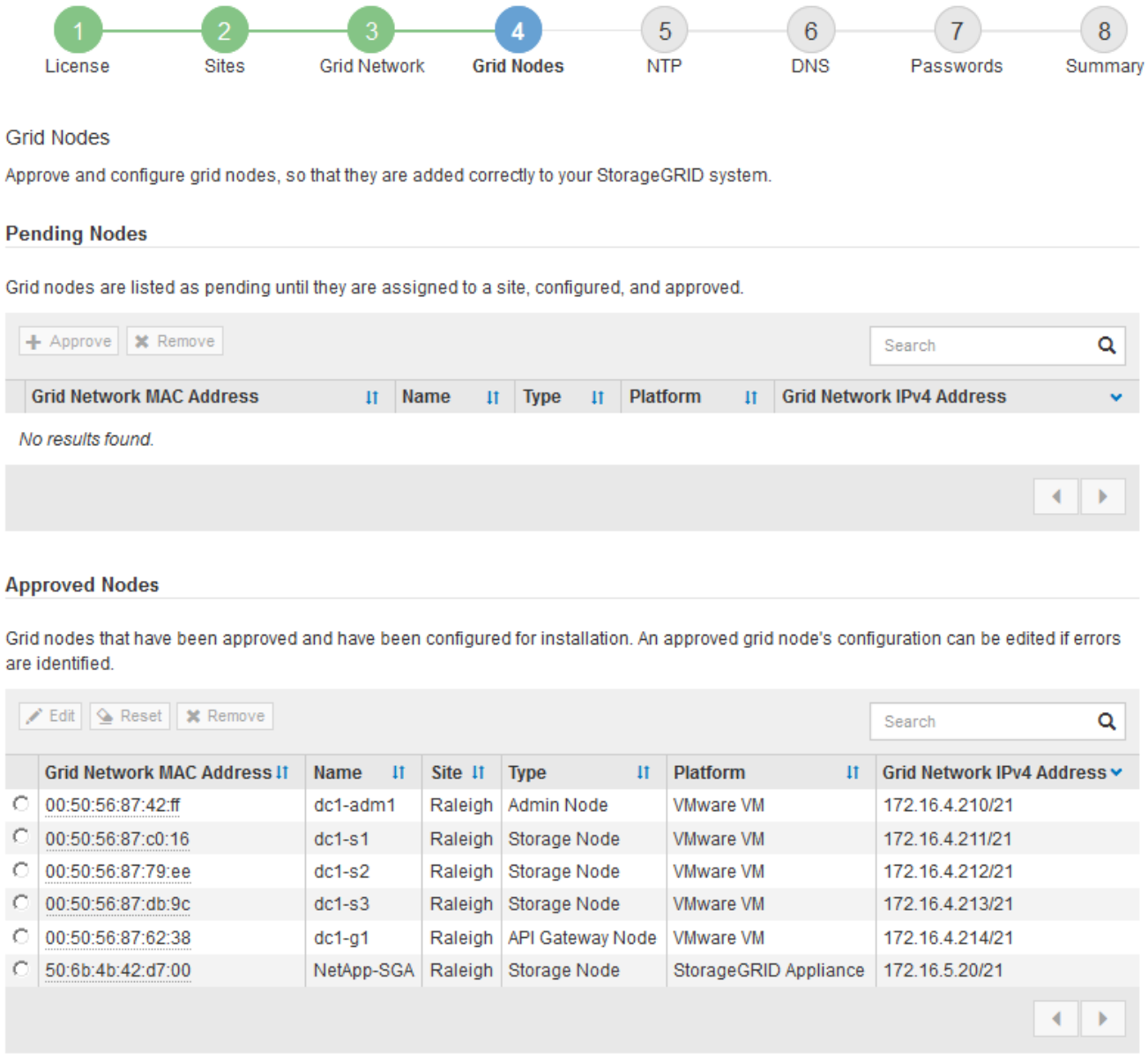
   g. Attendez que le nœud réapparaisse dans la liste nœuds en attente.

   h. Confirmez que vous pouvez configurer les réseaux appropriés. Elles doivent déjà être renseignées avec les informations que vous avez fournies sur la page Configuration IP du programme d'installation de l'appliance.

      Pour plus d'informations, reportez-vous au "Démarrage rapide pour l'installation du matériel" pour trouver les instructions relatives à votre appareil.

8. Cliquez sur **Enregistrer**.

   L'entrée de nœud de la grille passe à la liste nœuds approuvés.



9. Répétez ces étapes pour chaque nœud de grille en attente à approuver.

   Vous devez approuver tous les nœuds que vous souhaitez dans la grille. Cependant, vous pouvez revenir à cette page à tout moment avant de cliquer sur **installer** sur la page Résumé. Vous pouvez modifier les propriétés d'un nœud de grille approuvé en sélectionnant son bouton radio et en cliquant sur **Modifier**.

10. Lorsque vous avez terminé d'approuver les nœuds de la grille, cliquez sur **Suivant**.

Spécifiez les informations sur le serveur Network Time Protocol

Vous devez spécifier les informations de configuration du protocole NTP (Network Time Protocol) pour le système StorageGRID, de sorte que les opérations effectuées sur des serveurs distincts puissent rester synchronisées.

Description de la tâche

Vous devez indiquer des adresses IPv4 pour les serveurs NTP.

Vous devez indiquer des serveurs NTP externes. Les serveurs NTP spécifiés doivent utiliser le protocole NTP.

Vous devez spécifier quatre références de serveur NTP de Stratum 3 ou supérieur pour éviter les problèmes de dérive du temps.

> Lorsque vous spécifiez la source NTP externe pour une installation StorageGRID de niveau production, n'utilisez pas le service heure Windows (W32Time) sur une version de Windows antérieure à Windows Server 2016. Le service de temps des versions antérieures de Windows n'est pas suffisamment précis et n'est pas pris en charge par Microsoft pour une utilisation dans des environnements à haute précision, tels que StorageGRID.

"Limite de prise en charge pour configurer le service de temps Windows pour des environnements de haute précision"

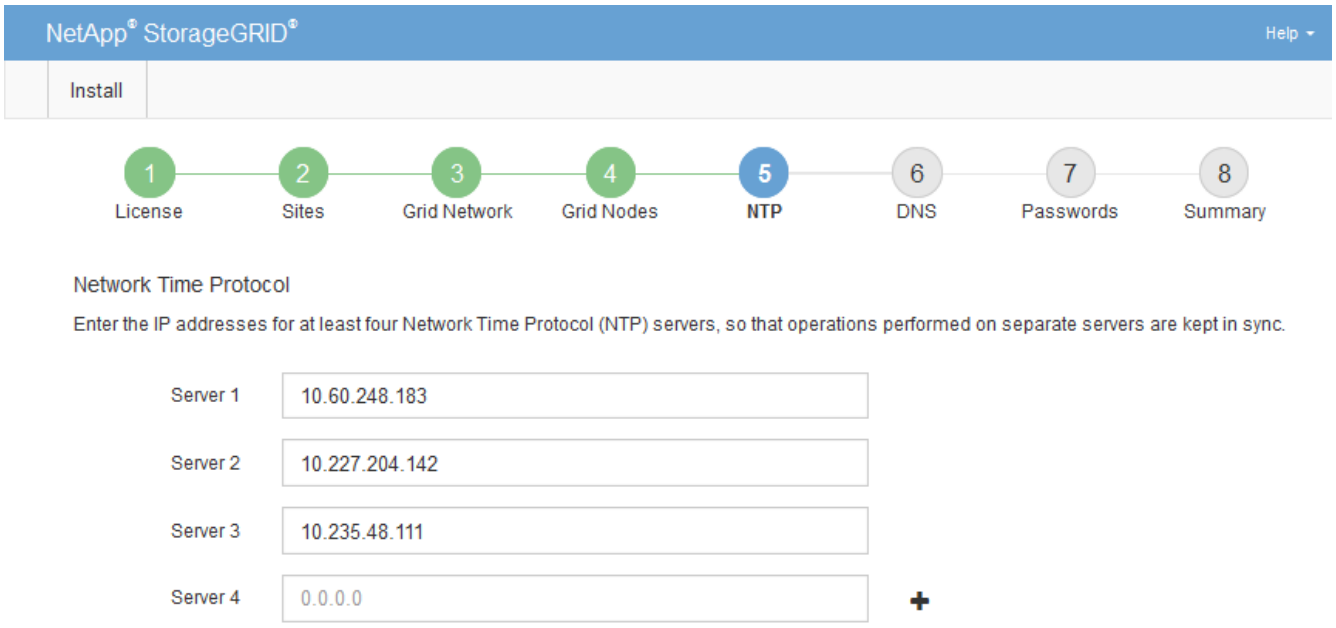
Les serveurs NTP externes sont utilisés par les nœuds auxquels vous avez précédemment attribué des rôles NTP primaires.

> Assurez-vous qu'au moins deux nœuds de chaque site peuvent accéder à au moins quatre sources NTP externes. Si un seul nœud d'un site peut atteindre les sources NTP, des problèmes de synchronisation surviennent en cas de panne de ce nœud. En outre, la désignation de deux nœuds par site en tant que sources NTP principales assure une synchronisation précise si un site est isolé du reste de la grille.

Effectuez des vérifications supplémentaires pour VMware, par exemple en vous assurant que l'hyperviseur utilise la même source NTP que la machine virtuelle, et en utilisant VMTools pour désactiver la synchronisation horaire entre l'hyperviseur et les machines virtuelles StorageGRID.

Étapes

1. Spécifiez les adresses IPv4 pour au moins quatre serveurs NTP dans les zones de texte **Server 1** à **Server 4**.
2. Si nécessaire, sélectionnez le signe plus en regard de la dernière entrée pour ajouter des entrées de serveur supplémentaires.



3. Sélectionnez **Suivant**.

Spécifiez les informations du serveur DNS

Vous devez spécifier des informations DNS pour votre système StorageGRID afin de pouvoir accéder aux serveurs externes en utilisant des noms d'hôte au lieu d'adresses IP.

Description de la tâche

Spécification "Informations sur le serveur DNS" Vous permet d'utiliser des noms d'hôte de nom de domaine complet (FQDN) plutôt que des adresses IP pour les notifications par e-mail et AutoSupport.

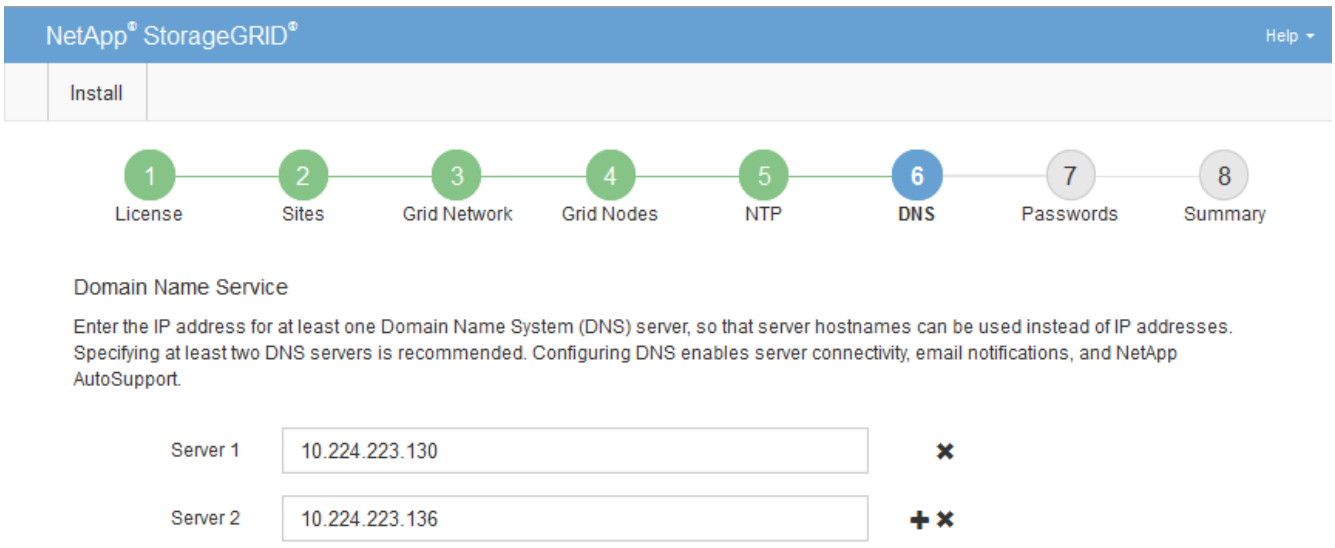
Pour garantir un fonctionnement correct, spécifiez deux ou trois serveurs DNS. Si vous spécifiez plus de trois, il est possible que seulement trois soient utilisés en raison des limitations connues du système d'exploitation sur certaines plates-formes. Si vous avez des restrictions de routage dans votre environnement, vous pouvez le faire "Personnaliser la liste des serveurs DNS" Pour les nœuds individuels (généralement tous les nœuds d'un site) d'utiliser un ensemble différent de trois serveurs DNS.

Si possible, utilisez des serveurs DNS auxquels chaque site peut accéder localement pour vous assurer qu'un site isdébarqué peut résoudre les FQDN pour les destinations externes.

Si les informations du serveur DNS sont omises ou mal configurées, une alarme DNST est déclenchée sur le service SSM de chaque nœud de la grille. L'alarme s'efface lorsque le DNS est configuré correctement et que les nouvelles informations sur le serveur ont atteint tous les nœuds de la grille.

Étapes

1. Spécifiez l'adresse IPv4 pour au moins un serveur DNS dans la zone de texte **Server 1**.
2. Si nécessaire, sélectionnez le signe plus en regard de la dernière entrée pour ajouter des entrées de serveur supplémentaires.



   La meilleure pratique consiste à spécifier au moins deux serveurs DNS. Vous pouvez indiquer jusqu'à six serveurs DNS.

3. Sélectionnez **Suivant**.

Spécifiez les mots de passe système StorageGRID

Dans le cadre de l'installation de votre système StorageGRID, vous devez saisir les mots de passe à utiliser pour sécuriser votre système et effectuer des tâches de maintenance.

Description de la tâche

Utilisez la page installer des mots de passe pour spécifier le mot de passe de provisionnement et le mot de passe utilisateur root de la gestion de grille.

- La phrase secrète de provisionnement est utilisée comme clé de chiffrement et n'est pas stockée par le système StorageGRID.
- Vous devez disposer du mot de passe de provisionnement pour les procédures d'installation, d'extension et de maintenance, y compris le téléchargement du progiciel de restauration. Il est donc important de stocker la phrase secrète de provisionnement dans un emplacement sécurisé.
- Vous pouvez modifier la phrase de passe de provisionnement à partir de Grid Manager si vous en avez la version actuelle.
- Le mot de passe de l'utilisateur root de la gestion de grille peut être modifié à l'aide de Grid Manager.
- La console de ligne de commande générée de manière aléatoire et les mots de passe SSH sont stockés dans le `Passwords.txt` Fichier dans le progiciel de restauration.

Étapes

1. Dans **phrase de passe d'approvisionnement**, entrez la phrase de passe d'approvisionnement qui sera nécessaire pour modifier la topologie de la grille de votre système StorageGRID.

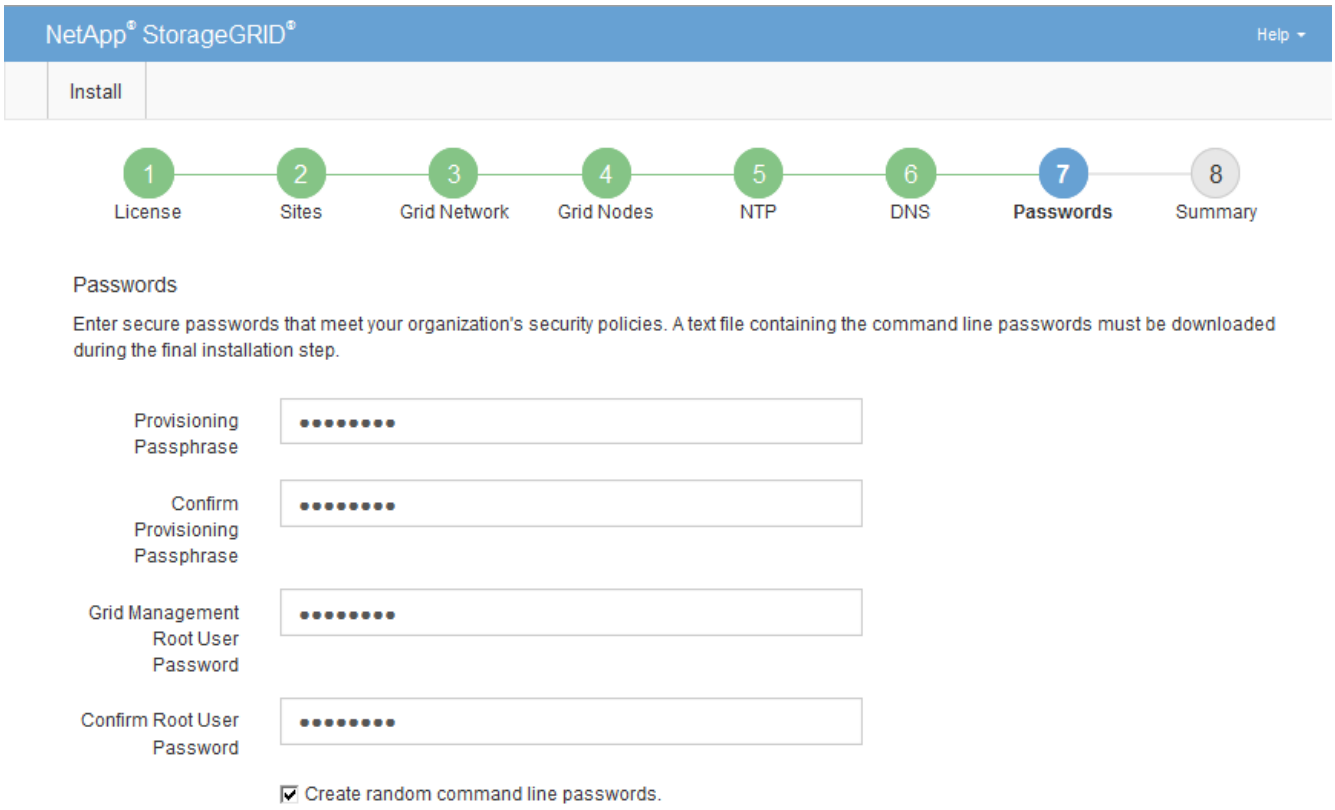
   Stockez la phrase secrète de provisionnement dans un endroit sécurisé.

   > Si une fois l'installation terminée et que vous souhaitez modifier ultérieurement le mot de passe de provisionnement, vous pouvez utiliser le Gestionnaire de grille. Sélectionnez **CONFIGURATION** > **contrôle d'accès** > **mots de passe de grille**.

2. Dans **Confirm Provisioning Passphrase**, saisissez à nouveau la phrase de passe de provisionnement pour la confirmer.
3. Dans **Grid Management Root User Password**, entrez le mot de passe à utiliser pour accéder au gestionnaire de grille en tant qu'utilisateur « root ».

   Stockez le mot de passe en lieu sûr.

4. Dans **confirmer le mot de passe de l'utilisateur racine**, entrez à nouveau le mot de passe de Grid Manager pour le confirmer.



5. Si vous installez une grille à des fins de démonstration de faisabilité ou de démonstration, désactivez éventuellement la case **Créer des mots de passe de ligne de commande aléatoires**.

   Pour les déploiements en production, des mots de passe aléatoires doivent toujours être utilisés pour des raisons de sécurité. Désactivez **Créez des mots de passe de ligne de commande aléatoires** uniquement pour les grilles de démonstration si vous souhaitez utiliser des mots de passe par défaut pour accéder aux nœuds de grille à partir de la ligne de commande à l'aide du compte "`root'" ou "'admin".

   > Vous êtes invité à télécharger le fichier du progiciel de récupération (`sgws-recovery-package-id-revision.zip`) Après avoir cliqué sur **installer** sur la page Résumé. Vous devez "téléchargez ce fichier" pour terminer l'installation. Les mots de passe requis pour accéder au système sont stockés dans le `Passwords.txt` Fichier, contenu dans le fichier du progiciel de récupération.

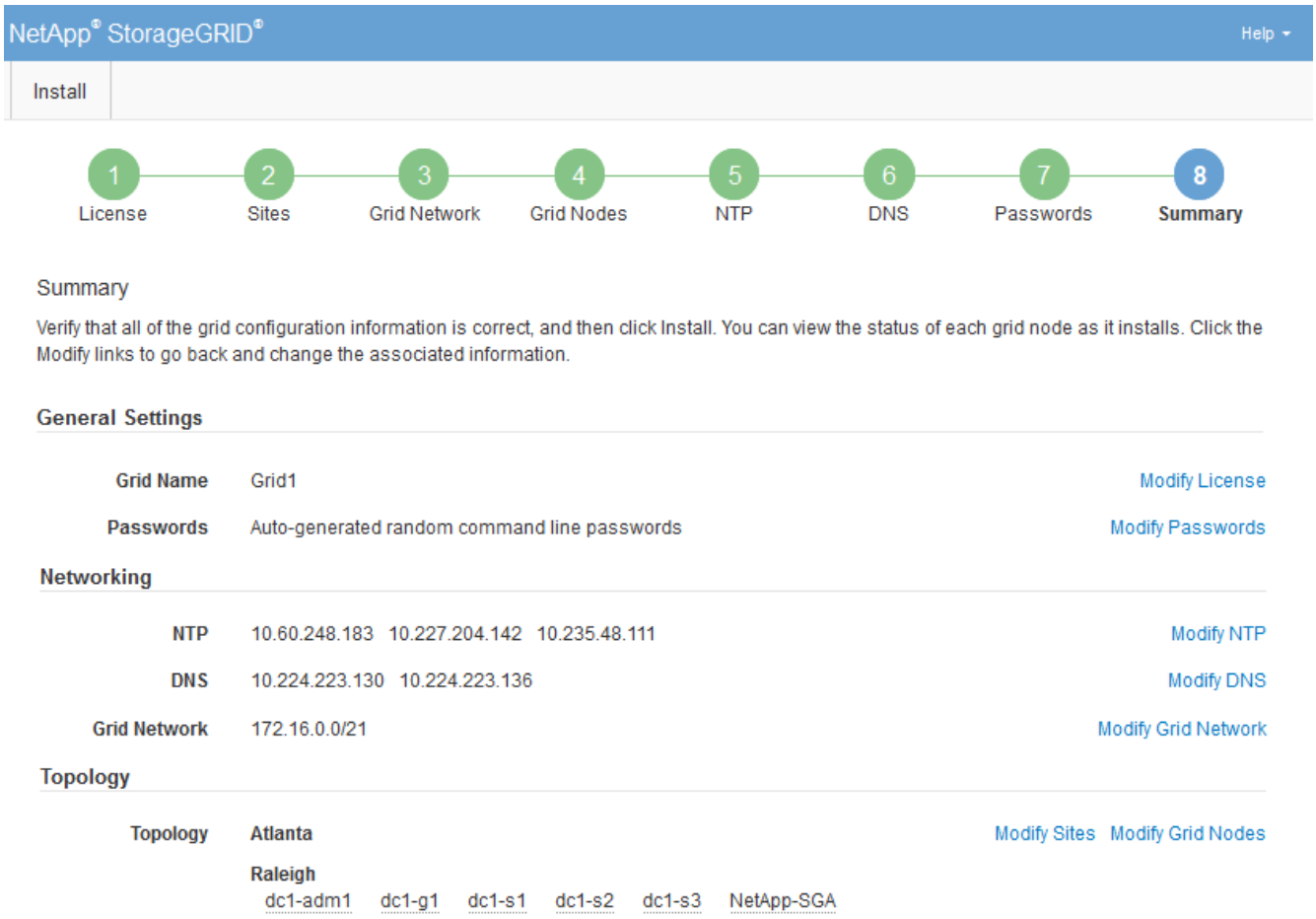
6. Cliquez sur **Suivant**.

Vérifiez votre configuration et terminez l'installation

Vous devez examiner attentivement les informations de configuration que vous avez saisies pour vous assurer que l'installation s'effectue correctement.

Étapes

1. Afficher la page **Résumé**.



2. Vérifiez que toutes les informations de configuration de la grille sont correctes. Utilisez les liens Modifier de la page Résumé pour revenir en arrière et corriger les erreurs.
3. Cliquez sur **installer**.

> Si un nœud est configuré pour utiliser le réseau client, la passerelle par défaut de ce nœud passe du réseau Grid au réseau client lorsque vous cliquez sur **installer**. Si vous perdez la connectivité, vous devez vous assurer que vous accédez au nœud d'administration principal via un sous-réseau accessible. Voir "Instructions de mise en réseau" pour plus d'informations.

4. Cliquez sur **Télécharger le progiciel de récupération**.

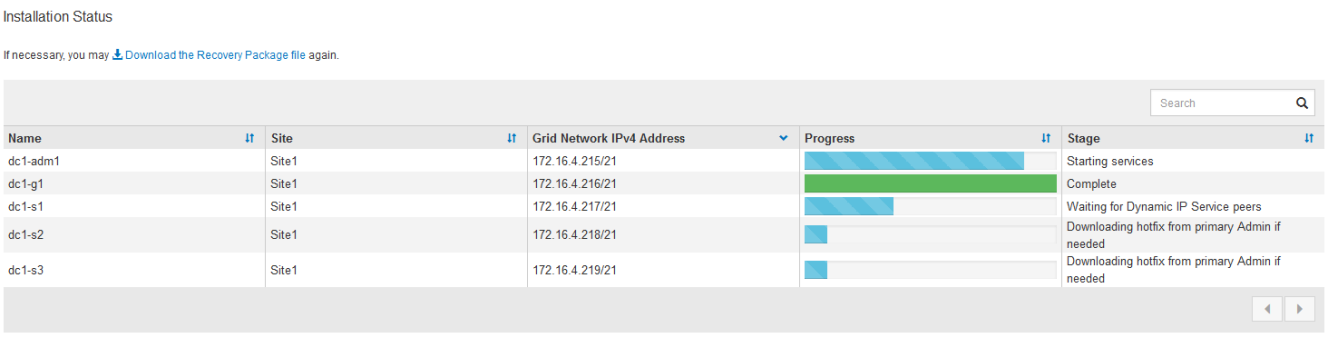
   Lorsque l'installation progresse jusqu'au point où la topologie de la grille est définie, vous êtes invité à télécharger le fichier du progiciel de récupération (`.zip`), et confirmez que vous pouvez accéder avec succès au contenu de ce fichier. Vous devez télécharger le fichier Recovery Package afin de pouvoir restaurer le système StorageGRID en cas de défaillance d'un ou de plusieurs nœuds de la grille. L'installation se poursuit en arrière-plan, mais vous ne pouvez pas terminer l'installation et accéder au système StorageGRID tant que vous n'avez pas téléchargé et vérifié ce fichier.

5. Vérifiez que vous pouvez extraire le contenu du `.zip` enregistrez-le ensuite à deux emplacements distincts, sécurisés et sécurisés.

> Le fichier du progiciel de récupération doit être sécurisé car il contient des clés de cryptage et des mots de passe qui peuvent être utilisés pour obtenir des données du système StorageGRID.

6. Cochez la case **J'ai téléchargé et vérifié le fichier du progiciel de récupération**, puis cliquez sur **Suivant**.

   Si l'installation est toujours en cours, la page d'état s'affiche. Cette page indique la progression de l'installation pour chaque nœud de la grille.



   Lorsque l'étape complète est atteinte pour tous les nœuds de la grille, la page de connexion de Grid Manager s'affiche.

7. Connectez-vous au gestionnaire de grille à l'aide de l'utilisateur « root » et du mot de passe que vous avez spécifié lors de l'installation.

Instructions de post-installation

Une fois le déploiement et la configuration des nœuds de la grille effectués, suivez ces instructions pour l'adressage DHCP et les modifications de configuration réseau.

- Si DHCP était utilisé pour attribuer des adresses IP, configurez une réservation DHCP pour chaque adresse IP sur les réseaux utilisés.

  Vous ne pouvez configurer DHCP que pendant la phase de déploiement. Vous ne pouvez pas configurer DHCP pendant la configuration.

  > Les nœuds redémarrent lors de la modification de leurs adresses IP, ce qui peut entraîner des pannes si une modification d'adresse DHCP affecte plusieurs nœuds simultanément.

- Vous devez utiliser les procédures Modifier IP pour modifier les adresses IP, les masques de sous-réseau et les passerelles par défaut pour un noeud de grille. Voir "Configurez les adresses IP".
- Si vous modifiez la configuration réseau, y compris le routage et les modifications de passerelle, la connectivité client au nœud d'administration principal et à d'autres nœuds de la grille risque d'être perdue. En fonction des modifications de réseau appliquées, vous devrez peut-être rétablir ces connexions.

Automatisation de l'installation (VMware)

Vous pouvez utiliser VMware vSphere pour automatiser le déploiement des nœuds grid. Vous pouvez également automatiser la configuration de StorageGRID.

Automatisez le déploiement de nœuds grid

Utilisez VMware vSphere pour automatiser le déploiement des nœuds grid.

Avant de commencer

- Vous avez accès à un système Linux/Unix avec Bash 3.2 ou version ultérieure.
- VMware OVF Tool 4.1 est installé et correctement configuré.
- Vous connaissez le nom d'utilisateur et le mot de passe requis pour accéder à VMware vSphere à l'aide de l'outil OVF.
- Vous connaissez l'URL d'infrastructure virtuelle (VI) pour l'emplacement dans vSphere où vous souhaitez déployer les machines virtuelles StorageGRID. Cette URL est généralement une vApp ou un pool de ressources. Par exemple : `vi://vcenter.example.com/vi/sgws`

> Vous pouvez utiliser VMware `ovftool` utilitaire pour déterminer cette valeur (voir `ovftool` documentation pour plus de détails).

> Si vous déployez une vApp, les machines virtuelles ne démarrent pas automatiquement la première fois et vous devez les mettre sous tension manuellement.

- Vous avez collecté toutes les informations requises pour le fichier de configuration. Voir "Collecte d'informations sur votre environnement de déploiement" pour plus d'informations.
- Vous avez accès aux fichiers suivants à partir de l'archive d'installation de VMware pour StorageGRID :

Nom du fichier	Description
NetApp-SG-version-SHA.vmdk	Fichier de disque de machine virtuelle utilisé comme modèle pour créer des machines virtuelles de nœud de grille. **Remarque :** ce fichier doit se trouver dans le même dossier que le `.ovf` et `.mf` fichiers.
vsphere-primary-admin.ovf vsphere-primary-admin.mf	Fichier modèle du format Open Virtualization (`.ovf`) et fichier manifeste (`.mf`) Pour le déploiement du nœud d'administration principal.
vsphere-non-primary-admin.ovf vsphere-non-primary-admin.mf	Le fichier de modèle (`.ovf`) et fichier manifeste (`.mf`) Pour le déploiement de nœuds d'administration non primaires.
vsphere-archive.ovf vsphere-archive.mf	Le fichier de modèle (`.ovf`) et fichier manifeste (`.mf`) Pour le déploiement des nœuds d'archivage.
vsphere-gateway.ovf vsphere-gateway.mf	Le fichier de modèle (`.ovf`) et fichier manifeste (`.mf`) Pour le déploiement des nœuds de passerelle.
vsphere-storage.ovf vsphere-storage.mf	Le fichier de modèle (`.ovf`) et fichier manifeste (`.mf`) Pour le déploiement de nœuds de stockage basés sur des machines virtuelles.
deploy-vsphere-ovftool.sh	Le script de shell Bash utilisé pour automatiser le déploiement des nœuds de grille virtuels.

Nom du fichier	Description
deploy-vsphere-ovftool-sample.ini	Exemple de fichier de configuration à utiliser avec le `deploy-vsphere-ovftool.sh` script.

Définissez le fichier de configuration pour votre déploiement

Vous spécifiez les informations nécessaires au déploiement de noeuds de grille virtuels pour StorageGRID dans un fichier de configuration utilisé par `deploy-vsphere-ovftool.sh` Script bash. Vous pouvez modifier un exemple de fichier de configuration pour ne pas avoir à créer le fichier à partir de zéro.

Étapes

1. Faites une copie du fichier de configuration exemple (`deploy-vsphere-ovftool.sample.ini`). Enregistrez le nouveau fichier sous `deploy-vsphere-ovftool.ini` dans le même répertoire que `deploy-vsphere-ovftool.sh`.
2. La transparence `deploy-vsphere-ovftool.ini`.
3. Entrez toutes les informations requises pour déployer des nœuds VMware Virtual Grid.

   Voir Paramètres du fichier de configuration pour plus d'informations.

4. Une fois que vous avez saisi et vérifié toutes les informations nécessaires, enregistrez et fermez le fichier.

Paramètres du fichier de configuration

Le `deploy-vsphere-ovftool.ini` le fichier de configuration contient les paramètres requis pour déployer des nœuds de grille virtuelle.

Le fichier de configuration répertorie d'abord les paramètres globaux, puis répertorie les paramètres spécifiques au nœud dans les sections définies par nom de nœud. Lorsque le fichier est utilisé :

- *Paramètres globaux* sont appliqués à tous les nœuds de la grille.
- *Node-Specific parameters* remplace les paramètres globaux.

Paramètres globaux

Les paramètres globaux sont appliqués à tous les nœuds de la grille, sauf s'ils sont remplacés par des paramètres dans des sections individuelles. Placez les paramètres qui s'appliquent à plusieurs nœuds dans la section des paramètres globaux, puis remplacez ces paramètres si nécessaire dans les sections de nœuds individuels.

- **OVFTOOL_ARGUMENTS** : vous pouvez spécifier OVFTOOL_ARGUMENTS comme paramètres globaux, ou vous pouvez appliquer des arguments individuellement à des nœuds spécifiques. Par exemple :

  ```
  OVFTOOL_ARGUMENTS = --powerOn --noSSLVerify --diskMode=eagerZeroedThick
  --datastore='datastore_name'
  ```

  Vous pouvez utiliser le `--powerOffTarget` et `--overwrite` options permettant d'arrêter et de remplacer des machines virtuelles existantes.

Vous devez déployer des nœuds dans différents datastores et spécifier OVFTOOL_ARGUMENTS pour chaque nœud, au lieu de global.

- **SOURCE** : chemin d'accès au modèle de machine virtuelle StorageGRID (`.vmdk`) et le `.ovf` et `.mf` fichiers pour des nœuds grid individuels. Par défaut, le répertoire courant est sélectionné.

```
SOURCE = /downloads/StorageGRID-Webscale-version/vsphere
```

- **TARGET** : URL de l'infrastructure virtuelle VMware vSphere (vi) pour l'emplacement où StorageGRID sera déployé. Par exemple :

```
TARGET = vi://vcenter.example.com/vm/sgws
```

- **GRID_NETWORK_CONFIG** : méthode utilisée pour acquérir des adresses IP, STATIQUES ou DHCP. La valeur par défaut est STATIQUE. Si tous les noeuds ou la plupart utilisent la même méthode pour acquérir des adresses IP, vous pouvez spécifier cette méthode ici. Vous pouvez alors remplacer le paramètre global en spécifiant différents paramètres pour un ou plusieurs nœuds individuels. Par exemple :

```
GRID_NETWORK_CONFIG = DHCP
```

- **GRID_NETWORK_TARGET** : nom d'un réseau VMware existant à utiliser pour le réseau Grid. Si tous les nœuds ou la plupart utilisent le même nom de réseau, vous pouvez le spécifier ici. Vous pouvez alors remplacer le paramètre global en spécifiant différents paramètres pour un ou plusieurs nœuds individuels. Par exemple :

```
GRID_NETWORK_TARGET = SG-Admin-Network
```

- **GRID_NETWORK_MASK** : masque de réseau pour le réseau de grille. Si tous les nœuds ou la plupart utilisent le même masque de réseau, vous pouvez le spécifier ici. Vous pouvez alors remplacer le paramètre global en spécifiant différents paramètres pour un ou plusieurs nœuds individuels. Par exemple :

```
GRID_NETWORK_MASK = 255.255.255.0
```

- **GRID_NETWORK_GATEWAY** : passerelle réseau pour le réseau Grid. Si tous les nœuds ou la plupart utilisent la même passerelle réseau, vous pouvez le spécifier ici. Vous pouvez alors remplacer le paramètre global en spécifiant différents paramètres pour un ou plusieurs nœuds individuels. Par exemple :

```
GRID_NETWORK_GATEWAY = 10.1.0.1
```

- **GRID_NETWORK_MTU** : FACULTATIF. L'unité de transmission maximale (MTU) sur le réseau Grid. Si elle est spécifiée, la valeur doit être comprise entre 1280 et 9216. Par exemple :

```
GRID_NETWORK_MTU = 8192
```

Si omis, 1400 est utilisé.

Si vous souhaitez utiliser des trames jumbo, définissez la valeur MTU sur une valeur adaptée aux trames jumbo, comme 9000. Sinon, conservez la valeur par défaut.

> La valeur MTU du réseau doit correspondre à la valeur configurée sur le port du commutateur auquel le nœud est connecté. Dans le cas contraire, des problèmes de performances réseau ou une perte de paquets peuvent se produire.

> Pour des performances réseau optimales, tous les nœuds doivent être configurés avec des valeurs MTU similaires sur leurs interfaces réseau Grid. L'alerte **Grid Network MTU mismatch** est déclenchée en cas de différence importante dans les paramètres MTU pour le réseau Grid sur les nœuds individuels. Les valeurs MTU ne doivent pas nécessairement être identiques pour tous les types de réseau.

- **ADMIN_NETWORK_CONFIG** : méthode utilisée pour acquérir des adresses IP, DÉSACTIVÉES, STATIQUE ou DHCP. La valeur par défaut EST DÉSACTIVÉE. Si tous les noeuds ou la plupart utilisent la même méthode pour acquérir des adresses IP, vous pouvez spécifier cette méthode ici. Vous pouvez alors remplacer le paramètre global en spécifiant différents paramètres pour un ou plusieurs nœuds individuels. Par exemple :

```
ADMIN_NETWORK_CONFIG = STATIC
```

- **ADMIN_NETWORK_TARGET** : nom d'un réseau VMware existant à utiliser pour le réseau Admin. Ce paramètre est requis, sauf si le réseau d'administration est désactivé. Si tous les nœuds ou la plupart utilisent le même nom de réseau, vous pouvez le spécifier ici. Vous pouvez alors remplacer le paramètre global en spécifiant différents paramètres pour un ou plusieurs nœuds individuels. Par exemple :

```
ADMIN_NETWORK_TARGET = SG-Admin-Network
```

- **ADMIN_NETWORK_MASK** : le masque réseau du réseau Admin. Ce paramètre est requis si vous utilisez l'adressage IP statique. Si tous les nœuds ou la plupart utilisent le même masque de réseau, vous pouvez le spécifier ici. Vous pouvez alors remplacer le paramètre global en spécifiant différents paramètres pour un ou plusieurs nœuds individuels. Par exemple :

```
ADMIN_NETWORK_MASK = 255.255.255.0
```

- **ADMIN_NETWORK_GATEWAY** : passerelle réseau pour le réseau Admin. Ce paramètre est requis si vous utilisez l'adressage IP statique et que vous spécifiez des sous-réseaux externes dans LE paramètre ADMIN_NETWORK_ESL. (C'est-à-dire que ce n'est pas nécessaire si ADMIN_NETWORK_ESL est vide.) Si tous les nœuds ou la plupart utilisent la même passerelle réseau, vous pouvez le spécifier ici. Vous pouvez alors remplacer le paramètre global en spécifiant différents paramètres pour un ou plusieurs nœuds individuels. Par exemple :

```
ADMIN_NETWORK_GATEWAY = 10.3.0.1
```

- **ADMIN_NETWORK_ESL** : liste de sous-réseaux externes (routes) pour le réseau Admin, spécifiée comme liste de destinations de routage CIDR séparées par des virgules. Si tous les nœuds ou la plupart utilisent la même liste de sous-réseaux externes, vous pouvez la spécifier ici. Vous pouvez alors remplacer le paramètre global en spécifiant différents paramètres pour un ou plusieurs nœuds individuels. Par exemple :

```
ADMIN_NETWORK_ESL = 172.16.0.0/21,172.17.0.0/21
```

- **ADMIN_NETWORK_MTU** : FACULTATIF. Unité de transmission maximale (MTU) sur le réseau Admin. Ne spécifiez pas si ADMIN_NETWORK_CONFIG = DHCP. Si elle est spécifiée, la valeur doit être comprise entre 1280 et 9216. Si omis, 1400 est utilisé. Si vous souhaitez utiliser des trames jumbo, définissez la valeur MTU sur une valeur adaptée aux trames jumbo, comme 9000. Sinon, conservez la valeur par défaut. Si tous les nœuds ou la plupart utilisent le même MTU pour le réseau d'administration, vous pouvez le spécifier ici. Vous pouvez alors remplacer le paramètre global en spécifiant différents paramètres pour un ou plusieurs nœuds individuels. Par exemple :

```
ADMIN_NETWORK_MTU = 8192
```

- **CLIENT_NETWORK_CONFIG** : méthode utilisée pour acquérir des adresses IP, DÉSACTIVÉES, STATIQUE ou DHCP. La valeur par défaut EST DÉSACTIVÉE. Si tous les noeuds ou la plupart utilisent la même méthode pour acquérir des adresses IP, vous pouvez spécifier cette méthode ici. Vous pouvez alors remplacer le paramètre global en spécifiant différents paramètres pour un ou plusieurs nœuds individuels. Par exemple :

```
CLIENT_NETWORK_CONFIG = STATIC
```

- **CLIENT_NETWORK_TARGET** : nom d'un réseau VMware existant à utiliser pour le réseau client. Ce paramètre est requis, sauf si le réseau client est désactivé. Si tous les nœuds ou la plupart utilisent le même nom de réseau, vous pouvez le spécifier ici. Vous pouvez alors remplacer le paramètre global en spécifiant différents paramètres pour un ou plusieurs nœuds individuels. Par exemple :

```
CLIENT_NETWORK_TARGET = SG-Client-Network
```

- **CLIENT_NETWORK_MASK** : le masque réseau du réseau client. Ce paramètre est requis si vous utilisez l'adressage IP statique. Si tous les nœuds ou la plupart utilisent le même masque de réseau, vous pouvez le spécifier ici. Vous pouvez alors remplacer le paramètre global en spécifiant différents paramètres pour un ou plusieurs nœuds individuels. Par exemple :

```
CLIENT_NETWORK_MASK = 255.255.255.0
```

- **CLIENT_NETWORK_GATEWAY** : passerelle réseau pour le réseau client. Ce paramètre est requis si vous utilisez l'adressage IP statique. Si tous les nœuds ou la plupart utilisent la même passerelle réseau,

vous pouvez le spécifier ici. Vous pouvez alors remplacer le paramètre global en spécifiant différents paramètres pour un ou plusieurs nœuds individuels. Par exemple :

```
CLIENT_NETWORK_GATEWAY = 10.4.0.1
```

- **CLIENT_NETWORK_MTU** : FACULTATIF. Unité de transmission maximale (MTU) sur le réseau client. Ne spécifiez pas si CLIENT_NETWORK_CONFIG = DHCP. Si elle est spécifiée, la valeur doit être comprise entre 1280 et 9216. Si omis, 1400 est utilisé. Si vous souhaitez utiliser des trames jumbo, définissez la valeur MTU sur une valeur adaptée aux trames jumbo, comme 9000. Sinon, conservez la valeur par défaut. Si tous les nœuds ou la plupart utilisent le même MTU pour le réseau client, vous pouvez le spécifier ici. Vous pouvez alors remplacer le paramètre global en spécifiant différents paramètres pour un ou plusieurs nœuds individuels. Par exemple :

```
CLIENT_NETWORK_MTU = 8192
```

- **PORT_REMAPPAGE** : remappe tout port utilisé par un nœud pour les communications internes de nœud de grille ou les communications externes. Le remappage des ports est nécessaire si les stratégies de mise en réseau d'entreprise limitent un ou plusieurs ports utilisés par StorageGRID. Pour obtenir la liste des ports utilisés par StorageGRID, reportez-vous à la section communications internes des nœuds de la grille et communications externes dans "Instructions de mise en réseau".

> Ne mappez pas les ports que vous prévoyez d'utiliser pour configurer les terminaux de l'équilibreur de charge.

> Si le PARAMÈTRE PORT_REMAPPAGE est défini uniquement, le mappage que vous spécifiez est utilisé pour les communications entrantes et sortantes. Si PORT_REMAPPAGE_INBOUND est également spécifié, PORT_REMAPPAGE s'applique uniquement aux communications sortantes.

Le format utilisé est : *`network type/protocol/default port used by grid node/new port`*, où le type de réseau est grid, admin, ou client, et le protocole est tcp ou udp.

Par exemple :

```
PORT_REMAP = client/tcp/18082/443
```

Utilisé seul, cet exemple de paramètre mappe de façon symétrique les communications entrantes et sortantes du nœud de grille entre le port 18082 et le port 443. Si utilisé conjointement avec PORT_REMAPPAGE_INBOUND, cet exemple de paramètre mappe les communications sortantes du port 18082 au port 443.

- **PORT_REMAPPAGE_INBOUND** : remappe les communications entrantes pour le port spécifié. Si vous spécifiez PORT_REMAP_INBOUND mais que vous ne spécifiez pas de valeur pour PORT_REMAP, les communications sortantes pour le port sont inchangées.

> Ne mappez pas les ports que vous prévoyez d'utiliser pour configurer les terminaux de l'équilibreur de charge.

Le format utilisé est : *network type/protocol/_default port used by grid node/new port*, où le type de réseau est grid, admin, ou client, et le protocole est tcp ou udp.

Par exemple :

```
PORT_REMAP_INBOUND = client/tcp/443/18082
```

Dans cet exemple, le trafic envoyé au port 443 passe par un pare-feu interne et le dirige vers le port 18082, où le nœud de la grille écoute les requêtes S3.

Paramètres spécifiques aux nœuds

Chaque nœud se trouve dans sa propre section du fichier de configuration. Chaque nœud nécessite les paramètres suivants :

- L'en-tête de section définit le nom du nœud qui sera affiché dans le Grid Manager. Vous pouvez remplacer cette valeur en spécifiant le paramètre optionnel NOM_NOEUD pour le noeud.
- **NODE_TYPE** : VM_Admin_Node, VM_Storage_Node, VM_Archive_Node ou VM_API_Gateway_Node
- **GRID_NETWORK_IP** : adresse IP du nœud sur le réseau Grid.
- **ADMIN_NETWORK_IP** : adresse IP du noeud sur le réseau Admin. Obligatoire uniquement si le nœud est connecté au réseau Admin et QUE ADMIN_NETWORK_CONFIG est défini SUR STATIQUE.
- **CLIENT_NETWORK_IP** : adresse IP du noeud sur le réseau client. Requis uniquement si le nœud est connecté au réseau client et QUE CLIENT_NETWORK_CONFIG pour ce nœud est défini sur STATIQUE.
- **ADMIN_IP** : adresse IP du nœud d'administration principal sur le réseau Grid. Utilisez la valeur que vous spécifiez comme GRID_NETWORK_IP pour le noeud d'administration principal. Si vous omettez ce paramètre, le nœud tente de détecter l'IP du nœud d'administration principal à l'aide de mDNS. Pour plus d'informations, voir "Mode de détection des nœuds du grid sur le nœud d'administration principal".

  > Le paramètre ADMIN_IP est ignoré pour le nœud d'administration principal.

- Tous les paramètres qui n'ont pas été définis globalement. Par exemple, si un nœud est associé au réseau Admin et que vous n'avez pas spécifié les paramètres ADMIN_NETWORK globalement, vous devez les spécifier pour le nœud.

Nœud d'administration principal

Les paramètres supplémentaires suivants sont requis pour le nœud d'administration principal :

- **NODE_TYPE** : VM_Admin_Node
- **ADMIN_ROLE** : principal

Cet exemple d'entrée concerne un noeud d'administration principal sur les trois réseaux :

```
[DC1-ADM1]
  ADMIN_ROLE = Primary
  NODE_TYPE = VM_Admin_Node

  GRID_NETWORK_IP = 10.1.0.2
  ADMIN_NETWORK_IP = 10.3.0.2
  CLIENT_NETWORK_IP = 10.4.0.2
```

Le paramètre supplémentaire suivant est facultatif pour le nœud d'administration principal :

- **DISQUE** : par défaut, les nœuds d'administration sont affectés à deux disques durs supplémentaires de 200 Go pour l'audit et l'utilisation de la base de données. Vous pouvez augmenter ces paramètres à l'aide du paramètre DISQUE. Par exemple :

  ```
  DISK = INSTANCES=2, CAPACITY=300
  ```

  Pour les nœuds Admin, LES INSTANCES doivent toujours être égales à 2.

Nœud de stockage

Le paramètre supplémentaire suivant est requis pour les nœuds de stockage :

- **NODE_TYPE** : VM_Storage_Node

  Cet exemple d'entrée concerne un noeud de stockage qui se trouve sur la grille et les réseaux d'administration, mais pas sur le réseau client. Ce nœud utilise le paramètre ADMIN_IP pour spécifier l'adresse IP du nœud d'administration principal sur le réseau Grid.

  ```
  [DC1-S1]
    NODE_TYPE = VM_Storage_Node

    GRID_NETWORK_IP = 10.1.0.3
    ADMIN_NETWORK_IP = 10.3.0.3

    ADMIN_IP = 10.1.0.2
  ```

  Ce deuxième exemple d'entrée concerne un nœud de stockage sur un réseau client dans lequel la stratégie de réseau d'entreprise du client indique qu'une application client S3 n'est autorisée qu'à accéder au nœud de stockage via le port 80 ou 443. Cet exemple de fichier de configuration utilise PORT_REMAP pour permettre au nœud de stockage d'envoyer et de recevoir des messages S3 sur le port 443.

```
[DC2-S1]
  NODE_TYPE = VM_Storage_Node

  GRID_NETWORK_IP = 10.1.1.3
  CLIENT_NETWORK_IP = 10.4.1.3
  PORT_REMAP = client/tcp/18082/443

  ADMIN_IP = 10.1.0.2
```

Le dernier exemple crée un remappage symétrique pour le trafic ssh du port 22 au port 3022, mais définit explicitement les valeurs pour le trafic entrant et sortant.

```
[DC1-S3]
  NODE_TYPE = VM_Storage_Node

  GRID_NETWORK_IP = 10.1.1.3

  PORT_REMAP = grid/tcp/22/3022
  PORT_REMAP_INBOUND = grid/tcp/3022/22

  ADMIN_IP = 10.1.0.2
```

Le paramètre supplémentaire suivant est facultatif pour les nœuds de stockage :

- **DISQUE** : par défaut, les nœuds de stockage sont affectés à trois disques de 4 To pour une utilisation RangeDB. Vous pouvez augmenter ces paramètres à l'aide du paramètre DISQUE. Par exemple :

```
DISK = INSTANCES=16, CAPACITY=4096
```

Nœud d'archivage

Le paramètre supplémentaire suivant est requis pour les nœuds d'archivage :

- **NODE_TYPE** : VM_Archive_Node

Cet exemple d'entrée concerne un noeud d'archivage qui se trouve sur la grille et les réseaux d'administration, mais pas sur le réseau client.

```
[DC1-ARC1]
  NODE_TYPE = VM_Archive_Node

  GRID_NETWORK_IP = 10.1.0.4
  ADMIN_NETWORK_IP = 10.3.0.4

  ADMIN_IP = 10.1.0.2
```

Nœud de passerelle

Le paramètre supplémentaire suivant est requis pour les nœuds de passerelle :

- **NODE_TYPE** : VM_API_GATEWAY

Cet exemple d'entrée concerne un exemple de nœud de passerelle sur les trois réseaux. Dans cet exemple, aucun paramètre du réseau client n'a été spécifié dans la section globale du fichier de configuration. Il faut donc les spécifier pour le nœud :

```
[DC1-G1]
  NODE_TYPE = VM_API_Gateway

  GRID_NETWORK_IP = 10.1.0.5
  ADMIN_NETWORK_IP = 10.3.0.5

  CLIENT_NETWORK_CONFIG = STATIC
  CLIENT_NETWORK_TARGET = SG-Client-Network
  CLIENT_NETWORK_MASK = 255.255.255.0
  CLIENT_NETWORK_GATEWAY = 10.4.0.1
  CLIENT_NETWORK_IP = 10.4.0.5

  ADMIN_IP = 10.1.0.2
```

Nœud d'administration non primaire

Les paramètres supplémentaires suivants sont requis pour les nœuds d'administration non primaires :

- **NODE_TYPE** : VM_Admin_Node
- **ADMIN_ROLE** : non-Primary

Cet exemple d'entrée concerne un noeud d'administration non primaire qui n'est pas sur le réseau client :

```
[DC2-ADM1]
  ADMIN_ROLE = Non-Primary
  NODE_TYPE = VM_Admin_Node

  GRID_NETWORK_TARGET = SG-Grid-Network
  GRID_NETWORK_IP = 10.1.0.6
  ADMIN_NETWORK_IP = 10.3.0.6

  ADMIN_IP = 10.1.0.2
```

Le paramètre supplémentaire suivant est facultatif pour les nœuds d'administration non primaires :

- **DISQUE** : par défaut, les nœuds d'administration sont affectés à deux disques durs supplémentaires de 200 Go pour l'audit et l'utilisation de la base de données. Vous pouvez augmenter ces paramètres à l'aide du paramètre DISQUE. Par exemple :

  ```
  DISK = INSTANCES=2, CAPACITY=300
  ```

  Pour les nœuds Admin, LES INSTANCES doivent toujours être égales à 2.

Exécutez le script Bash

Vous pouvez utiliser le `deploy-vsphere-ovftool.sh` Le script bash et le fichier de configuration deploy-vsphere-ovftool.ini que vous avez modifié pour automatiser le déploiement des nœuds grid StorageGRID dans VMware vSphere.

Avant de commencer

- Vous avez créé un fichier de configuration deploy-vsphere-ovftool.ini pour votre environnement.

Vous pouvez utiliser l'aide disponible avec le script Bash en entrant les commandes d'aide (`-h/--help`). Par exemple :

```
./deploy-vsphere-ovftool.sh -h
```

ou

```
./deploy-vsphere-ovftool.sh --help
```

Étapes

1. Connectez-vous à la machine Linux que vous utilisez pour exécuter le script Bash.
2. Accédez au répertoire dans lequel vous avez extrait l'archive d'installation.

   Par exemple :

```
cd StorageGRID-Webscale-version/vsphere
```

3. Pour déployer tous les nœuds de la grille, exécutez le script Bash avec les options appropriées pour votre environnement.

   Par exemple :

```
./deploy-vsphere-ovftool.sh --username=user --password=pwd ./deploy-
vsphere-ovftool.ini
```

4. Si un nœud de grille n'a pas pu être déployé en raison d'une erreur, résolvez l'erreur et relancez le script de Bash pour ce nœud uniquement.

   Par exemple :

```
./deploy-vsphere-ovftool.sh --username=user --password=pwd --single
-node="DC1-S3" ./deploy-vsphere-ovftool.ini
```

Le déploiement est terminé lorsque le statut de chaque nœud est « passé ».

```
Deployment Summary
+------------------------------+----------+----------------------+
| node                         | attempts | status               |
+------------------------------+----------+----------------------+
| DC1-ADM1                     |        1 | Passed               |
| DC1-G1                       |        1 | Passed               |
| DC1-S1                       |        1 | Passed               |
| DC1-S2                       |        1 | Passed               |
| DC1-S3                       |        1 | Passed               |
+------------------------------+----------+----------------------+
```

Automatiser la configuration de StorageGRID

Une fois les nœuds grid déployés, vous pouvez automatiser la configuration du système StorageGRID.

Avant de commencer

- Vous connaissez l'emplacement des fichiers suivants à partir de l'archive d'installation.

Nom du fichier	Description
configure-storagegrid.py	Script Python utilisé pour automatiser la configuration

Nom du fichier	Description
configurez-storagegrid.sample.json	Exemple de fichier de configuration à utiliser avec le script
configurez-storagegrid.blank.json	Fichier de configuration vierge à utiliser avec le script

- Vous avez créé un `configure-storagegrid.json` fichier de configuration. Pour créer ce fichier, vous pouvez modifier l'exemple de fichier de configuration (`configure-storagegrid.sample.json`) ou le fichier de configuration vierge (`configure-storagegrid.blank.json`).

Vous pouvez utiliser le `configure-storagegrid.py` Script Python et le `configure-storagegrid.json` Fichier de configuration pour automatiser la configuration de votre système StorageGRID.

> Vous pouvez également configurer le système à l'aide de Grid Manager ou de l'API d'installation.

Étapes

1. Connectez-vous à la machine Linux que vous utilisez pour exécuter le script Python.
2. Accédez au répertoire dans lequel vous avez extrait l'archive d'installation.

   Par exemple :

   ```
   cd StorageGRID-Webscale-version/platform
   ```

   où `platform` est deps, rpms ou vsphere.

3. Exécutez le script Python et utilisez le fichier de configuration que vous avez créé.

   Par exemple :

   ```
   ./configure-storagegrid.py ./configure-storagegrid.json --start-install
   ```

Résultat

Un progiciel de récupération `.zip` le fichier est généré pendant le processus de configuration et il est téléchargé dans le répertoire où vous exécutez le processus d'installation et de configuration. Vous devez sauvegarder le fichier de package de restauration afin de pouvoir restaurer le système StorageGRID en cas de défaillance d'un ou plusieurs nœuds de la grille. Par exemple, copiez-le dans un emplacement sécurisé, sauvegardé sur le réseau et dans un emplacement de stockage cloud sécurisé.

> Le fichier du progiciel de récupération doit être sécurisé car il contient des clés de cryptage et des mots de passe qui peuvent être utilisés pour obtenir des données du système StorageGRID.

Si vous avez indiqué que des mots de passe aléatoires doivent être générés, ouvrez le `Passwords.txt` Fichier et recherche les mots de passe requis pour accéder au système StorageGRID.

```
######################################################################
##### The StorageGRID "recovery package" has been downloaded as: #####
#####           ./sgws-recovery-package-994078-rev1.zip          #####
#####   Safeguard this file as it will be needed in case of a    #####
#####                 StorageGRID node recovery.                 #####
######################################################################
```

Votre système StorageGRID est installé et configuré lorsqu'un message de confirmation s'affiche.

```
StorageGRID has been configured and installed.
```

Informations associées

"Accédez au Grid Manager"

"Présentation de l'API REST d'installation"

Présentation de l'API REST d'installation

StorageGRID fournit l'API d'installation StorageGRID pour effectuer des tâches d'installation.

L'API utilise la plate-forme swagger open source API pour fournir la documentation de l'API. Swagger permet aux développeurs et aux non-développeurs d'interagir avec l'API dans une interface utilisateur qui illustre la façon dont l'API répond aux paramètres et aux options. Cette documentation suppose que vous êtes familiarisé avec les technologies Web standard et le format de données JSON.

> Toutes les opérations d'API que vous effectuez à l'aide de la page Web API Docs sont des opérations en direct. Veillez à ne pas créer, mettre à jour ou supprimer des données de configuration ou d'autres données par erreur.

Chaque commande de l'API REST inclut l'URL de l'API, une action HTTP, tous les paramètres d'URL requis ou facultatifs et une réponse de l'API attendue.

API d'installation de StorageGRID

L'API d'installation de StorageGRID n'est disponible que lors de la configuration initiale du système StorageGRID et si vous devez effectuer une restauration du nœud d'administration principal. L'API d'installation est accessible via HTTPS depuis le Grid Manager.

Pour accéder à la documentation de l'API, accédez à la page Web d'installation sur le nœud d'administration principal et sélectionnez **aide** > **documentation de l'API** dans la barre de menus.

L'API d'installation de StorageGRID comprend les sections suivantes :

- **Config** — opérations liées à la version du produit et aux versions de l'API. Vous pouvez lister la version du produit ainsi que les versions principales de l'API prises en charge par cette version.
- **Grid** — opérations de configuration au niveau de la grille. Vous pouvez obtenir et mettre à jour les paramètres de la grille, y compris les détails de la grille, les sous-réseaux de la grille, les mots de passe de

la grille et les adresses IP des serveurs NTP et DNS.

- **Noeuds** — opérations de configuration au niveau des noeuds. Vous pouvez récupérer une liste de nœuds de la grille, supprimer un nœud de la grille, configurer un nœud de la grille, afficher un nœud de la grille et réinitialiser la configuration d'un nœud de la grille.
- **Provision** — opérations de provisionnement. Vous pouvez démarrer l'opération de provisionnement et afficher l'état de cette opération.
- **Recovery** — opérations de restauration du noeud d'administration principal. Vous pouvez réinitialiser les informations, télécharger le progiciel de restauration, démarrer la récupération et afficher l'état de l'opération de récupération.
- **Progiciel de récupération** — opérations pour télécharger le progiciel de récupération.
- **Schémas** — schémas API pour les déploiements avancés
- **Sites** — opérations de configuration au niveau du site. Vous pouvez créer, afficher, supprimer et modifier un site.

Par où aller plus loin

Une fois l'installation terminée, effectuez les tâches d'intégration et de configuration requises. Vous pouvez effectuer les tâches facultatives nécessaires.

Tâches requises

- Configurez l'hyperviseur VMware vSphere pour le redémarrage automatique.

  Vous devez configurer l'hyperviseur pour redémarrer les machines virtuelles lorsque le serveur redémarre. Sans redémarrage automatique, les machines virtuelles et les nœuds de la grille restent arrêtés après le redémarrage du serveur. Pour en savoir plus, consultez la documentation relative à l'hyperviseur VMware vSphere.

- "Créez un compte de locataire" Pour chaque protocole client (Swift ou S3) qui sera utilisé pour stocker des objets sur votre système StorageGRID.
- "Contrôler l'accès au système" en configurant des groupes et des comptes utilisateur. Si vous le souhaitez, vous pouvez "configurer un référentiel d'identité fédéré" (Comme Active Directory ou OpenLDAP), vous pouvez importer des groupes et des utilisateurs d'administration. Ou bien, c'est possible "créer des groupes et des utilisateurs locaux".
- Intégrer et tester le "API S3" ou "API Swift" Applications client que vous utiliserez pour télécharger des objets sur votre système StorageGRID.
- "Configuration des règles de gestion du cycle de vie des informations (ILM) et de la règle ILM" utilisez pour protéger les données d'objet.
- Si votre installation inclut des nœuds de stockage de l'appliance, effectuez les tâches suivantes avec SANtricity OS :
  - Connectez-vous à chaque appliance StorageGRID.
  - Vérifiez la réception des données AutoSupport.

    Voir "Configurer le matériel".

- Examinez et suivez les "Instructions de renforcement du système StorageGRID" pour éliminer les risques de sécurité.
- "Configurez les notifications par e-mail pour les alertes système".

- Si votre système StorageGRID inclut des nœuds d'archivage (obsolètes), configurez la connexion du nœud d'archivage au système de stockage d'archives externe cible.

Tâches facultatives

- "Mettre à jour les adresses IP des nœuds de la grille" S'ils ont changé depuis que vous avez planifié votre déploiement et généré le package de récupération.
- "Configurer le chiffrement du stockage", si nécessaire.
- "Configurer la compression du stockage" pour réduire la taille des objets stockés, si nécessaire.
- "Configurez l'accès au système à des fins d'audit" Par le biais d'un partage de fichiers NFS.

Résoudre les problèmes d'installation

En cas de problème lors de l'installation de votre système StorageGRID, vous pouvez accéder aux fichiers journaux d'installation.

Voici les principaux fichiers journaux d'installation dont le support technique peut avoir besoin pour résoudre les problèmes.

- `/var/local/log/install.log` (disponible sur tous les nœuds de la grille)
- `/var/local/log/gdu-server.log` (Trouvé sur le nœud d'administration principal)

Informations associées

Pour savoir comment accéder aux fichiers journaux, reportez-vous à la section "Référence des fichiers journaux".

Si vous avez besoin d'aide supplémentaire, contactez "Support NetApp".

La réservation de ressources de machine virtuelle nécessite un ajustement

Les fichiers OVF incluent une réservation de ressources conçue pour garantir que chaque nœud de grille dispose de suffisamment de RAM et de CPU pour fonctionner efficacement. Si vous créez des machines virtuelles en déployant ces fichiers OVF sur VMware et que le nombre prédéfini de ressources n'est pas disponible, les machines virtuelles ne démarrent pas.

Description de la tâche

Si vous êtes certain que l'hôte VM dispose de ressources suffisantes pour chaque nœud de la grille, ajustez manuellement les ressources allouées à chaque machine virtuelle, puis essayez de démarrer les machines virtuelles.

Étapes

1. Dans l'arborescence du client VMware vSphere Hypervisor, sélectionnez la machine virtuelle qui n'a pas démarré.
2. Cliquez avec le bouton droit de la souris sur la machine virtuelle et sélectionnez **Modifier les paramètres**.
3. Dans la fenêtre Propriétés des machines virtuelles, sélectionnez l'onglet **Ressources**.
4. Ajustez les ressources allouées à la machine virtuelle :
   a. Sélectionnez **CPU**, puis utilisez le curseur réservation pour régler la fréquence réservée à cette machine virtuelle.

b. Sélectionnez **mémoire**, puis utilisez le curseur réservation pour régler le Mo réservé pour cette machine virtuelle.

5. Cliquez sur **OK**.
6. Répétez cette procédure si nécessaire pour les autres machines virtuelles hébergées sur le même hôte VM.

Mettez à niveau le logiciel StorageGRID

Mettre à niveau le logiciel StorageGRID : présentation

Suivez ces instructions pour mettre à niveau un système StorageGRID vers une nouvelle version.

À propos de ces instructions

Ces instructions décrivent les nouveautés d'StorageGRID 11.7 et fournissent des instructions détaillées pour la mise à niveau de tous les nœuds de votre système StorageGRID vers la nouvelle version.

Avant de commencer

Consultez ces rubriques pour en savoir plus sur les nouvelles fonctionnalités et les améliorations de StorageGRID 11.7, déterminer si des fonctionnalités ont été obsolètes ou supprimées et découvrir les modifications apportées aux API StorageGRID.

- "Nouveautés de StorageGRID 11.7"
- "Fonctions supprimées ou obsolètes"
- "Modifications apportées à l'API de gestion du grid"
- "Modifications apportées à l'API de gestion des locataires"

Nouveautés d'StorageGRID 11.7

Cette version de StorageGRID présente les fonctionnalités et modifications fonctionnelles suivantes.

Nouvelles fonctionnalités

fédération des grilles

Vous pouvez configurer une connexion de fédération de grille entre deux systèmes StorageGRID pour cloner les informations de compte de locataire et répliquer des objets de compartiment entre les grilles à des fins de reprise après incident. Voir "Qu'est-ce que la fédération de grille ?", "Qu'est-ce que le clone de compte", et "Qu'est-ce que la réplication cross-grid".

Meilleure disponibilité en lecture

Le contrôle de cohérence read-after-New-write (par défaut) a été amélioré pour être plus disponible. Les requêtes GET/HEAD pour des objets inexistants réussiront avec jusqu'à un nœud de stockage hors ligne sur chaque site. Il n'est plus nécessaire de définir les compartiments sur le contrôle de cohérence disponible pour ce scénario. Par exemple, les applications qui vérifient l'existence d'un objet avant sa création fonctionneront correctement en lecture après une nouvelle écriture, même pendant la mise à niveau logicielle lorsqu'un nœud

de stockage est hors ligne.

Renommez la grille, les sites et les nœuds

Une nouvelle procédure de maintenance vous permet de modifier les noms d'affichage affichés dans le Gestionnaire de grille. Vous pouvez mettre à jour les noms d'affichage en toute sécurité et à tout moment. Voir "Renommez la grille, les sites et les nœuds".

Assistant d'installation de FabricPool et S3

L'assistant d'installation de FabricPool et S3 vous guide à chaque étape de configuration d'StorageGRID pour une utilisation avec ONTAP FabricPool ou une autre application client S3 et génère un fichier que vous pouvez utiliser lorsque vous entrez les valeurs requises dans une autre application. Voir "Utilisez l'assistant d'installation FabricPool" et "Utilisation de l'assistant d'installation S3".

En relation avec cette modification, une bannière s'affiche désormais sur le tableau de bord pour rappeler aux nouveaux utilisateurs de configurer "Noms de domaine de terminaux S3" Pour les demandes de type hébergement virtuel S3 et la configuration "notifications par e-mail pour les alertes".

Contrôles de pare-feu

La page de contrôle du pare-feu vous permet de gérer l'accès externe aux ports sur les nœuds de votre grille et de définir les adresses hôtes et les sous-réseaux IP autorisés à accéder aux ports fermés. La nouvelle page inclut également les paramètres réseau client non approuvé, qui vous permettent désormais de sélectionner des ports supplémentaires que vous souhaitez ouvrir lorsque le réseau client non approuvé est configuré. Voir "Configurer le pare-feu interne".

Stratégies de sécurité améliorées

Vous pouvez désormais déterminer quels protocoles et chiffrements sont utilisés pour établir des connexions TLS sécurisées avec les applications client et des connexions SSH sécurisées avec les services StorageGRID internes. Voir "Gestion des règles TLS et SSH".

Modifications du noeud final de l'équilibreur de charge

Quand "configuration des terminaux d'équilibrage de charge", vous pouvez maintenant :

- Autorisez tous les locataires à accéder au point final (par défaut) ou spécifiez une liste de locataires autorisés ou bloqués afin d'améliorer l'isolation de sécurité entre les locataires et leurs points finaux.
- Utilisez le mode de liaison **Node Type** pour demander aux clients d'utiliser l'adresse IP (ou le nom de domaine complet correspondant) d'un nœud Admin ou l'adresse IP d'un nœud Gateway, en fonction du type de nœud que vous sélectionnez.

Appliance 100 % Flash SGF6112

La nouvelle appliance de stockage StorageGRID SGF6112 présente une conception compacte avec contrôleur de calcul et contrôleur de stockage intégré dans un châssis 1U. L'appliance prend en charge 12 disques NVMe SSD avec une capacité de stockage allant jusqu'à 15.3 To par disque. Les disques SSD font partie d'un système RAID qui fournit un stockage objet résilient. Voir "Appliance SGF6112 : présentation".

Autres améliorations de Grid Manager

Améliorations des règles ILM

L'assistant ILM amélioré facilite la définition des filtres, la saisie des périodes et des placements, ainsi que l'affichage des diagrammes de conservation. Les profils de code d'effacement sont créés automatiquement lorsque vous sélectionnez un pool de stockage et un schéma EC pour un placement. Pour les nouvelles installations StorageGRID 11.7 (et non les mises à niveau), un pool de stockage est automatiquement créé pour chaque site et la nouvelle règle par défaut **1 copie par site** garantit que les nouvelles installations multi-sites auront une protection contre les pertes de site par défaut. Voir "Gestion des objets avec ILM".

Tableau de bord personnalisable

Vous pouvez désormais configurer des tableaux de bord personnalisés pour Grid Manager. Voir "Affichez et gérez le tableau de bord".

Interface de restauration de volume

La restauration du volume de stockage vous permet de restaurer les données d'objet en cas de défaillance d'un volume de stockage. Pour StorageGRID 11.7, vous pouvez lancer la restauration de volumes à partir du Gestionnaire de grille en plus de la méthode existante de saisie manuelle des commandes. L'utilisation de Grid Manager est désormais la méthode préférée pour restaurer les données d'objet. Voir "Restaurez les données d'objet à l'aide de Grid Manager".

Interface de mise à niveau et de correctif

Lorsque vous effectuez une mise à niveau vers StorageGRID 11.7, vous pouvez appliquer le dernier correctif 11.7 en même temps. La page de mise à niveau StorageGRID affiche le chemin de mise à niveau recommandé et renvoie directement aux pages de téléchargement correctes. Voir "Effectuer la mise à niveau".

Unités pour les valeurs de stockage

Vous pouvez maintenant sélectionner les unités de base 10 ou 2 pour les valeurs de stockage affichées dans le Gestionnaire de grille et le Gestionnaire de locataires. Sélectionnez la liste déroulante utilisateur dans le coin supérieur droit du Gestionnaire de grille ou du Gestionnaire de locataires, puis sélectionnez **Préférences utilisateur**.

Accédez à MIB depuis Grid Manager

Vous pouvez désormais accéder aux fichiers MIB compatibles SNMP à partir de Grid Manager à l'aide de la page agent SNMP. Voir "Accéder aux fichiers MIB".

Nuances de stockage personnalisées pour les nouveaux nœuds

Lorsque vous effectuez une extension pour ajouter un nouveau site ou de nouveaux nœuds de stockage, vous pouvez désormais attribuer une note de stockage personnalisée à chaque nouveau nœud. Voir "Réaliser une extension".

Mises à jour du Gestionnaire des locataires

Réplication entre plusieurs grilles

Comptes de tenant qui ont l'autorisation d'utiliser un connexion de fédération de grille Elle peut cloner des groupes de locataires, des utilisateurs et des clés S3 d'une grille à une autre et utiliser la réplication inter-grid pour répliquer les objets de compartiment entre deux grilles. Voir "Cloner des groupes de locataires et des utilisateurs" et "Gérer la réplication entre les grilles".

Supprimez tous les objets du compartiment

Les utilisateurs de tenant Manager peuvent désormais supprimer tous les objets d'un compartiment. Voir "Supprime les objets du compartiment".

Conservation par défaut du verrouillage objet S3

Les utilisateurs de tenant Manager peuvent désormais activer et configurer la conservation par défaut lors de la création de compartiments S3 Object Lock. Voir "Créer un compartiment S3".

Mises à jour S3

Mode de gouvernance S3 Object Lock

Lorsque vous spécifiez les paramètres de verrouillage objet S3 pour un objet ou les paramètres de conservation par défaut d'un compartiment, vous pouvez désormais utiliser le mode de gouvernance. Ce mode de rétention permet aux utilisateurs disposant d'une autorisation spéciale de contourner certains paramètres de rétention. Voir "Utilisez le verrouillage d'objet S3 pour conserver les objets" et "Utilisez l'API REST S3 pour configurer le verrouillage objet S3".

Règle de groupe S3 pour la réduction des attaques par ransomware

Lorsqu'elle est ajoutée en tant que règle de groupe pour un compte de locataire S3, l'exemple de règle permet de limiter les attaques par ransomware. Elle empêche la suppression définitive des anciennes versions d'objets. Voir "Créez des groupes pour un locataire S3".

Seuil NewerNoncurrentVersions pour les compartiments S3

Le `NewerNoncurrentVersions` L'action dans la configuration du cycle de vie du compartiment spécifie le nombre de versions non actuelles conservées dans un compartiment S3 versionné. Ce seuil remplace les règles de cycle de vie fournies par ILM. Voir "Comment supprimer les objets".

Mises à jour de S3 Select

S3 SelectObjectContent prend désormais en charge les objets parquet. En outre, vous pouvez désormais utiliser S3 Select avec les terminaux d'administration et d'équilibrage de la charge de passerelle qui sont des nœuds bare Metal exécutant un noyau avec cgroup v2 activé. Voir "S3 SelectObjectContent".

Autres améliorations

Objet du certificat facultatif

Le champ objet du certificat est désormais facultatif. Si ce champ est laissé vide, le certificat généré utilise le premier nom de domaine ou l'adresse IP comme nom commun de l'objet (CN). Voir "Gérer les certificats de sécurité".

Catégorie de messages d'audit ILM et nouveaux messages

Une catégorie de messages d'audit a été ajoutée pour les opérations ILM et comprend les messages IDEL, LKCU et ORLM. Cette nouvelle catégorie est définie sur **Normal**. Voir "Messages d'audit des opérations ILM".

De plus, de nouveaux messages de vérification ont été ajoutés pour prendre en charge la nouvelle fonctionnalité 11.7 :

- "BROR : demande en lecture seule du compartiment"

- "CGRR : demande de réplication croisée"
- "EBDL : suppression du compartiment vide"
- "EBKR : demande de godet vide"
- "S3SL: S3 Select Request"

Nouvelles alertes

Les nouvelles alertes suivantes ont été ajoutées pour StorageGRID 11.7 :

- Panne du lecteur DAS de l'appliance détectée
- Reconstruction des disques DAS du dispositif
- Panne du ventilateur de l'appareil détectée
- Défaillance de la carte réseau de l'appareil détectée
- Avertissement critique sur les disques SSD de l'appliance
- Échec de l'envoi du message AutoSupport
- Erreur d'écriture surdimensionnée Cassandra
- Échec de la demande permanente de réplication entre les grilles
- Ressources de réplication intergrid indisponibles
- Impact sur les performances de débogage
- Expiration du certificat de fédération GRID
- Le paramètre de cohérence du compartiment FabricPool n'est pas pris en charge
- Échec de la configuration du pare-feu
- Échec de la connexion de fédération de grille
- Panne du ventilateur du dispositif de stockage détectée
- Le nœud de stockage n'est pas dans l'état de stockage souhaité
- Le volume de stockage nécessite votre attention
- Le volume de stockage doit être restauré
- Volume de stockage hors ligne
- Configuration de trace activée
- La restauration de volume n'a pas pu démarrer la réparation des données répliquées

Modifications de la documentation

- Découvrez dans ce guide de référence rapide comment StorageGRID prend en charge les API Amazon simple Storage Service (S3). Voir "Référence rapide : demandes d'API S3 prises en charge".
- La nouvelle "Démarrage rapide de StorageGRID" Le répertorie les étapes générales de configuration et d'utilisation d'un système StorageGRID et fournit des liens vers les instructions correspondantes.
- Les instructions d'installation du matériel de l'appliance ont été combinées et consolidées pour faciliter l'utilisation. Un guide de démarrage rapide a été ajouté pour guider l'installation du matériel. Voir"Démarrage rapide pour l'installation du matériel".
- Les instructions de maintenance communes à tous les modèles d'appliance ont été combinées, consolidées et déplacées vers la section de maintenance du site doc. Voir "Maintenance de nœuds communs : présentation".

- Les instructions de maintenance spécifiques à chaque modèle d'appareil ont également été déplacées vers la section de maintenance :

  "Maintenance du matériel SGF6112"

  "Maintenance du matériel SG6000"

  "Maintenance du matériel SG5700"

  "Maintenance du matériel SG100 et SG1000"

Fonctions supprimées ou obsolètes

Certaines fonctionnalités ont été supprimées ou obsolètes dans cette version. Consultez ces éléments pour savoir si vous devez mettre à jour les applications client ou modifier votre configuration avant de procéder à la mise à niveau.

Service d'équilibrage de la charge de connexion (CLB) supprimé

Le service CLB (Connection Load Balancer) sur les nœuds de passerelle a été obsolète dans StorageGRID 11.4 et a été complètement supprimé du logiciel. Pour distribuer les connexions réseau entrantes des applications client aux nœuds de stockage, vous pouvez configurer des terminaux d'équilibrage de la charge pour le service Load Balancer, qui est inclus sur tous les nœuds d'administration et les nœuds de passerelle, ou vous pouvez intégrer un équilibreur de charge tiers. Voir "Considérations relatives à l'équilibrage de charge".

Si des certificats personnalisés ont été configurés pour l'API S3 ou Swift dans la version StorageGRID existante, les ports CLB 8082, 8083, 8084 et 8085 seront automatiquement convertis en terminaux d'équilibrage de charge lors de la mise à niveau vers StorageGRID 11.7.

L'appliance SG5600 n'est plus prise en charge

L'appliance SG5600 n'est plus prise en charge. Contactez votre ingénieur commercial NetApp pour connaître les options de mise à jour du matériel.

Si vous devez effectuer des procédures de maintenance sur du matériel SG5600, utilisez le "Instructions pour StorageGRID 11.6".

Support Swift obsolète

Depuis la version 11.7 de StorageGRID, la prise en charge des applications clientes Swift a été obsolète. L'interface utilisateur et les API qui prennent en charge les applications du client Swift seront supprimées dans une prochaine version.

Support du nœud d'archivage obsolète

La prise en charge des nœuds d'archivage (pour l'archivage dans le cloud à l'aide de l'API S3 et l'archivage sur bande à l'aide du middleware TSM) est obsolète et sera supprimée dans une prochaine version. Le déplacement d'objets d'un nœud d'archivage vers un système de stockage d'archives externe a été remplacé par les pools de stockage cloud ILM pour offrir davantage de fonctionnalités.

Voir :

- "Migration des objets vers un pool de stockage cloud"
- "Utilisation des pools de stockage cloud"

De plus, vous devez supprimer les nœuds d'archivage de la règle ILM active dans StorageGRID 11.7 ou version antérieure. La suppression des données d'objet stockées sur les nœuds d'archivage simplifie les mises à niveau futures. Voir "Utilisation des règles ILM et des règles ILM".

Exportation d'audit via CIFS/Samba supprimée

L'exportation des audits via CIFS/Samba a été obsolète dans StorageGRID Webscale 11.1 et a été supprimée. Si nécessaire, c'est possible "utilisez un serveur syslog externe" ou "Configurer l'accès client d'audit pour NFS".

Option permettant de spécifier un pool de stockage comme emplacement temporaire supprimé

Auparavant, lorsque vous avez créé une règle ILM avec un placement d'objets incluant un pool de stockage unique, vous étiez invité à spécifier un deuxième pool de stockage à utiliser comme emplacement temporaire. Depuis StorageGRID 11.7, cette option a été supprimée.

Options de Grid Manager déplacées ou supprimées

Plusieurs options Grid Manager ont été déplacées ou supprimées.

- Le "Compresser les objets stockés" L'option a été déplacée vers **CONFIGURATION** > **système** > **compression objet**.
- Le paramètre de connexion interne **Network Transfer Encryption** a été supprimé et remplacé par le "Règles TLS et SSH" Sur la nouvelle page **CONFIGURATION** > **sécurité** > **Paramètres de sécurité**.

> L'option AES256-SHA était la valeur par défaut dans StorageGRID 11.6 et est le seul paramètre disponible dans StorageGRID 11.7. La valeur AES128-SHA est ignorée dans l'API de gestion de grille. Lors de la mise à niveau vers StorageGRID 11.7, l'algorithme de chiffrement du transfert réseau est défini sur AES256-SHA.

- Les options **chiffrement d'objet stocké**, **empêcher la modification du client** et **Activer HTTP pour les connexions au noeud de stockage** ont été déplacées vers le "Onglet réseau et objets" Sur la nouvelle page **CONFIGURATION** > **sécurité** > **Paramètres de sécurité**.
- Le "Délai d'inactivité du navigateur dépassé" L'option a été déplacée vers la nouvelle page **CONFIGURATION** > **sécurité** > **Paramètres de sécurité**.
- Le "Coût des liens" L'option a été déplacée vers **SUPPORT** > **autre** > **coût de liaison**.
- La liste des entités NMS a été déplacée vers **SUPPORT** > **autre** > **entités NMS**.
- L'option **Stored Object hach** a été supprimée. Les paramètres **SHA-1** et **SHA-256** ne sont plus utilisés pour la vérification interne en arrière-plan, car ils nécessitent des ressources CPU supplémentaires par rapport au contrôle MD5 et CRC32 du paquet.
- L'option **expéditeur préféré** a été supprimée. Si votre déploiement StorageGRID inclut plusieurs nœuds d'administration, le nœud d'administration principal est l'expéditeur préféré pour les notifications d'alerte, les messages AutoSupport, les traps et les notifications SNMP et les notifications d'alarme héritées. Si le nœud d'administration principal n'est plus disponible, les notifications sont envoyées temporairement par d'autres nœuds d'administration. Voir "Qu'est-ce qu'un nœud d'administration ?".
- Le "Paramètres réseau client non approuvés" Ont été déplacés vers **CONFIGURATION** > **contrôle du pare-feu**.

Restrictions de format du nom de domaine du terminal S3

L'utilisation d'adresses IP comme noms de domaine de noeud final n'est pas prise en charge. Les versions ultérieures empêcheront la configuration. Si vous devez utiliser des adresses IP pour les noms de domaine de point de terminaison, contactez le support technique. Voir "Noms de domaine de terminaux S3".

Commande Volume perdu lancée par l'utilisateur supprimée

Le `proc/CMSI/Volume_Lost` a été supprimé. Utilisez le `repair-data start-replicated-volume-repair` commande permettant de restaurer les données répliquées d'un volume.

Modifications apportées à l'API de gestion du grid

StorageGRID 11.7 utilise la version 3 de l'API de gestion du grid. La version 3 dégénère la version 2 ; cependant, les versions 1 et 2 sont toujours prises en charge.

> Vous pouvez continuer à utiliser les versions 1 et 2 de l'API de gestion avec StorageGRID 11.7. Cependant, la prise en charge de ces versions de l'API sera supprimée dans une prochaine version de StorageGRID. Après la mise à niveau vers StorageGRID 11.7, les API v1 et v2 obsolètes peuvent être désactivées à l'aide du `PUT /grid/config/management` API.

Pour en savoir plus, rendez-vous sur "Utilisez l'API de gestion du grid".

Afficher les noms désormais inclus dans les réponses aux demandes d'intégrité de nœud

Lié au nouveau "Procédure : renommer la grille, les sites et les nœuds", Après avoir renommé un site ou un nœud, le nom de l'élément (son nom système) et son nom d'affichage sont tous deux renvoyés par l'API **node-Health**.

Création d'un compartiment et de clés d'accès pour un nouveau locataire S3

Nouveau `s3Bucket` et `s3AccessKey` Des options ont été ajoutées à l'API **accounts**. Lorsque vous créez un compte de locataire S3 à l'aide de l'API de gestion du grid, vous pouvez éventuellement créer un compartiment pour ce locataire, ainsi que l'ID de clé d'accès et la clé secrète de l'utilisateur root du locataire.

Peut modifier l'état de stockage du nœud de stockage

Vous pouvez utiliser les nouveaux noeuds finaux de l'API **node-Storage-state** pour déterminer et modifier l'état du stockage dans un noeud de stockage (en ligne, hors ligne, en lecture seule).

Modifications apportées à l'API de gestion des locataires

StorageGRID 11.7 utilise la version 3 de l'API de gestion des locataires. La version 3 dégénère la version 2 ; cependant, les versions 1 et 2 sont toujours prises en charge.

> Vous pouvez continuer à utiliser les versions 1 et 2 de l'API de gestion avec StorageGRID 11.7. Cependant, la prise en charge de ces versions de l'API sera supprimée dans une prochaine version de StorageGRID. Après la mise à niveau vers StorageGRID 11.7, les API v1 et v2 obsolètes peuvent être désactivées à l'aide du `PUT /grid/config/management` API.

Nouveaux terminaux pour la fédération des grilles

Vous pouvez utiliser les noeuds finaux de l'API **grid-federation-connections** pour répertorier les connexions de fédération de grille pour le locataire actuel et pour effacer la dernière erreur de réplication de grille croisée pour le locataire actuel et la connexion de fédération de grille sélectionnée.

Pour en savoir plus, rendez-vous sur "Découvrez l'API de gestion des locataires".

Planifiez et préparez la mise à niveau

Estimer le temps nécessaire pour effectuer une mise à niveau

Lorsque vous planifiez une mise à niveau vers StorageGRID 11.7, vous devez déterminer le moment opportun pour la mise à niveau, en fonction de la durée de la mise à niveau. Vous devez également connaître les opérations que vous pouvez et ne pouvez pas effectuer à chaque étape de la mise à niveau.

Description de la tâche

Le temps nécessaire à une mise à niveau d'StorageGRID dépend de divers facteurs, tels que la charge client et les performances matérielles.

Le tableau résume les principales tâches de mise à niveau et indique le temps approximatif requis pour chaque tâche. Les étapes qui suivent le tableau fournissent des instructions que vous pouvez utiliser pour estimer le temps de mise à niveau de votre système.

Tâche de mise à niveau	Description	Temps approximatif requis	Au cours de cette tâche
Exécutez des contrôles préalables et mettez à niveau le nœud d'administration principal	Les précontrôles de mise à niveau sont exécutés et le nœud d'administration principal est arrêté, mis à niveau et redémarré.	De 30 minutes à 1 heure, avec les nœuds d'appliance SG100 et SG1000 nécessitant le plus de temps. Les erreurs de vérification préalable non résolues augmentent ce temps.	Vous ne pouvez pas accéder au nœud d'administration principal. Des erreurs de connexion peuvent être signalées, que vous pouvez ignorer. L'exécution des contrôles préalables à la mise à niveau avant le démarrage de la mise à niveau vous permet de résoudre les erreurs avant la fenêtre de maintenance de mise à niveau planifiée.
Démarrez le service de mise à niveau	Le fichier logiciel est distribué et le service de mise à niveau démarre.	3 minutes par nœud de grid	

Tâche de mise à niveau	Description	Temps approximatif requis	Au cours de cette tâche
Mettez à niveau les autres nœuds grid	Le logiciel de tous les autres nœuds de la grille est mis à niveau, dans l'ordre dans lequel vous approuvez les nœuds. Chaque nœud de votre système est mis hors service un par un.	de 15 minutes à 1 heure par nœud, avec des nœuds d'appliance exigeant le plus de temps **Remarque** : pour les nœuds d'appliance, le programme d'installation de l'appliance StorageGRID est automatiquement mis à jour vers la dernière version.	• Ne modifiez pas la configuration de la grille. • Ne modifiez pas la configuration du niveau d'audit. • Ne mettez pas à jour la configuration ILM. • Vous n'êtes pas en mesure d'effectuer d'autres procédures de maintenance, comme le correctif, la mise hors service ou l'extension. **Remarque** : si vous devez effectuer une récupération, contactez le support technique.
Activer les fonctions	Les nouvelles fonctionnalités de la nouvelle version sont activées.	Moins de 5 minutes	• Ne modifiez pas la configuration de la grille. • Ne modifiez pas la configuration du niveau d'audit. • Ne mettez pas à jour la configuration ILM. • Vous ne pouvez pas effectuer une autre procédure de maintenance.
Mettre à niveau la base de données	Le processus de mise à niveau vérifie chaque nœud pour vérifier que la base de données Cassandra n'a pas besoin d'être mise à jour.	10 secondes par nœud ou quelques minutes pour l'ensemble du grid	La mise à niveau de StorageGRID 11.6 vers 11.7 ne nécessite pas de mise à niveau de la base de données Cassandra. Cependant, le service Cassandra sera arrêté et redémarré sur chaque nœud de stockage. Pour les futures versions d'StorageGRID, l'étape de mise à jour de la base de données Cassandra peut prendre plusieurs jours.
Dernières étapes de mise à niveau	Les fichiers temporaires sont supprimés et la mise à niveau vers la nouvelle version se termine.	5 minutes	Lorsque la tâche **étapes finales de mise à niveau** est terminée, vous pouvez effectuer toutes les procédures de maintenance.

Étapes

1. Estimez le temps nécessaire à la mise à niveau de tous les nœuds du grid.
   a. Multipliez par 1 heure/nœud le nombre de nœuds de votre système StorageGRID.

      En règle générale, les nœuds d'appliance sont plus longs à mettre à niveau que les nœuds basés sur logiciel.

b. Ajoutez 1 heure à cette heure pour prendre en compte le temps requis pour télécharger le `.upgrade` file, exécutez les validations de pré-vérification et effectuez les étapes de mise à niveau finale.

2. Si vous avez des nœuds Linux, ajoutez 15 minutes pour chaque nœud afin de tenir compte du temps nécessaire au téléchargement et à l'installation du package RPM ou DEB.
3. Calculer le temps total estimé pour la mise à niveau en ajoutant les résultats des étapes 1 et 2.

Exemple : temps estimé pour la mise à niveau vers StorageGRID 11.7

Supposons que votre système dispose de 14 nœuds de grille, dont 8 sont des nœuds Linux.

1. Multipliez 14 par 1 heure/nœud.
2. Ajoutez 1 heure pour prendre en compte les étapes de téléchargement, de vérification préalable et finales.

   La durée estimée de mise à niveau de tous les nœuds est de 15 heures.

3. Multipliez 8 par 15 minutes/nœud pour tenir compte du temps nécessaire à l'installation du package RPM ou DEB sur les nœuds Linux.

   La durée estimée de cette étape est de 2 heures.

4. Ajoutez les valeurs ensemble.

   Vous devez prévoir jusqu'à 17 heures pour effectuer la mise à niveau de votre système vers StorageGRID 11.7.0.

> Si nécessaire, vous pouvez diviser la fenêtre de maintenance en fenêtres plus petites en approuvant des sous-ensembles de nœuds de grille pour la mise à niveau dans plusieurs sessions. Par exemple, vous pouvez préférer mettre à niveau les nœuds sur le site A en une session, puis mettre à niveau les nœuds sur le site B dans une session ultérieure. Si vous choisissez d'effectuer la mise à niveau dans plusieurs sessions, sachez que vous ne pouvez pas commencer à utiliser les nouvelles fonctionnalités tant que tous les nœuds n'ont pas été mis à niveau.

Quel est l'impact de votre système pendant la mise à niveau

Vous devez comprendre en quoi votre système StorageGRID sera affecté lors de la mise à niveau.

Les mises à niveau de StorageGRID ne générant pas de perturbation

Le système StorageGRID peut ingérer et récupérer les données depuis les applications client tout au long du processus de mise à niveau. Si vous approuvez la mise à niveau de tous les nœuds du même type (par exemple, nœuds de stockage), les nœuds sont arrêtés un par un. Ainsi, il n'y a pas de temps lorsque tous les nœuds de grid ou tous les nœuds de grid d'un certain type sont indisponibles.

Pour assurer une disponibilité continue, vérifiez que votre règle ILM contient des règles qui spécifient le stockage de plusieurs copies de chaque objet. Vous devez également vous assurer que tous les clients S3 ou Swift externes sont configurés pour envoyer des demandes à l'un des éléments suivants :

- Adresse IP virtuelle d'un groupe haute disponibilité (HA)
- Équilibreur de charge tiers haute disponibilité

- Plusieurs nœuds de passerelle pour chaque client
- Plusieurs nœuds de stockage pour chaque client

Le micrologiciel de l'appliance est mis à niveau

Pendant la mise à niveau de StorageGRID 11.7 :

- Tous les nœuds d'appliance StorageGRID sont automatiquement mis à niveau vers la version 3.7 du firmware du programme d'installation de l'appliance StorageGRID.
- Les appliances SG6060 et SGF6024 sont automatiquement mises à niveau vers la version du firmware du BIOS 3B07.EX et la version 3.97.07 du firmware du contrôleur BMC.
- Les appliances SG100 et SG1000 sont automatiquement mises à niveau vers la version 3B12.EC du firmware du BIOS et la version 4.71.07 du firmware du BMC.

Il est possible que des alertes soient déclenchées

Des alertes peuvent être déclenchées lorsque les services démarrent et s'arrêtent, et lorsque le système StorageGRID fonctionne comme un environnement de version mixte (certains nœuds de grid exécutant une version antérieure, alors que d'autres ont été mis à niveau vers une version plus récente). D'autres alertes peuvent être déclenchées une fois la mise à niveau terminée.

Par exemple, vous pouvez voir l'alerte **Impossible de communiquer avec le nœud** lorsque les services sont arrêtés, ou vous pouvez voir l'alerte **Cassandra communication error** lorsque certains nœuds ont été mis à niveau vers StorageGRID 11.7 mais que d'autres nœuds exécutent encore StorageGRID 11.6. En général, ces alertes s'efface une fois la mise à niveau terminée.

L'alerte **ILM placement unatteignable** peut être déclenchée lorsque les nœuds de stockage sont arrêtés lors de la mise à niveau vers StorageGRID 11.7. Cette alerte peut persister 1 jour après la fin de la mise à niveau.

Une fois la mise à niveau terminée, vous pouvez consulter toutes les alertes liées à la mise à niveau en sélectionnant **alertes récemment résolues** ou **alertes actuelles** dans le tableau de bord de Grid Manager.

De nombreuses notifications SNMP sont générées

Notez que de nombreuses notifications SNMP peuvent être générées lorsque les nœuds de la grille sont arrêtés et redémarrés lors de la mise à niveau. Pour éviter les notifications excessives, décochez la case **Activer les notifications d'agent SNMP** (**CONFIGURATION** > **surveillance** > **agent SNMP**) pour désactiver les notifications SNMP avant de démarrer la mise à niveau. Ensuite, réactivez les notifications une fois la mise à niveau terminée.

Les modifications de configuration sont restreintes

> Cette liste s'applique spécifiquement aux mises à niveau de StorageGRID 11.6 vers StorageGRID 11.7. Si vous effectuez une mise à niveau vers une autre version de StorageGRID, reportez-vous à la liste des modifications restreintes dans les instructions de mise à niveau de cette version.

Jusqu'à la fin de la tâche **Activer la nouvelle fonction** :

- N'apportez aucune modification à la configuration de la grille.
- N'activez ou ne désactivez aucune nouvelle fonctionnalité. Par exemple, n'essayez pas de créer une connexion de fédération de grille tant que les deux systèmes StorageGRID n'ont pas été mis à jour vers StorageGRID 11.7.

- Ne mettez pas à jour la configuration ILM. Sinon, vous risquez d'avoir un comportement ILM incohérent et inattendu.
- N'appliquez pas de correctif ou ne restaurez pas de nœud de grille.

> Contactez le support technique si vous avez besoin de restaurer un nœud pendant la mise à niveau.

- Lors de la mise à niveau vers StorageGRID 11.7, vous ne devez pas gérer les groupes haute disponibilité, les interfaces VLAN ni les terminaux d'équilibrage de la charge.
- Ne supprimez aucun groupe haute disponibilité qu'une fois la mise à niveau vers StorageGRID 11.7 terminée. Les adresses IP virtuelles d'autres groupes haute disponibilité peuvent devenir inaccessibles.

Jusqu'à la fin de la tâche **étapes de mise à niveau finale** :

- N'effectuez pas de procédure d'extension.
- N'effectuez pas de procédure de mise hors service.

Vous ne pouvez pas afficher les détails des compartiments ni gérer ces compartiments depuis le gestionnaire de locataires

Lors de la mise à niveau vers StorageGRID 11.7 (c'est-à-dire lorsque le système fonctionne comme un environnement à versions mixtes), vous ne pouvez pas afficher les détails des compartiments ni gérer les compartiments à l'aide du gestionnaire de locataires. L'une des erreurs suivantes apparaît sur la page compartiments du Gestionnaire de locataires :

- Vous ne pouvez pas utiliser cette API pendant la mise à niveau vers 11.7.
- Vous ne pouvez pas afficher les détails de la gestion des versions du compartiment dans le Gestionnaire de locataires pendant la mise à niveau vers la version 11.7.

Cette erreur se résoudra une fois la mise à niveau vers 11.7 terminée.

Solution de contournement

Pendant la mise à niveau vers la version 11.7, utilisez les outils suivants pour afficher les détails des compartiments ou gérer les compartiments au lieu d'utiliser le gestionnaire de locataires :

- Pour effectuer des opérations S3 standard sur un compartiment, utilisez l'un ou l'autre "L'API REST S3" ou le "API de gestion des locataires".
- Pour exécuter des opérations personnalisées StorageGRID sur un compartiment (par exemple, affichage et modification du niveau de cohérence du compartiment, activation ou désactivation des mises à jour du dernier accès ou configuration de l'intégration de la recherche), utilisez l'API de gestion des locataires.

Le chiffrement TLS ou les configurations SSH peuvent changer

Si le chiffrement TLS ou les configurations SSH ont été modifiés manuellement ou sont incohérents sur l'ensemble des nœuds, tous les nœuds seront remplacés par des modèles de compatibilité héritée ou moderne après la mise à niveau. Si vous avez utilisé `fips-ciphers.sh` Dans StorageGRID 11.6, la règle critères communs est appliquée à tous les nœuds. Dans le cas contraire, la stratégie de compatibilité héritée est appliquée. Si vous avez besoin de configurations validées par critères communs, vous devez utiliser la règle critères communs ou la règle stricte FIPS. Si vous n'avez pas utilisé `fips-ciphers.sh`, Vous devez utiliser le nouveau paramètre de compatibilité moderne une fois la mise à niveau terminée. Pour configurer les chiffrements, accédez à **CONFIGURATION** > **sécurité** > **Paramètres de sécurité** et sélectionnez **règles TLS et SSH**.

Les ports CLB peuvent être convertis en terminaux d'équilibrage de charge

Le service CLB (Connection Load Balancer) hérité a été supprimé dans StorageGRID 11.7. Si la configuration CLB est détectée pendant les précontrôles de mise à niveau, l'alerte **activité d'équilibreur de charge CLB héritée détectée** est déclenchée. Si des certificats personnalisés ont été configurés pour l'API S3 ou Swift dans la version StorageGRID existante, les ports CLB 8082, 8083, 8084 et 8085 seront convertis en terminaux d'équilibrage de charge lors de la mise à niveau vers StorageGRID 11.7.

Voir aussi "Considérations relatives à l'équilibrage de charge".

Impact d'une mise à niveau sur les groupes et les comptes d'utilisateurs

Vous devez comprendre l'impact de la mise à niveau StorageGRID, afin de pouvoir mettre à jour les groupes et les comptes utilisateur de manière appropriée une fois la mise à niveau terminée.

Modification des autorisations et des options de groupe

Après la mise à niveau vers StorageGRID 11.7, vous pouvez éventuellement attribuer la nouvelle autorisation suivante aux groupes d'utilisateurs locataires.

Autorisations	Description
Gestionnaire de locataires > gérer les objets avec la console S3	Associée à l'autorisation gérer tous les compartiments, cette autorisation permet aux utilisateurs d'accéder à "Console S3 expérimentale" À partir de la page compartiments. Les utilisateurs qui disposent de cette autorisation mais qui ne disposent pas de l'autorisation gérer tous les compartiments peuvent toujours naviguer directement vers la console S3 expérimentale.

Voir "Autorisations de gestion des locataires".

Vérifier la version installée de StorageGRID

Avant de démarrer la mise à niveau, vous devez vérifier que la version précédente de StorageGRID est actuellement installée avec le dernier correctif disponible appliqué.

Description de la tâche

Avant de procéder à la mise à niveau vers StorageGRID 11.7, StorageGRID 11.6 doit être installé sur votre grille. Si vous utilisez actuellement une version précédente de StorageGRID, vous devez installer tous les fichiers de mise à niveau précédents avec leurs derniers correctifs (fortement recommandés) jusqu'à ce que la version actuelle de votre grille soit StorageGRID 11.6.*x.y*.

Un chemin de mise à niveau possible est indiqué dans la exemple.

> NetApp vous recommande fortement d'appliquer le dernier correctif pour chaque version de StorageGRID avant de procéder à la mise à niveau vers la version suivante et d'appliquer également le dernier correctif à chaque nouvelle version que vous installez. Dans certains cas, vous devez appliquer un correctif pour éviter le risque de perte de données. Voir "Téléchargement NetApp : StorageGRID" et les notes de mise à jour de chaque correctif pour en savoir plus.

Notez que vous pouvez exécuter un script pour effectuer une mise à jour de 11.3.0.13+ à 11.4.0.*y* en une étape et de 11.4.0.7+ à 11.5.0.*y* en une étape. Voir "Base de connaissances NetApp : comment exécuter conjointement des mises à niveau majeures et un script de hot fix pour StorageGRID".

Étapes

1. Connectez-vous au Grid Manager à l'aide d'un "navigateur web pris en charge".
2. Dans le haut du Gestionnaire de grille, sélectionnez **aide** > **About**.
3. Vérifiez que **version** est 11.6.*x.y*.

   Dans StorageGRID 11.6.*x.y* numéro de version :

   - La **version majeure** a une valeur *x* de 0 (11.6.0).
   - Un **hotfix**, s'il a été appliqué, a une valeur *y* (par exemple, 11.6.0.1).
4. Si **version** n'est pas 11.6.*x.y*, passez à l' "Téléchargement NetApp : StorageGRID" pour télécharger les fichiers de chaque version précédente, y compris le dernier correctif pour chaque version.
5. Obtenez les instructions de mise à niveau pour chaque version que vous avez téléchargée. Exécutez ensuite la procédure de mise à niveau du logiciel pour cette version et appliquez le dernier correctif pour cette version (fortement recommandé).

   Voir la "Procédure de correctif StorageGRID".

Exemple : mise à niveau vers StorageGRID 11.6 à partir de la version 11.3.0.8

L'exemple suivant montre les étapes de mise à niveau de StorageGRID version 11.3.0.8 vers la version 11.6 en vue de la mise à niveau de StorageGRID 11.7.

> ⓘ Vous pouvez également exécuter un script pour combiner les étapes 2 et 3 (mise à jour de 11.3.0.13+ à 11.4.0.*y*) et pour combiner les étapes 4 et 5 (mise à jour de 11.4.0.7+ à 11.5.0.*y*). Voir "Base de connaissances NetApp : comment exécuter conjointement des mises à niveau majeures et un script de hot fix pour StorageGRID".

Téléchargez et installez le logiciel dans l'ordre suivant pour préparer votre système à la mise à niveau :

1. Appliquez le dernier correctif StorageGRID 11.3.0.*y*.
2. Passez à la version principale de StorageGRID 11.4.0.
3. Appliquez le dernier correctif StorageGRID 11.4.0.*y*.
4. Passez à la version principale de StorageGRID 11.5.0.
5. Appliquez le dernier correctif StorageGRID 11.5.0.*y*.
6. Mise à niveau vers la version majeure de StorageGRID 11.6.0.
7. Appliquez le dernier correctif StorageGRID 11.6.0.*y*.

Procurez-vous les ressources nécessaires à une mise à niveau logicielle

Avant de commencer la mise à niveau du logiciel, vous devez obtenir tous les supports nécessaires pour que la mise à niveau soit effectuée avec succès.

Élément	Remarques
L'ordinateur portable de service	L'ordinateur portable de service doit posséder : • Port réseau • Client SSH (par exemple, PuTTY)
"Navigateur Web pris en charge"	La prise en charge des navigateurs a généralement été modifiée pour chaque version de StorageGRID. Assurez-vous que votre navigateur est compatible avec la nouvelle version de StorageGRID.
Phrase secrète pour le provisionnement	La phrase de passe est créée et documentée lors de l'installation initiale du système StorageGRID. La phrase de passe de provisionnement n'est pas répertoriée dans le `Passwords.txt` fichier.
Archive RPM ou DEB Linux	Si des nœuds sont déployés sur des hôtes Linux, vous devez "Téléchargez et installez le progiciel RPM ou DEB sur tous les hôtes" avant de commencer la mise à niveau. **Important** : Assurez-vous que votre système d'exploitation est mis à niveau vers le noyau Linux 4.15 ou supérieur.
Documentation StorageGRID	• "Notes de mise à jour" Pour StorageGRID 11.7 (connexion requise). Lisez-les attentivement avant de commencer la mise à niveau. • "Guide de résolution des mises à niveau logicielles StorageGRID" pour la version majeure vers laquelle vous effectuez la mise à niveau (connexion requise) • Autre "Documentation StorageGRID 11.7", selon les besoins.

Vérifier l'état du système

Avant de mettre à niveau un système StorageGRID, vous devez vérifier que celui-ci est prêt à effectuer la mise à niveau. Vous devez vous assurer que le système fonctionne normalement et que tous les nœuds de la grille sont opérationnels.

Étapes

1. Connectez-vous au Grid Manager à l'aide d'un "navigateur web pris en charge".
2. Recherchez et résolvez les alertes actives.
3. Confirmez qu'aucune tâche de grille en conflit n'est active ou en attente.
   a. Sélectionnez **SUPPORT** > **Outils** > **topologie de grille**.
   b. Sélectionnez ***site*** > ***primary Admin Node*** > **CMN** > **Grid Tasks** > **Configuration**.

      Les tâches d'évaluation de la gestion du cycle de vie des informations (IDME) sont les seules tâches de grille pouvant être exécutées simultanément avec la mise à niveau logicielle.

   c. Si d'autres tâches de grille sont actives ou en attente, attendez qu'elles aient terminé ou lâchés leur verrouillage.

Contactez le support technique si une tâche ne se termine pas ou ne relâche pas son verrouillage.

4. Reportez-vous à la section "Communications internes sur les nœuds de la grille" et "Communications externes" Pour vous assurer que tous les ports requis pour StorageGRID 11.7 sont ouverts avant la mise à niveau.

   Les éléments suivants "ports internes" Doit être ouvert avant la mise à niveau vers StorageGRID 11.7 :

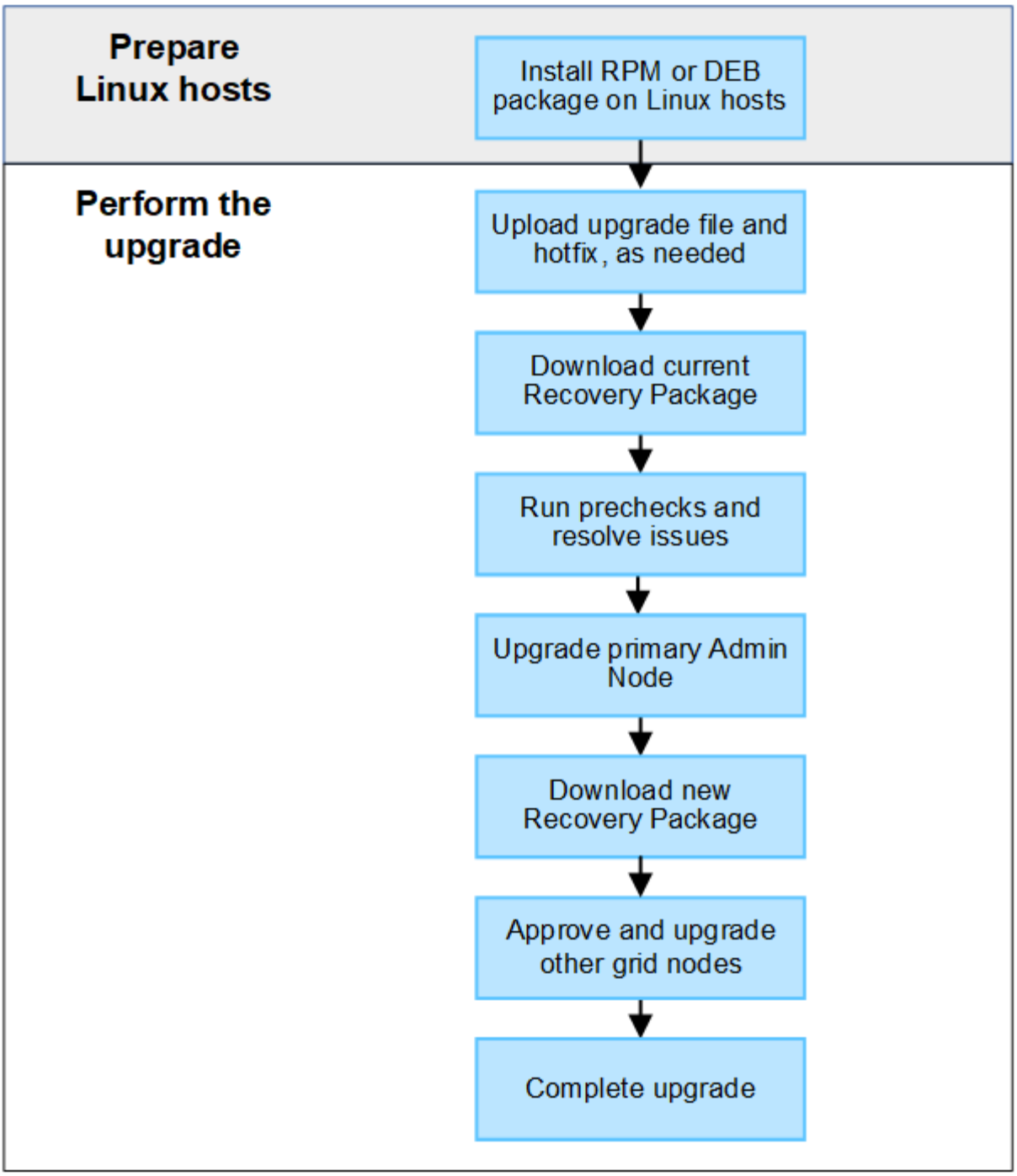
Port	Description
1055 8011 10342	Utilisé pour le protocole de cognement des contrôles de pare-feu. Avant de procéder à la mise à niveau, vérifiez que ce port est ouvert entre tous les nœuds de la grille du réseau.
18086	Port TCP utilisé pour le nouveau service LDR. Avant de procéder à la mise à niveau, vérifiez que ce port est ouvert de tous les nœuds de grid à tous les nœuds de stockage.

Si vous avez ouvert des ports de pare-feu personnalisés, vous êtes averti au cours de la vérification préalable de la mise à niveau. Vous devez contacter le support technique avant de procéder à la mise à niveau.

Mise à niveau du logiciel

Mise à niveau du workflow

Avant de commencer la mise à niveau, passez en revue le workflow général. La page mise à niveau de StorageGRID vous guide à chaque étape de la mise à niveau.



1. Si des nœuds StorageGRID sont déployés sur des hôtes Linux, "Installez le package RPM ou DEB sur chaque hôte" avant de commencer la mise à niveau.
2. Depuis le nœud d'administration principal, accédez à la page mise à niveau StorageGRID et téléchargez le fichier de mise à niveau et le fichier correctif, si nécessaire.
3. Téléchargez le progiciel de récupération actuel.
4. Exécutez des précontrôles de mise à niveau pour détecter et résoudre tout problème avant de démarrer la mise à niveau réelle.
5. Démarrez la mise à niveau, qui exécute automatiquement des précontrôles et met à niveau le nœud d'administration principal. Vous ne pouvez pas accéder au gestionnaire de grille pendant la mise à niveau du nœud d'administration principal. Les journaux d'audit seront également indisponibles. Cette mise à niveau peut prendre jusqu'à 30 minutes.

6. Une fois le nœud d'administration principal mis à niveau, téléchargez un nouveau package de récupération.
7. Approuver les nœuds de la grille. Vous pouvez approuver des nœuds grid individuels, des groupes de nœuds grid ou tous les nœuds.

   > N'approuvez pas la mise à niveau d'un nœud grid sauf si vous êtes sûr que ce nœud est prêt à être arrêté et redémarré.

8. Reprendre les opérations. Une fois tous les nœuds de la grille mis à niveau, de nouvelles fonctionnalités sont activées et vous pouvez reprendre les opérations. Vous devez attendre d'effectuer une procédure de mise hors service ou d'extension jusqu'à ce que la tâche d'arrière-plan **mettre à niveau la base de données** et la tâche **étapes finales de mise à niveau** soient terminées.

Informations associées

"Estimer le temps nécessaire pour effectuer une mise à niveau"

Linux : téléchargez et installez le progiciel RPM ou DEB sur tous les hôtes

Si des nœuds StorageGRID sont déployés sur des hôtes Linux, vous devez télécharger et installer un package RPM ou DEB supplémentaire sur chacun de ces hôtes avant de démarrer la mise à niveau.

Téléchargez les fichiers de mise à niveau, Linux et de correctif

Lorsque vous effectuez une mise à niveau StorageGRID à partir du Gestionnaire de grille, vous êtes invité à télécharger l'archive de mise à niveau et tout correctif requis dans la première étape. Cependant, si vous devez télécharger des fichiers pour mettre à niveau les hôtes Linux, vous pouvez gagner du temps en téléchargeant à l'avance tous les fichiers requis.

Étapes

1. Accédez à "Téléchargement NetApp : StorageGRID".
2. Sélectionnez le bouton pour télécharger la dernière version ou sélectionnez une autre version dans le menu déroulant et sélectionnez **Go**.

   Les versions du logiciel StorageGRID ont le format suivant : 11.*x.y*. Les correctifs StorageGRID ont le format suivant : 11.*x.y.z*.

3. Connectez-vous avec le nom d'utilisateur et le mot de passe de votre compte NetApp.
4. Si un avertissement attention/MustRead apparaît, notez le numéro du correctif et cochez la case.
5. Lisez le contrat de licence de l'utilisateur final, cochez la case, puis sélectionnez **accepter et continuer**.

   La page des téléchargements de la version sélectionnée s'affiche. La page contient trois colonnes.

6. A partir de la deuxième colonne (**Upgrade StorageGRID**), téléchargez deux fichiers :
   - L'archive de mise à niveau pour la dernière version (il s'agit du fichier dans la section intitulée **VMware, SG1000 ou SG100 Primary Admin Node**). Ce fichier n'est pas nécessaire tant que vous n'avez pas effectué la mise à niveau, mais le téléchargement de ce fichier permet de gagner du temps.
   - Une archive RPM ou DEB dans l'une ou l'autre `.tgz` ou `.zip` format. Sélectionner `.zip` Fichier si vous exécutez Windows sur l'ordinateur portable de service.
     - Red Hat Enterprise Linux ou CentOS

```
StorageGRID-Webscale-version-RPM-uniqueID.zip
StorageGRID-Webscale-version-RPM-uniqueID.tgz
```

- Ubuntu ou Debian

```
StorageGRID-Webscale-version-DEB-uniqueID.zip
StorageGRID-Webscale-version-DEB-uniqueID.tgz
```

7. Si vous devez accepter un avis attention/MustRead en raison d'un correctif requis, téléchargez le correctif :
   a. Revenir à "Téléchargement NetApp : StorageGRID".
   b. Sélectionnez le numéro de correctif dans la liste déroulante.
   c. Acceptez à nouveau la mise en garde et le CLUF.
   d. Téléchargez et enregistrez le correctif et son fichier README.

      Vous serez invité à télécharger le fichier de correctif sur la page mise à niveau StorageGRID lorsque vous démarrez la mise à niveau.

Installez l'archive sur tous les hôtes Linux

Procédez comme suit avant de mettre à niveau le logiciel StorageGRID.

Étapes

1. Extrayez les packages RPM ou DEB du fichier d'installation.
2. Installez les packages RPM ou DEB sur tous les hôtes Linux.

   Reportez-vous aux étapes d'installation des services d'hôte StorageGRID dans les instructions d'installation :

   - "Red Hat Enterprise Linux ou CentOS : installez les services hôtes StorageGRID"
   - "Ubuntu ou Debian : installez les services hôtes StorageGRID"

   Les nouveaux packages sont installés en tant que modules supplémentaires. Ne supprimez pas les packages existants.

Effectuez la mise à niveau

Vous pouvez effectuer une mise à niveau vers StorageGRID 11.7 et appliquer simultanément le dernier correctif pour cette version. La page de mise à niveau StorageGRID fournit le chemin de mise à niveau recommandé et des liens directs vers les pages de téléchargement correctes.

Avant de commencer

Vous avez passé en revue toutes les considérations et terminé toutes les étapes de planification et de préparation.

Accédez à la page mise à niveau StorageGRID

Dans un premier temps, accédez à la page mise à niveau StorageGRID dans le Gestionnaire de grille.

Étapes

1. Connectez-vous au Grid Manager à l'aide d'un "navigateur web pris en charge".

2. Sélectionnez **MAINTENANCE** > **système** > **mise à jour logicielle**.
3. Dans la mosaïque de mise à niveau StorageGRID, sélectionnez **mettre à niveau**.

Sélectionnez fichiers

Le chemin de mise à jour de la page mise à niveau StorageGRID indique les versions majeures (par exemple, 11.7.0) et les correctifs (par exemple, 11.7.0.1) que vous devez installer pour obtenir la dernière version de StorageGRID. Vous devez installer les versions et correctifs recommandés dans l'ordre indiqué.

> Si aucun chemin de mise à jour n'est affiché, il se peut que votre navigateur ne puisse pas accéder au site de support NetApp ou que la case à cocher **Rechercher les mises à jour logicielles** sur la page AutoSupport (**SUPPORT** > **Outils** > **AutoSupport**) soit désactivée.

Étapes

1. Pour l'étape **Sélectionner des fichiers**, vérifiez le chemin de mise à jour.
2. Dans la section Télécharger les fichiers, sélectionnez chaque lien **Télécharger** pour télécharger les fichiers requis depuis le site de support NetApp.

   Si aucun chemin de mise à jour n'est affiché, passer à l' "Téléchargement NetApp : StorageGRID" pour déterminer si une nouvelle version ou un correctif est disponible et pour télécharger les fichiers dont vous avez besoin.

   > Si vous avez besoin de télécharger et d'installer un package RPM ou DEB sur tous les hôtes Linux, il se peut que vous ayez déjà répertorié les fichiers de mise à niveau et de correctif StorageGRID dans le chemin de mise à jour.

3. Sélectionnez **Parcourir** pour télécharger le fichier de mise à niveau de version vers StorageGRID : `NetApp_StorageGRID_11.7.0_Software_uniqueID.upgrade`

   Une fois le processus de téléchargement et de validation terminé, une coche verte apparaît en regard du nom du fichier.

4. Si vous avez téléchargé un fichier correctif, sélectionnez **Parcourir** pour télécharger ce fichier. Le correctif sera automatiquement appliqué dans le cadre de la mise à niveau de la version.
5. Sélectionnez **Continuer**.

Exécutez des contrôles préalables

L'exécution de contrôles préalables vous permet de détecter et de résoudre les problèmes de mise à niveau avant de commencer à mettre à niveau votre grille.

Étapes

1. Pour l'étape **Exécuter les précontrôles**, commencez par saisir la phrase de passe de provisionnement pour votre grille.
2. Sélectionnez **Télécharger le paquet de récupération**.

   Vous devez télécharger la copie actuelle du fichier du package de récupération avant de mettre à niveau le nœud d'administration principal. Le fichier du progiciel de récupération vous permet de restaurer le système en cas de défaillance.

3. Une fois le fichier téléchargé, vérifiez que vous pouvez accéder au contenu, y compris au

`Passwords.txt` fichier.

4. Copiez le fichier téléchargé (`.zip`) à deux emplacements sûrs, sécurisés et séparés.

> Le fichier du progiciel de récupération doit être sécurisé car il contient des clés de cryptage et des mots de passe qui peuvent être utilisés pour obtenir des données du système StorageGRID.

5. Sélectionnez **Exécuter les précontrôles** et attendez que les précontrôles soient terminés.
6. Passez en revue les détails de chaque vérification préalable signalée et résolvez les erreurs signalées. Voir la "Guide de résolution des mises à niveau logicielles StorageGRID" Pour la version StorageGRID 11.7.

   Vous devez résoudre tous les problèmes de vérification préalable *erreurs* avant de pouvoir mettre à niveau votre système. Cependant, vous n'avez pas besoin de corriger les *avertissements* de prévérification avant de procéder à la mise à niveau.

> Si vous avez ouvert des ports de pare-feu personnalisés, vous êtes averti lors de la validation de contrôle préalable. Vous devez contacter le support technique avant de procéder à la mise à niveau.

7. Si vous avez apporté des modifications à la configuration pour résoudre les problèmes signalés, sélectionnez **Exécuter les contrôles préalables** à nouveau pour obtenir des résultats mis à jour.

   Si toutes les erreurs ont été résolues, vous êtes invité à démarrer la mise à niveau.

Démarrez la mise à niveau et mettez à niveau le nœud d'administration principal

Lorsque vous démarrez la mise à niveau, les précontrôles de mise à niveau sont de nouveau exécutés et le nœud d'administration principal est automatiquement mis à niveau. Cette partie de la mise à niveau peut prendre jusqu'à 30 minutes.

> Vous ne pourrez accéder à aucune autre page Grid Manager pendant la mise à niveau du nœud d'administration principal. Les journaux d'audit seront également indisponibles.

Étapes

1. Sélectionnez **Démarrer la mise à niveau**.

   Un avertissement s'affiche pour vous rappeler que vous perdrez temporairement l'accès au Gestionnaire de grille.

2. Sélectionnez **OK** pour accuser réception de l'avertissement et démarrer la mise à niveau.
3. Attendez que les contrôles préalables de mise à niveau soient effectués et que le nœud d'administration principal soit mis à niveau.

> Si des erreurs de vérification préalable sont signalées, résolvez-les et sélectionnez de nouveau **Démarrer la mise à niveau**.

   Si la grille dispose d'un autre nœud d'administration en ligne et prêt, vous pouvez l'utiliser pour contrôler l'état du nœud d'administration principal. Dès que le nœud d'administration principal est mis à niveau, vous pouvez approuver les autres nœuds de la grille.

4. Si nécessaire, sélectionnez **Continuer** pour accéder à l'étape **mettre à niveau les autres nœuds**.

Mise à niveau des autres nœuds

Vous devez mettre à niveau tous les nœuds de la grille, mais vous pouvez effectuer plusieurs sessions de mise à niveau et personnaliser la séquence de mise à niveau. Par exemple, vous pouvez préférer mettre à niveau les nœuds sur le site A en une session, puis mettre à niveau les nœuds sur le site B dans une session ultérieure. Si vous choisissez d'effectuer la mise à niveau dans plusieurs sessions, sachez que vous ne pouvez pas commencer à utiliser les nouvelles fonctionnalités tant que tous les nœuds n'ont pas été mis à niveau.

Si l'ordre de mise à niveau des nœuds est important, approuvez les nœuds ou les groupes de nœuds un par un et attendez que la mise à niveau soit terminée sur chaque nœud avant d'approuver le prochain nœud ou groupe de nœuds.

> Lorsque la mise à niveau démarre sur un nœud de la grille, les services de ce nœud sont arrêtés. Plus tard, le nœud de la grille est redémarré. Pour éviter toute interruption de service pour les applications client qui communiquent avec le nœud, n'approuvez pas la mise à niveau d'un nœud, sauf si vous êtes sûr que le nœud est prêt à être arrêté et redémarré. Si nécessaire, planifiez une fenêtre de maintenance ou avisez les clients.

Étapes

1. Pour l'étape **mettre à niveau d'autres nœuds**, consultez le résumé, qui fournit l'heure de début de la mise à niveau dans son ensemble et l'état de chaque tâche de mise à niveau majeure.
   - **Démarrer le service de mise à niveau** est la première tâche de mise à niveau. Au cours de cette tâche, le fichier logiciel est distribué aux nœuds de grille et le service de mise à niveau est lancé sur chaque nœud.
   - Lorsque la tâche **Démarrer le service de mise à niveau** est terminée, la tâche **mettre à niveau d'autres nœuds de grille** démarre et vous êtes invité à télécharger une nouvelle copie du progiciel de récupération.
2. Lorsque vous y êtes invité, saisissez votre phrase de passe de provisionnement et téléchargez une nouvelle copie du pack de récupération.

   > Vous devez télécharger une nouvelle copie du fichier du package de récupération après la mise à niveau du nœud d'administration principal. Le fichier du progiciel de récupération vous permet de restaurer le système en cas de défaillance.

3. Consultez les tableaux d'état pour chaque type de nœud. Il existe des tableaux pour les nœuds d'administration non primaires, les nœuds de passerelle, les nœuds de stockage et les nœuds d'archivage.

   Un nœud de grille peut se trouver dans l'une des étapes suivantes lorsque les tables apparaissent pour la première fois :

   - Déballage de la mise à niveau
   - Téléchargement
   - En attente d'approbation
4. lorsque vous êtes prêt à sélectionner des nœuds de grille pour la mise à niveau (ou si vous devez annuler l'approbation des nœuds sélectionnés), utilisez les instructions suivantes :

Tâche	Instructions
Recherchez des nœuds spécifiques à approuver, tels que tous les nœuds d'un site particulier	Entrez la chaîne de recherche dans le champ **Search**
Sélectionnez tous les nœuds à mettre à niveau	Sélectionnez **approuver tous les nœuds**
Sélectionnez tous les nœuds du même type pour la mise à niveau (par exemple, tous les nœuds de stockage)	Sélectionnez le bouton **Approve All** pour le type de noeud Si vous approuvez plusieurs nœuds du même type, les nœuds seront mis à niveau un par un.
Sélectionnez un nœud individuel pour la mise à niveau	Sélectionnez le bouton **Approve** du nœud
Reporter la mise à niveau sur tous les nœuds sélectionnés	Sélectionnez **Annuler l'approbation de tous les nœuds**
Reporter la mise à niveau sur tous les nœuds sélectionnés du même type	Sélectionnez le bouton **Annuler tout** pour le type de noeud
Reporter la mise à niveau sur un nœud individuel	Sélectionnez le bouton **Unapprove** du nœud

5. Attendez que les nœuds approuvés passent par ces étapes de mise à niveau :
   - Approuvé et en attente de mise à niveau
   - Arrêt des services

     Vous ne pouvez pas supprimer un nœud lorsque sa scène atteint **Arrêt des services**. Le bouton **Unapprove** est désactivé.

   - Arrêt du conteneur
   - Nettoyage des images Docker
   - Mise à niveau des packages OS de base

     Lorsqu'un nœud d'appliance atteint ce stade, le logiciel StorageGRID Appliance installer de l'appliance est mis à jour. Ce processus automatisé garantit que la version du programme d'installation de l'appliance StorageGRID reste synchronisée avec la version du logiciel StorageGRID.

   - Redémarrage

     Certains modèles d'appliance peuvent redémarrer plusieurs fois pour mettre à niveau le micrologiciel et le BIOS.

   - Exécution des étapes après le redémarrage
   - Démarrage des services

- L'a fait

6. Répétez le étape d'approbation autant de fois que nécessaire jusqu'à la mise à niveau de tous les nœuds grid.

Mise à niveau terminée

Lorsque tous les nœuds de grille ont terminé les étapes de mise à niveau, la tâche **mettre à niveau d'autres nœuds de grille** s'affiche comme terminée. Les tâches de mise à niveau restantes sont effectuées automatiquement en arrière-plan.

Étapes

1. Dès que la tâche **Activer les fonctions** est terminée (ce qui se produit rapidement), vous pouvez commencer à utiliser le "nouvelles fonctionnalités" Dans la version StorageGRID mise à niveau.
2. Pendant la tâche **mettre à niveau la base de données**, le processus de mise à niveau vérifie chaque nœud pour vérifier que la base de données Cassandra n'a pas besoin d'être mise à jour.

> La mise à niveau de StorageGRID 11.6 vers 11.7 ne nécessite pas de mise à niveau de la base de données Cassandra. Cependant, le service Cassandra sera arrêté et redémarré sur chaque nœud de stockage. Pour les futures versions d'StorageGRID, l'étape de mise à jour de la base de données Cassandra peut prendre plusieurs jours.

3. Une fois la tâche **mettre à niveau la base de données** terminée, attendez quelques minutes pour que les **étapes finales de la mise à niveau** soient terminées.
4. Lorsque les **étapes finales de la mise à niveau** sont terminées, la mise à niveau est effectuée. La première étape, **Sélectionner les fichiers**, est réaffichée avec une bannière de succès verte.
5. Vérifiez que les opérations de la grille sont à nouveau normales :
   a. Vérifiez que les services fonctionnent normalement et qu'il n'y a pas d'alerte inattendue.
   b. Vérifiez que les connexions client au système StorageGRID fonctionnent comme prévu.

Résoudre les problèmes de mise à niveau

Si un problème se produit lors de la mise à niveau, vous pouvez résoudre le problème vous-même. Si vous ne parvenez pas à résoudre un problème, collectez autant d'informations que possible, puis contactez le support technique.

La mise à niveau n'est pas terminée

Les sections suivantes décrivent comment effectuer une restauration à partir de situations où la mise à niveau a partiellement échoué.

Erreurs de contrôle préalable de mise à niveau

Pour détecter et résoudre les problèmes, vous pouvez exécuter manuellement les contrôles préalables à la mise à niveau avant de démarrer la mise à niveau réelle. La plupart des erreurs de précontrôle fournissent des informations sur la façon de résoudre le problème.

Défaillances de provisionnement

Si le processus de provisionnement automatique échoue, contactez le support technique.

Le nœud de la grille tombe en panne ou ne parvient pas à démarrer

Si un nœud de la grille tombe en panne lors du processus de mise à niveau ou ne parvient pas à démarrer avec succès une fois la mise à niveau terminée, contactez le support technique pour rechercher et corriger les problèmes sous-jacents.

L'ingestion ou la récupération des données est interrompue

Si l'ingestion ou la récupération des données est interrompue de manière inattendue alors que vous ne mettez pas à niveau un nœud de grid, contactez le support technique.

Erreurs de mise à niveau de base de données

Si la mise à niveau de la base de données échoue avec une erreur, essayez à nouveau la mise à niveau. En cas d'échec à nouveau, contactez le support technique.

Informations associées

"Vérification de l'état du système avant la mise à niveau du logiciel"

Problèmes liés à l'interface utilisateur

Vous pourriez rencontrer des problèmes avec le gestionnaire de grille ou le gestionnaire de locataires pendant ou après la mise à niveau.

Grid Manager affiche plusieurs messages d'erreur lors de la mise à niveau

Si vous actualisez votre navigateur ou naviguez vers une autre page Grid Manager pendant la mise à niveau du nœud d'administration principal, vous pouvez voir plusieurs messages « 503 : service non disponible » et « problème de connexion au serveur ». Vous pouvez ignorer ces messages en toute sécurité ; ils ne s'affichent plus dès que le nœud est mis à niveau.

Si ces messages s'affichent pendant plus d'une heure après le démarrage de la mise à niveau, il se peut que quelque chose ait empêché la mise à niveau du nœud d'administration principal. Si vous ne parvenez pas à résoudre le problème par vous-même, contactez le support technique.

L'interface Web ne répond pas comme prévu

Le gestionnaire de grid ou le gestionnaire de locataires peut ne pas répondre comme prévu après la mise à niveau du logiciel StorageGRID.

Si vous rencontrez des problèmes avec l'interface Web :

- Assurez-vous d'utiliser un "navigateur web pris en charge".

  > La prise en charge des navigateurs a généralement été modifiée pour chaque version de StorageGRID.

- Effacez le cache de votre navigateur Web.

  L'effacement du cache supprime les ressources obsolètes utilisées par la version précédente du logiciel StorageGRID et permet à l'interface utilisateur de fonctionner de nouveau correctement. Pour obtenir des instructions, reportez-vous à la documentation de votre navigateur Web.

Messages d'erreur "Docker image Availability check"

Lorsque vous tentez de démarrer le processus de mise à niveau, un message d'erreur indiquant « les problèmes suivants ont été identifiés par la suite de validation des contrôles de disponibilité des images Docker » s'affiche. Tous les problèmes doivent être résolus avant la fin de la mise à niveau.

Contactez le support technique si vous n'êtes pas certain des modifications requises pour résoudre les problèmes identifiés.

Messagerie	Cause	Solution
Impossible de déterminer la version de la mise à niveau. Mettre à niveau le fichier d'informations de version `{file_path}` ne correspond pas au format attendu.	Le package de mise à niveau est corrompu.	Téléchargez à nouveau le package de mise à niveau, puis réessayez. Si le problème persiste, contactez le support technique.
Mettre à niveau le fichier d'informations de version `{file_path}` n'a pas été trouvé. Impossible de déterminer la version de la mise à niveau.	Le package de mise à niveau est corrompu.	Téléchargez à nouveau le package de mise à niveau, puis réessayez. Si le problème persiste, contactez le support technique.
Impossible de déterminer la version de version actuellement installée sur `{node_name}`.	Un fichier critique du nœud est corrompu.	Contactez l'assistance technique.
Erreur de connexion lors de la tentative de liste des versions sur `{node_name}`	Le nœud est hors ligne ou la connexion a été interrompue.	Vérifiez que tous les nœuds sont en ligne et accessibles depuis le nœud d'administration principal, puis réessayez.
Hôte pour le nœud `{node_name}` N'a pas de StorageGRID `{upgrade_version}` image chargée. Les images et les services doivent être installés sur l'hôte avant que la mise à niveau ne puisse se poursuivre.	Les packages RPM ou DEB pour la mise à niveau n'ont pas été installés sur l'hôte sur lequel le nœud est en cours d'exécution, ou les images sont toujours en cours d'importation. **Remarque :** cette erreur s'applique uniquement aux nœuds qui s'exécutent en tant que conteneurs sous Linux.	Assurez-vous que les packages RPM ou DEB ont été installés sur tous les hôtes Linux sur lesquels des nœuds sont exécutés. Assurez-vous que la version est correcte pour le service et le fichier d'images. Attendez quelques minutes, puis réessayez. Voir "Linux : installez le package RPM ou DEB sur tous les hôtes".
Erreur lors de la vérification du nœud `{node_name}`	Une erreur inattendue s'est produite.	Attendez quelques minutes, puis réessayez.
Erreur de suppression lors de l'exécution de contrôles préalables. `{error_string}`	Une erreur inattendue s'est produite.	Attendez quelques minutes, puis réessayez.

Configurez et gérez

Administrer StorageGRID

StorageGRID d'administration : présentation

Suivez ces instructions pour configurer et administrer un système StorageGRID.

À propos de ces instructions

Ces instructions expliquent comment utiliser Grid Manager pour configurer des groupes et des utilisateurs, créer des comptes de locataires pour permettre aux applications client S3 et Swift de stocker et récupérer des objets, configurer et gérer des réseaux StorageGRID, configurer AutoSupport, gérer des paramètres de nœud, etc.

Ces instructions s'adresse au personnel technique qui devra configurer, administrer et prendre en charge un système StorageGRID après son installation.

Avant de commencer

- Vous disposez d'une compréhension générale du système StorageGRID.
- Vous disposez d'une connaissance assez détaillée des shells de commande Linux, de la mise en réseau et de la configuration matérielle du serveur.

Lancez-vous avec Grid Manager

Navigateurs Web pris en charge

Vous devez utiliser un navigateur Web pris en charge.

Navigateur Web	Version minimale prise en charge
Google Chrome	107
Microsoft Edge	107
Mozilla Firefox	106

Vous devez régler la fenêtre du navigateur sur une largeur recommandée.

Largeur du navigateur	Pixels
Minimum	1024
Optimale	1280

Connectez-vous au Grid Manager

Vous accédez à la page de connexion de Grid Manager en entrant le nom de domaine complet (FQDN) ou l'adresse IP d'un noeud d'administration dans la barre d'adresse d'un navigateur Web pris en charge.

Présentation

Chaque système StorageGRID comprend un nœud d'administration principal et un nombre quelconque de nœuds d'administration non primaires. Vous pouvez vous connecter au Gestionnaire de grille sur n'importe quel noeud d'administration pour gérer le système StorageGRID. Cependant, les nœuds d'administration sont différents :

- Les accusés de réception d'alarme (système hérité) effectués sur un nœud d'administration ne sont pas copiés sur d'autres nœuds d'administration. Pour cette raison, les informations affichées pour les alarmes peuvent ne pas être identiques sur chaque nœud d'administration.
- Certaines procédures de maintenance peuvent uniquement être effectuées depuis le nœud d'administration principal.

Se connecter au groupe haute disponibilité

Si des nœuds admin sont inclus dans un groupe haute disponibilité (HA), vous vous connectez à l'aide de l'adresse IP virtuelle du groupe haute disponibilité ou d'un nom de domaine complet mappé sur l'adresse IP virtuelle. Le nœud d'administration principal doit être sélectionné comme interface principale du groupe, de sorte que lorsque vous accédez à Grid Manager, vous y accédez sur le nœud d'administration principal, sauf si le nœud d'administration principal n'est pas disponible. Voir "Gérez les groupes haute disponibilité".

Utiliser SSO

Les étapes de connexion sont légèrement différentes si "L'authentification unique (SSO) a été configurée".

Connectez-vous à Grid Manager sur le premier nœud d'administration

Avant de commencer

- Vous disposez de vos identifiants de connexion.
- Vous utilisez un "navigateur web pris en charge".
- Les cookies sont activés dans votre navigateur Web.
- Vous appartenez à un groupe d'utilisateurs disposant d'au moins une autorisation.
- Vous avez l'URL du Gestionnaire de grille :

  `https://FQDN_or_Admin_Node_IP/`

  Vous pouvez utiliser le nom de domaine complet, l'adresse IP d'un nœud d'administration ou l'adresse IP virtuelle d'un groupe haute disponibilité de nœuds d'administration.

  Pour accéder au Gestionnaire de grille sur un port autre que le port par défaut pour HTTPS (443), indiquez le numéro de port dans l'URL :

  `https://FQDN_or_Admin_Node_IP:port/`

  SSO n'est pas disponible sur le port Grid Manager restreint. Vous devez utiliser le port 443.

Étapes

1. Lancez un navigateur Web pris en charge.
2. Dans la barre d'adresse du navigateur, entrez l'URL du Gestionnaire de grille.
3. Si vous êtes invité à recevoir une alerte de sécurité, installez le certificat à l'aide de l'assistant d'installation du navigateur. Voir "Gérer les certificats de sécurité".
4. Connectez-vous au Grid Manager.

   L'écran de connexion qui s'affiche dépend de la configuration de l'authentification unique (SSO) pour StorageGRID.

Pas d'utilisation de SSO

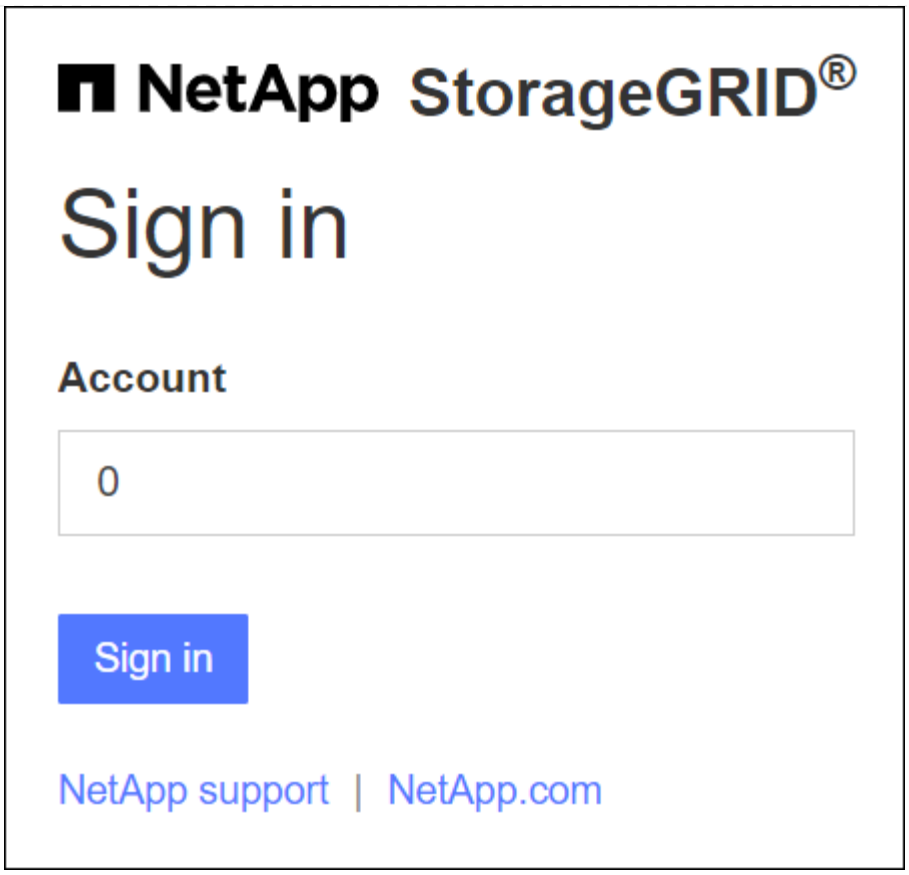
a. Saisissez votre nom d'utilisateur et votre mot de passe pour le Grid Manager.

b. Sélectionnez **connexion**.

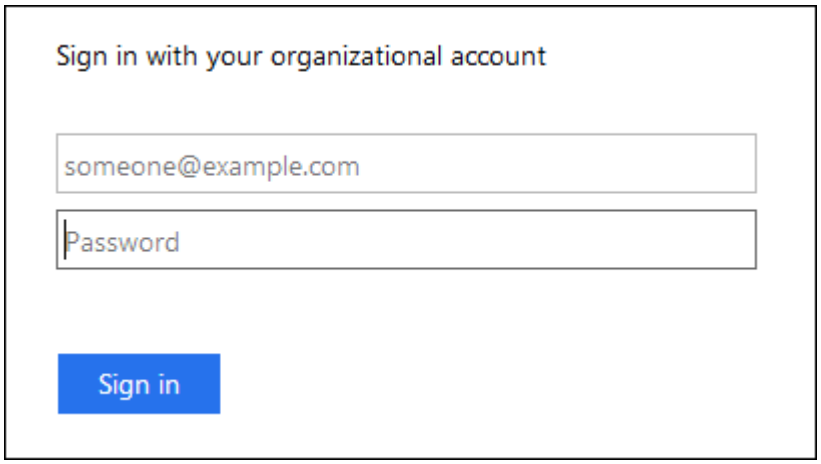
Utilisation de SSO

◦ Si StorageGRID utilise SSO pour la première fois que vous accédez à l'URL de ce navigateur :

i. Sélectionnez **connexion**. Vous pouvez laisser le 0 dans le champ compte.



ii. Saisissez vos identifiants SSO standard sur la page de connexion SSO de votre entreprise. Par exemple :



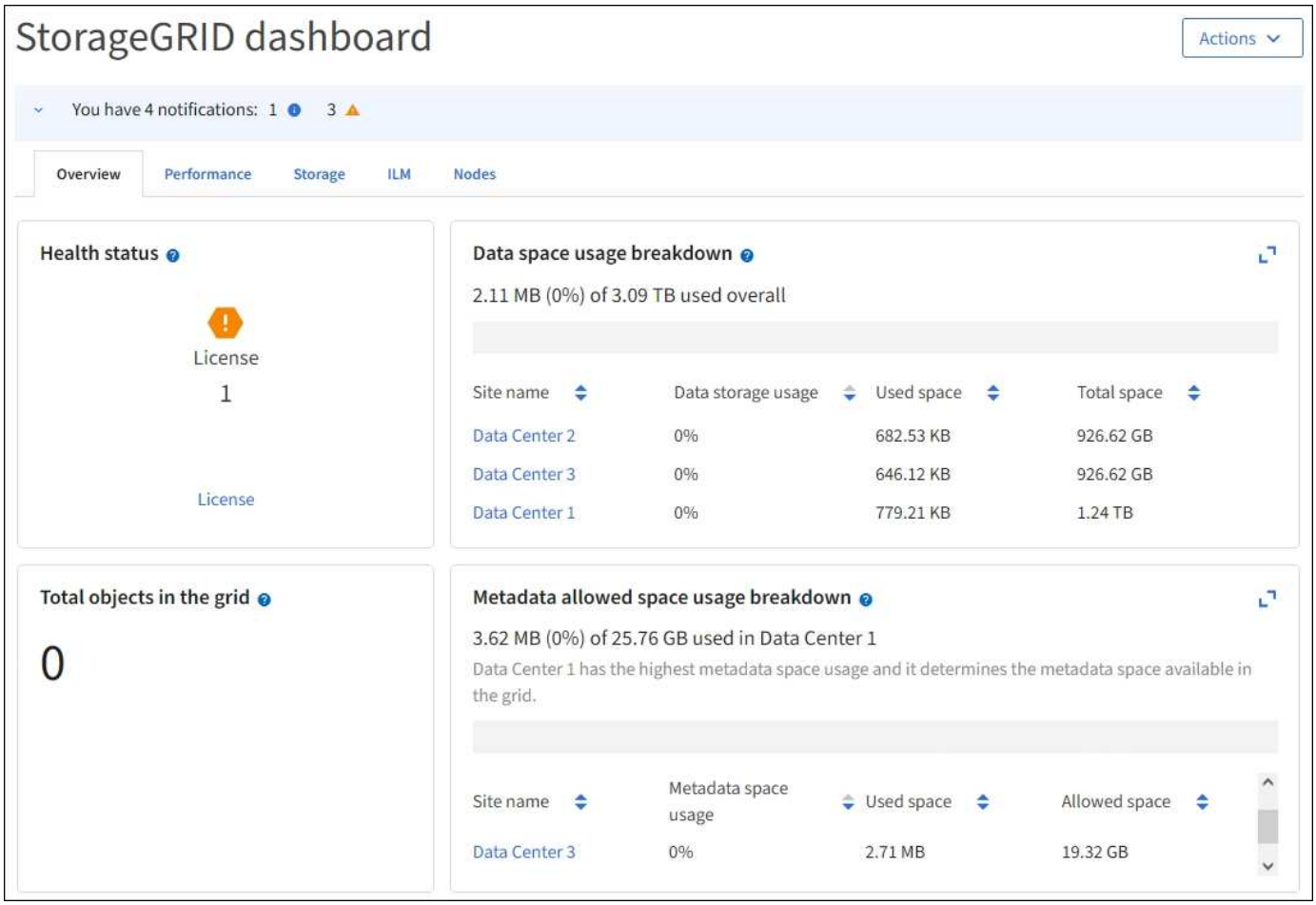
- Si StorageGRID utilise SSO et que vous avez déjà accédé au Gestionnaire de grille ou à un compte de locataire :

  i. Entrez **0** (l'ID de compte du gestionnaire de grille) ou sélectionnez **Grid Manager** s'il apparaît dans la liste des comptes récents.

ii. Sélectionnez **connexion**.

iii. Connectez-vous à l'aide de vos identifiants SSO standard sur la page de connexion SSO de votre entreprise.

Lorsque vous êtes connecté, la page d'accueil du Gestionnaire de grille s'affiche, qui inclut le tableau de bord. Pour connaître les informations fournies, reportez-vous à la section "Affichez et gérez le tableau de bord".



Connectez-vous à un autre nœud d'administration

Procédez comme suit pour vous connecter à un autre nœud d'administration.

Pas d'utilisation de SSO

Étapes

1. Dans la barre d'adresse du navigateur, entrez le nom de domaine complet ou l'adresse IP de l'autre noeud d'administration. Indiquez le numéro de port requis.
2. Saisissez votre nom d'utilisateur et votre mot de passe pour le Grid Manager.
3. Sélectionnez **connexion**.

Utilisation de SSO

Si StorageGRID utilise SSO et que vous vous êtes connecté à un nœud d'administration, vous pouvez accéder à d'autres nœuds d'administration sans avoir à vous reconnecter.

Étapes

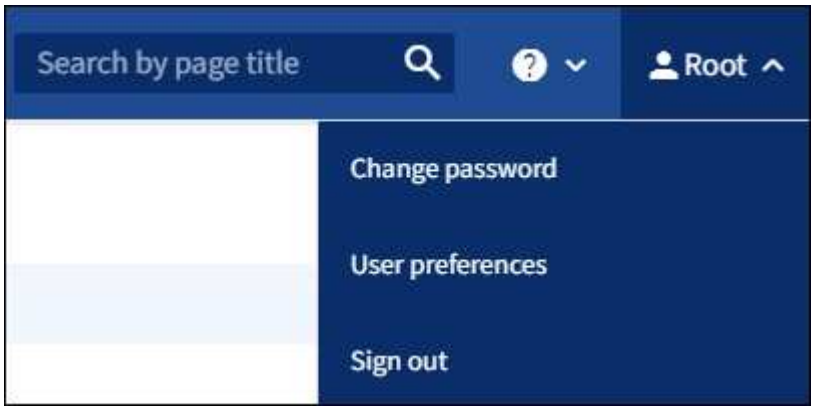
1. Entrez le nom de domaine complet ou l'adresse IP de l'autre noeud d'administration dans la barre d'adresse du navigateur.
2. Si votre session SSO a expiré, saisissez à nouveau vos informations d'identification.

Déconnectez-vous du Grid Manager

Lorsque vous avez terminé de travailler avec le Gestionnaire de grille, vous devez vous déconnecter pour vous assurer que les utilisateurs non autorisés ne peuvent pas accéder au système StorageGRID. La fermeture de votre navigateur risque de ne pas vous déconnecter du système, en fonction des paramètres des cookies du navigateur.

Étapes

1. Sélectionnez votre nom d'utilisateur dans le coin supérieur droit.



2. Sélectionnez **Déconnexion**.

Option	Description
SSO non utilisé	Vous êtes déconnecté du nœud d'administration. La page de connexion de Grid Manager s'affiche. **Remarque :** si vous vous êtes connecté à plusieurs nœuds d'administration, vous devez vous déconnecter de chaque nœud.
SSO activé	Vous êtes déconnecté de tous les nœuds d'administration auxquels vous accédiez. La page de connexion StorageGRID s'affiche. **Grid Manager** est répertorié comme valeur par défaut dans la liste déroulante **comptes récents** et le champ **ID compte** affiche 0. **Remarque :** si SSO est activé et que vous êtes également connecté au gestionnaire de locataires, vous devez également le faire "déconnectez-vous du compte du locataire" à "Déconnectez-vous de SSO".

Changer votre mot de passe

Si vous êtes un utilisateur local de Grid Manager, vous pouvez modifier votre propre mot de passe.

Avant de commencer

Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".

Description de la tâche

Si vous vous connectez à StorageGRID en tant qu'utilisateur fédéré ou si l'authentification unique (SSO) est activée, vous ne pouvez pas modifier votre mot de passe dans le Gestionnaire de grille. Vous devez plutôt modifier votre mot de passe dans le référentiel d'identité externe, par exemple Active Directory ou OpenLDAP.

Étapes

1. Dans l'en-tête de Grid Manager, sélectionnez ***votre nom*** > **changer mot de passe**.
2. Saisissez votre mot de passe actuel.
3. Saisissez un nouveau mot de passe.

   Votre mot de passe doit contenir au moins 8 caractères et pas plus de 32 caractères. Les mots de passe sont sensibles à la casse.

4. Saisissez à nouveau le nouveau mot de passe.
5. Sélectionnez **Enregistrer**.

Afficher les informations de licence StorageGRID

Vous pouvez afficher les informations relatives aux licences de votre système StorageGRID, comme la capacité de stockage maximale de votre réseau, si nécessaire.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".

Description de la tâche

En cas de problème avec la licence logicielle de ce système StorageGRID, la carte d'état d'intégrité du tableau de bord comprend une icône d'état de la licence et un lien **Licence**. Ce numéro indique le nombre de problèmes liés à la licence.

Étapes

1. Accédez à la page Licence en effectuant l'une des opérations suivantes :
   - Dans la carte d'état d'intégrité du tableau de bord, sélectionnez l'icône d'état de la licence ou le lien **Licence**. Ce lien apparaît uniquement en cas de problème avec la licence.
   - Sélectionnez **MAINTENANCE** > **système** > **Licence**.
2. Afficher les détails en lecture seule de la licence actuelle :

- ID du système StorageGRID, qui est le numéro d'identification unique de cette installation StorageGRID
- Numéro de série de la licence
- Type de licence, soit **perpétuel** soit **abonnement**
- Capacité de stockage sous licence de la grille
- Capacité de stockage prise en charge
- Date de fin de licence. **N/A** apparaît pour une licence perpétuelle.
- Date de fin du contrat de service de support

  Cette date est lue à partir du fichier de licence actuel et peut être obsolète si vous avez prolongé ou renouvelé le contrat de service de support après avoir obtenu le fichier de licence. Pour mettre à jour cette valeur, reportez-vous à "Mettez à jour les informations de licence StorageGRID"la . Vous pouvez également afficher la date de fin réelle du contrat à l'aide du conseiller numérique Active IQ (également appelé conseiller numérique).

- Contenu du fichier texte de licence

> Pour les licences émises avant StorageGRID 10.3, la capacité de stockage sous licence n'est pas incluse dans le fichier de licence et un message « Voir contrat de licence » s'affiche au lieu d'une valeur.

Mettez à jour les informations de licence StorageGRID

Vous devez mettre à jour les informations de licence de votre système StorageGRID à tout moment que les conditions de votre modification de licence changent. Par exemple, vous devez mettre à jour les informations de licence si vous achetez de la capacité de stockage supplémentaire pour votre grid.

Avant de commencer

- Vous avez un nouveau fichier de licence à appliquer à votre système StorageGRID.
- Vous disposez d'autorisations d'accès spécifiques.
- Vous avez la phrase secrète pour le provisionnement.

Étapes

1. Sélectionnez **MAINTENANCE** > **système** > **Licence**.
2. Entrez la phrase de passe de provisionnement pour votre système StorageGRID dans la zone de texte **phrase de passe de provisionnement**, puis sélectionnez **Parcourir**.
3. Dans la boîte de dialogue Ouvrir, localisez et sélectionnez le nouveau fichier de licence (`.txt`) Et sélectionnez **Ouvrir**.

   Le nouveau fichier de licence est validé et affiché.

4. Sélectionnez **Enregistrer**.

Utilisez l'API

Vous pouvez effectuer des tâches de gestion du système à l'aide de l'API REST Grid Management plutôt que de l'interface utilisateur Grid Manager. Par exemple, vous pouvez utiliser l'API pour automatiser les opérations ou créer plusieurs entités plus rapidement (par exemple, les utilisateurs).

Ressources générales

L'API de gestion du grid fournit les ressources de premier niveau suivantes :

- `/grid`: L'accès est limité aux utilisateurs de Grid Manager et est basé sur les autorisations de groupe configurées.
- `/org`: L'accès est limité aux utilisateurs qui appartiennent à un groupe LDAP local ou fédéré pour un compte locataire. Pour plus de détails, voir "Utilisez un compte de locataire".
- `/private`: L'accès est limité aux utilisateurs de Grid Manager et est basé sur les autorisations de groupe configurées. Les API privées sont susceptibles d'être modifiées sans préavis. Les terminaux privés StorageGRID ignorent également la version API de la demande.

Émettre des requêtes API

L'API Grid Management utilise la plateforme d'API open source swagger. Swagger fournit une interface utilisateur intuitive qui permet aux développeurs et aux non-développeurs d'effectuer des opérations en temps réel dans StorageGRID avec l'API.

L'interface utilisateur swagger fournit des détails complets et de la documentation pour chaque opération API.

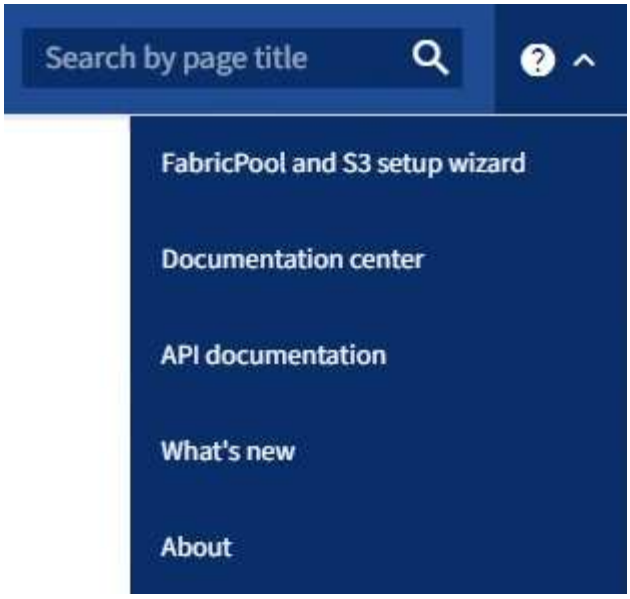
Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous disposez d'autorisations d'accès spécifiques.

> Toutes les opérations d'API que vous effectuez à l'aide de la page Web API Docs sont des opérations en direct. Veillez à ne pas créer, mettre à jour ou supprimer des données de configuration ou d'autres données par erreur.

Étapes

1. Dans l'en-tête Grid Manager, sélectionnez l'icône d'aide et sélectionnez **documentation API**.



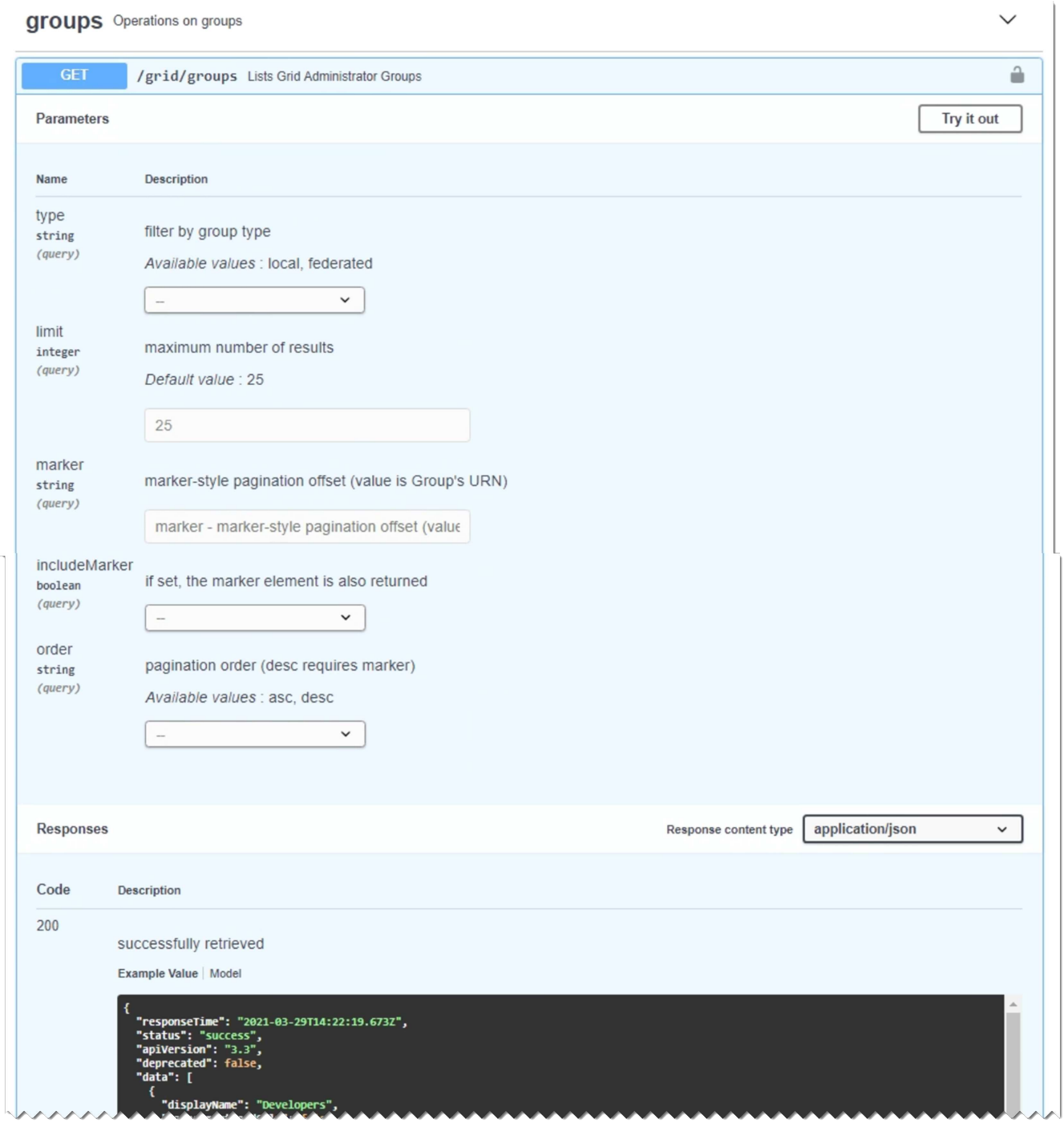
2. Pour effectuer une opération avec l'API privée, sélectionnez **accéder à la documentation API privée** sur la page API de gestion StorageGRID.

   Les API privées sont susceptibles d'être modifiées sans préavis. Les terminaux privés StorageGRID ignorent également la version API de la demande.

3. Sélectionnez l'opération souhaitée.

   Lorsque vous développez une opération API, vous pouvez voir les actions HTTP disponibles, telles QUE GET, PUT, UPDATE ou DELETE.

4. Sélectionnez une action HTTP pour afficher les détails de la demande, notamment l'URL du noeud final, la liste de tous les paramètres obligatoires ou facultatifs, un exemple de l'organisme de demande (si nécessaire) et les réponses possibles.



5. Déterminez si la demande nécessite des paramètres supplémentaires, tels qu'un ID de groupe ou d'utilisateur. Ensuite, obtenir ces valeurs. Vous devrez peut-être d'abord lancer une autre demande d'API pour obtenir les informations dont vous avez besoin.
6. Déterminez si vous devez modifier l'exemple de corps de la demande. Si c'est le cas, vous pouvez sélectionner **modèle** pour connaître les exigences de chaque champ.
7. Sélectionnez **essayez-le**.
8. Fournir tous les paramètres requis ou modifier le corps de la demande selon les besoins.
9. Sélectionnez **Exécuter**.
10. Vérifiez le code de réponse pour déterminer si la demande a réussi.

L'API Grid Management organise les opérations disponibles dans les sections suivantes.

Cette liste inclut uniquement les opérations disponibles dans l'API publique.

- **Comptes** : opérations de gestion des comptes de locataires de stockage, y compris la création de nouveaux comptes et la récupération de l'utilisation du stockage pour un compte donné.
- **Alarmes** : opérations permettant de répertorier les alarmes actuelles (système hérité) et de renvoyer des informations sur l'intégrité de la grille, y compris les alertes actuelles et un résumé des États de connexion des nœuds.
- **Alert-history** : opérations sur les alertes résolues.
- **Alerteurs** : opérations sur les récepteurs de notification d'alerte (e-mail).
- **Alert-rules** : opérations sur les règles d'alerte.
- **Silences d'alerte** : opérations sur les silences d'alerte.
- **Alertes** : opérations sur les alertes.
- **Audit** : opérations pour répertorier et mettre à jour la configuration de l'audit.
- **Auth** : opérations pour effectuer l'authentification de session utilisateur.

  L'API Grid Management prend en charge le schéma d'authentification par jeton Bearer. Pour vous connecter, vous fournissez un nom d'utilisateur et un mot de passe dans le corps JSON de la demande d'authentification (c'est-à-dire, `POST /api/v3/authorize`). Si l'utilisateur est authentifié, un jeton de sécurité est renvoyé. Ce token doit être fourni dans l'en-tête des requêtes API suivantes (« autorisation : porteur *token* »).

  Si l'authentification unique est activée pour le système StorageGRID, vous devez effectuer différentes étapes pour l'authentification. Voir « authentification dans l'API si l'authentification unique est activée ».

  Pour plus d'informations sur l'amélioration de la sécurité d'authentification, reportez-vous à la section « protection contre la falsification de demandes intersites ».

- **Certificats-client** : opérations permettant de configurer les certificats client afin que StorageGRID soit accessible en toute sécurité à l'aide d'outils de surveillance externes.
- **Config** : opérations liées à la version du produit et aux versions de l'API Grid Management. Vous pouvez répertorier la version du produit et les principales versions de l'API Grid Management prises en charge par cette version, et désactiver les versions obsolètes de l'API.
- **Désactivé-features** : opérations permettant d'afficher les fonctions qui auraient pu être désactivées.
- **dns-servers** : opérations permettant de répertorier et de modifier les serveurs DNS externes configurés.
- **Endpoint-domain-names** : opérations permettant de répertorier et de modifier les noms de domaine des noeuds finaux S3.
- **Code d'effacement** : opérations sur les profils de code d'effacement.
- **Expansion** : opérations d'expansion (au niveau de la procédure).
- **Noeuds-expansion**: Opérations sur expansion (niveau noeud).
- **Sites d'expansion** : opérations d'expansion (au niveau du site).
- **GRID-Networks** : opérations permettant de répertorier et de modifier la liste des réseaux de la grille.

- **GRID-mots de passe** : opérations pour la gestion des mots de passe de la grille.
- **Groupes** : opérations permettant de gérer les groupes d'administrateurs de grille locaux et de récupérer les groupes d'administrateurs de grille fédérés à partir d'un serveur LDAP externe.
- **Identity-source** : opérations permettant de configurer un référentiel d'identité externe et de synchroniser manuellement les informations relatives au groupe fédéré et à l'utilisateur.
- **ilm** : opérations sur la gestion du cycle de vie de l'information (ILM).
- **License** : opérations de récupération et de mise à jour de la licence StorageGRID.
- **Logs** : opérations de collecte et de téléchargement de fichiers journaux.
- **Metrics** : opérations sur les métriques StorageGRID, y compris les requêtes métriques instantanées à un point dans le temps et les requêtes métriques de plage sur une plage de temps. L'API de gestion du grid utilise l'outil de contrôle des systèmes Prometheus comme source de données back-end. Pour plus d'informations sur la création de requêtes Prometheus, consultez le site Web Prometheus.

> Indicateurs qui incluent *`private`* dans leur nom sont destinés à un usage interne uniquement. Ces metrics sont susceptibles d'être modifiés sans préavis entre les versions d'StorageGRID.

- **Node-details** : opérations sur les détails de noeud.
- **Node-Health** : opérations sur l'état d'intégrité du nœud.
- **État-stockage-noeud** : opérations sur l'état de stockage du noeud.
- **ntp-servers** : opérations de liste ou de mise à jour des serveurs NTP (Network Time Protocol) externes.
- **Objets** : opérations sur les objets et les métadonnées des objets.
- **Récupération** : opérations pour la procédure de récupération.
- **Recovery-package**: Opérations pour télécharger le progiciel de récupération.
- **Régions** : opérations pour afficher et créer des régions.
- **s3-object-lock** : opérations sur les paramètres globaux de verrouillage d'objet S3.
- **Server-certificate** : opérations pour afficher et mettre à jour les certificats de serveur Grid Manager.
- **snmp** : opérations sur la configuration SNMP actuelle.
- **Classes de trafic** : opérations pour les politiques de classification du trafic.
- **Ingest-client-network** : opérations sur la configuration réseau client non fiable.
- **Utilisateurs** : opérations permettant d'afficher et de gérer les utilisateurs de Grid Manager.

Gestion des versions de l'API de gestion du grid

L'API de gestion du grid utilise la gestion des versions pour prendre en charge les mises à niveau sans interruption.

Par exemple, cette URL de demande spécifie la version 3 de l'API.

`https://hostname_or_ip_address/api/v3/authorize`

La version majeure de l'API de gestion des locataires est incrémentée lorsque des modifications sont effectuées, qui sont ***non compatibles*** avec des versions antérieures. La version mineure de l'API de gestion des locataires est incrémentée lorsque des modifications sont effectuées que ***sont compatibles*** avec des versions antérieures. Les modifications compatibles incluent l'ajout de nouveaux noeuds finaux ou de

nouvelles propriétés. L'exemple suivant illustre comment la version de l'API est incrémentée en fonction du type de modifications apportées.

Type de modification de l'API	Ancienne version	Nouvelle version
Compatible avec les versions plus anciennes	2.1	2.2
Non compatible avec les versions plus anciennes	2.1	3.0

Lors de la première installation du logiciel StorageGRID, seule la version la plus récente de l'API de gestion de grille est activée. Cependant, lorsque vous effectuez une mise à niveau vers une nouvelle version de StorageGRID, vous continuez à accéder à l'ancienne version de l'API pour au moins une version de StorageGRID.

> Vous pouvez utiliser l'API Grid Management pour configurer les versions prises en charge. Pour plus d'informations, reportez-vous à la section « config » de la documentation de l'API swagger. Vous devez désactiver la prise en charge de l'ancienne version après avoir mis à jour tous les clients de l'API Grid Management pour utiliser la version la plus récente.

Les requêtes obsolètes sont marquées comme obsolètes de l'une des manières suivantes :

- L'en-tête de réponse est « obsolète : vrai »
- Le corps de la réponse JSON inclut « obsolète » : vrai
- Un avertissement obsolète est ajouté à nms.log. Par exemple :

```
Received call to deprecated v1 API at POST "/api/v1/authorize"
```

Identification des versions d'API prises en charge dans la version actuelle

Utilisez la requête d'API suivante pour renvoyer une liste des versions principales de l'API prises en charge :

```
GET https://{{IP-Address}}/api/versions
{
  "responseTime": "2019-01-10T20:41:00.845Z",
  "status": "success",
  "apiVersion": "3.0",
  "data": [
    2,
    3
  ]
}
```

Spécifiez une version API pour une demande

Vous pouvez spécifier la version de l'API à l'aide d'un paramètre de chemin d'accès (`/api/v3`) ou un en-tête (`Api-Version: 3`). Si vous indiquez les deux valeurs, la valeur de l'en-tête remplace la valeur du chemin d'accès.

```
curl https://[IP-Address]/api/v3/grid/accounts

curl -H "Api-Version: 3" https://[IP-Address]/api/grid/accounts
```

Protection contre la contrefaçon de demandes intersites (CSRF)

Vous pouvez vous protéger contre les attaques de contrefaçon de requêtes intersites (CSRF) contre StorageGRID en utilisant des jetons CSRF pour améliorer l'authentification qui utilise des cookies. Grid Manager et tenant Manager activent automatiquement cette fonction de sécurité ; les autres clients API peuvent choisir de l'activer lorsqu'ils se connectent.

Un attaquant pouvant déclencher une requête vers un autre site (par exemple avec UN POST de formulaire HTTP) peut créer certaines requêtes à l'aide des cookies de l'utilisateur connecté.

StorageGRID contribue à la protection contre les attaques CSRF en utilisant des jetons CSRF. Lorsque cette option est activée, le contenu d'un cookie spécifique doit correspondre au contenu d'un en-tête spécifique ou d'un paramètre DE CORPS POST spécifique.

Pour activer la fonction, définissez l' `csrfToken` paramètre à `true` pendant l'authentification. La valeur par défaut est `false`.

```
curl -X POST --header "Content-Type: application/json" --header "Accept:
application/json" -d "{
  \"username\": \"MyUserName\",
  \"password\": \"MyPassword\",
  \"cookie\": true,
  \"csrfToken\": true
}" "https://example.com/api/v3/authorize"
```

Si vrai, un `GridCsrfToken` Le cookie est défini avec une valeur aléatoire pour les connexions dans Grid Manager et dans `AccountCsrfToken` Le cookie est défini avec une valeur aléatoire pour les connexions au Gestionnaire de locataires.

Si le cookie est présent, toutes les demandes pouvant modifier l'état du système (POST, PUT, PATCH, DELETE) doivent inclure l'une des options suivantes :

- Le `X-Csrf-Token` En-tête, avec la valeur de l'en-tête définie sur la valeur du cookie de jeton CSRF.
- Pour les noeuds finaux qui acceptent un corps codé par formulaire : a `csrfToken` paramètre corps de demande codé par formulaire.

Reportez-vous à la documentation en ligne de l'API pour obtenir des exemples et des détails supplémentaires.

Les demandes disposant d'un jeu de cookies de jeton CSRF appliquent également le `"Content-Type: application/json"` En-tête pour toute demande qui attend un corps de requête JSON comme une protection supplémentaire contre les attaques CSRF.

Utilisez l'API si l'authentification unique est activée (Active Directory)

Si vous l'avez "Authentification unique (SSO) configurée et activée" Et vous utilisez Active Directory comme fournisseur SSO, vous devez émettre une série de requêtes API pour obtenir un jeton d'authentification valide pour l'API Grid Management ou l'API tenant Management.

Connectez-vous à l'API si l'authentification unique est activée

Ces instructions s'appliquent si vous utilisez Active Directory comme fournisseur d'identité SSO.

Avant de commencer

- Vous connaissez le nom d'utilisateur et le mot de passe SSO d'un utilisateur fédéré appartenant à un groupe d'utilisateurs StorageGRID.
- Pour accéder à l'API de gestion des locataires, vous connaissez l'ID du compte locataire.

Description de la tâche

Pour obtenir un jeton d'authentification, vous pouvez utiliser l'un des exemples suivants :

- Le `storagegrid-ssoauth.py` Script Python, situé dans le répertoire des fichiers d'installation de StorageGRID (`./rpms` Pour Red Hat Enterprise Linux ou CentOS, `./debs` Pour Ubuntu ou Debian, et `./vsphere` Pour VMware).
- Un exemple de flux de travail des requêtes Curl.

  Le flux de travail de boucle risque de s'échapper si vous l'effectuez trop lentement. L'erreur peut s'afficher : `A valid SubjectConfirmation was not found on this Response`.

  L'exemple de flux de travail Curl ne protège pas le mot de passe d'être vu par d'autres utilisateurs.

Si vous avez un problème de codage d'URL, l'erreur peut s'afficher : `Unsupported SAML version`.

Étapes

1. Sélectionnez l'une des méthodes suivantes pour obtenir un jeton d'authentification :
   - Utilisez le `storagegrid-ssoauth.py` Script Python. Passez à l'étape 2.
   - Utiliser les demandes de gondoles. Passez à l'étape 3.
2. Si vous souhaitez utiliser le `storagegrid-ssoauth.py` Passez le script à l'interpréteur Python et exécutez le script.

   Lorsque vous y êtes invité, entrez des valeurs pour les arguments suivants :

   - Méthode SSO. Entrez ADFS ou adfs.

- Le nom d'utilisateur SSO
- Domaine dans lequel StorageGRID est installé
- L'adresse de StorageGRID
- L'ID du compte de locataire, pour accéder à l'API de gestion des locataires.

```
python3 storagegrid-ssoauth.py
sso_method: adfs
saml_user: my-sso-username
saml_domain: my-domain
sg_address: storagegrid.example.com
tenant_account_id: 12345
Enter the user's SAML password:
********************************************************************************

********************************************************************************
StorageGRID Auth Token: 56eb07bf-21f6-40b7-afob-5c6cacfb25e7
```

Le jeton d'autorisation StorageGRID est fourni dans la sortie. Vous pouvez maintenant utiliser le token pour d'autres requêtes, de la même manière que vous utilisiez l'API si SSO n'était pas utilisé.

3. Si vous souhaitez utiliser des requêtes Curl, suivez la procédure ci-dessous.

   a. Déclarez les variables nécessaires pour la connexion.

```
export SAMLUSER='my-sso-username'
export SAMLPASSWORD='my-password'
export SAMLDOMAIN='my-domain'
export TENANTACCOUNTID='12345'
export STORAGEGRID_ADDRESS='storagegrid.example.com'
export AD_FS_ADDRESS='adfs.example.com'
```

   > Pour accéder à l'API de gestion de grille, utilisez 0 comme `TENANTACCOUNTID`.

   b. Pour recevoir une URL d'authentification signée, lancez une demande POST à `/api/v3/authorize-saml`, Et supprimez le codage JSON supplémentaire de la réponse.

   Cet exemple montre une demande POST pour une URL d'authentification signée pour `TENANTACCOUNTID`. Les résultats seront transmis à `python -m json.tool` Pour supprimer l'encodage JSON.

```
curl -X POST "https://$STORAGEGRID_ADDRESS/api/v3/authorize-saml" \
  -H "accept: application/json" -H  "Content-Type: application/json"
\
  --data "{\"accountId\": \"$TENANTACCOUNTID\"}" | python -m
json.tool
```

   La réponse dans cet exemple inclut une URL signée codée par URL, mais n'inclut pas la couche

supplémentaire de codage JSON.

```
{
    "apiVersion": "3.0",
    "data":
"https://adfs.example.com/adfs/ls/?SAMLRequest=fZHLbsIwEEV%2FJTuv7...
sSl%2BfQ33cvfwA%3D&RelayState=12345",
    "responseTime": "2018-11-06T16:30:23.355Z",
    "status": "success"
}
```

c. Enregistrez le `SAMLRequest` à partir de la réponse pour une utilisation dans les commandes suivantes.

```
export SAMLREQUEST='fZHLbsIwEEV%2FJTuv7...sSl%2BfQ33cvfwA%3D'
```

d. Obtenir une URL complète incluant l'ID de demande client d'AD FS.

Une option consiste à demander le formulaire de connexion à l'aide de l'URL de la réponse précédente.

```
curl "https://$AD_FS_ADDRESS/adfs/ls/?SAMLRequest=
$SAMLREQUEST&RelayState=$TENANTACCOUNTID" | grep 'form method="post"
id="loginForm"'
```

La réponse inclut l'ID de demande client :

```
<form method="post" id="loginForm" autocomplete="off"
novalidate="novalidate" onKeyPress="if (event && event.keyCode == 13)
Login.submitLoginRequest();" action="/adfs/ls/?
SAMLRequest=fZHRToMwFIZfhb...UJikvo77sXPw%3D%3D&RelayState=12345&clie
nt-request-id=00000000-0000-0000-ee02-0080000000de" >
```

e. Enregistrez l'ID de la demande client à partir de la réponse.

```
export SAMLREQUESTID='00000000-0000-0000-ee02-0080000000de'
```

f. Envoyez vos informations d'identification à l'action de formulaire de la réponse précédente.

```
curl -X POST "https://$AD_FS_ADDRESS
/adfs/ls/?SAMLRequest=$SAMLREQUEST&RelayState=$TENANTACCOUNTID&client
-request-id=$SAMLREQUESTID" \
--data "UserName=$SAMLUSER@$SAMLDOMAIN&Password=
$SAMLPASSWORD&AuthMethod=FormsAuthentication" --include
```

AD FS renvoie une redirection 302, avec des informations supplémentaires dans les en-têtes.

> Si l'authentification multifacteur (MFA) est activée pour votre système SSO, le post du formulaire contiendra également le deuxième mot de passe ou d'autres informations d'identification.

```
HTTP/1.1 302 Found
Content-Length: 0
Content-Type: text/html; charset=utf-8
Location:
https://adfs.example.com/adfs/ls/?SAMLRequest=fZHRToMwFIZfhb...UJikvo
77sXPw%3D%3D&RelayState=12345&client-request-id=00000000-0000-0000-
ee02-0080000000de
Set-Cookie: MSISAuth=AAEAADAvsHpXk6ApV...pmP0aEiNtJvWY=; path=/adfs;
HttpOnly; Secure
Date: Tue, 06 Nov 2018 16:55:05 GMT
```

g. Enregistrez le `MSISAuth` cookie de la réponse.

```
export MSISAuth='AAEAADAvsHpXk6ApV...pmP0aEiNtJvWY='
```

h. Envoyez une demande GET à l'emplacement spécifié avec les cookies du POST d'authentification.

```
curl "https://$AD_FS_ADDRESS/adfs/ls/?SAMLRequest=
$SAMLREQUEST&RelayState=$TENANTACCOUNTID&client-request-
id=$SAMLREQUESTID" \
--cookie "MSISAuth=$MSISAuth" --include
```

Les en-têtes de réponse contiennent des informations sur la session AD FS pour une utilisation de déconnexion ultérieure et le corps de réponse contient SAMLResponse dans un champ de formulaire masqué.

```
HTTP/1.1 200 OK
Cache-Control: no-cache,no-store
Pragma: no-cache
Content-Length: 5665
Content-Type: text/html; charset=utf-8
Expires: -1
Server: Microsoft-HTTPAPI/2.0
P3P: ADFS doesn't have P3P policy, please contact your site's admin
for more details
Set-Cookie:
SamlSession=a3dpbnRlcnMtUHJpbWFyeS1BZG1pbi0xNzgmRmFsc2Umcng4NnJDZmFKV
XFxVWx3bkl1MnFuUSUzZCUzZCYmJiYmXzE3MjAyZTA5LThmMDgtNDRkZC04Yzg5LTQ3ND
UxYzA3ZjkzYw==; path=/adfs; HttpOnly; Secure
Set-Cookie: MSISAuthenticated=MTEvNy8yMDE4IDQ6MzI6NTkgUE0=;
path=/adfs; HttpOnly; Secure
Set-Cookie: MSISLoopDetectionCookie=MjAxOC0xMS0wNzoxNjozMjo1OVpcMQ==;
path=/adfs; HttpOnly; Secure
Date: Wed, 07 Nov 2018 16:32:59 GMT

<form method="POST" name="hiddenform"
action="https://storagegrid.example.com:443/api/saml-response">
  <input type="hidden" name="SAMLResponse"
value="PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4=" /><input
type="hidden" name="RelayState" value="12345" />
```

i. Enregistrez le `SAMLResponse` dans le champ masqué :

```
export SAMLResponse='PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4='
```

j. À l'aide de la sauvegarde `SAMLResponse`, Faire un StorageGRID`/api/saml-response` Demande de génération d'un jeton d'authentification StorageGRID.

Pour `RelayState`, Utilisez l'ID du compte locataire ou 0 si vous souhaitez vous connecter à l'API Grid Management.

```
curl -X POST "https://$STORAGEGRID_ADDRESS:443/api/saml-response" \
  -H "accept: application/json" \
  --data-urlencode "SAMLResponse=$SAMLResponse" \
  --data-urlencode "RelayState=$TENANTACCOUNTID" \
  | python -m json.tool
```

La réponse inclut le jeton d'authentification.

```
{
    "apiVersion": "3.0",
    "data": "56eb07bf-21f6-40b7-af0b-5c6cacfb25e7",
    "responseTime": "2018-11-07T21:32:53.486Z",
    "status": "success"
}
```

a. Enregistrez le jeton d'authentification dans la réponse sous `MYTOKEN`.

```
export MYTOKEN="56eb07bf-21f6-40b7-af0b-5c6cacfb25e7"
```

Vous pouvez maintenant utiliser `MYTOKEN` Pour les autres demandes, comme le ferait l'utilisation de l'API si SSO n'était pas utilisé.

Déconnectez-vous de l'API si l'authentification unique est activée

Si l'authentification unique (SSO) a été activée, vous devez émettre une série de requêtes API pour vous déconnecter de l'API de gestion Grid ou de l'API de gestion des locataires. Ces instructions s'appliquent si vous utilisez Active Directory comme fournisseur d'identité SSO

Description de la tâche

Si nécessaire, vous pouvez vous déconnecter de l'API StorageGRID en vous déconnectant de la page de déconnexion unique de votre organisation. Vous pouvez également déclencher une déconnexion unique (SLO) à partir de StorageGRID, ce qui nécessite un jeton de porteur StorageGRID valide.

Étapes

1. Pour générer une demande de déconnexion signée, passez `cookie "sso=true"` Pour l'API SLO :

```
curl -k -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--cookie "sso=true" \
| python -m json.tool
```

Une URL de déconnexion est renvoyée :

```
{
    "apiVersion": "3.0",
    "data":
"https://adfs.example.com/adfs/ls/?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3
D",
    "responseTime": "2018-11-20T22:20:30.839Z",
    "status": "success"
}
```

2. Enregistrez l'URL de déconnexion.

```
export LOGOUT_REQUEST
='https://adfs.example.com/adfs/ls/?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%
3D'
```

3. Envoyez une demande à l'URL de déconnexion pour déclencher SLO et rerediriger vers StorageGRID.

```
curl --include "$LOGOUT_REQUEST"
```

La réponse 302 est renvoyée. L'emplacement de redirection ne s'applique pas à la déconnexion API uniquement.

```
HTTP/1.1 302 Found
Location: https://$STORAGEGRID_ADDRESS:443/api/saml-
logout?SAMLResponse=fVLLasMwEPwVo7ss%...%23rsa-sha256
Set-Cookie: MSISSignoutProtocol=U2FtbA==; expires=Tue, 20 Nov 2018
22:35:03 GMT; path=/adfs; HttpOnly; Secure
```

4. Supprimez le jeton de support StorageGRID.

La suppression du jeton de support StorageGRID fonctionne de la même manière que sans SSO. Si `cookie "sso=true"` Non fourni, l'utilisateur est déconnecté de StorageGRID sans affecter l'état SSO.

```
curl -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--include
```

A `204 No Content` reponse indique que l'utilisateur est déconnecté.

```
HTTP/1.1 204 No Content
```

Utiliser l'API si l'authentification unique est activée (Azure)

Si vous l'avez "Authentification unique (SSO) configurée et activée" Vous pouvez également utiliser Azure en tant que fournisseur SSO pour obtenir un jeton d'authentification valide pour l'API de gestion du grid ou l'API de gestion des locataires.

Connectez-vous à l'API si l'authentification unique Azure est activée

Ces instructions s'appliquent si vous utilisez Azure comme fournisseur d'identité SSO

Avant de commencer

- Vous connaissez l'adresse e-mail SSO et le mot de passe d'un utilisateur fédéré appartenant à un groupe d'utilisateurs StorageGRID.
- Pour accéder à l'API de gestion des locataires, vous connaissez l'ID du compte locataire.

Description de la tâche

Pour obtenir un jeton d'authentification, vous pouvez utiliser les exemples de scripts suivants :

- Le `storagegrid-ssoauth-azure.py` Script Python
- Le `storagegrid-ssoauth-azure.js` Script Node.js

Les deux scripts se trouvent dans le répertoire des fichiers d'installation de StorageGRID (`./rpms` Pour Red Hat Enterprise Linux ou CentOS, `./debs` Pour Ubuntu ou Debian, et `./vsphere` Pour VMware).

Pour écrire votre propre intégration d'API avec Azure, consultez le `storagegrid-ssoauth-azure.py` script. Le script Python fait deux requêtes directement à StorageGRID (d'abord pour obtenir la SAMLRequest et plus tard pour obtenir le jeton d'autorisation), et appelle également le script Node.js pour interagir avec Azure afin d'effectuer les opérations SSO.

Les opérations SSO peuvent être exécutées à l'aide d'une série de requêtes d'API, mais cette opération n'est pas simple. Le module Puppeteer Node.js est utilisé pour gratter l'interface SSO Azure.

Si vous avez un problème de codage d'URL, l'erreur peut s'afficher : `Unsupported SAML version`.

Étapes

1. Installez les dépendances requises comme suit :
   a. Installez Node.js (voir "https://nodejs.org/en/download/").
   b. Installez les modules Node.js requis (maripeteer et jsdom) :

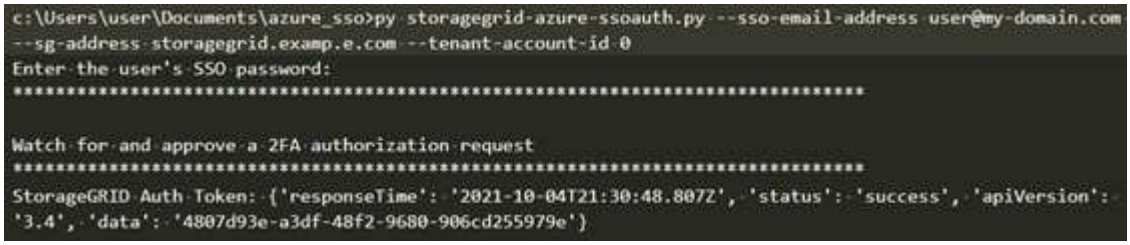
      ```
      npm install -g <module>
      ```

2. Passez le script Python à l'interpréteur Python pour exécuter le script.

   Le script Python appelle ensuite le script Node.js correspondant pour exécuter les interactions SSO Azure.

3. Lorsque vous y êtes invité, entrez des valeurs pour les arguments suivants (ou transmettez-les à l'aide de paramètres) :
   - Adresse e-mail SSO utilisée pour se connecter à Azure
   - L'adresse de StorageGRID
   - L'ID du compte de locataire, pour accéder à l'API de gestion des locataires

4. Lorsque vous y êtes invité, saisissez le mot de passe et préparez-vous à fournir une autorisation MFA à Azure si nécessaire.



> Le script suppose que l'authentification multifacteur est effectuée à l'aide de l'authentificateur Microsoft. Vous devrez peut-être modifier le script pour prendre en charge d'autres formes de MFA (comme la saisie d'un code reçu dans un message texte).

Le jeton d'autorisation StorageGRID est fourni dans la sortie. Vous pouvez maintenant utiliser le token pour d'autres requêtes, de la même manière que vous utilisiez l'API si SSO n'était pas utilisé.

Utilisez l'API si l'authentification unique est activée (PingFederate)

Si vous l'avez "Authentification unique (SSO) configurée et activée" De plus, vous utilisez PingFederate comme fournisseur SSO, vous devez émettre une série de requêtes API pour obtenir un jeton d'authentification valide pour l'API Grid Management ou l'API tenant Management.

Connectez-vous à l'API si l'authentification unique est activée

Ces instructions s'appliquent si vous utilisez PingFederate comme fournisseur d'identité SSO

Avant de commencer

- Vous connaissez le nom d'utilisateur et le mot de passe SSO d'un utilisateur fédéré appartenant à un groupe d'utilisateurs StorageGRID.
- Pour accéder à l'API de gestion des locataires, vous connaissez l'ID du compte locataire.

Description de la tâche

Pour obtenir un jeton d'authentification, vous pouvez utiliser l'un des exemples suivants :

- Le `storagegrid-ssoauth.py` Script Python, situé dans le répertoire des fichiers d'installation de StorageGRID (`./rpms` Pour Red Hat Enterprise Linux ou CentOS, `./debs` Pour Ubuntu ou Debian, et `./vsphere` Pour VMware).
- Un exemple de flux de travail des requêtes Curl.

  Le flux de travail de boucle risque de s'échapper si vous l'effectuez trop lentement. L'erreur peut s'afficher : `A valid SubjectConfirmation was not found on this Response`.

  > L'exemple de flux de travail Curl ne protège pas le mot de passe d'être vu par d'autres utilisateurs.

  Si vous avez un problème de codage d'URL, l'erreur peut s'afficher : `Unsupported SAML version`.

Étapes

1. Sélectionnez l'une des méthodes suivantes pour obtenir un jeton d'authentification :
   - Utilisez le `storagegrid-ssoauth.py` Script Python. Passez à l'étape 2.
   - Utiliser les demandes de gondoles. Passez à l'étape 3.
2. Si vous souhaitez utiliser le `storagegrid-ssoauth.py` Passez le script à l'interpréteur Python et exécutez le script.

   Lorsque vous y êtes invité, entrez des valeurs pour les arguments suivants :

   - Méthode SSO. Vous pouvez entrer n'importe quelle variation de ""pingdéin"" (PINGFEDERATE, pingfédéré, etc.).
   - Le nom d'utilisateur SSO
   - Domaine dans lequel StorageGRID est installé. Ce champ n'est pas utilisé pour PingFederate. Vous pouvez le laisser vide ou entrer n'importe quelle valeur.
   - L'adresse de StorageGRID
   - L'ID du compte de locataire, pour accéder à l'API de gestion des locataires.

   ```
   python3 storagegrid-ssoauth.py
   sso_method: pingfederate
   saml_user: my-sso-username
   saml_domain:
   sg_address: storagegrid.example.com
   tenant_account_id: 12345
   Enter the user's SAML password:
   ********************************************************************************

   ********************************************************************************
   StorageGRID Auth Token: 56eb07bf-21f6-40b7-afob-5c6cacfb25e7
   ```

   Le jeton d'autorisation StorageGRID est fourni dans la sortie. Vous pouvez maintenant utiliser le token pour d'autres requêtes, de la même manière que vous utilisiez l'API si SSO n'était pas utilisé.

3. Si vous souhaitez utiliser des requêtes Curl, suivez la procédure ci-dessous.

   a. Déclarez les variables nécessaires pour la connexion.

   ```
   export SAMLUSER='my-sso-username'
   export SAMLPASSWORD='my-password'
   export TENANTACCOUNTID='12345'
   export STORAGEGRID_ADDRESS='storagegrid.example.com'
   ```

   > ⓘ Pour accéder à l'API de gestion de grille, utilisez 0 comme `TENANTACCOUNTID`.

   b. Pour recevoir une URL d'authentification signée, lancez une demande POST à `/api/v3/authorize-saml`, Et supprimez le codage JSON supplémentaire de la réponse.

   Cet exemple montre une demande POST pour une URL d'authentification signée pour TENANTACCOUNTID. Les résultats seront transmis à python -m json.tool pour supprimer l'encodage

JSON.

```
curl -X POST "https://$STORAGEGRID_ADDRESS/api/v3/authorize-saml" \
  -H "accept: application/json" -H  "Content-Type: application/json"
\
  --data "{\"accountId\": \"$TENANTACCOUNTID\"}" | python -m
json.tool
```

La réponse dans cet exemple inclut une URL signée codée par URL, mais n'inclut pas la couche supplémentaire de codage JSON.

```
{
    "apiVersion": "3.0",
    "data": "https://my-pf-baseurl/idp/SSO.saml2?...",
    "responseTime": "2018-11-06T16:30:23.355Z",
    "status": "success"
}
```

c. Enregistrez le `SAMLRequest` à partir de la réponse pour une utilisation dans les commandes suivantes.

```
export SAMLREQUEST="https://my-pf-baseurl/idp/SSO.saml2?..."
```

d. Exportez la réponse et le cookie, et écho la réponse :

```
RESPONSE=$(curl -c - "$SAMLREQUEST")
```

```
echo "$RESPONSE" | grep 'input type="hidden" name="pf.adapterId"
id="pf.adapterId"'
```

e. Exporter la valeur 'pf.adapterId' et réafficher la réponse :

```
export ADAPTER='myAdapter'
```

```
echo "$RESPONSE" | grep 'base'
```

f. Exporter la valeur « href » (supprimer la barre oblique inverse /) et afficher en écho la réponse :

```
export BASEURL='https://my-pf-baseurl'
```

```
echo "$RESPONSE" | grep 'form method="POST"'
```

g. Exporter la valeur « action » :

```
export SSOPING='/idp/.../resumeSAML20/idp/SSO.ping'
```

h. Envoyer des cookies avec des informations d'identification :

```
curl -b <(echo "$RESPONSE") -X POST "$BASEURL$SSOPING" \
--data "pf.username=$SAMLUSER&pf.pass=
$SAMLPASSWORD&pf.ok=clicked&pf.cancel=&pf.adapterId=$ADAPTER"
--include
```

i. Enregistrez le `SAMLResponse` dans le champ masqué :

```
export SAMLResponse='PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4='
```

j. À l'aide de la sauvegarde `SAMLResponse`, Faire un StorageGRID`/api/saml-response` Demande de génération d'un jeton d'authentification StorageGRID.

Pour `RelayState`, Utilisez l'ID du compte locataire ou 0 si vous souhaitez vous connecter à l'API Grid Management.

```
curl -X POST "https://$STORAGEGRID_ADDRESS:443/api/saml-response" \
  -H "accept: application/json" \
  --data-urlencode "SAMLResponse=$SAMLResponse" \
  --data-urlencode "RelayState=$TENANTACCOUNTID" \
  | python -m json.tool
```

La réponse inclut le jeton d'authentification.

```
{
    "apiVersion": "3.0",
    "data": "56eb07bf-21f6-40b7-af0b-5c6cacfb25e7",
    "responseTime": "2018-11-07T21:32:53.486Z",
    "status": "success"
}
```

a. Enregistrez le jeton d'authentification dans la réponse sous `MYTOKEN`.

```
export MYTOKEN="56eb07bf-21f6-40b7-af0b-5c6cacfb25e7"
```

Vous pouvez maintenant utiliser `MYTOKEN` Pour les autres demandes, comme le ferait l'utilisation de l'API si SSO n'était pas utilisé.

Déconnectez-vous de l'API si l'authentification unique est activée

Si l'authentification unique (SSO) a été activée, vous devez émettre une série de requêtes API pour vous déconnecter de l'API de gestion Grid ou de l'API de gestion des locataires. Ces instructions s'appliquent si vous utilisez PingFederate comme fournisseur d'identité SSO

Description de la tâche

Si nécessaire, vous pouvez vous déconnecter de l'API StorageGRID en vous déconnectant de la page de déconnexion unique de votre organisation. Vous pouvez également déclencher une déconnexion unique (SLO) à partir de StorageGRID, ce qui nécessite un jeton de porteur StorageGRID valide.

Étapes

1. Pour générer une demande de déconnexion signée, passez `cookie "sso=true"` Pour l'API SLO :

```
curl -k -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--cookie "sso=true" \
| python -m json.tool
```

Une URL de déconnexion est renvoyée :

```
{
    "apiVersion": "3.0",
    "data": "https://my-ping-
url/idp/SLO.saml2?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3D",
    "responseTime": "2021-10-12T22:20:30.839Z",
    "status": "success"
}
```

2. Enregistrez l'URL de déconnexion.

```
export LOGOUT_REQUEST='https://my-ping-
url/idp/SLO.saml2?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3D'
```

3. Envoyez une demande à l'URL de déconnexion pour déclencher SLO et rerediriger vers StorageGRID.

```
curl --include "$LOGOUT_REQUEST"
```

La réponse 302 est renvoyée. L'emplacement de redirection ne s'applique pas à la déconnexion API uniquement.

```
HTTP/1.1 302 Found
Location: https://$STORAGEGRID_ADDRESS:443/api/saml-
logout?SAMLResponse=fVLLasMwEPwVo7ss%...%23rsa-sha256
Set-Cookie: PF=QoKs...SgCC; Path=/; Secure; HttpOnly; SameSite=None
```

4. Supprimez le jeton de support StorageGRID.

   La suppression du jeton de support StorageGRID fonctionne de la même manière que sans SSO. Si `cookie "sso=true"` Non fourni, l'utilisateur est déconnecté de StorageGRID sans affecter l'état SSO.

```
curl -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--include
```

   A `204 No Content` reponse indique que l'utilisateur est déconnecté.

```
HTTP/1.1 204 No Content
```

Désactivez les fonctions à l'aide de l'API

Vous pouvez utiliser l'API de gestion de grille pour désactiver complètement certaines fonctions du système StorageGRID. Lorsqu'une fonction est désactivée, aucune autorisation ne peut être attribuée pour effectuer les tâches associées à cette fonctionnalité.

Description de la tâche

Le système de fonctions désactivées vous permet d'empêcher l'accès à certaines fonctions du système StorageGRID. La désactivation d'une fonctionnalité est le seul moyen d'empêcher l'utilisateur racine ou les utilisateurs appartenant à des groupes d'administration disposant de l'autorisation **accès racine** d'utiliser cette fonctionnalité.

Pour comprendre l'utilité de cette fonctionnalité, prenez en compte le scénario suivant :

La Société A est un fournisseur de services qui loue la capacité de stockage de son système StorageGRID en créant des comptes de tenant. Pour protéger la sécurité des objets de leurs détenteurs de bail, la Société A veut s'assurer que ses employés ne peuvent jamais accéder à un compte de locataire après le déploiement du compte.

Société A peut atteindre cet objectif en utilisant le système Désactiver les fonctions dans l'API de gestion de

*grille. En désactivant complètement la fonction **Modifier le mot de passe racine du locataire** dans le gestionnaire de grille (à la fois l'interface utilisateur et l'API), la société A peut s'assurer qu'aucun utilisateur Admin, y compris l'utilisateur racine et les utilisateurs appartenant à des groupes avec l'autorisation **accès racine**, ne peut modifier le mot de passe de l'utilisateur racine d'un compte locataire.*

Étapes

1. Accédez à la documentation de swagger pour l'API Grid Management. Voir "Utilisez l'API de gestion du grid".
2. Localisez le point d'extrémité Désactiver les fonctions.
3. Pour désactiver une fonction, par exemple changer le mot de passe racine du locataire, envoyez un corps à l'API comme suit :

   ```
   { "grid": {"changeTenantRootPassword": true} }
   ```

   Une fois la demande terminée, la fonction de modification du mot de passe racine du locataire est désactivée. L'autorisation de gestion **Modifier le mot de passe racine du locataire** n'apparaît plus dans l'interface utilisateur et toute demande d'API qui tente de modifier le mot de passe racine d'un locataire échouera avec ""403 interdit".

Réactiver les fonctions désactivées

Par défaut, vous pouvez utiliser l'API Grid Management pour réactiver une fonction qui a été désactivée. Toutefois, si vous souhaitez empêcher la réactivation des fonctions désactivées, vous pouvez désactiver la fonction **activeFeatures** elle-même.

> La fonction **activateFeatures** ne peut pas être réactivée. Si vous décidez de désactiver cette fonction, sachez que vous perdrez définitivement la capacité de réactiver les autres fonctions désactivées. Vous devez contacter le support technique pour restaurer toute fonctionnalité perdue.

Étapes

1. Accédez à la documentation de swagger pour l'API Grid Management.
2. Localisez le point d'extrémité Désactiver les fonctions.
3. Pour réactiver toutes les fonctions, envoyez un corps à l'API comme suit :

   ```
   { "grid": null }
   ```

   Lorsque cette demande est terminée, toutes les fonctions, y compris la fonction Modifier le mot de passe racine du locataire, sont réactivées. L'autorisation de gestion **Modifier le mot de passe racine** du locataire apparaît maintenant dans l'interface utilisateur et toute demande d'API qui tente de modifier le mot de passe racine d'un locataire va réussir, en supposant que l'utilisateur dispose de l'autorisation de gestion **accès racine** ou **changer le mot de passe racine du locataire**.

> L'exemple précédent provoque la réactivation des fonctions *All* DESACTIVE. Si d'autres fonctions doivent rester désactivées, vous devez les spécifier explicitement dans la demande PUT. Par exemple, pour réactiver la fonction Modifier le mot de passe racine du locataire et continuer à désactiver la fonction d'acquittement d'alarme, envoyez cette demande PUT :
>
> ```
> { "grid": { "alarmAcknowledgment": true } }
> ```

Contrôle de l'accès à StorageGRID

Contrôle de l'accès à StorageGRID : présentation

Vous pouvez contrôler qui peut accéder à StorageGRID et quelles tâches les utilisateurs peuvent effectuer en créant ou en important des groupes et des utilisateurs et en attribuant des autorisations à chaque groupe. Vous pouvez également activer l'authentification unique (SSO), créer des certificats client et modifier les mots de passe de la grille.

Contrôle de l'accès au Grid Manager

Vous déterminez qui peut accéder à Grid Manager et à l'API Grid Management en important des groupes et des utilisateurs à partir d'un service de fédération des identités ou en configurant des groupes locaux et des utilisateurs locaux.

À l'aide de "fédération des identités" effectue la configuration "groupes" et "utilisateurs" Plus rapide, elle permet aux utilisateurs de se connecter à StorageGRID à l'aide d'informations d'identification connues. Vous pouvez configurer la fédération des identités si vous utilisez Active Directory, OpenLDAP ou Oracle Directory Server.

> Contactez le support technique si vous souhaitez utiliser un autre service LDAP v3.

Vous déterminez les tâches que chaque utilisateur peut effectuer en affectant différentes "autorisations" à chaque groupe. Par exemple, il peut être nécessaire que les utilisateurs d'un groupe puissent gérer les règles ILM et les utilisateurs d'un autre groupe pour effectuer les tâches de maintenance. Un utilisateur doit appartenir à au moins un groupe pour accéder au système.

Vous pouvez également configurer un groupe pour qu'il soit en lecture seule. Les utilisateurs d'un groupe en lecture seule peuvent uniquement afficher les paramètres et les fonctions. Ils ne peuvent pas apporter de modifications ni effectuer d'opérations dans l'API Grid Manager ou Grid Management.

Activez l'authentification unique

Le système StorageGRID prend en charge la fonctionnalité SSO (Single Sign-on) en utilisant la 2.0 norme SAML 2.0 (Security assertion Markup Language). Après vous "Configurer et activer SSO", Tous les utilisateurs doivent être authentifiés par un fournisseur d'identité externe avant de pouvoir accéder au Gestionnaire de grille, au Gestionnaire de locataires, à l'API de gestion de grille ou à l'API de gestion des locataires. Les utilisateurs locaux ne peuvent pas se connecter à StorageGRID.

Modifiez la phrase secrète du provisionnement

La phrase de passe de provisionnement est requise pour de nombreuses procédures d'installation et de maintenance, ainsi que pour le téléchargement du package de restauration StorageGRID. Une phrase secrète est également nécessaire pour télécharger les sauvegardes des informations de topologie de la grille et des clés de chiffrement pour le système StorageGRID. C'est possible "modifiez la phrase de passe" selon les besoins.

Changer les mots de passe de la console du nœud

Chaque nœud de votre grid dispose d'un mot de passe unique de console de nœud. Vous devez vous connecter au nœud en tant qu'administrateur via SSH ou à l'utilisateur root sur une connexion VM/console physique. Si nécessaire, c'est possible "modifiez le mot de passe de la console du nœud" pour chaque nœud.

Modifiez la phrase secrète de provisionnement

Utilisez cette procédure pour modifier la phrase secrète du provisionnement StorageGRID. La phrase de passe est requise pour les procédures de restauration, d'extension et de maintenance. La phrase de passe est également requise pour télécharger les sauvegardes du pack de récupération qui incluent les informations de topologie de la grille, les mots de passe de la console des nœuds grid et les clés de chiffrement pour le système StorageGRID.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous disposez d'autorisations d'accès à la racine ou à la maintenance.
- Vous disposez de la phrase secrète pour le provisionnement.

Description de la tâche

La phrase secrète de provisionnement est requise pour la plupart des procédures d'installation et de maintenance, et pour "Téléchargement du progiciel de restauration". La phrase de passe de provisionnement n'est pas répertoriée dans le `Passwords.txt` fichier. Veillez à documenter la phrase de passe de provisionnement et à la conserver dans un emplacement sûr et sécurisé.

Étapes

1. Sélectionnez **CONFIGURATION** > **contrôle d'accès**> **mots de passe de grille**.
2. Sous **Modifier la phrase de passe de provisionnement**, sélectionnez **faire une modification**
3. Saisissez votre phrase secrète pour le provisionnement.
4. Saisissez la nouvelle phrase de passe. La phrase de passe doit contenir au moins 8 caractères et pas plus de 32 caractères. Les phrases passe sont sensibles à la casse.
5. Stocker la nouvelle phrase secrète pour le provisionnement dans un emplacement sécurisé Elle est requise pour les procédures d'installation, d'extension et de maintenance.
6. Saisissez à nouveau la nouvelle phrase de passe et sélectionnez **Enregistrer**.

   Le système affiche une bannière verte de réussite lorsque la modification de la phrase de passe de provisionnement est terminée.

7. Sélectionnez **progiciel de récupération**.
8. Entrez la nouvelle phrase de passe de provisionnement pour télécharger le nouveau progiciel de restauration.

> Après avoir modifié la phrase de passe de provisionnement, vous devez télécharger immédiatement un nouveau progiciel de restauration. Le fichier du progiciel de récupération vous permet de restaurer le système en cas de défaillance.

Changer les mots de passe de la console du nœud

Chaque nœud de votre grid dispose d'un mot de passe de console de nœud unique que vous devez vous connecter au nœud. Procédez comme suit pour modifier chaque mot de

passe de console de nœud unique pour chaque nœud de votre grille.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous disposez de l'autorisation Maintenance ou accès racine.
- Vous disposez de la phrase secrète pour le provisionnement.

Description de la tâche

Utilisez le mot de passe de la console du nœud pour vous connecter à un nœud en tant qu'administrateur via SSH ou à l'utilisateur root sur une connexion de console physique/machine virtuelle. Le processus de modification du mot de passe de la console de nœud crée de nouveaux mots de passe pour chaque nœud de votre grille et stocke les mots de passe dans une mise à jour `Passwords.txt` fichier dans le package de restauration. Les mots de passe sont répertoriés dans la colonne Mot de passe du fichier Passwords.txt.

Il existe des mots de passe d'accès SSH distincts pour les clés SSH utilisées pour la communication entre les nœuds. Les mots de passe d'accès SSH ne sont pas modifiés par cette procédure.

Accéder à l'assistant

Étapes

1. Sélectionnez **CONFIGURATION** > **contrôle d'accès** > **mots de passe de grille**.
2. Sous **Modifier les mots de passe de la console de nœuds**, sélectionnez **faire une modification**.

Saisissez la phrase secrète pour le provisionnement

Étapes

1. Saisissez la phrase de passe de provisionnement pour votre grid.
2. Sélectionnez **Continuer**.

Téléchargez le package de récupération actuel

Avant de modifier les mots de passe de la console de nœuds, téléchargez le pack de restauration actuel. Vous pouvez utiliser les mots de passe de ce fichier si le processus de modification du mot de passe échoue pour un noeud quelconque.

Étapes

1. Sélectionnez **Télécharger le paquet de récupération**.
2. Copiez le fichier du package de récupération (`.zip`) à deux emplacements sûrs, sécurisés et séparés.

Le fichier de package de récupération doit être sécurisé car il contient des clés de cryptage et des mots de passe qui peuvent être utilisés pour obtenir des données du système StorageGRID.

3. Sélectionnez **Continuer**.
4. Lorsque la boîte de dialogue de confirmation apparaît, sélectionnez **Oui** si vous êtes prêt à modifier les mots de passe de la console du nœud.

   Vous ne pouvez pas annuler ce processus après son démarrage.

Changer les mots de passe de la console du nœud

Lorsque le processus de mot de passe de la console du nœud démarre, un nouveau package de restauration est généré qui inclut les nouveaux mots de passe. Les mots de passe sont ensuite mis à jour sur chaque nœud.

Étapes

1. Attendez que le nouveau package de restauration soit généré, ce qui peut prendre quelques minutes.
2. Sélectionnez **Télécharger nouveau paquet de récupération**.
3. Une fois le téléchargement terminé :

   a. Ouvrez le `.zip` fichier.

   b. Vérifiez que vous pouvez accéder au contenu, y compris au `Passwords.txt` qui contient les nouveaux mots de passe de la console du nœud.

   c. Copiez le nouveau fichier de package de récupération (`.zip`) à deux emplacements sûrs, sécurisés et séparés.

   > Ne remplacez pas l'ancien package de récupération.

   Le fichier de package de récupération doit être sécurisé car il contient des clés de cryptage et des mots de passe qui peuvent être utilisés pour obtenir des données du système StorageGRID.

4. Cochez la case pour indiquer que vous avez téléchargé le nouveau package de récupération et vérifié le contenu.
5. Sélectionnez **Modifier les mots de passe de la console de nœuds** et attendez que tous les nœuds soient mis à jour avec les nouveaux mots de passe. Cette opération peut prendre quelques minutes.

   Si les mots de passe sont modifiés pour tous les nœuds, une bannière de réussite verte s'affiche. Passez à l'étape suivante.

   En cas d'erreur lors du processus de mise à jour, un message de bannière indique le nombre de nœuds dont les mots de passe n'ont pas été modifiés. Le système réexécute automatiquement le processus sur tout nœud dont le mot de passe n'a pas été modifié. Si le processus se termine avec certains nœuds qui n'ont toujours pas de mot de passe modifié, le bouton **Réessayer** s'affiche.

   Si la mise à jour du mot de passe a échoué pour un ou plusieurs nœuds :

   a. Vérifiez les messages d'erreur répertoriés dans le tableau.

   b. Résolvez les problèmes.

   c. Sélectionnez **Réessayer**.

   > La tentative de nouveau modifie uniquement les mots de passe de la console de nœud sur les nœuds qui ont échoué lors des précédentes tentatives de changement de mot de passe.

6. Une fois que les mots de passe de la console du nœud ont été modifiés pour tous les nœuds, supprimez le premier paquet de récupération que vous avez téléchargé.
7. Vous pouvez également utiliser le lien **Recovery package** pour télécharger une copie supplémentaire du nouveau package de récupération.

Utiliser la fédération des identités

L'utilisation de la fédération des identités accélère la configuration des groupes et des utilisateurs et permet aux utilisateurs de se connecter à StorageGRID à l'aide des informations d'identification familières.

Configurer la fédération des identités pour Grid Manager

Vous pouvez configurer la fédération des identités dans Grid Manager si vous souhaitez que les groupes et les utilisateurs d'administration soient gérés dans un autre système, tel qu'Active Directory, Azure Active Directory (Azure AD), OpenLDAP ou Oracle Directory Server.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous disposez d'autorisations d'accès spécifiques.
- Vous utilisez Active Directory, Azure AD, OpenLDAP ou Oracle Directory Server comme fournisseur d'identité.

> Si vous souhaitez utiliser un service LDAP v3 non répertorié, contactez le support technique.

- Si vous avez l'intention d'utiliser OpenLDAP, vous devez configurer le serveur OpenLDAP. Voir Instructions de configuration d'un serveur OpenLDAP.
- Si vous avez l'intention d'activer l'authentification unique (SSO), vous avez examiné le "configuration requise et considérations pour l'authentification unique".
- Si vous prévoyez d'utiliser TLS (transport Layer Security) pour les communications avec le serveur LDAP, le fournisseur d'identités utilise TLS 1.2 ou 1.3. Voir "Chiffrement pris en charge pour les connexions TLS sortantes".

Description de la tâche

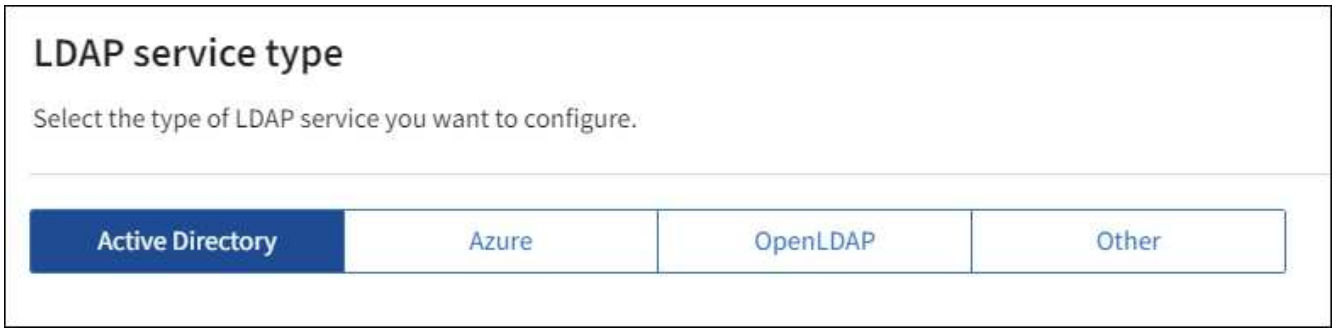
Vous pouvez configurer un référentiel d'identité pour Grid Manager si vous souhaitez importer des groupes à partir d'un autre système, tel qu'Active Directory, Azure AD, OpenLDAP ou Oracle Directory Server. Vous pouvez importer les types de groupes suivants :

- Groupes d'administration. Les utilisateurs des groupes admin peuvent se connecter au gestionnaire de grille et effectuer des tâches en fonction des autorisations de gestion attribuées au groupe.
- Groupes d'utilisateurs locataires pour les locataires qui n'utilisent pas leur propre référentiel d'identité. Les utilisateurs des groupes de locataires peuvent se connecter au Gestionnaire de locataires et effectuer des tâches en fonction des autorisations attribuées au groupe dans le Gestionnaire de locataires. Voir "Créer un compte de locataire" et "Utilisez un compte de locataire" pour plus d'informations.

Entrez la configuration

Étapes

1. Sélectionnez **CONFIGURATION** > **contrôle d'accès** > **fédération d'identités**.
2. Sélectionnez **Activer la fédération d'identités**.
3. Dans la section Type de service LDAP, sélectionnez le type de service LDAP que vous souhaitez configurer.



Sélectionnez **autre** pour configurer les valeurs d'un serveur LDAP qui utilise Oracle Directory Server.

4. Si vous avez sélectionné **autre**, renseignez les champs de la section attributs LDAP. Dans le cas contraire, passez à l'étape suivante.
   - **Nom unique utilisateur** : nom de l'attribut qui contient l'identifiant unique d'un utilisateur LDAP. Cet attribut est équivalent à `sAMAccountName` Pour Active Directory et `uid` Pour OpenLDAP. Si vous configurez Oracle Directory Server, entrez `uid`.
   - **UUID d'utilisateur** : nom de l'attribut qui contient l'identifiant unique permanent d'un utilisateur LDAP. Cet attribut est équivalent à `objectGUID` Pour Active Directory et `entryUUID` Pour OpenLDAP. Si vous configurez Oracle Directory Server, entrez `nsuniqueid`. La valeur de chaque utilisateur pour l'attribut spécifié doit être un nombre hexadécimal à 32 chiffres au format 16 octets ou chaîne, où les tirets sont ignorés.
   - **Nom unique de groupe** : nom de l'attribut qui contient l'identifiant unique d'un groupe LDAP. Cet attribut est équivalent à `sAMAccountName` Pour Active Directory et `cn` Pour OpenLDAP. Si vous configurez Oracle Directory Server, entrez `cn`.
   - **UUID de groupe** : nom de l'attribut qui contient l'identificateur unique permanent d'un groupe LDAP. Cet attribut est équivalent à `objectGUID` Pour Active Directory et `entryUUID` Pour OpenLDAP. Si vous configurez Oracle Directory Server, entrez `nsuniqueid`. La valeur de chaque groupe pour l'attribut spécifié doit être un nombre hexadécimal à 32 chiffres au format 16 octets ou chaîne, où les tirets sont ignorés.
5. Pour tous les types de services LDAP, entrez les informations de connexion réseau et de serveur LDAP requises dans la section configurer le serveur LDAP.
   - **Nom d'hôte** : le nom de domaine complet (FQDN) ou l'adresse IP du serveur LDAP.
   - **Port** : port utilisé pour se connecter au serveur LDAP.

     Le port par défaut de STARTTLS est 389 et le port par défaut de LDAPS est 636. Cependant, vous pouvez utiliser n'importe quel port tant que votre pare-feu est configuré correctement.

   - **Nom d'utilisateur** : chemin complet du nom distinctif (DN) de l'utilisateur qui se connectera au serveur LDAP.

     Pour Active Directory, vous pouvez également spécifier le nom de connexion bas niveau ou le nom principal d'utilisateur.

     L'utilisateur spécifié doit être autorisé à répertorier les groupes et les utilisateurs et à accéder aux attributs suivants :

     - `sAMAccountName` ou `uid`

- `objectGUID`, `entryUUID`, ou `nsuniqueid`
- `cn`
- `memberOf` ou `isMemberOf`
- **Active Directory** : `objectSid`, `primaryGroupID`, `userAccountControl`, et `userPrincipalName`
- **Azure**: `accountEnabled` et `userPrincipalName`

◦ **Mot de passe** : mot de passe associé au nom d'utilisateur.

◦ **DN de base de groupe** : chemin complet du nom distinctif (DN) pour une sous-arborescence LDAP que vous voulez rechercher des groupes. Dans l'exemple Active Directory (ci-dessous), tous les groupes dont le nom unique est relatif au DN de base (DC=storagegrid,DC=exemple,DC=com) peuvent être utilisés comme groupes fédérés.

> Les valeurs **Nom unique de groupe** doivent être uniques dans le **DN de base de groupe** auquel elles appartiennent.

◦ **DN de base d'utilisateurs** : le chemin complet du nom distinctif (DN) d'une sous-arborescence LDAP que vous voulez rechercher des utilisateurs.

> Les valeurs **Nom unique utilisateur** doivent être uniques dans le **DN de base utilisateur** auquel elles appartiennent.

◦ **Bind username format** (facultatif) : le nom d'utilisateur par défaut StorageGRID devrait utiliser si le modèle ne peut pas être déterminé automatiquement.

Il est recommandé de fournir le format **Bind username** car il peut permettre aux utilisateurs de se connecter si StorageGRID ne parvient pas à se lier avec le compte de service.

Entrez l'un des motifs suivants :

- **Modèle UserPrincipalName (Active Directory et Azure)** : `[USERNAME]@*example*.com`
- **Modèle de nom de connexion bas niveau (Active Directory et Azure)** : `*example*\[USERNAME]`
- **Modèle de nom unique** : `CN=[USERNAME],CN=Users,DC=*example*,DC=com`

  Inclure **[NOM D'UTILISATEUR]** exactement comme écrit.

6. Dans la section transport Layer Security (TLS), sélectionnez un paramètre de sécurité.

◦ **Utilisez STARTTLS** : utilisez STARTTLS pour sécuriser les communications avec le serveur LDAP. Il s'agit de l'option recommandée pour Active Directory, OpenLDAP ou autre, mais cette option n'est pas prise en charge pour Azure.

◦ **Utilisez LDAPS** : l'option LDAPS (LDAP sur SSL) utilise TLS pour établir une connexion au serveur LDAP. Vous devez sélectionner cette option pour Azure.

◦ **N'utilisez pas TLS** : le trafic réseau entre le système StorageGRID et le serveur LDAP ne sera pas sécurisé. Cette option n'est pas prise en charge pour Azure.

> L'utilisation de l'option **ne pas utiliser TLS** n'est pas prise en charge si votre serveur Active Directory applique la signature LDAP. Vous devez utiliser STARTTLS ou LDAPS.

7. Si vous avez sélectionné STARTTLS ou LDAPS, choisissez le certificat utilisé pour sécuriser la connexion.
   - **Utilisez le certificat CA du système d'exploitation** : utilisez le certificat CA de la grille par défaut installé sur le système d'exploitation pour sécuriser les connexions.
   - **Utilisez un certificat d'autorité de certification personnalisé** : utilisez un certificat de sécurité personnalisé.

     Si vous sélectionnez ce paramètre, copiez et collez le certificat de sécurité personnalisé dans la zone de texte certificat de l'autorité de certification.

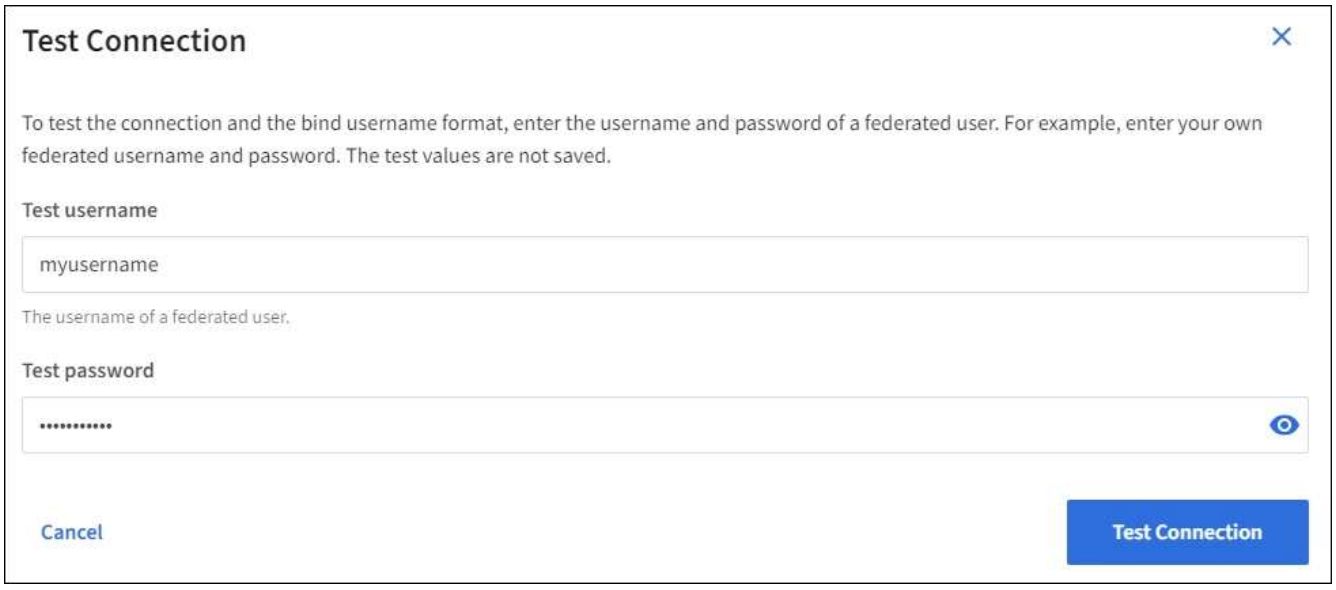
Testez la connexion et enregistrez la configuration

Après avoir saisi toutes les valeurs, vous devez tester la connexion avant de pouvoir enregistrer la configuration. StorageGRID vérifie les paramètres de connexion pour le serveur LDAP et le format de nom d'utilisateur BIND, si vous en avez fourni un.

Étapes

1. Sélectionnez **Tester la connexion**.
2. Si vous n'avez pas fourni de format de nom d'utilisateur de liaison :
   - Un message « Test connexion réussie » s'affiche si les paramètres de connexion sont valides. Sélectionnez **Enregistrer** pour enregistrer la configuration.
   - Un message « Impossible d'établir la connexion test » s'affiche si les paramètres de connexion ne sont pas valides. Sélectionnez **Fermer**. Ensuite, résolvez tout problème et testez à nouveau la connexion.
3. Si vous avez fourni un format de nom d'utilisateur BIND, entrez le nom d'utilisateur et le mot de passe d'un utilisateur fédéré valide.

   Par exemple, entrez votre nom d'utilisateur et votre mot de passe. N'incluez pas de caractères spéciaux dans le nom d'utilisateur, tels que @ ou /.



   - Un message « Test connexion réussie » s'affiche si les paramètres de connexion sont valides. Sélectionnez **Enregistrer** pour enregistrer la configuration.
   - Un message d'erreur s'affiche si les paramètres de connexion, le format du nom d'utilisateur de liaison ou le nom d'utilisateur et le mot de passe du test sont incorrects. Résolvez tout problème et testez à nouveau la connexion.

Forcer la synchronisation avec le référentiel d'identité

Le système StorageGRID synchronise régulièrement les groupes fédérés et les utilisateurs à partir du référentiel d'identité. Vous pouvez forcer la synchronisation à démarrer si vous souhaitez activer ou restreindre les autorisations utilisateur le plus rapidement possible.

Étapes

1. Accédez à la page fédération des identités.
2. Sélectionnez **serveur de synchronisation** en haut de la page.

   Le processus de synchronisation peut prendre un certain temps en fonction de votre environnement.

> L'alerte **échec de synchronisation de la fédération d'identités** est déclenchée en cas de problème de synchronisation des groupes fédérés et des utilisateurs à partir du référentiel d'identité.

Désactiver la fédération des identités

Vous pouvez désactiver temporairement ou définitivement la fédération des identités pour les groupes et les utilisateurs. Lorsque la fédération des identités est désactivée, il n'y a aucune communication entre StorageGRID et le référentiel d'identité. Cependant, tous les paramètres que vous avez configurés sont conservés, ce qui vous permet de réactiver facilement la fédération d'identités à l'avenir.

Description de la tâche

Avant de désactiver la fédération des identités, vous devez prendre connaissance des points suivants :

- Les utilisateurs fédérés ne pourront pas se connecter.
- Les utilisateurs fédérés qui sont actuellement connectés conservent l'accès au système StorageGRID jusqu'à l'expiration de leur session, mais ils ne pourront pas se connecter après l'expiration de leur session.
- La synchronisation entre le système StorageGRID et le référentiel d'identité ne se produira pas et des alertes ou des alarmes ne seront pas émises pour les comptes qui n'ont pas été synchronisés.
- La case **Activer la fédération d'identité** est désactivée si l'authentification unique (SSO) est définie sur **activé** ou **mode Sandbox**. Le statut SSO sur la page connexion unique doit être **désactivé** avant de pouvoir désactiver la fédération d'identités. Voir "Désactiver l'authentification unique".

Étapes

1. Accédez à la page fédération des identités.
2. Décochez la case **Activer la fédération d'identité**.

Instructions de configuration d'un serveur OpenLDAP

Si vous souhaitez utiliser un serveur OpenLDAP pour la fédération des identités, vous devez configurer des paramètres spécifiques sur le serveur OpenLDAP.

> Pour les référentiels d'identité qui ne sont pas ActiveDirectory ou Azure, StorageGRID ne bloquera pas automatiquement l'accès S3 aux utilisateurs désactivés en externe. Pour bloquer l'accès S3, supprimez les clés S3 de l'utilisateur ou supprimez l'utilisateur de tous les groupes.

Recouvrements de memberOf et de raffint

Les recouvrements de membre et de raffinage doivent être activés. Pour plus d'informations, reportez-vous aux instructions relatives à la maintenance de l'adhésion au groupe inverse dans lehttp://www.openldap.org/doc/admin24/index.html["Documentation OpenLDAP : version 2.4 - Guide de l'administrateur"^].

Indexation

Vous devez configurer les attributs OpenLDAP suivants avec les mots-clés d'index spécifiés :

- `olcDbIndex: objectClass eq`
- `olcDbIndex: uid eq,pres,sub`
- `olcDbIndex: cn eq,pres,sub`
- `olcDbIndex: entryUUID eq`

De plus, assurez-vous que les champs mentionnés dans l'aide pour le nom d'utilisateur sont indexés pour des performances optimales.

Reportez-vous aux informations relatives à la maintenance de l'adhésion au groupe inverse dans lehttp://www.openldap.org/doc/admin24/index.html["Documentation OpenLDAP : version 2.4 - Guide de l'administrateur"^].

Gérez les groupes d'administration

Vous pouvez créer des groupes d'administration pour gérer les autorisations de sécurité d'un ou plusieurs utilisateurs administrateurs. Les utilisateurs doivent appartenir à un groupe pour pouvoir accéder au système StorageGRID.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous disposez d'autorisations d'accès spécifiques.
- Si vous envisagez d'importer un groupe fédéré, vous avez configuré la fédération des identités et le groupe fédéré existe déjà dans le référentiel d'identité configuré.

Créer un groupe d'administration

Les groupes Admin vous permettent de déterminer quels utilisateurs peuvent accéder aux fonctions et opérations du gestionnaire de grille et de l'API Grid Management.

Accéder à l'assistant

Étapes

1. Sélectionnez **CONFIGURATION** > **contrôle d'accès** > **groupes Admin**.
2. Sélectionnez **Créer groupe**.

Choisissez un type de groupe

Vous pouvez créer un groupe local ou importer un groupe fédéré.

- Créez un groupe local si vous souhaitez attribuer des autorisations aux utilisateurs locaux.
- Créez un groupe fédéré pour importer des utilisateurs à partir du référentiel d'identité.

Groupe local

Étapes

1. Sélectionnez **Groupe local**.
2. Saisissez un nom d'affichage pour le groupe, que vous pourrez mettre à jour ultérieurement si nécessaire. Par exemple, « Maintenance Users » ou « ILM Administrators ».
3. Entrez un nom unique pour le groupe que vous ne pourrez pas mettre à jour ultérieurement.
4. Sélectionnez **Continuer**.

Groupe fédéré

Étapes

1. Sélectionnez **Groupe fédéré**.
2. Entrez le nom du groupe à importer, exactement tel qu'il apparaît dans le référentiel d'identité configuré.
   - Pour Active Directory et Azure, utilisez sAMAccountName.
   - Pour OpenLDAP, utilisez le CN (Common Name).
   - Pour un autre LDAP, utilisez le nom unique approprié pour le serveur LDAP.
3. Sélectionnez **Continuer**.

Gérer les autorisations de groupe

Étapes

1. Pour **mode d'accès**, sélectionnez si les utilisateurs du groupe peuvent modifier les paramètres et effectuer des opérations dans le gestionnaire de grille et l'API de gestion de grille ou s'ils ne peuvent afficher que les paramètres et les fonctionnalités.
   - **Lecture-écriture** (par défaut) : les utilisateurs peuvent modifier les paramètres et effectuer les opérations autorisées par leurs autorisations de gestion.
   - **Lecture seule** : les utilisateurs peuvent uniquement afficher les paramètres et les fonctionnalités. Ils ne peuvent pas apporter de modifications ni effectuer d'opérations dans l'API Grid Manager ou Grid Management. Les utilisateurs locaux en lecture seule peuvent modifier leurs propres mots de passe.

   > Si un utilisateur appartient à plusieurs groupes et qu'un groupe est défini sur **lecture seule**, l'utilisateur dispose d'un accès en lecture seule à tous les paramètres et fonctions sélectionnés.

2. Sélectionnez une ou plusieurs options "autorisations de groupe d'administration".

   Vous devez attribuer au moins une autorisation à chaque groupe ; sinon, les utilisateurs appartenant au groupe ne pourront pas se connecter à StorageGRID.

3. Si vous créez un groupe local, sélectionnez **Continuer**. Si vous créez un groupe fédéré, sélectionnez **Créer groupe** et **Terminer**.

Ajouter des utilisateurs (groupes locaux uniquement)

Étapes

1. Vous pouvez également sélectionner un ou plusieurs utilisateurs locaux pour ce groupe.

   Si vous n'avez pas encore créé d'utilisateurs locaux, vous pouvez enregistrer le groupe sans ajouter d'utilisateurs. Vous pouvez ajouter ce groupe à l'utilisateur sur la page utilisateurs. Voir"Gérer les utilisateurs" pour plus d'informations.

2. Sélectionnez **Créer groupe** et **Terminer**.

Afficher et modifier les groupes d'administration

Vous pouvez afficher les détails des groupes existants, modifier un groupe ou dupliquer un groupe.

- Pour afficher les informations de base de tous les groupes, consultez le tableau de la page groupes.
- Pour afficher tous les détails d'un groupe spécifique ou pour modifier un groupe, utilisez le menu **actions** ou la page de détails.

Tâche	Menu actions	Page de détails
Afficher les détails du groupe	a. Cochez la case du groupe. b. Sélectionnez **actions** > **Afficher les détails du groupe**.	Sélectionnez le nom du groupe dans le tableau.
Modifier le nom d'affichage (groupes locaux uniquement)	a. Cochez la case du groupe. b. Sélectionnez **actions** > **Modifier le nom du groupe**. c. Saisissez le nouveau nom. d. Sélectionnez **Enregistrer les modifications**.	a. Sélectionnez le nom du groupe pour afficher les détails. b. Sélectionnez l'icône de modification . c. Saisissez le nouveau nom. d. Sélectionnez **Enregistrer les modifications**.
Modifier le mode d'accès ou les autorisations	a. Cochez la case du groupe. b. Sélectionnez **actions** > **Afficher les détails du groupe**. c. Si vous le souhaitez, modifiez le mode d'accès du groupe. d. Si vous le souhaitez, sélectionnez ou désélectionnez "autorisations de groupe d'administration". e. Sélectionnez **Enregistrer les modifications**.	a. Sélectionnez le nom du groupe pour afficher les détails. b. Si vous le souhaitez, modifiez le mode d'accès du groupe. c. Si vous le souhaitez, sélectionnez ou désélectionnez "autorisations de groupe d'administration". d. Sélectionnez **Enregistrer les modifications**.

Dupliquer un groupe

Étapes

1. Cochez la case du groupe.

2. Sélectionnez **actions** > **Dupliquer le groupe**.
3. Suivez l'assistant de duplication de groupe.

Supprimer un groupe

Vous pouvez supprimer un groupe d'administration lorsque vous souhaitez supprimer le groupe du système et supprimer toutes les autorisations associées au groupe. La suppression d'un groupe admin supprime tous les utilisateurs du groupe, mais ne les supprime pas.

Étapes

1. Dans la page groupes, cochez la case correspondant à chaque groupe à supprimer.
2. Sélectionnez **actions** > **Supprimer le groupe**.
3. Sélectionnez **Supprimer les groupes**.

Autorisations de groupe d'administration

Lors de la création de groupes d'utilisateurs admin, vous sélectionnez une ou plusieurs autorisations pour contrôler l'accès à des fonctions spécifiques de Grid Manager. Vous pouvez ensuite affecter chaque utilisateur à un ou plusieurs de ces groupes d'administration pour déterminer les tâches que l'utilisateur peut effectuer.

Vous devez affecter au moins une autorisation à chaque groupe ; sinon, les utilisateurs appartenant à ce groupe ne pourront pas se connecter au Grid Manager ou à l'API Grid Management.

Par défaut, tout utilisateur appartenant à un groupe disposant d'au moins une autorisation peut effectuer les tâches suivantes :

- Connectez-vous au Grid Manager
- Afficher le tableau de bord
- Affichez les pages nœuds
- Surveiller la topologie de la grille
- Afficher les alertes actuelles et résolues
- Afficher les alarmes actuelles et historiques (système hérité)
- Modifier son propre mot de passe (utilisateurs locaux uniquement)
- Afficher certaines informations fournies sur les pages Configuration et Maintenance

Interaction entre les autorisations et le mode d'accès

Pour toutes les autorisations, le paramètre **mode d'accès** du groupe détermine si les utilisateurs peuvent modifier les paramètres et effectuer des opérations ou s'ils ne peuvent afficher que les paramètres et les fonctionnalités associés. Si un utilisateur appartient à plusieurs groupes et qu'un groupe est défini sur **lecture seule**, l'utilisateur dispose d'un accès en lecture seule à tous les paramètres et fonctions sélectionnés.

Les sections suivantes décrivent les autorisations que vous pouvez attribuer lors de la création ou de la modification d'un groupe d'administration. Toute fonctionnalité qui n'est pas explicitement mentionnée requiert l'autorisation **accès racine**.

Accès racine

Cette autorisation donne accès à toutes les fonctions d'administration de la grille.

Accuser réception d'alarmes (existantes)

Cette autorisation permet d'accuser réception et de répondre aux alarmes (système hérité). Tous les utilisateurs connectés peuvent afficher les alarmes actuelles et historiques.

Si vous souhaitez qu'un utilisateur surveille la topologie de la grille et accuse réception des alarmes uniquement, vous devez attribuer cette autorisation.

Modifier le mot de passe root du locataire

Cette autorisation donne accès à l'option **changer mot de passe root** de la page locataires, ce qui vous permet de contrôler qui peut modifier le mot de passe de l'utilisateur racine local du locataire. Cette autorisation est également utilisée pour migrer les clés S3 lorsque la fonctionnalité d'importation de clés S3 est activée. Les utilisateurs qui ne disposent pas de cette autorisation ne peuvent pas voir l'option **Modifier le mot de passe root**.

> Pour accorder l'accès à la page locataires, qui contient l'option **changer mot de passe racine**, attribuez également l'autorisation **comptes locataire**.

Configuration de la page de topologie grid

Cette autorisation permet d'accéder aux onglets Configuration de la page **SUPPORT** > **Outils** > **topologie de grille**.

ILM

Cette autorisation permet d'accéder aux options de menu **ILM** suivantes :

- Règles
- Stratégies
- Le code d'effacement
- Régions
- Pools de stockage

> Les utilisateurs doivent disposer des autorisations **autre configuration de grille** et **Configuration de page de topologie de grille** pour gérer les classes de stockage.

Maintenance

Les utilisateurs doivent disposer de l'autorisation Maintenance pour utiliser les options suivantes :

- **CONFIGURATION** > **contrôle d'accès** :
  - Mots de passe de grille
- **CONFIGURATION** > **réseau** :
  - Noms de domaine de terminaux S3
- **MAINTENANCE** > **tâches** :

    - Désaffectation
    - De développement
    - Vérification de l’existence d’objet
    - Reprise après incident
- **MAINTENANCE** > **système** :
    - Package de restauration
    - Mise à jour logicielle
- **SUPPORT** > **Outils** :
    - Journaux

Les utilisateurs qui ne disposent pas de l’autorisation Maintenance peuvent afficher, mais pas modifier, les pages suivantes :

- **MAINTENANCE** > **réseau** :
    - Serveurs DNS
    - Réseau Grid
    - Serveurs NTP
- **MAINTENANCE** > **système** :
    - Licence
- **CONFIGURATION** > **réseau** :
    - Noms de domaine de terminaux S3
- **CONFIGURATION** > **sécurité** :
    - Certificats
- **CONFIGURATION** > **surveillance** :
    - Serveur d’audit et syslog

Gérer les alertes

Cette autorisation donne accès aux options de gestion des alertes. Les utilisateurs doivent disposer de cette autorisation pour gérer les silences, les notifications d’alerte et les règles d’alerte.

Interrogation de metrics

Cette autorisation permet d’accéder aux éléments suivants :

- **SUPPORT** > **Outils** > **métriques** page
- Requêtes de metrics Prometheus personnalisées à l’aide de la section **Metrics** de l’API de gestion de grille
- Cartes de tableau de bord de Grid Manager qui contiennent des metrics

Recherche de métadonnées d’objet

Cette autorisation permet d’accéder à la page **ILM** > **recherche de métadonnées objet**.

Autre configuration de grille

Cette autorisation donne accès à d'autres options de configuration de grille.

> Pour voir ces options supplémentaires, les utilisateurs doivent également disposer de l'autorisation **Grid topology page configuration**.

- **ILM** :
  - Niveaux de stockage
- **CONFIGURATION** > **système** :
  - Options de stockage
- **PRISE EN CHARGE** > **alarmes (hérité)** :
  - Événements personnalisés
  - Alarmes globales
  - Configuration de la messagerie existante
- **SUPPORT** > **autre** :
  - Coût des liens

Administrateur de l'appliance de stockage

Cette autorisation permet d'accéder à la gamme E-Series SANtricity System Manager sur les appliances de stockage via Grid Manager.

Comptes de locataires

Cette autorisation permet de :

- Accédez à la page tenants, où vous pouvez créer, modifier et supprimer des comptes de tenant
- Afficher les stratégies de classification du trafic existantes
- Affichez les cartes du tableau de bord Grid Manager qui contiennent les détails du locataire

Gérer les utilisateurs

Vous pouvez afficher les utilisateurs locaux et fédérés. Vous pouvez également créer des utilisateurs locaux et les affecter à des groupes d'administration locaux pour déterminer les fonctions de Grid Manager auxquelles ces utilisateurs peuvent accéder.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous disposez d'autorisations d'accès spécifiques.

Créez un utilisateur local

Vous pouvez créer un ou plusieurs utilisateurs locaux et attribuer chaque utilisateur à un ou plusieurs groupes locaux. Les autorisations du groupe contrôlent les fonctionnalités de Grid Manager et de Grid Management auxquelles l'utilisateur peut accéder.

Vous ne pouvez créer que des utilisateurs locaux. Utilisez le référentiel d'identité externe pour gérer des

utilisateurs et des groupes fédérés.

Le gestionnaire de grille comprend un utilisateur local prédéfini, nommé « root ». Vous ne pouvez pas supprimer l'utilisateur racine.

> Si l'authentification unique (SSO) est activée, les utilisateurs locaux ne peuvent pas se connecter à StorageGRID.

Accéder à l'assistant

Étapes

1. Sélectionnez **CONFIGURATION** > **contrôle d'accès** > **utilisateurs Admin**.
2. Sélectionnez **Créer utilisateur**.

Saisissez les informations d'identification de l'utilisateur

Étapes

1. Saisissez le nom complet de l'utilisateur, un nom d'utilisateur unique et un mot de passe.
2. Vous pouvez également sélectionner **Oui** si cet utilisateur ne doit pas avoir accès à Grid Manager ou à l'API de gestion de grille.
3. Sélectionnez **Continuer**.

Affecter à des groupes

Étapes

1. Vous pouvez éventuellement attribuer l'utilisateur à un ou plusieurs groupes pour déterminer les autorisations de l'utilisateur.

   Si vous n'avez pas encore créé de groupes, vous pouvez enregistrer l'utilisateur sans sélectionner de groupes. Vous pouvez ajouter cet utilisateur à un groupe sur la page groupes.

   Si un utilisateur appartient à plusieurs groupes, les autorisations sont cumulatives. Voir"Gérez les groupes d'administration" pour plus d'informations.

2. Sélectionnez **Créer utilisateur** et **Terminer**.

Afficher et modifier les utilisateurs locaux

Vous pouvez afficher les détails des utilisateurs locaux et fédérés existants. Vous pouvez modifier un utilisateur local pour modifier son nom complet, son mot de passe ou son appartenance à un groupe. Vous pouvez également empêcher temporairement un utilisateur d'accéder au Grid Manager et à l'API Grid Management.

Vous ne pouvez modifier que les utilisateurs locaux. Utilisez le référentiel d'identité externe pour gérer les utilisateurs fédérés.

- Pour afficher les informations de base de tous les utilisateurs locaux et fédérés, consultez le tableau de la page utilisateurs.
- Pour afficher tous les détails d'un utilisateur spécifique, modifier un utilisateur local ou modifier le mot de passe d'un utilisateur local, utilisez le menu **actions** ou la page de détails.

  Toutes les modifications sont appliquées la prochaine fois que l'utilisateur se déconnecte, puis se reconnecte au Grid Manager.

Les utilisateurs locaux peuvent modifier leurs propres mots de passe à l'aide de l'option **Modifier le mot de passe** de la bannière Grid Manager.

Tâche	Menu actions	Page de détails
Afficher les détails de l'utilisateur	a. Cochez la case de l'utilisateur. b. Sélectionnez **actions** > **Afficher les détails de l'utilisateur**.	Sélectionnez le nom de l'utilisateur dans le tableau.
Modifier le nom complet (utilisateurs locaux uniquement)	a. Cochez la case de l'utilisateur. b. Sélectionnez **actions** > **Modifier le nom complet**. c. Saisissez le nouveau nom. d. Sélectionnez **Enregistrer les modifications**.	a. Sélectionnez le nom de l'utilisateur pour afficher les détails. b. Sélectionnez l'icône de modification . c. Saisissez le nouveau nom. d. Sélectionnez **Enregistrer les modifications**.
Refuser ou autoriser l'accès StorageGRID	a. Cochez la case de l'utilisateur. b. Sélectionnez **actions** > **Afficher les détails de l'utilisateur**. c. Sélectionnez l'onglet accès. d. Sélectionnez **Oui** pour empêcher l'utilisateur de se connecter au Grid Manager ou à l'API de gestion de la grille ou sélectionnez **non** pour permettre à l'utilisateur de se connecter. e. Sélectionnez **Enregistrer les modifications**.	a. Sélectionnez le nom de l'utilisateur pour afficher les détails. b. Sélectionnez l'onglet accès. c. Sélectionnez **Oui** pour empêcher l'utilisateur de se connecter au Grid Manager ou à l'API de gestion de la grille ou sélectionnez **non** pour permettre à l'utilisateur de se connecter. d. Sélectionnez **Enregistrer les modifications**.
Modifier le mot de passe (utilisateurs locaux uniquement)	a. Cochez la case de l'utilisateur. b. Sélectionnez **actions** > **Afficher les détails de l'utilisateur**. c. Sélectionnez l'onglet Mot de passe. d. Saisissez un nouveau mot de passe. e. Sélectionnez **changer mot de passe**.	a. Sélectionnez le nom de l'utilisateur pour afficher les détails. b. Sélectionnez l'onglet Mot de passe. c. Saisissez un nouveau mot de passe. d. Sélectionnez **changer mot de passe**.

Tâche	Menu actions	Page de détails
Modifier les groupes (utilisateurs locaux uniquement)	a. Cochez la case de l'utilisateur. b. Sélectionnez **actions** > **Afficher les détails de l'utilisateur**. c. Sélectionnez l'onglet groupes. d. Vous pouvez également sélectionner le lien après le nom d'un groupe pour afficher les détails du groupe dans un nouvel onglet de navigateur. e. Sélectionnez **Modifier les groupes** pour sélectionner différents groupes. f. Sélectionnez **Enregistrer les modifications**.	a. Sélectionnez le nom de l'utilisateur pour afficher les détails. b. Sélectionnez l'onglet groupes. c. Vous pouvez également sélectionner le lien après le nom d'un groupe pour afficher les détails du groupe dans un nouvel onglet de navigateur. d. Sélectionnez **Modifier les groupes** pour sélectionner différents groupes. e. Sélectionnez **Enregistrer les modifications**.

Dupliquer un utilisateur

Vous pouvez dupliquer un utilisateur existant pour créer un nouvel utilisateur avec les mêmes autorisations.

Étapes

1. Cochez la case de l'utilisateur.
2. Sélectionnez **actions** > **Dupliquer utilisateur**.
3. Suivez l'assistant Dupliquer.

Supprimer un utilisateur

Vous pouvez supprimer un utilisateur local pour supprimer définitivement cet utilisateur du système.

Vous ne pouvez pas supprimer l'utilisateur root.

Étapes

1. Dans la page utilisateurs, cochez la case correspondant à chaque utilisateur à supprimer.
2. Sélectionnez **actions** > **Supprimer l'utilisateur**.
3. Sélectionnez **Supprimer l'utilisateur**.

Utilisation de la connexion unique (SSO)

Configurer l'authentification unique

Lorsque l'authentification unique (SSO) est activée, les utilisateurs n'ont accès qu'au Grid Manager, au tenant Manager, à l'API Grid Management ou à l'API de gestion des locataires si leurs identifiants sont autorisés à l'aide du processus de connexion SSO mis en œuvre par votre entreprise. Les utilisateurs locaux ne peuvent pas se connecter à StorageGRID.

Fonctionnement de l'authentification unique

Le système StorageGRID prend en charge la fonctionnalité SSO (Single Sign-on) en utilisant la 2.0 norme SAML 2.0 (Security assertion Markup Language).

Avant d'activer l'authentification unique (SSO), vérifiez comment les processus de connexion et de déconnexion StorageGRID sont affectés lorsque l'authentification SSO est activée.

Connectez-vous lorsque SSO est activé

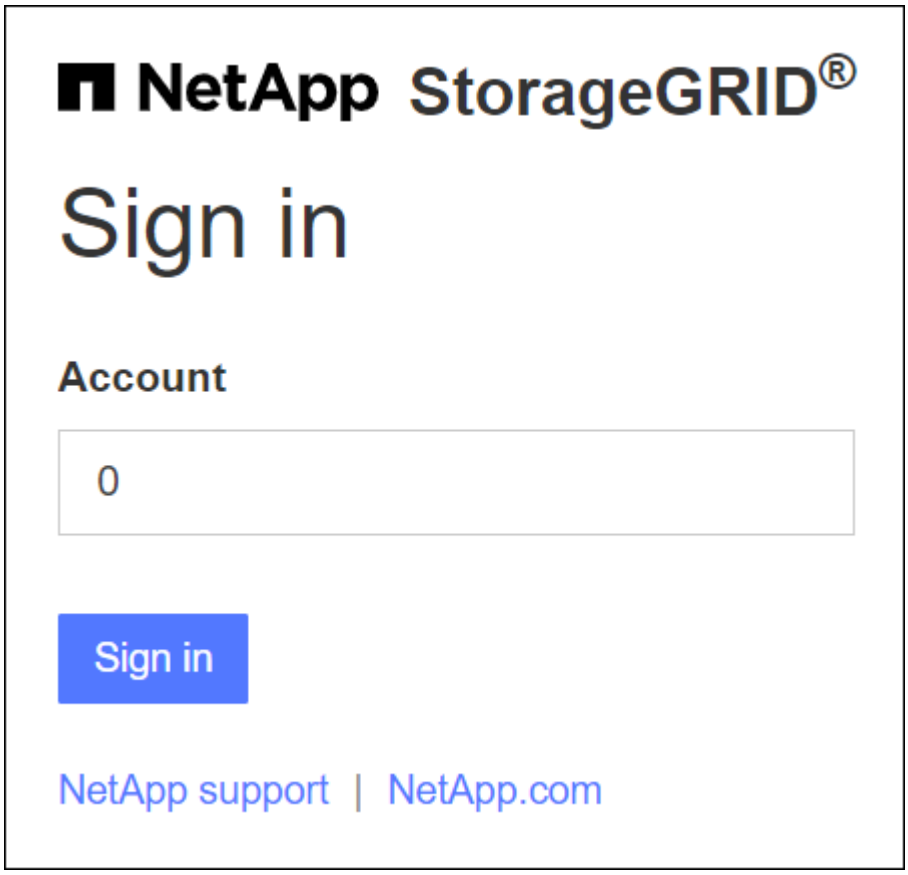
Lorsque l'authentification SSO est activée et que vous vous connectez à StorageGRID, vous êtes redirigé vers la page SSO de votre entreprise afin de valider vos identifiants.

Étapes

1. Entrez le nom de domaine complet ou l'adresse IP d'un nœud d'administration StorageGRID dans un navigateur Web.

   La page de connexion StorageGRID s'affiche.

   - S'il s'agit de la première fois que vous accédez à l'URL sur ce navigateur, vous êtes invité à entrer un ID de compte :

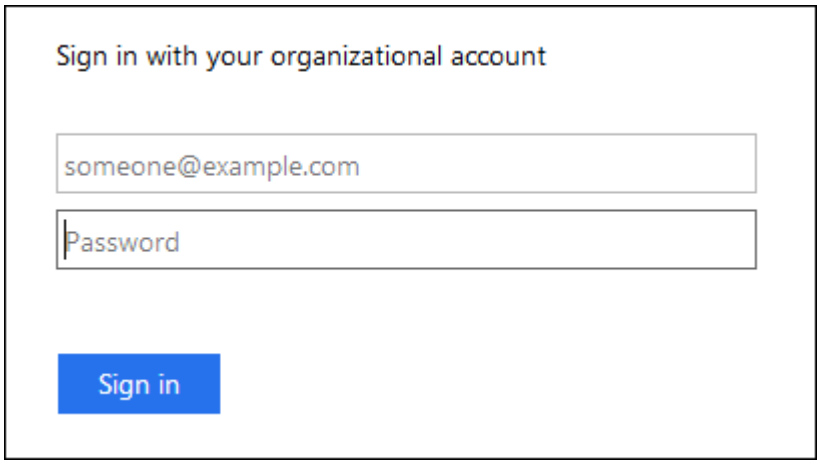


   - Si vous avez déjà accédé au Grid Manager ou au tenant Manager, vous êtes invité à sélectionner un compte récent ou à saisir un ID de compte :

La page de connexion StorageGRID n'apparaît pas lorsque vous saisissez l'URL complète d'un compte de locataire (c'est-à-dire un nom de domaine complet ou une adresse IP suivi de `/?accountId=20-digit-account-id`). Au lieu de cela, vous êtes immédiatement redirigé vers la page de connexion SSO de votre entreprise, où vous pouvez Connectez-vous à l'aide de vos identifiants SSO.

2. Indiquez si vous souhaitez accéder au Grid Manager ou au tenant Manager :
   - Pour accéder au Gestionnaire de grille, laissez le champ **ID de compte** vide, saisissez **0** comme ID de compte ou sélectionnez **Grid Manager** si celui-ci apparaît dans la liste des comptes récents.
   - Pour accéder au Gestionnaire de locataires, entrez l'ID de compte de tenant à 20 chiffres ou sélectionnez un locataire par nom s'il apparaît dans la liste des comptes récents.
3. Sélectionnez **connexion**

   StorageGRID vous redirige vers la page de connexion SSO de votre entreprise. Par exemple :



4. Connectez-vous à l'aide de vos identifiants SSO.

Si vos informations d'identification SSO sont correctes :

a. Le fournisseur d'identités fournit une réponse d'authentification à StorageGRID.
b. StorageGRID valide la réponse d'authentification.
c. Si la réponse est valide et que vous appartenez à un groupe fédéré avec des autorisations d'accès StorageGRID, vous êtes connecté au Gestionnaire de grille ou au Gestionnaire des locataires, selon le compte que vous avez sélectionné.

> Si le compte de service est inaccessible, vous pouvez toujours vous connecter tant que vous êtes un utilisateur existant appartenant à un groupe fédéré avec des autorisations d'accès StorageGRID.

5. Accédez éventuellement à d'autres nœuds d'administration ou à Grid Manager ou au tenant Manager, si vous disposez des autorisations adéquates.

   Il n'est pas nécessaire de saisir à nouveau vos informations d'identification SSO.

Déconnectez-vous lorsque SSO est activé

Lorsque l'authentification SSO est activée pour StorageGRID, le processus de déconnexion dépend de ce que vous êtes connecté et de l'endroit où vous vous déconnectez.

Étapes

1. Localisez le lien **Déconnexion** dans le coin supérieur droit de l'interface utilisateur.
2. Sélectionnez **Déconnexion**.

   La page de connexion StorageGRID s'affiche. La liste déroulante **comptes récents** est mise à jour pour inclure **Grid Manager** ou le nom du locataire, afin que vous puissiez accéder plus rapidement à ces interfaces utilisateur à l'avenir.

Si vous êtes connecté à…	Et vous vous déconnectez de…	Vous êtes déconnecté de…
Grid Manager sur un ou plusieurs nœuds d'administration	Grid Manager sur n'importe quel nœud d'administration	Grid Manager sur tous les nœuds d'administration **Remarque :** si vous utilisez Azure pour SSO, la session de tous les nœuds d'administration peut prendre quelques minutes.
Gestionnaire de locataires sur un ou plusieurs nœuds d'administration	Gestionnaire de locataires sur n'importe quel nœud d'administration	Gestionnaire de locataires sur tous les nœuds d'administration
Grid Manager et tenant Manager	Gestionnaire de grille	Le Grid Manager uniquement. Vous devez également vous déconnecter du tenant Manager pour vous déconnecter de SSO.

Le tableau résume ce qui se passe lorsque vous vous déconnectez si vous utilisez une seule session de navigateur. Si vous êtes connecté à StorageGRID à travers plusieurs sessions de navigateur, vous devez vous déconnecter de toutes les sessions de navigateur séparément.

Configuration requise et considérations pour l'authentification unique

Avant d'activer la signature unique (SSO) pour un système StorageGRID, consultez les conditions requises et les considérations à prendre en compte.

Exigences du fournisseur d'identités

StorageGRID prend en charge les fournisseurs d'identités SSO suivants :

- Service de fédération Active Directory (AD FS)
- Azure Active Directory (Azure AD)
- PingFederate

Vous devez configurer la fédération des identités de votre système StorageGRID avant de pouvoir configurer un fournisseur d'identités SSO. Le type de service LDAP que vous utilisez pour la fédération des identités contrôle le type de SSO que vous pouvez implémenter.

Type de service LDAP configuré	Options pour le fournisseur d'identité SSO
Active Directory	• Active Directory • Azure • PingFederate
Azure	Azure

Exigences AD FS

Vous pouvez utiliser l'une des versions suivantes d'AD FS :

- Système de fichiers AD Windows Server 2022
- Système de fichiers AD Windows Server 2019
- Système de fichiers AD Windows Server 2016

Windows Server 2016 doit utiliser le "Mise à jour KB3201845", ou supérieur.

- AD FS 3.0, inclus avec la mise à jour Windows Server 2012 R2, ou une version ultérieure.

Supplémentaires requise

- TLS (transport Layer Security) 1.2 ou 1.3
- Microsoft .NET Framework, version 3.5.1 ou supérieure

Avantages d'Azure

Si vous utilisez Azure comme type SSO et que les utilisateurs ont des noms d'utilisateur principaux qui n'utilisent pas le préfixe sAMAccountName, des problèmes de connexion peuvent se produire si StorageGRID perd sa connexion avec le serveur LDAP. Pour autoriser les utilisateurs à se connecter, vous devez restaurer la connexion au serveur LDAP.

Configuration requise pour le certificat de serveur

Par défaut, StorageGRID utilise un certificat d'interface de gestion sur chaque nœud d'administration pour sécuriser l'accès au Grid Manager, au tenant Manager, à l'API de gestion du grid et à l'API de gestion des locataires. Lorsque vous configurez des approbations de tiers de confiance (AD FS), des applications d'entreprise (Azure) ou des connexions de fournisseur de services (PingFederate) pour StorageGRID, vous utilisez le certificat de serveur comme certificat de signature pour les requêtes StorageGRID.

Si ce n'est pas déjà fait "configuré un certificat personnalisé pour l'interface de gestion", vous devriez le faire maintenant. Lorsque vous installez un certificat de serveur personnalisé, il est utilisé pour tous les nœuds d'administration et vous pouvez l'utiliser dans toutes les approbations de tiers StorageGRID, les applications d'entreprise ou les connexions SP.

> Il n'est pas recommandé d'utiliser le certificat de serveur par défaut d'un nœud d'administration dans une connexion de confiance, d'une application d'entreprise ou d'un SP. Si le nœud échoue et que vous le récupérez, un nouveau certificat de serveur par défaut est généré. Avant de pouvoir vous connecter au nœud restauré, vous devez mettre à jour la confiance de la partie utilisatrices, l'application d'entreprise ou la connexion SP avec le nouveau certificat.

Vous pouvez accéder au certificat de serveur d'un nœud d'administration en vous connectant au shell de commande du nœud et en allant à `/var/local/mgmt-api` répertoire. Un certificat de serveur personnalisé est nommé `custom-server.crt`. Le certificat de serveur par défaut du nœud est nommé `server.crt`.

Configuration requise pour les ports

L'authentification unique (SSO) n'est pas disponible sur les ports du gestionnaire de grille restreinte ou du gestionnaire de locataires. Vous devez utiliser le port HTTPS par défaut (443) si vous souhaitez que les utilisateurs s'authentifient avec une connexion unique. Voir "Contrôler l'accès au niveau du pare-feu externe".

Confirmez que les utilisateurs fédérés peuvent se connecter

Avant d'activer l'authentification unique (SSO), vous devez confirmer qu'au moins un utilisateur fédéré peut se connecter au Grid Manager et au tenant Manager pour tout compte de tenant existant.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous disposez d'autorisations d'accès spécifiques.
- Vous avez déjà configuré la fédération des identités.

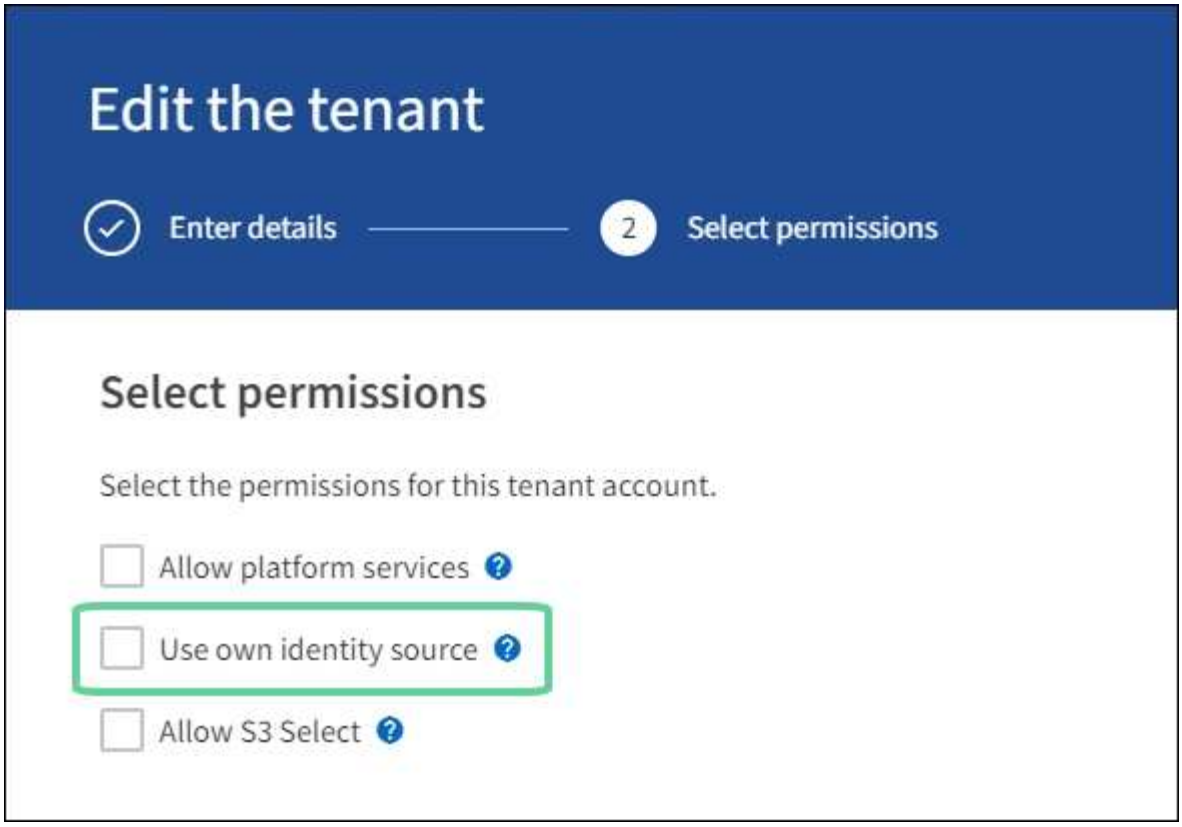
Étapes

1. S'il existe des comptes de tenant existants, vérifiez qu'aucun des locataires n'utilise son propre référentiel d'identité.

Lorsque vous activez SSO, un référentiel d'identité configuré dans le Gestionnaire de locataires est remplacé par le référentiel d'identité configuré dans le Gestionnaire de grille. Les utilisateurs appartenant au référentiel d'identité du locataire ne pourront plus se connecter à moins qu'ils aient un compte avec le référentiel d'identité Grid Manager.

a. Connectez-vous au Gestionnaire de locataires pour chaque compte de locataire.
b. Sélectionnez **ACCESS MANAGEMENT** > **identity federation**.
c. Vérifiez que la case **Activer la fédération d'identité** n'est pas cochée.
d. Si c'est le cas, vérifiez que tous les groupes fédérés pouvant être utilisés pour ce compte de tenant ne sont plus nécessaires, décochez la case et sélectionnez **Enregistrer**.

2. Vérifiez qu'un utilisateur fédéré peut accéder au Grid Manager :
   a. Dans Grid Manager, sélectionnez **CONFIGURATION** > **contrôle d'accès** > **groupes d'administration**.
   b. Assurez-vous qu'au moins un groupe fédéré a été importé du référentiel d'identité Active Directory et qu'il a reçu l'autorisation d'accès racine.
   c. Se déconnecter.
   d. Confirmez que vous pouvez vous reconnecter au Grid Manager en tant qu'utilisateur dans le groupe fédéré.
3. S'il existe des comptes de tenant existants, confirmez qu'un utilisateur fédéré disposant d'une autorisation d'accès racine peut se connecter :
   a. Dans Grid Manager, sélectionnez **TENANTS**.
   b. Sélectionnez le compte locataire, puis sélectionnez **actions** > **Modifier**.
   c. Dans l'onglet entrer les détails, sélectionnez **Continuer**.
   d. Si la case **utiliser le propre référentiel d'identité** est cochée, décochez la case et sélectionnez **Enregistrer**.



La page tenant s'affiche.

a. Sélectionnez le compte de tenant, sélectionnez **connexion** et connectez-vous au compte de tenant en tant qu'utilisateur racine local.

b. Dans le Gestionnaire de locataires, sélectionnez **ACCESS MANAGEMENT** > **Groups**.

c. Assurez-vous qu'au moins un groupe fédéré du Grid Manager a reçu l'autorisation d'accès racine pour ce locataire.

d. Se déconnecter.

e. Confirmez que vous pouvez vous reconnecter au locataire en tant qu'utilisateur dans le groupe fédéré.

Informations associées

- "Configuration requise et considérations pour l'authentification unique"
- "Gérez les groupes d'administration"
- "Utilisez un compte de locataire"

Utiliser le mode sandbox

Vous pouvez utiliser le mode sandbox pour configurer et tester l'authentification unique (SSO) avant de l'activer pour tous les utilisateurs StorageGRID. Une fois SSO activé, vous pouvez revenir en mode sandbox chaque fois que vous devez modifier ou tester à nouveau la configuration.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous disposez de l'autorisation d'accès racine.

- Vous avez configuré la fédération des identités pour votre système StorageGRID.
- Pour le type de service LDAP * de fédération d'identités, vous avez sélectionné Active Directory ou Azure, en fonction du fournisseur d'identité SSO que vous envisagez d'utiliser.

Type de service LDAP configuré	Options pour le fournisseur d'identité SSO
Active Directory	• Active Directory • Azure • PingFederate
Azure	Azure

Description de la tâche

Lorsque SSO est activé et qu'un utilisateur tente de se connecter à un nœud d'administration, StorageGRID envoie une demande d'authentification au fournisseur d'identité SSO. Le fournisseur d'identité SSO renvoie une réponse d'authentification à StorageGRID, indiquant si la demande d'authentification a réussi. Pour les demandes réussies :

- La réponse d'Active Directory ou PingFederate inclut un identifiant unique universel (UUID) pour l'utilisateur.
- La réponse d'Azure inclut un nom d'utilisateur principal (UPN).

Pour permettre à StorageGRID (le fournisseur de services) et au fournisseur d'identité SSO de communiquer en toute sécurité au sujet des demandes d'authentification des utilisateurs, vous devez configurer certains paramètres dans StorageGRID. Ensuite, vous devez utiliser le logiciel du fournisseur d'identités SSO pour créer une confiance de tiers de confiance (AD FS), une application d'entreprise (Azure) ou un fournisseur de services (PingFederate) pour chaque nœud d'administration. Enfin, vous devez revenir à StorageGRID pour activer le SSO.

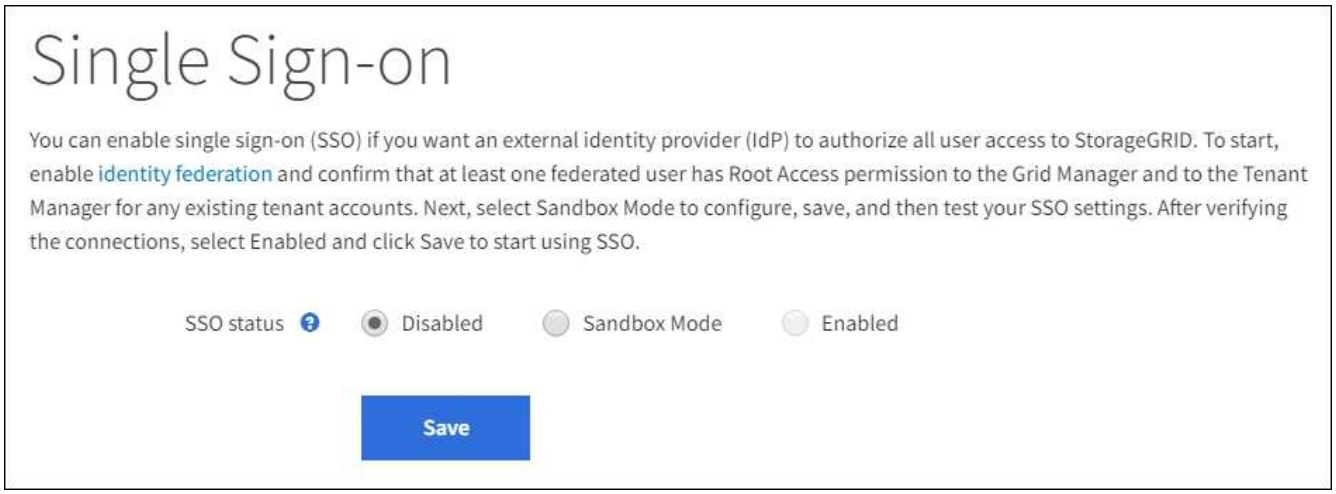
Le mode sandbox facilite l'exécution de cette configuration et le test de tous vos paramètres avant l'activation de SSO. Lorsque vous utilisez le mode sandbox, les utilisateurs ne peuvent pas se connecter à l'aide de SSO.

Accéder au mode sandbox

Étapes

1. Sélectionnez **CONFIGURATION** > **contrôle d'accès** > **connexion unique**.

   La page connexion unique s'affiche, avec l'option **Disabled** sélectionnée.



Si les options Statut SSO ne s'affichent pas, vérifiez que vous avez configuré le fournisseur d'identité comme référentiel d'identité fédéré. Voir "Configuration requise et considérations pour l'authentification unique".

2. Sélectionnez **Sandbox mode**.

   La section fournisseur d'identité s'affiche.

Saisissez les détails du fournisseur d'identité

Étapes

1. Sélectionnez le **SSO type** dans la liste déroulante.
2. Renseignez les champs de la section Identity Provider en fonction du type SSO sélectionné.

Active Directory

1. Entrez le nom du service de fédération * pour le fournisseur d'identités, exactement comme il apparaît dans Active Directory Federation Service (AD FS).

   Pour localiser le nom du service de fédération, accédez à Windows Server Manager. Sélectionnez **Outils** > **AD FS Management**. Dans le menu action, sélectionnez **Modifier les propriétés du service de fédération**. Le nom du service de fédération est indiqué dans le second champ.

2. Spécifiez le certificat TLS qui sera utilisé pour sécuriser la connexion lorsque le fournisseur d'identité envoie des informations de configuration SSO en réponse aux requêtes StorageGRID.
   - **Utilisez le certificat CA du système d'exploitation** : utilisez le certificat CA par défaut installé sur le système d'exploitation pour sécuriser la connexion.
   - **Utilisez un certificat d'autorité de certification personnalisé** : utilisez un certificat d'autorité de certification personnalisé pour sécuriser la connexion.

     Si vous sélectionnez ce paramètre, copiez le texte du certificat personnalisé et collez-le dans la zone de texte **certificat CA**.

   - **N'utilisez pas TLS**: N'utilisez pas de certificat TLS pour sécuriser la connexion.
3. Dans la section partie de confiance, spécifiez l'identificateur de partie de confiance* pour StorageGRID. Cette valeur contrôle le nom que vous utilisez pour chaque confiance de partie utilisatrices dans AD FS.
   - Par exemple, si votre grid ne comporte qu'un seul nœud d'administration et que vous ne prévoyez pas d'ajouter d'autres nœuds d'administration à l'avenir, entrez `SG` ou `StorageGRID`.
   - Si votre grid inclut plusieurs nœuds d'administration, incluez la chaîne `[HOSTNAME]` dans l'identificateur. Par exemple : `SG-[HOSTNAME]`. Cette commande génère une table qui affiche l'identifiant de partie comptant pour chaque nœud d'administration de votre système, en fonction du nom d'hôte du nœud.

   Vous devez créer une confiance en tiers pour chaque nœud d'administration de votre système StorageGRID. Le fait d'avoir une confiance de partie de confiance pour chaque nœud d'administration permet aux utilisateurs de se connecter et de se déconnecter en toute sécurité à n'importe quel nœud d'administration.

4. Sélectionnez **Enregistrer**.

   Une coche verte apparaît sur le bouton **Save** pendant quelques secondes.

Azure

1. Spécifiez le certificat TLS qui sera utilisé pour sécuriser la connexion lorsque le fournisseur d'identité envoie des informations de configuration SSO en réponse aux requêtes StorageGRID.
   - **Utilisez le certificat CA du système d'exploitation** : utilisez le certificat CA par défaut installé sur le système d'exploitation pour sécuriser la connexion.

- **Utilisez un certificat d'autorité de certification personnalisé** : utilisez un certificat d'autorité de certification personnalisé pour sécuriser la connexion.

  Si vous sélectionnez ce paramètre, copiez le texte du certificat personnalisé et collez-le dans la zone de texte **certificat CA**.

- **N'utilisez pas TLS**: N'utilisez pas de certificat TLS pour sécuriser la connexion.

2. Dans la section application entreprise, spécifiez le **Nom de l'application entreprise** pour StorageGRID. Cette valeur contrôle le nom que vous utilisez pour chaque application d'entreprise dans Azure AD.

   - Par exemple, si votre grid ne comporte qu'un seul nœud d'administration et que vous ne prévoyez pas d'ajouter d'autres nœuds d'administration à l'avenir, entrez `SG` ou `StorageGRID`.
   - Si votre grid inclut plusieurs nœuds d'administration, incluez la chaîne `[HOSTNAME]` dans l'identificateur. Par exemple : `SG-[HOSTNAME]`. Cela génère une table qui indique le nom d'une application d'entreprise pour chaque noeud d'administration de votre système, en fonction du nom d'hôte du noeud.

   > Vous devez créer une application d'entreprise pour chaque nœud d'administration de votre système StorageGRID. La présence d'une application d'entreprise pour chaque nœud d'administration garantit que les utilisateurs peuvent se connecter et se déconnecter en toute sécurité à n'importe quel nœud d'administration.

3. Suivez les étapes de la section "Création d'applications d'entreprise dans Azure AD" Pour créer une application d'entreprise pour chaque noeud d'administration répertorié dans le tableau.
4. Depuis Azure AD, copiez l'URL des métadonnées de fédération pour chaque application d'entreprise. Ensuite, collez cette URL dans le champ URL* des métadonnées de fédération correspondant dans StorageGRID.
5. Après avoir copié et collé une URL de métadonnées de fédération pour tous les nœuds d'administration, sélectionnez **Enregistrer**.

   Une coche verte apparaît sur le bouton **Save** pendant quelques secondes.

PingFederate

1. Spécifiez le certificat TLS qui sera utilisé pour sécuriser la connexion lorsque le fournisseur d'identité envoie des informations de configuration SSO en réponse aux requêtes StorageGRID.
   - **Utilisez le certificat CA du système d'exploitation** : utilisez le certificat CA par défaut installé sur le système d'exploitation pour sécuriser la connexion.
   - **Utilisez un certificat d'autorité de certification personnalisé** : utilisez un certificat d'autorité de certification personnalisé pour sécuriser la connexion.

     Si vous sélectionnez ce paramètre, copiez le texte du certificat personnalisé et collez-le dans la zone de texte **certificat CA**.

   - **N'utilisez pas TLS**: N'utilisez pas de certificat TLS pour sécuriser la connexion.
2. Dans la section SP (Service Provider), spécifiez l'ID de connexion **SP** pour StorageGRID. Cette valeur contrôle le nom que vous utilisez pour chaque connexion SP dans PingFederate.

- Par exemple, si votre grid ne comporte qu'un seul nœud d'administration et que vous ne prévoyez pas d'ajouter d'autres nœuds d'administration à l'avenir, entrez `SG` ou `StorageGRID`.
- Si votre grid inclut plusieurs nœuds d'administration, incluez la chaîne `[HOSTNAME]` dans l'identificateur. Par exemple : `SG-[HOSTNAME]`. Ce tableau génère un ID de connexion SP pour chaque nœud d'administration de votre système, en fonction du nom d'hôte du nœud.

> Vous devez créer une connexion SP pour chaque nœud d'administration de votre système StorageGRID. La présence d'une connexion SP pour chaque nœud d'administration permet aux utilisateurs de se connecter et de se déconnecter en toute sécurité à n'importe quel nœud d'administration.

3. Spécifiez l'URL des métadonnées de fédération pour chaque noeud d'administration dans le champ **URL des métadonnées de fédération**.

   Utilisez le format suivant :

   ```
   https://<Federation Service Name>:<port>/pf/federation_metadata.ping?PartnerSpId=<SP Connection ID>
   ```

4. Sélectionnez **Enregistrer**.

   Une coche verte apparaît sur le bouton **Save** pendant quelques secondes.

Configurez les approbations des parties utilisatrices, les applications d'entreprise ou les connexions SP

Lorsque la configuration est enregistrée, l'avis de confirmation du mode Sandbox s'affiche. Cet avis confirme que le mode sandbox est désormais activé et fournit des instructions de présentation.

StorageGRID peut rester en mode sandbox tant que nécessaire. Toutefois, lorsque **Sandbox mode** est sélectionné sur la page connexion unique, SSO est désactivé pour tous les utilisateurs StorageGRID. Seuls les utilisateurs locaux peuvent se connecter.

Procédez comme suit pour configurer les approbations de tiers de confiance (Active Directory), les applications d'entreprise complètes (Azure) ou les connexions SP (PingFederate).

Active Directory

Étapes

1. Accédez à Active Directory Federation Services (AD FS).
2. Créez une ou plusieurs fiducies de tiers de confiance pour StorageGRID, en utilisant chaque identifiant de partie de confiance indiqué dans le tableau de la page authentification unique StorageGRID.

   Vous devez créer une confiance pour chaque noeud d'administration indiqué dans le tableau.

   Pour obtenir des instructions, reportez-vous à la section "Créer des fiducies de tiers de confiance dans AD FS".

Azure

Étapes

1. Dans la page Single Sign-on du noeud d'administration auquel vous êtes actuellement connecté, sélectionnez le bouton pour télécharger et enregistrer les métadonnées SAML.
2. Ensuite, pour tout autre nœud d'administration de votre grid, répétez la procédure suivante :
   a. Connectez-vous au nœud.
   b. Sélectionnez **CONFIGURATION** > **contrôle d'accès** > **connexion unique**.
   c. Téléchargez et enregistrez les métadonnées SAML pour ce nœud.
3. Accédez au portail Azure.
4. Suivez les étapes de la section "Création d'applications d'entreprise dans Azure AD" Pour charger le fichier de métadonnées SAML de chaque nœud d'administration dans l'application d'entreprise Azure correspondante.

PingFederate

Étapes

1. Dans la page Single Sign-on du noeud d'administration auquel vous êtes actuellement connecté, sélectionnez le bouton pour télécharger et enregistrer les métadonnées SAML.
2. Ensuite, pour tout autre nœud d'administration de votre grid, répétez la procédure suivante :
   a. Connectez-vous au nœud.
   b. Sélectionnez **CONFIGURATION** > **contrôle d'accès** > **connexion unique**.
   c. Téléchargez et enregistrez les métadonnées SAML pour ce nœud.
3. Accédez à PingFederate.
4. "Créez une ou plusieurs connexions de fournisseur de services pour StorageGRID". Utilisez l'ID de connexion SP pour chaque nœud d'administration (indiqué dans le tableau de la page d'authentification unique StorageGRID) et les métadonnées SAML que vous avez téléchargées pour ce nœud d'administration.

   Vous devez créer une connexion SP pour chaque nœud d'administration affiché dans le tableau.

Tester les connexions SSO

Avant d'appliquer l'utilisation de l'authentification unique pour l'ensemble de votre système StorageGRID, vous

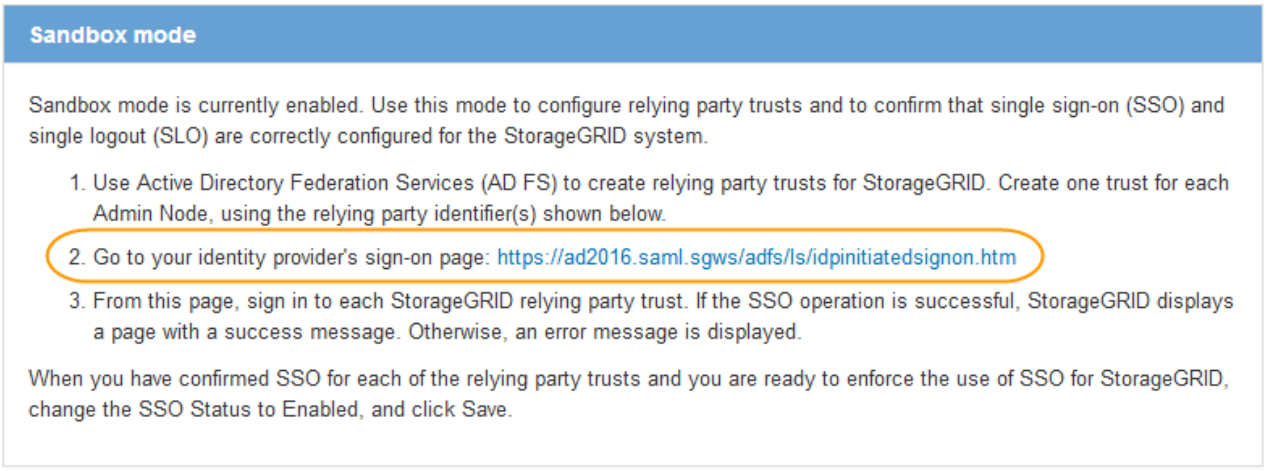
devez confirmer que l’authentification unique et la déconnexion unique sont correctement configurées pour chaque nœud d’administration.

Active Directory

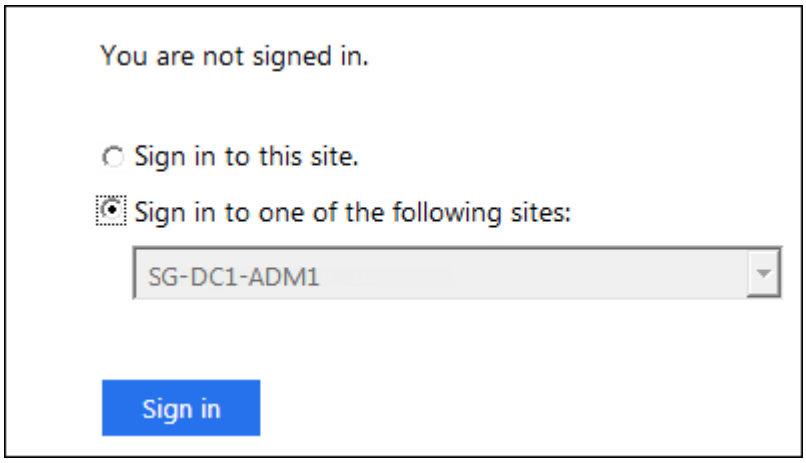
Étapes

1. Sur la page d'ouverture de session unique de StorageGRID, localisez le lien dans le message en mode Sandbox.

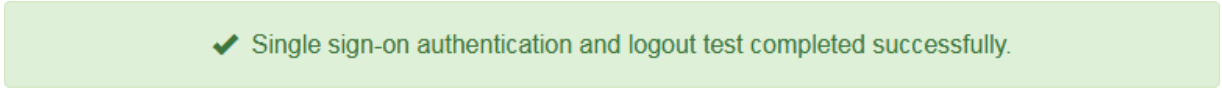
   L'URL est dérivée de la valeur que vous avez saisie dans le champ **Nom du service de fédération**.



2. Sélectionnez le lien ou copiez-collez l'URL dans un navigateur pour accéder à la page de connexion de votre fournisseur d'identités.
3. Pour confirmer que vous pouvez utiliser l'authentification SSO pour vous connecter à StorageGRID, sélectionnez **connexion à l'un des sites suivants**, sélectionnez l'identifiant de partie de confiance pour votre nœud d'administration principal et sélectionnez **connexion**.



4. Entrez votre nom d'utilisateur et votre mot de passe fédérés.
   - Si les opérations de connexion SSO et de déconnexion ont réussi, un message de réussite s'affiche.



   - Si l'opération SSO échoue, un message d'erreur s'affiche. Corrigez le problème, effacez les cookies du navigateur et réessayez.
5. Répétez ces étapes pour vérifier la connexion SSO pour chaque nœud d'administration de votre

grille.

Azure

Étapes

1. Accédez à la page d'identification unique sur le portail Azure.
2. Sélectionnez **Tester cette application**.
3. Entrez les informations d'identification d'un utilisateur fédéré.
   - Si les opérations de connexion SSO et de déconnexion ont réussi, un message de réussite s'affiche.

     ✔ Single sign-on authentication and logout test completed successfully.

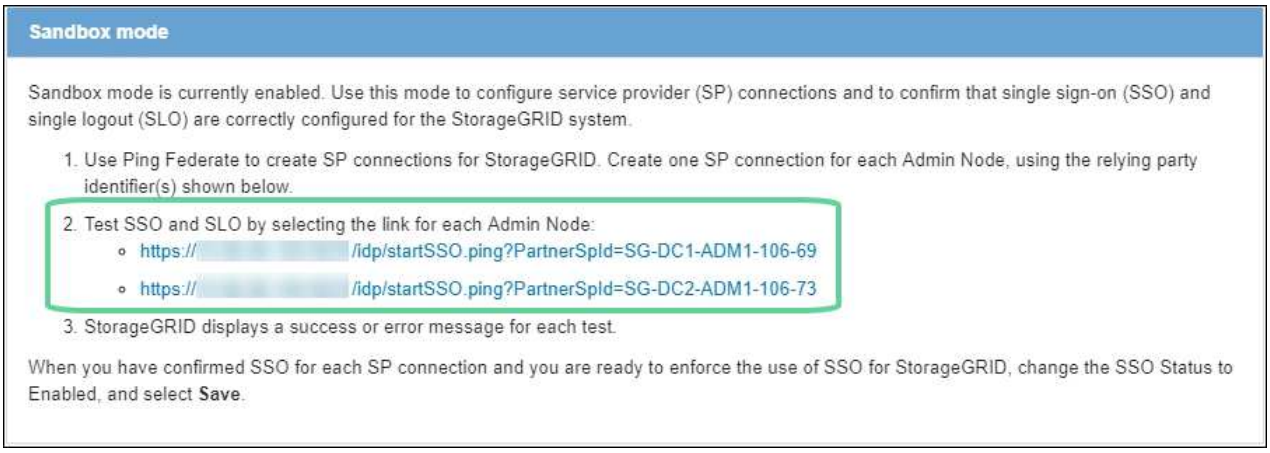
   - Si l'opération SSO échoue, un message d'erreur s'affiche. Corrigez le problème, effacez les cookies du navigateur et réessayez.
4. Répétez ces étapes pour vérifier la connexion SSO pour chaque nœud d'administration de votre grille.

PingFederate

Étapes

1. Sur la page d'ouverture de session unique de StorageGRID, sélectionnez le premier lien dans le message en mode Sandbox.

   Sélectionnez et testez un lien à la fois.

2. Entrez les informations d'identification d'un utilisateur fédéré.
   - Si les opérations de connexion SSO et de déconnexion ont réussi, un message de réussite s'affiche.

     ✔ Single sign-on authentication and logout test completed successfully.

   - Si l'opération SSO échoue, un message d'erreur s'affiche. Corrigez le problème, effacez les cookies du navigateur et réessayez.
3. Cliquez sur le lien suivant pour vérifier la connexion SSO pour chaque nœud d'administration de votre grille.

Si un message page expirée s'affiche, sélectionnez le bouton **Retour** dans votre navigateur et soumettez à nouveau vos informations d'identification.

Activez l'authentification unique

Une fois que vous avez confirmé que vous pouvez utiliser la fonctionnalité SSO pour vous connecter à chaque nœud d'administration, vous pouvez activer cette fonctionnalité pour l'ensemble du système StorageGRID.

Lorsque l'authentification SSO est activée, tous les utilisateurs doivent utiliser l'authentification SSO pour accéder au Grid Manager, au tenant Manager, à l'API Grid Management et à l'API tenant Management. Les utilisateurs locaux ne peuvent plus accéder à StorageGRID.

Étapes

1. Sélectionnez **CONFIGURATION** > **contrôle d'accès** > **connexion unique**.
2. Définissez l'état SSO sur **activé**.
3. Sélectionnez **Enregistrer**.
4. Vérifiez le message d'avertissement et sélectionnez **OK**.

   L'authentification unique est désormais activée.

Si vous utilisez le portail Azure et que vous accédez à StorageGRID à partir du même ordinateur que celui que vous utilisez pour accéder à Azure, assurez-vous que l'utilisateur du portail Azure est également un utilisateur StorageGRID autorisé (utilisateur d'un groupe fédéré importé dans StorageGRID) Ou déconnectez-vous du portail Azure avant de tenter de vous connecter à StorageGRID.

Créer des fiducies de tiers de confiance dans AD FS

Vous devez utiliser Active Directory Federation Services (AD FS) pour créer une confiance de partie de confiance pour chaque nœud d'administration de votre système. Vous pouvez créer des approbations tierces via les commandes PowerShell, en important les métadonnées SAML depuis StorageGRID ou en saisissant manuellement les données.

Avant de commencer

- Vous avez configuré l'authentification unique pour StorageGRID et sélectionné **AD FS** comme type SSO.
- **Sandbox mode** est sélectionné sur la page Single Sign-on dans Grid Manager. Voir "Utiliser le mode sandbox".
- Vous connaissez le nom de domaine complet (ou l'adresse IP) et l'identifiant de partie comptant pour chaque nœud d'administration de votre système. Ces valeurs sont disponibles dans le tableau des détails des nœuds d'administration de la page d'ouverture de session unique StorageGRID.

Vous devez créer une confiance en tiers pour chaque nœud d'administration de votre système StorageGRID. Le fait d'avoir une confiance de partie de confiance pour chaque nœud d'administration permet aux utilisateurs de se connecter et de se déconnecter en toute sécurité à n'importe quel nœud d'administration.

- Vous avez l'expérience de créer des approbations de tiers de confiance dans AD FS, ou vous avez accès à la documentation Microsoft AD FS.
- Vous utilisez le composant logiciel enfichable AD FS Management et vous appartenez au groupe administrateurs.
- Si vous créez manuellement la confiance de la partie utilisatrices, vous disposez du certificat personnalisé chargé pour l'interface de gestion StorageGRID, ou vous savez comment vous connecter à un nœud d'administration à partir du shell de commande.

Description de la tâche

Ces instructions s'appliquent à Windows Server 2016 AD FS. Si vous utilisez une version différente d'AD FS, vous remarquerez de légères différences dans la procédure. Pour toute question, consultez la documentation Microsoft AD FS.

Créez une confiance en vous appuyant sur Windows PowerShell

Vous pouvez utiliser Windows PowerShell pour créer rapidement une ou plusieurs approbations de parties qui font confiance.

Étapes

1. Dans le menu Démarrer de Windows, sélectionnez l'icône PowerShell avec le bouton droit de la souris et sélectionnez **Exécuter en tant qu'administrateur**.
2. À l'invite de commande PowerShell, saisissez la commande suivante :

   ```
   Add-AdfsRelyingPartyTrust -Name "Admin_Node_Identifer" -MetadataURL
   "https://Admin_Node_FQDN/api/saml-metadata"
   ```

   - Pour `Admin_Node_Identifier`, Entrez l'identifiant de partie de confiance du noeud d'administration, exactement comme il apparaît sur la page Single Sign-On. Par exemple : `SG-DC1-ADM1`.
   - Pour `Admin_Node_FQDN`, Entrez le nom de domaine complet du même nœud d'administration. (Si nécessaire, vous pouvez utiliser l'adresse IP du nœud à la place. Toutefois, si vous saisissez une adresse IP ici, sachez que vous devez mettre à jour ou recréer cette confiance de partie de confiance si cette adresse IP change.)
3. Dans le Gestionnaire de serveur Windows, sélectionnez **Outils** > **AD FS Management**.

   L'outil de gestion AD FS s'affiche.
4. Sélectionnez **AD FS** > **confiance de la partie de confiance**.

   La liste des fiducies de tiers de confiance s'affiche.
5. Ajouter une stratégie de contrôle d'accès à la confiance de la partie qui vient d'être créée :
   a. Recherchez la confiance de la partie de confiance que vous venez de créer.
   b. Cliquez avec le bouton droit de la souris sur la confiance et sélectionnez **Modifier la stratégie de contrôle d'accès**.
   c. Sélectionnez une stratégie de contrôle d'accès.
   d. Sélectionnez **appliquer**, puis **OK**
6. Ajouter une politique d'émission de demandes de remboursement à la nouvelle fiducie de compte comptant :
   a. Recherchez la confiance de la partie de confiance que vous venez de créer.

b. Cliquez avec le bouton droit de la souris sur la fiducie et sélectionnez **Modifier la politique d'émission des sinistres**.

c. Sélectionnez **Ajouter règle**.

d. Sur la page Sélectionner un modèle de règle, sélectionnez **Envoyer attributs LDAP en tant que revendications** dans la liste et sélectionnez **Suivant**.

e. Sur la page configurer la règle, entrez un nom d'affichage pour cette règle.

   Par exemple, **objectGUID to Name ID**.

f. Pour le magasin d'attributs, sélectionnez **Active Directory**.

g. Dans la colonne attribut LDAP de la table mappage, saisissez **objectGUID**.

h. Dans la colonne Type de demande sortante de la table mappage, sélectionnez **Nom ID** dans la liste déroulante.

i. Sélectionnez **Terminer** et sélectionnez **OK**.

7. Confirmez que les métadonnées ont été importées avec succès.

   a. Cliquez avec le bouton droit de la souris sur la confiance de la partie utilisatrices pour ouvrir ses propriétés.

   b. Vérifiez que les champs des onglets **Endpoints**, **identificateurs** et **Signature** sont renseignés.

      Si les métadonnées sont manquantes, vérifiez que l'adresse des métadonnées de fédération est correcte ou entrez les valeurs manuellement.

8. Répétez ces étapes pour configurer une confiance de tiers pour tous les nœuds d'administration de votre système StorageGRID.

9. Lorsque vous avez terminé, revenez à StorageGRID et testez toutes les approbations de parties utilisatrices pour confirmer qu'elles sont correctement configurées. Voir "Utiliser le mode Sandbox" pour obtenir des instructions.

Créez une confiance de partie de confiance en vous important des métadonnées de fédération

Vous pouvez importer les valeurs de chaque confiance de fournisseur en accédant aux métadonnées SAML de chaque nœud d'administration.

Étapes

1. Dans le Gestionnaire de serveur Windows, sélectionnez **Outils**, puis **AD FS Management**.
2. Sous actions, sélectionnez **Ajouter la confiance de la partie de confiance**.
3. Sur la page de bienvenue, choisissez **revendications Aware** et sélectionnez **Démarrer**.
4. Sélectionnez **Importer les données concernant la partie de confiance publiée en ligne ou sur un réseau local**.
5. Dans **adresse de métadonnées de fédération (nom d'hôte ou URL)**, saisissez l'emplacement des métadonnées SAML pour ce noeud d'administration :

   `https://Admin_Node_FQDN/api/saml-metadata`

   Pour *`Admin_Node_FQDN`*, Entrez le nom de domaine complet du même nœud d'administration. (Si nécessaire, vous pouvez utiliser l'adresse IP du nœud à la place. Toutefois, si vous saisissez une adresse IP ici, sachez que vous devez mettre à jour ou recréer cette confiance de partie de confiance si cette adresse IP change.)

6. Terminez l'assistant confiance de la partie de confiance, enregistrez la confiance de la partie de confiance et fermez l'assistant.

> Lors de la saisie du nom d'affichage, utilisez l'identificateur de partie comptant pour le noeud d'administration, exactement comme il apparaît sur la page d'ouverture de session unique dans le Gestionnaire de grille. Par exemple : `SG-DC1-ADM1`.

7. Ajouter une règle de sinistre :
   a. Cliquez avec le bouton droit de la souris sur la fiducie et sélectionnez **Modifier la politique d'émission des sinistres**.
   b. Sélectionnez **Ajouter règle** :
   c. Sur la page Sélectionner un modèle de règle, sélectionnez **Envoyer attributs LDAP en tant que revendications** dans la liste et sélectionnez **Suivant**.
   d. Sur la page configurer la règle, entrez un nom d'affichage pour cette règle.

      Par exemple, **objectGUID to Name ID**.

   e. Pour le magasin d'attributs, sélectionnez **Active Directory**.
   f. Dans la colonne attribut LDAP de la table mappage, saisissez **objectGUID**.
   g. Dans la colonne Type de demande sortante de la table mappage, sélectionnez **Nom ID** dans la liste déroulante.
   h. Sélectionnez **Terminer** et sélectionnez **OK**.
8. Confirmez que les métadonnées ont été importées avec succès.
   a. Cliquez avec le bouton droit de la souris sur la confiance de la partie utilisatrices pour ouvrir ses propriétés.
   b. Vérifiez que les champs des onglets **Endpoints**, **identificateurs** et **Signature** sont renseignés.

      Si les métadonnées sont manquantes, vérifiez que l'adresse des métadonnées de fédération est correcte ou entrez les valeurs manuellement.

9. Répétez ces étapes pour configurer une confiance de tiers pour tous les nœuds d'administration de votre système StorageGRID.
10. Lorsque vous avez terminé, revenez à StorageGRID et testez toutes les approbations de parties utilisatrices pour confirmer qu'elles sont correctement configurées. Voir "Utiliser le mode Sandbox" pour obtenir des instructions.

Créer une confiance de partie de confiance manuellement

Si vous choisissez de ne pas importer les données pour les approbations de pièces de confiance, vous pouvez entrer les valeurs manuellement.

Étapes

1. Dans le Gestionnaire de serveur Windows, sélectionnez **Outils**, puis **AD FS Management**.
2. Sous actions, sélectionnez **Ajouter la confiance de la partie de confiance**.
3. Sur la page de bienvenue, choisissez **revendications Aware** et sélectionnez **Démarrer**.
4. Sélectionnez **Entrez les données relatives à la partie de confiance manuellement** et sélectionnez **Suivant**.

5. Suivez l'assistant confiance de la partie de confiance :

   a. Entrez un nom d'affichage pour ce nœud d'administration.

      Pour plus de cohérence, utilisez l'identifiant de partie utilisatrices du nœud d'administration, exactement comme il apparaît sur la page Single Sign-On du Grid Manager. Par exemple : `SG-DC1-ADM1`.

   b. Ignorez l'étape pour configurer un certificat de chiffrement de jeton facultatif.

   c. Sur la page configurer l'URL, cochez la case **Activer la prise en charge du protocole SAML 2.0 WebSSO**.

   d. Saisissez l'URL du noeud final du service SAML pour le noeud d'administration :

      `https://Admin_Node_FQDN/api/saml-response`

      Pour *`Admin_Node_FQDN`*, Entrez le nom de domaine complet du nœud d'administration. (Si nécessaire, vous pouvez utiliser l'adresse IP du nœud à la place. Toutefois, si vous saisissez une adresse IP ici, sachez que vous devez mettre à jour ou recréer cette confiance de partie de confiance si cette adresse IP change.)

   e. Sur la page configurer les identificateurs, spécifiez l'identificateur de partie de confiance pour le même noeud d'administration :

      `Admin_Node_Identifier`

      Pour *`Admin_Node_Identifier`*, Entrez l'identifiant de partie de confiance du noeud d'administration, exactement comme il apparaît sur la page Single Sign-On. Par exemple : `SG-DC1-ADM1`.

   f. Vérifiez les paramètres, enregistrez la confiance de la partie utilisatrices et fermez l'assistant.

      La boîte de dialogue Modifier la politique d'émission des demandes de remboursement s'affiche.

      Si la boîte de dialogue ne s'affiche pas, cliquez avec le bouton droit de la souris sur la fiducie et sélectionnez **Modifier la politique d'émission des sinistres**.

6. Pour démarrer l'assistant règle de sinistre, sélectionnez **Ajouter règle** :

   a. Sur la page Sélectionner un modèle de règle, sélectionnez **Envoyer attributs LDAP en tant que revendications** dans la liste et sélectionnez **Suivant**.

   b. Sur la page configurer la règle, entrez un nom d'affichage pour cette règle.

      Par exemple, **objectGUID to Name ID**.

   c. Pour le magasin d'attributs, sélectionnez **Active Directory**.

   d. Dans la colonne attribut LDAP de la table mappage, saisissez **objectGUID**.

   e. Dans la colonne Type de demande sortante de la table mappage, sélectionnez **Nom ID** dans la liste déroulante.

   f. Sélectionnez **Terminer** et sélectionnez **OK**.

7. Cliquez avec le bouton droit de la souris sur la confiance de la partie utilisatrices pour ouvrir ses propriétés.

8. Dans l'onglet **Endpoints**, configurez le noeud final pour une déconnexion unique (SLO) :

a. Sélectionnez **Ajouter SAML**.

b. Sélectionnez **Endpoint Type** > **SAML Logout**.

c. Sélectionnez **Redirect** > **Redirect**.

d. Dans le champ **URL de confiance**, entrez l'URL utilisée pour la déconnexion unique (SLO) à partir de ce noeud d'administration :

```
https://Admin_Node_FQDN/api/saml-logout
```

Pour *Admin_Node_FQDN*, Entrez le nom de domaine complet du nœud d'administration. (Si nécessaire, vous pouvez utiliser l'adresse IP du nœud à la place. Toutefois, si vous saisissez une adresse IP ici, sachez que vous devez mettre à jour ou recréer cette confiance de partie de confiance si cette adresse IP change.)

a. Sélectionnez **OK**.

9. Dans l'onglet **Signature**, spécifiez le certificat de signature pour la fiducie de cette partie de confiance :

a. Ajouter le certificat personnalisé :

- Si vous disposez du certificat de gestion personnalisé que vous avez téléchargé vers StorageGRID, sélectionnez ce certificat.
- Si vous ne disposez pas du certificat personnalisé, connectez-vous au nœud d'administration, accédez au `/var/local/mgmt-api` Répertoire du nœud d'administration et ajoutez le `custom-server.crt` fichier de certificat.

  Remarque : utilisation du certificat par défaut du noeud d'administration (`server.crt`) n'est pas recommandé. Si le nœud d'administration échoue, le certificat par défaut sera régénéré lorsque vous restaurez le nœud et vous devrez mettre à jour la confiance de l'organisme de confiance.

b. Sélectionnez **appliquer**, puis **OK**.

Les propriétés de la partie de confiance sont enregistrées et fermées.

10. Répétez ces étapes pour configurer une confiance de tiers pour tous les nœuds d'administration de votre système StorageGRID.
11. Lorsque vous avez terminé, revenez à StorageGRID et testez toutes les approbations de parties utilisatrices pour confirmer qu'elles sont correctement configurées. Voir "Utiliser le mode sandbox" pour obtenir des instructions.

Création d'applications d'entreprise dans Azure AD

Vous utilisez Azure AD pour créer une application d'entreprise pour chaque nœud d'administration de votre système.

Avant de commencer

- Vous avez commencé à configurer la connexion unique pour StorageGRID et vous avez sélectionné **Azure** comme type SSO.
- **Sandbox mode** est sélectionné sur la page Single Sign-on dans Grid Manager. Voir "Utiliser le mode sandbox".
- Vous disposez du **Nom d'application entreprise** pour chaque noeud d'administration de votre système. Vous pouvez copier ces valeurs à partir du tableau des détails du nœud d'administration sur la page d'authentification unique StorageGRID.

Vous devez créer une application d'entreprise pour chaque nœud d'administration de votre système StorageGRID. La présence d'une application d'entreprise pour chaque nœud d'administration garantit que les utilisateurs peuvent se connecter et se déconnecter en toute sécurité à n'importe quel nœud d'administration.

- Vous avez de l'expérience dans la création d'applications d'entreprise dans Azure Active Directory.
- Vous disposez d'un compte Azure avec un abonnement actif.
- Vous avez l'un des rôles suivants dans le compte Azure : administrateur global, administrateur des applications clouds, administrateur d'applications clouds ou propriétaire du principal du service.

Accéder à Azure AD

Étapes

1. Connectez-vous au "Portail Azure".
2. Accédez à "Azure Active Directory".
3. Sélectionnez "Les applications d'entreprise".

Créez des applications d'entreprise et enregistrez la configuration SSO de StorageGRID

Pour enregistrer la configuration SSO pour Azure dans StorageGRID, vous devez utiliser Azure afin de créer une application d'entreprise pour chaque nœud d'administration. Vous allez copier les URL de métadonnées de la fédération à partir d'Azure et les coller dans les champs URL* de métadonnées de la fédération correspondants sur la page d'ouverture de session unique de StorageGRID.

Étapes

1. Répétez les étapes suivantes pour chaque nœud d'administration.
   a. Dans le volet applications Azure Enterprise, sélectionnez **Nouvelle application**.
   b. Sélectionnez **Créez votre propre application**.
   c. Pour le nom, entrez le **nom de l'application entreprise** que vous avez copié à partir du tableau Détails du noeud d'administration sur la page connexion unique StorageGRID.
   d. Laissez le bouton radio **intégrer toute autre application que vous ne trouvez pas dans la galerie (hors galerie)** sélectionné.
   e. Sélectionnez **Créer**.
   f. Sélectionnez le lien **Get Started** dans **2. Configurez la case Single Sign On** ou sélectionnez le lien **Single Sign-on** dans la marge de gauche.
   g. Sélectionnez la case **SAML**.
   h. Copiez l'URL **App Federation Metadata URL**, que vous trouverez sous **étape 3 SAML Signing Certificate**.
   i. Accédez à la page d'ouverture de session unique StorageGRID et collez l'URL dans le champ **URL de métadonnées de fédération** qui correspond au nom de l'application **entreprise** que vous avez utilisée.
2. Une fois que vous avez collé une URL de métadonnées de fédération pour chaque nœud d'administration et apporté toutes les autres modifications nécessaires à la configuration SSO, sélectionnez **Enregistrer** sur la page d'ouverture de session unique StorageGRID.

Téléchargez les métadonnées SAML pour chaque nœud d'administration

Une fois la configuration SSO enregistrée, vous pouvez télécharger un fichier de métadonnées SAML pour chaque nœud d'administration de votre système StorageGRID.

Étapes

1. Répétez ces étapes pour chaque nœud d'administration.
   a. Connectez-vous à StorageGRID à partir du nœud d'administration.
   b. Sélectionnez **CONFIGURATION** > **contrôle d'accès** > **connexion unique**.
   c. Sélectionnez le bouton pour télécharger les métadonnées SAML de ce nœud d'administration.
   d. Enregistrez le fichier que vous allez télécharger dans Azure AD.

Téléchargez les métadonnées SAML sur chaque application d'entreprise

Après le téléchargement d'un fichier de métadonnées SAML pour chaque nœud d'administration StorageGRID, effectuez les opérations suivantes dans Azure AD :

Étapes

1. Revenez au portail Azure.
2. Répétez cette procédure pour chaque application d'entreprise :

   > Vous devrez peut-être actualiser la page applications d'entreprise pour voir les applications que vous avez précédemment ajoutées dans la liste.

   a. Accédez à la page Propriétés de l'application d'entreprise.
   b. Définissez **affectation requise** sur **non** (sauf si vous souhaitez configurer séparément les affectations).
   c. Accédez à la page Single Sign-on.
   d. Terminez la configuration SAML.
   e. Sélectionnez le bouton **Télécharger le fichier de métadonnées** et sélectionnez le fichier de métadonnées SAML que vous avez téléchargé pour le nœud d'administration correspondant.
   f. Une fois le fichier chargé, sélectionnez **Enregistrer**, puis **X** pour fermer le volet. Vous revenez à la page configurer un Single Sign-on avec SAML.
3. Suivez les étapes de la section "Utiliser le mode sandbox" pour tester chaque application.

Créer des connexions de fournisseur de services (SP) dans PingFederate

Vous utilisez PingFederate pour créer une connexion de fournisseur de services (SP) pour chaque noeud d'administration de votre système. Pour accélérer le processus, vous importez les métadonnées SAML à partir de StorageGRID.

Avant de commencer

- Vous avez configuré l'authentification unique pour StorageGRID et sélectionné **Ping Federate** comme type SSO.
- **Sandbox mode** est sélectionné sur la page Single Sign-on dans Grid Manager. Voir "Utiliser le mode sandbox".
- Vous disposez de l'ID de connexion * SP* pour chaque noeud d'administration de votre système. Ces

valeurs sont disponibles dans le tableau des détails des nœuds d'administration de la page d'ouverture de session unique StorageGRID.

- Vous avez téléchargé les métadonnées **SAML** pour chaque noeud d'administration de votre système.
- Vous avez l'expérience de la création de connexions SP dans PingFederate Server.
- Vous avez lehttps://docs.pingidentity.com/bundle/pingfederate-103/page/kfj1564002962494.html["Guide de référence de l'administrateur"^] Pour PingFederate Server. La documentation PingFederate fournit des instructions détaillées étape par étape et des explications.
- Vous disposez de l'autorisation Admin pour PingFederate Server.

Description de la tâche

Ces instructions résument comment configurer PingFederate Server version 10.3 en tant que fournisseur SSO pour StorageGRID. Si vous utilisez une autre version de PingFederate, vous devrez peut-être adapter ces instructions. Reportez-vous à la documentation du serveur PingFederate pour obtenir des instructions détaillées sur votre version.

Remplir les conditions préalables dans PingFederate

Avant de pouvoir créer les connexions SP que vous utiliserez pour StorageGRID, vous devez effectuer les tâches préalables dans PingFederate. Vous utiliserez les informations de ces prérequis lors de la configuration des connexions du processeur de service.

Créer un magasin de données

Si ce n'est pas déjà fait, créez un magasin de données pour connecter PingFederate au serveur LDAP AD FS. Utilisez les valeurs que vous avez utilisées lorsque "configuration de la fédération des identités" À StorageGRID.

- **Type**: Répertoire (LDAP)
- **Type LDAP** : Active Directory
- **Nom d'attribut binaire** : saisissez **objectGUID** dans l'onglet attributs binaires LDAP exactement comme indiqué.

Créer un validateur d'informations d'identification de mot de passe

Si ce n'est pas déjà fait, créez un validateur pour les informations d'identification du mot de passe.

- **Type**: LDAP Nom d'utilisateur Mot de passe validateur des informations d'identification
- **Magasin de données** : sélectionnez le magasin de données que vous avez créé.
- **Base de recherche** : saisissez des informations à partir de LDAP (par exemple, DC=saml,DC=sgws).
- **Filtre de recherche** : sAMAccountName=${username}
- **Portée** : sous-arbre

Créer une instance d'adaptateur IDP

Si ce n'est déjà fait, créez une instance de carte IDP.

Étapes

1. Accédez à **Authentication** > **Integration** > **IDP Adapters**.
2. Sélectionnez **Créer une nouvelle instance**.

3. Dans l'onglet Type, sélectionnez **HTML Form IDP adapter**.
4. Dans l'onglet carte IDP, sélectionnez **Ajouter une nouvelle ligne à 'Validators Credentials'**.
5. Sélectionner validateur des informations d'identification du mot de passe vous avez créé.
6. Dans l'onglet attributs de l'adaptateur, sélectionnez l'attribut **nom d'utilisateur** pour **pseudonyme**.
7. Sélectionnez **Enregistrer**.

Créer ou importer un certificat de signature

Si ce n'est déjà fait, créez ou importez le certificat de signature.

Étapes

1. Accédez à **sécurité** > **clés de signature et de déchiffrement**.
2. Créez ou importez le certificat de signature.

Créer une connexion SP dans PingFederate

Lorsque vous créez une connexion SP dans PingFederate, vous importez les métadonnées SAML téléchargées depuis StorageGRID pour le noeud d'administration. Le fichier de métadonnées contient la plupart des valeurs spécifiques dont vous avez besoin.

> Vous devez créer une connexion SP pour chaque nœud d'administration de votre système StorageGRID afin que les utilisateurs puissent se connecter en toute sécurité à n'importe quel nœud et en dehors. Suivez ces instructions pour créer la première connexion du processeur de service. Ensuite, passez à Créer des connexions SP supplémentaires pour créer des connexions supplémentaires dont vous avez besoin.

Choisissez le type de connexion SP

Étapes

1. Accédez à **applications** > **intégration** > **connexions SP**.
2. Sélectionnez **Créer connexion**.
3. Sélectionnez **ne pas utiliser de modèle pour cette connexion**.
4. Sélectionnez **Browser SSO Profiles** et **SAML 2.0** comme protocole.

Importation des métadonnées SP

Étapes

1. Dans l'onglet Importer les métadonnées, sélectionnez **fichier**.
2. Choisissez le fichier de métadonnées SAML que vous avez téléchargé à partir de la page d'authentification unique StorageGRID pour le nœud d'administration.
3. Passez en revue le résumé des métadonnées et les informations fournies dans l'onglet Infos générales.

   L'ID d'entité du partenaire et le nom de connexion sont définis sur l'ID de connexion SP StorageGRID. (Par exemple, 10.96.105.200-DC1-ADM1-105-200). L'URL de base est l'adresse IP du nœud d'administration StorageGRID.

4. Sélectionnez **Suivant**.

Configurer SSO du navigateur IDP

Étapes

1. Dans l'onglet SSO du navigateur, sélectionnez **configurer SSO du navigateur**.
2. Dans l'onglet des profils SAML, sélectionnez les options **SSO** initiée par le SP, **SLO initial du SP**, **SSO initié par l'IDP** et **SLO** lancé par l'IDP.
3. Sélectionnez **Suivant**.
4. Dans l'onglet durée de vie de l'assertion, n'apportez aucune modification.
5. Dans l'onglet création d'assertion, sélectionnez **configurer la création d'assertion**.
   a. Dans l'onglet mappage d'identité, sélectionnez **Standard**.
   b. Dans l'onglet Contrat d'attribut, utilisez **SAML_SUBJECT** comme Contrat d'attribut et le format de nom non spécifié qui a été importé.
6. Pour prolonger le contrat, sélectionnez **Supprimer** pour supprimer le `urn:oid`, qui n'est pas utilisé.

Mapper l'instance de l'adaptateur

Étapes

1. Dans l'onglet mappage de la source d'authentification, sélectionnez **mappage d'une nouvelle instance de carte**.
2. Dans l'onglet instance de la carte, sélectionnez instance d'adaptateur vous avez créé.
3. Dans l'onglet méthode de mappage, sélectionnez **récupérer des attributs supplémentaires à partir d'un magasin de données**.
4. Dans l'onglet Source d'attribut et recherche utilisateur, sélectionnez **Ajouter une source d'attribut**.
5. Dans l'onglet magasin de données, fournissez une description et sélectionnez magasin de données que vous avez ajouté.
6. Dans l'onglet LDAP Directory Search :
   - Saisissez le **DN de base**, qui doit correspondre exactement à la valeur que vous avez saisie dans StorageGRID pour le serveur LDAP.
   - Pour l'étendue de la recherche, sélectionnez **sous-arbre**.
   - Pour la classe d'objet racine, recherchez l'attribut **objectGUID** et ajoutez-le.
7. Dans l'onglet types d'encodage d'attribut binaire LDAP, sélectionnez **Base64** pour l'attribut **objectGUID**.
8. Dans l'onglet filtre LDAP, entrez **sAMAccountName=${username}**.
9. Dans l'onglet attribut Contract Expédié par contrat, sélectionnez **LDAP (attribut)** dans la liste déroulante Source et sélectionnez **objectGUID** dans la liste déroulante valeur.
10. Vérifiez et enregistrez la source d'attribut.
11. Dans l'onglet Source de l'attribut FailSave, sélectionnez **abandonner la transaction SSO**.
12. Passez en revue le résumé et sélectionnez **Done**.
13. Sélectionnez **Done**.

Configurer les paramètres de protocole

Étapes

1. Dans l'onglet **connexion SP** > **connexion du navigateur SSO** > **Paramètres de protocole**, sélectionnez

configurer les paramètres de protocole.

2. Dans l'onglet URL du service client assertion, acceptez les valeurs par défaut qui ont été importées à partir des métadonnées SAML StorageGRID (**POST** pour la liaison et `/api/saml-response` Pour l'URL du point final).
3. Dans l'onglet URL du service SLO, acceptez les valeurs par défaut qui ont été importées à partir des métadonnées StorageGRID SAML (**REDIRECT** pour la liaison et `/api/saml-logout` Pour l'URL du point final.
4. Dans l'onglet Allowable SAML Bindings, désactivez **ARTEFACT** et **SOAP**. Seuls **POST** et **REDIRECT** sont requis.
5. Dans l'onglet Signature Policy, laissez les cases **exiger la signature des requêtes Authn** et **toujours signer l'assertion** cochées.
6. Dans l'onglet Stratégie de cryptage, sélectionnez **aucun**.
7. Consultez le résumé et sélectionnez **Done** pour enregistrer les paramètres du protocole.
8. Consultez le résumé et sélectionnez **Done** pour enregistrer les paramètres SSO du navigateur.

Configurer les informations d'identification

Étapes

1. Dans l'onglet connexion SP, sélectionnez **informations d'identification**.
2. Dans l'onglet informations d'identification, sélectionnez **configurer les informations d'identification**.
3. Sélectionner signature du certificat vous avez créé ou importé.
4. Sélectionnez **Suivant** pour accéder à **gérer les paramètres de vérification de signature**.
   a. Dans l'onglet modèle de confiance, sélectionnez **non ancré**.
   b. Dans l'onglet certificat de vérification de signature, vérifiez les informations de certificat de signature, qui ont été importées à partir des métadonnées SAML StorageGRID.
5. Passez en revue les écrans de résumé et sélectionnez **Enregistrer** pour enregistrer la connexion SP.

Créer des connexions SP supplémentaires

Vous pouvez copier la première connexion du processeur de service pour créer les connexions du processeur de service dont vous avez besoin pour chaque nœud d'administration de votre grille. Vous téléchargez de nouvelles métadonnées pour chaque copie.

> Les connexions SP des différents nœuds d'administration utilisent des paramètres identiques, à l'exception de l'ID d'entité du partenaire, de l'URL de base, de l'ID de connexion, du nom de connexion, de la vérification de signature, Et l'URL de réponse SLO.

Étapes

1. Sélectionnez **action** > **copie** pour créer une copie de la connexion SP initiale pour chaque nœud d'administration supplémentaire.
2. Entrez l'ID de connexion et le nom de connexion de la copie, puis sélectionnez **Enregistrer**.
3. Choisissez le fichier de métadonnées correspondant au nœud d'administration :
   a. Sélectionnez **action** > **mettre à jour avec métadonnées**.
   b. Sélectionnez **Choisissez fichier** et chargez les métadonnées.
   c. Sélectionnez **Suivant**.

d. Sélectionnez **Enregistrer**.

4. Résoudre l'erreur en raison de l'attribut inutilisé :
   a. Sélectionnez la nouvelle connexion.
   b. Sélectionnez **configurer le navigateur SSO > configurer la création d'assertion > Contrat d'attribut**.
   c. Supprimez l'entrée pour **urn:oid**.
   d. Sélectionnez **Enregistrer**.

Désactiver l'authentification unique

Vous pouvez désactiver l'authentification unique (SSO) si vous ne souhaitez plus utiliser cette fonctionnalité. Vous devez désactiver l'authentification unique avant de pouvoir désactiver la fédération des identités.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous disposez d'autorisations d'accès spécifiques.

Étapes

1. Sélectionnez **CONFIGURATION** > **contrôle d'accès** > **connexion unique**.

   La page authentification unique s'affiche.

2. Sélectionnez l'option **Disabled**.
3. Sélectionnez **Enregistrer**.

   Un message d'avertissement s'affiche pour indiquer que les utilisateurs locaux pourront maintenant se connecter.

4. Sélectionnez **OK**.

   La prochaine fois que vous vous connectez à StorageGRID, la page de connexion StorageGRID s'affiche et vous devez entrer le nom d'utilisateur et le mot de passe d'un utilisateur StorageGRID local ou fédéré.

Désactivez et réactivez temporairement l'authentification unique pour un nœud d'administration

Il se peut que vous ne puissiez pas vous connecter à Grid Manager si le système d'authentification unique (SSO) est en panne. Dans ce cas, vous pouvez temporairement désactiver et réactiver SSO pour un noeud d'administration. Pour désactiver puis réactiver SSO, vous devez accéder au shell de commande du nœud.

Avant de commencer

- Vous disposez d'autorisations d'accès spécifiques.
- Vous avez le `Passwords.txt` fichier.
- Vous connaissez le mot de passe de l'utilisateur racine local.

Description de la tâche

Après avoir désactivé SSO pour un noeud d'administration, vous pouvez vous connecter à Grid Manager en

tant qu'utilisateur racine local. Pour sécuriser votre système StorageGRID, vous devez utiliser le shell de commande du nœud pour réactiver SSO sur le nœud d'administration dès que vous vous déconnectez.

> La désactivation de SSO pour un nœud d'administration n'affecte pas les paramètres SSO pour les autres nœuds d'administration de la grille. La case **Activer SSO** de la page ouverture de session unique du gestionnaire de grille reste cochée et tous les paramètres SSO existants sont conservés, sauf si vous les mettez à jour.

Étapes

1. Connectez-vous à un nœud d'administration :
   a. Saisissez la commande suivante : `ssh admin@Admin_Node_IP`
   b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
   c. Entrez la commande suivante pour passer à la racine : `su -`
   d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

      Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

2. Exécutez la commande suivante :`disable-saml`

   Un message indique que la commande s'applique uniquement à ce nœud d'administration.

3. Confirmez que vous souhaitez désactiver l'authentification SSO.

   Un message indique que l'authentification unique est désactivée sur le nœud.

4. À partir d'un navigateur Web, accédez à Grid Manager sur le même nœud d'administration.

   La page de connexion à Grid Manager s'affiche car SSO a été désactivé.

5. Connectez-vous avec le nom d'utilisateur root et le mot de passe de l'utilisateur root local.
6. Si vous avez désactivé l'authentification SSO temporairement car vous avez besoin de corriger la configuration SSO :
   a. Sélectionnez **CONFIGURATION** > **contrôle d'accès** > **connexion unique**.
   b. Modifiez les paramètres SSO incorrects ou obsolètes.
   c. Sélectionnez **Enregistrer**.

      La sélection de **Enregistrer** sur la page ouverture de session unique permet de réactiver automatiquement SSO pour l'ensemble de la grille.

7. Si vous avez désactivé l'authentification SSO temporairement car vous devez accéder au Grid Manager pour une autre raison :
   a. Effectuez les tâches que vous souhaitez effectuer.
   b. Sélectionnez **se déconnecter** et fermez le Gestionnaire de grille.
   c. Réactivez SSO sur le nœud d'administration. Vous pouvez effectuer l'une des opérations suivantes :
      - Exécutez la commande suivante : `enable-saml`

        Un message indique que la commande s'applique uniquement à ce nœud d'administration.

Confirmez que vous souhaitez activer le SSO.

Un message indique que l'authentification unique est activée sur le nœud.

- Redémarrez le nœud grid : `reboot`

8. À partir d'un navigateur Web, accédez à Grid Manager à partir du même nœud d'administration.
9. Vérifiez que la page de connexion StorageGRID s'affiche et que vous devez saisir vos informations d'identification SSO pour accéder au Gestionnaire de grille.

Utiliser la fédération de grille

Qu'est-ce que la fédération de grille ?

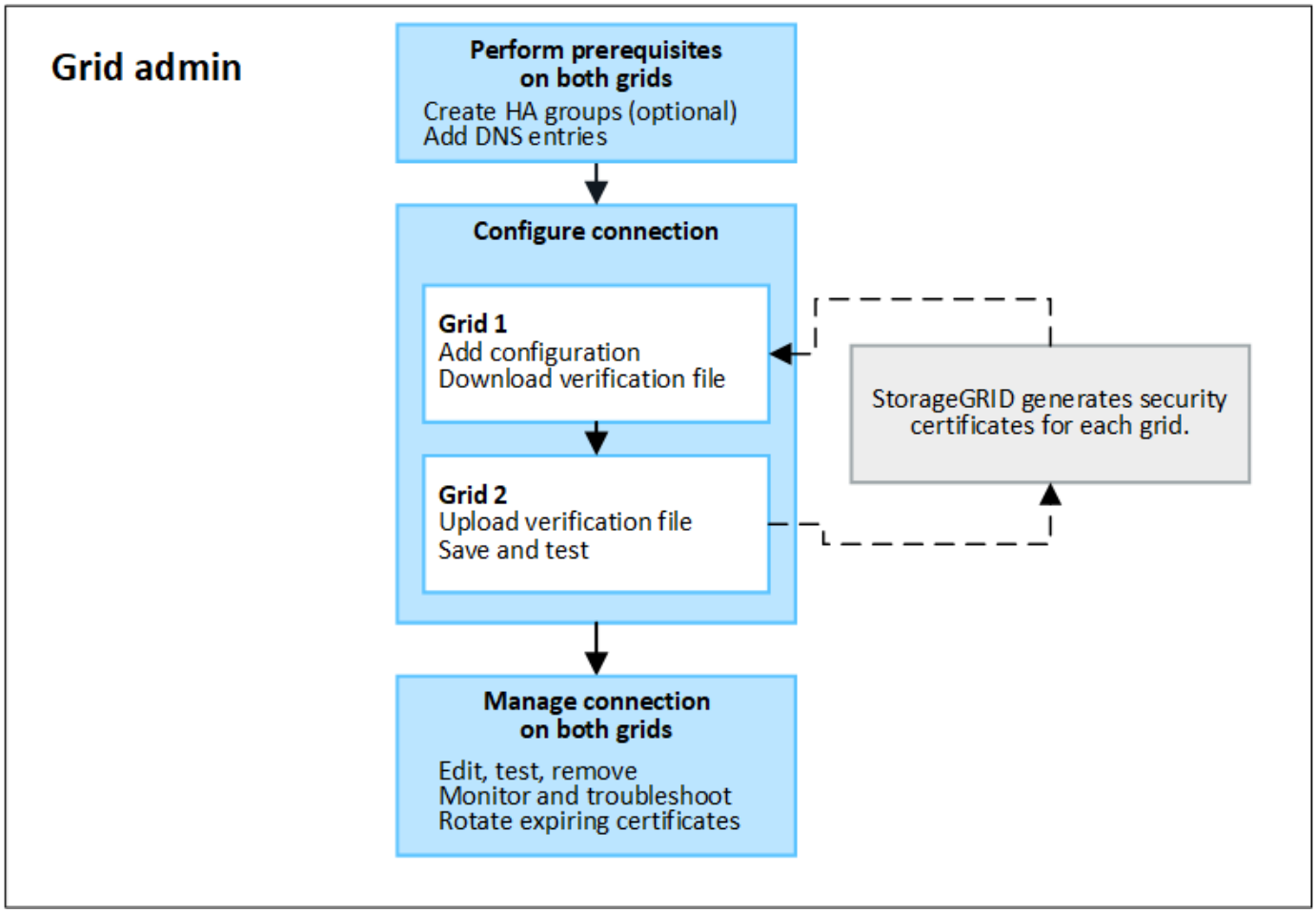
Vous pouvez utiliser la fédération de grid pour cloner les locataires et répliquer leurs objets entre deux systèmes StorageGRID à des fins de reprise après incident.

Qu'est-ce qu'une connexion de fédération de grille ?

Une connexion de fédération grid est une connexion bidirectionnelle, fiable et sécurisée entre les nœuds d'administration et de passerelle dans deux systèmes StorageGRID.

Flux de travail pour la fédération de grille

Le diagramme de flux de travail résume les étapes de configuration d'une connexion de fédération de grille entre deux grilles.



Considérations et conditions requises pour les connexions de fédération de grille

- Les deux grilles utilisées pour la fédération de grille doivent exécuter StorageGRID 11.7.
- Une grille peut avoir une ou plusieurs connexions de fédération de grille à d'autres grilles. Chaque connexion de fédération de grille est indépendante des autres connexions. Par exemple, si la grille 1 a une connexion avec la grille 2 et une seconde connexion avec la grille 3, il n'y a pas de connexion implicite entre la grille 2 et la grille 3.
- Les connexions de fédération de grille sont bidirectionnelles. Une fois la connexion établie, vous pouvez surveiller et gérer la connexion à partir de l'une ou l'autre grille.
- Au moins une connexion de fédération de grille doit exister avant que vous puissiez utiliser "clone de compte" ou "réplication entre plusieurs grilles".

Exigences en matière de mise en réseau et d'adresse IP

- Les connexions de fédération de grille peuvent se produire sur le réseau de grille, le réseau d'administration ou le réseau client.
- Une connexion de fédération de grille connecte une grille à une autre grille. La configuration de chaque grille spécifie un point de terminaison de fédération grid sur l'autre grille composé de nœuds d'administration, de nœuds de passerelle ou des deux.
- La meilleure pratique est de se connecter "Groupes haute disponibilité (HA)" De nœuds de passerelle et d'administration sur chaque grid. L'utilisation des groupes haute disponibilité permet de s'assurer que les connexions de fédération du grid resteront en ligne si les nœuds ne sont plus disponibles. En cas de défaillance de l'interface active de l'un ou l'autre groupe haute disponibilité, la connexion peut utiliser une

interface de sauvegarde.

- Il n'est pas recommandé de créer une connexion de fédération de grille qui utilise l'adresse IP d'un nœud d'administration ou d'un nœud de passerelle unique. Si le nœud devient indisponible, la connexion de fédération de grille devient également indisponible.
- "Réplication entre plusieurs grilles" D'objets exige que les nœuds de stockage de chaque grid puissent accéder aux nœuds d'administration et de passerelle configurés sur l'autre grid. Pour chaque grid, vérifiez que tous les nœuds de stockage disposent d'une route à large bande passante vers en tant que nœuds d'administration ou nœuds de passerelle utilisés pour la connexion.

Utilisez des FQDN pour équilibrer la charge de la connexion

Pour un environnement de production, utilisez des noms de domaine complets (FQDN) pour identifier chaque grille de la connexion. Créez ensuite les entrées DNS appropriées, comme suit :

- Le nom de domaine complet de la grille 1 est mappé à une ou plusieurs adresses IP virtuelles (VIP) pour les groupes haute disponibilité de la grille 1 ou à l'adresse IP d'un ou plusieurs nœuds d'administration ou de passerelle de la grille 1.
- Le nom de domaine complet de la grille 2 est mappé à une ou plusieurs adresses VIP pour la grille 2 ou à l'adresse IP d'un ou plusieurs nœuds d'administration ou de passerelle dans la grille 2.

Lorsque vous utilisez plusieurs entrées DNS, les demandes d'utilisation de la connexion sont équilibrées de la manière suivante :

- Les entrées DNS qui correspondent aux adresses VIP de plusieurs groupes haute disponibilité sont équilibrées de charge entre les nœuds actifs des groupes haute disponibilité.
- Les entrées DNS qui correspondent aux adresses IP de plusieurs nœuds d'administration ou nœuds de passerelle sont équilibrées de charge entre les nœuds mappés.

Configuration requise pour les ports

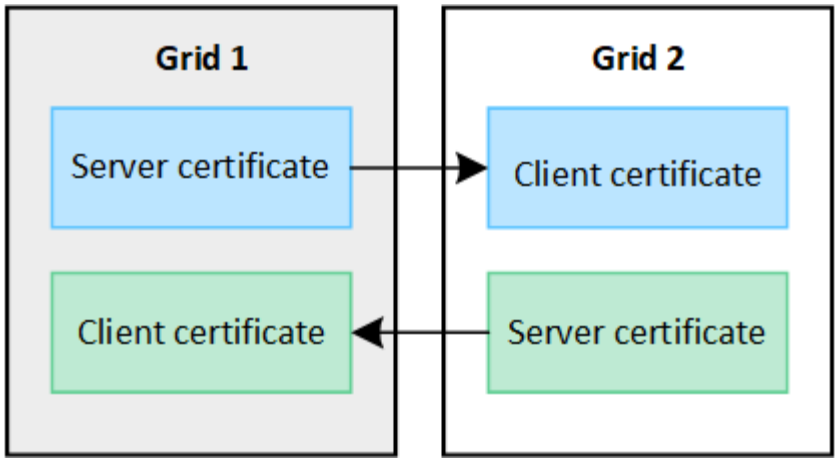
Lors de la création d'une connexion de fédération de grille, vous pouvez spécifier tout numéro de port inutilisé compris entre 23000 et 23999. Les deux grilles de cette connexion utilisent le même port.

Vous devez vous assurer qu'aucun nœud d'une grille n'utilise ce port pour d'autres connexions.

Exigences en matière de certificat

Lorsque vous configurez une connexion de fédération de grille, StorageGRID génère automatiquement quatre certificats SSL :

- Certificats de serveur et de client pour authentifier et crypter les informations envoyées de la grille 1 à la grille 2
- Certificats de serveur et de client pour authentifier et crypter les informations envoyées de la grille 2 à la grille 1



Par défaut, les certificats sont valides pendant 730 jours (2 ans). Lorsque ces certificats sont proches de leur date d'expiration, l'alerte **expiration du certificat de fédération GRID** vous rappelle de faire pivoter les certificats, ce que vous pouvez faire à l'aide de Grid Manager.

> Si les certificats à l'une des extrémités de la connexion expirent, la connexion cesse de fonctionner. La réplication des données sera en attente jusqu'à la mise à jour des certificats.

En savoir plus >>

- "Créer des connexions de fédération de grille"
- "Gérer les connexions de fédération de grille"
- "Dépanner les erreurs de fédération de grille"

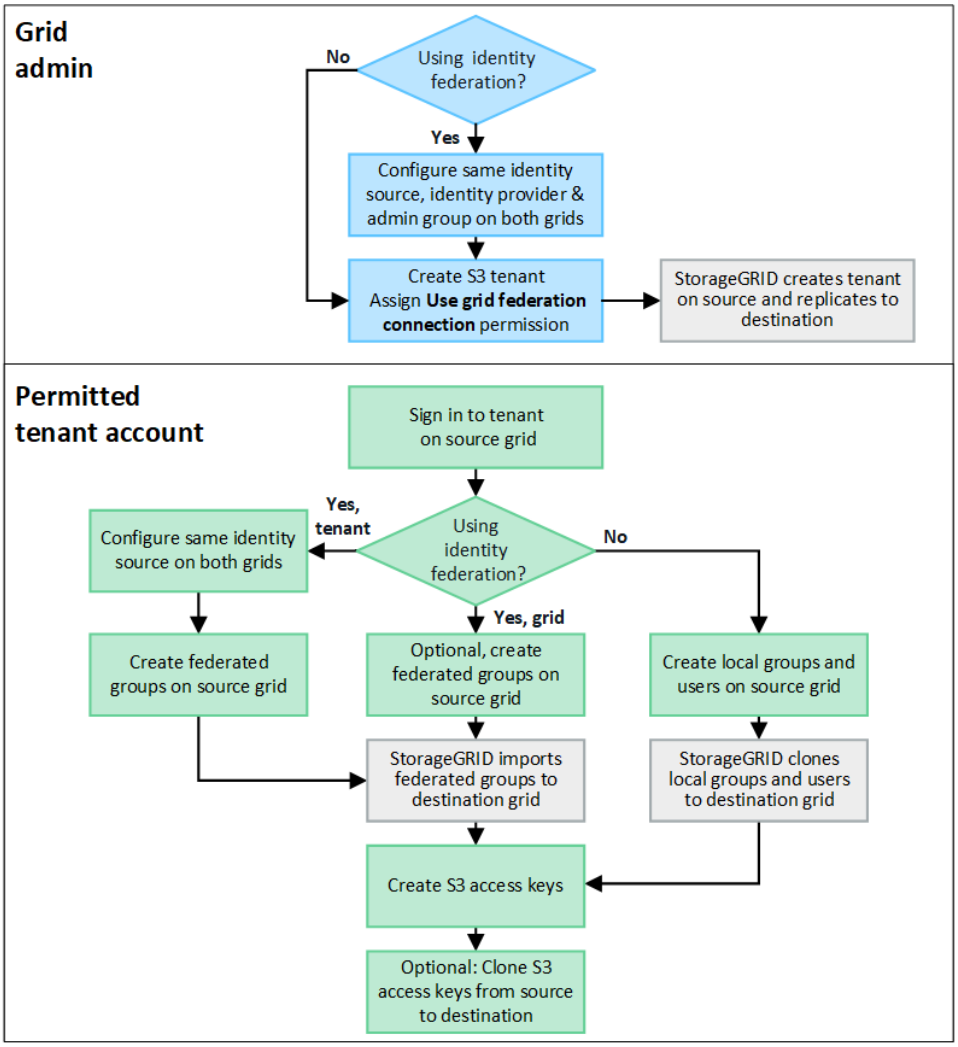
Qu'est-ce que le clone du compte ?

Le clone du compte correspond à la réplication automatique d'un compte de locataire, de groupes de locataires, d'utilisateurs de locataires et, éventuellement, Clés d'accès S3 entre les systèmes StorageGRID dans un "connexion de fédération de grille".

Le clone du compte est requis pour "réplication entre plusieurs grilles". Le clonage des informations de compte d'un système StorageGRID source vers un système StorageGRID de destination permet de s'assurer que les utilisateurs et groupes de locataires peuvent accéder aux compartiments et objets correspondants dans les deux grilles.

Workflow de clonage de compte

Le schéma de workflow présente les étapes que les administrateurs du grid et les locataires autorisés doivent suivre pour configurer le clone de compte. Ces étapes sont effectuées après le "la connexion de fédération de grille est configurée".



Workflow d'administration du grid

Les étapes effectuées par les administrateurs du grid dépendent du système StorageGRID du "connexion de fédération de grille" Utilisez l'authentification unique (SSO) ou la fédération des identités.

configurer SSO pour le clone de compte (facultatif)

Si l'un des systèmes StorageGRID de la connexion de fédération de grille utilise SSO, les deux grilles doivent utiliser SSO. Avant de créer les comptes de tenant pour la fédération de grille, les administrateurs de grille pour les grilles source et de destination du locataire doivent effectuer ces étapes.

Étapes

1. Configurez le même référentiel d'identité pour les deux grilles. Voir "Utiliser la fédération des identités".
2. Configurez le même fournisseur d'identité SSO pour les deux grilles. Voir "Configurer l'authentification unique".
3. "Créez le même groupe d'administration" sur les deux grilles en important le même groupe fédéré.

   Lorsque vous créez le tenant, vous sélectionnez ce groupe pour obtenir l'autorisation d'accès racine initiale pour les comptes de tenant source et de destination.

Si ce groupe d'administration n'existe pas sur les deux grilles avant la création du tenant, celui-ci n'est pas répliqué vers la destination.

configurer la fédération des identités au niveau de la grille pour le clone de compte (facultatif)

Si l'un ou l'autre des systèmes StorageGRID utilise la fédération des identités sans SSO, les deux grilles doivent utiliser la fédération des identités. Avant de créer les comptes de tenant pour la fédération de grille, les administrateurs de grille pour les grilles source et de destination du locataire doivent effectuer ces étapes.

Étapes

1. Configurez le même référentiel d'identité pour les deux grilles. Voir "Utiliser la fédération des identités".
2. Si un groupe fédéré dispose d'une autorisation d'accès racine initiale pour les comptes de tenant source et de destination, "créez le même groupe d'administration" sur les deux grilles en important le même groupe fédéré.

   Si vous attribuez l'autorisation d'accès racine à un groupe fédéré qui n'existe pas sur les deux grilles, le tenant n'est pas répliqué sur la grille de destination.

3. Si vous ne souhaitez pas qu'un groupe fédéré dispose d'une autorisation d'accès racine initiale pour les deux comptes, spécifiez un mot de passe pour l'utilisateur root local.

Créez un compte de locataire S3 autorisé

Après avoir configuré éventuellement une SSO ou une fédération d'identités, un administrateur du grid effectue ces étapes pour déterminer quels locataires peuvent répliquer des objets de compartiment vers d'autres systèmes StorageGRID.

Étapes

1. Déterminez la grille source du locataire pour les opérations de clonage de compte.

   La grille dans laquelle le locataire est créé à l'origine est appelée *grille source* du locataire. La grille dans laquelle le locataire est répliqué est appelée *grille de destination* du locataire.

2. Créez un compte locataire S3 sur cette grille.
3. Attribuez l'autorisation **utiliser la connexion de fédération de grille**.
4. Si le compte de tenant gère ses propres utilisateurs fédérés, attribuez l'autorisation **utiliser son propre référentiel d'identité**.

   Si cette autorisation est attribuée, les comptes de tenant source et de destination doivent configurer le même référentiel d'identité avant de créer des groupes fédérés. Les groupes fédérés ajoutés au locataire source ne peuvent pas être clonés dans le locataire de destination sauf si les deux grilles utilisent le même référentiel d'identité.

5. Sélectionnez une connexion de fédération de grille spécifique.
6. Enregistrez le locataire.

   Lorsqu'un nouveau locataire avec l'autorisation **utiliser la connexion de fédération de grille** est enregistré, StorageGRID crée automatiquement une réplique de ce locataire sur l'autre grille, comme suit :

   - Les deux comptes de tenant possèdent les mêmes ID de compte, nom, quota de stockage et autorisations attribuées.

- Si vous avez sélectionné un groupe fédéré pour obtenir l'autorisation d'accès racine pour le tenant, ce groupe est cloné vers le tenant de destination.
- Si vous avez sélectionné un utilisateur local pour obtenir l'autorisation d'accès racine pour le locataire, cet utilisateur est cloné vers le locataire de destination. Toutefois, le mot de passe de cet utilisateur n'est pas cloné.

Pour plus de détails, voir"Gestion des locataires autorisés pour la fédération dans le grid".

Workflow de compte de locataire autorisé

Après la réplication d'un locataire doté de l'autorisation **utiliser la connexion de fédération GRID** dans la grille de destination, les comptes de locataires autorisés peuvent effectuer ces étapes pour cloner des groupes de locataires, des utilisateurs et des clés d'accès S3.

Étapes

1. Connectez-vous au compte du locataire sur la grille source du locataire.
2. Si vous êtes autorisé, configurez la fédération d'identification sur les comptes de locataire source et de destination.
3. Créez des groupes et des utilisateurs sur le locataire source.

   Lorsque de nouveaux groupes ou utilisateurs sont créés sur le locataire source, StorageGRID les clone automatiquement dans le locataire de destination, mais aucun clonage n'a lieu de la destination vers la source.

4. Création de clés d'accès S3
5. Vous pouvez également cloner les clés d'accès S3 du locataire source vers le locataire de destination.

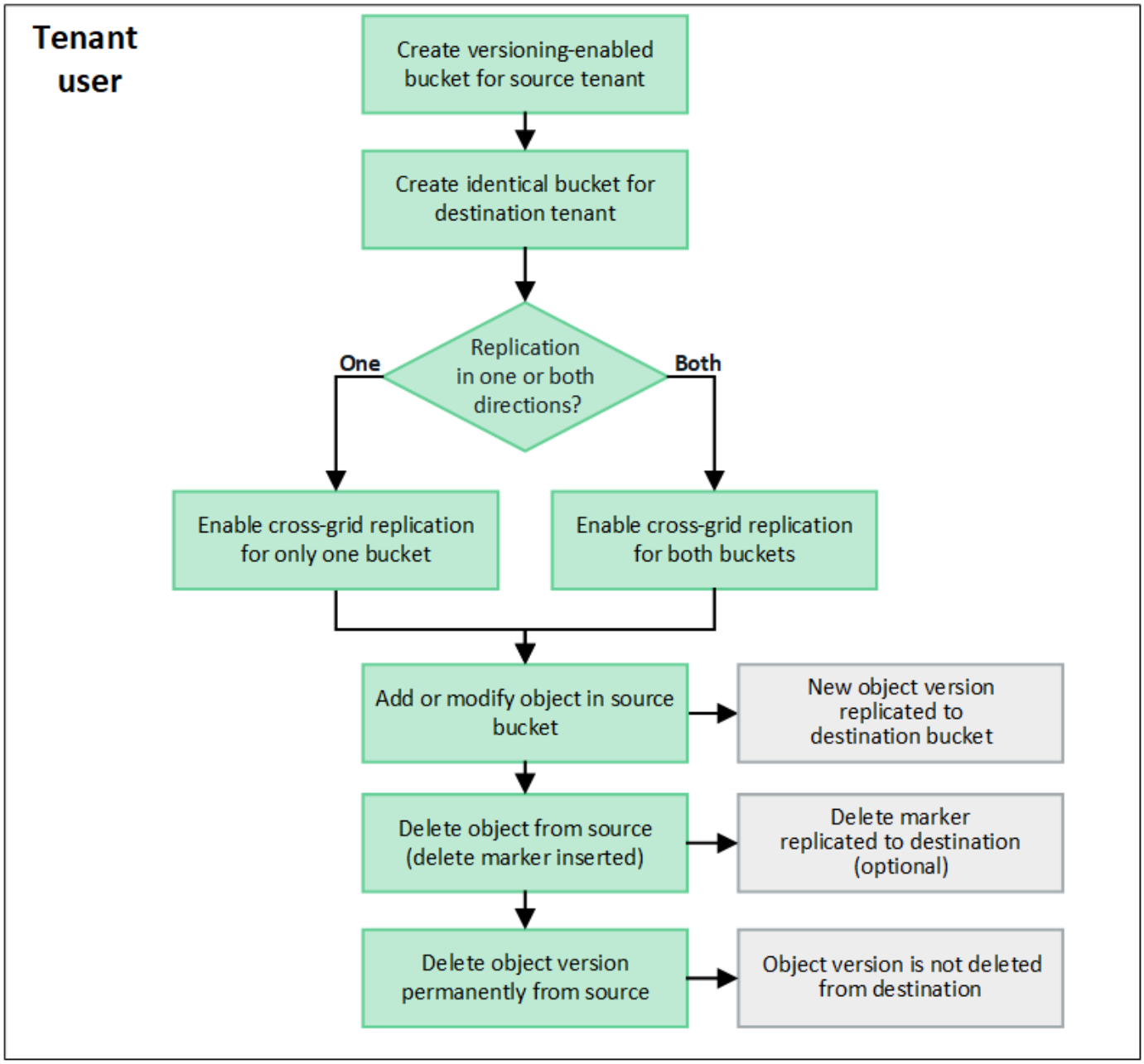
Pour en savoir plus sur le workflow des comptes de locataires autorisés et sur le clonage des groupes, des utilisateurs et des clés d'accès S3, reportez-vous à la section "Cloner des groupes de locataires et des utilisateurs" et "Cloner les clés d'accès S3 à l'aide de l'API".

Qu'est-ce que la réplication inter-grid ?

La réplication inter-grid est la réplication automatique d'objets entre des compartiments S3 sélectionnés dans deux systèmes StorageGRID connectés dans un "connexion de fédération de grille". "Clone de compte" est nécessaire pour la réplication entre les grilles.

Flux de production pour la réplication entre les grilles

Le diagramme de flux de travail résume les étapes de configuration de la réplication inter-grille entre les compartiments sur deux grilles.



Conditions requises pour la réplication entre les grilles

Si un compte de locataire dispose de l'autorisation **utiliser la connexion de fédération de grille** pour utiliser un ou plusieurs comptes "connexions de fédération de grille", Un utilisateur de tenant disposant de l'autorisation d'accès racine peut créer des compartiments identiques dans les comptes de tenant correspondants sur chaque grille. Ces compartiments :

- Doit avoir le même nom et la même région
- La gestion des versions doit être activée
- Le verrouillage d'objet S3 doit être désactivé
- Doit être vide

Une fois les deux compartiments créés, la réplication inter-grid peut être configurée pour l'un ou l'autre des compartiments, ou pour les deux.

En savoir plus >>

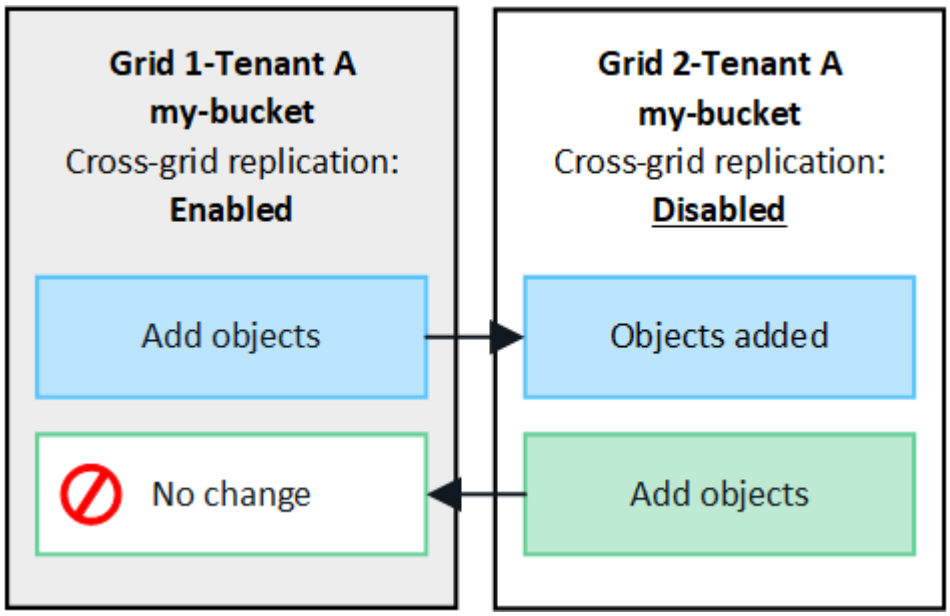
"Gérer la réplication entre les grilles"

Fonctionnement de la réplication entre les grilles

La réplication inter-grille peut être configurée pour se produire dans une direction ou dans les deux directions.

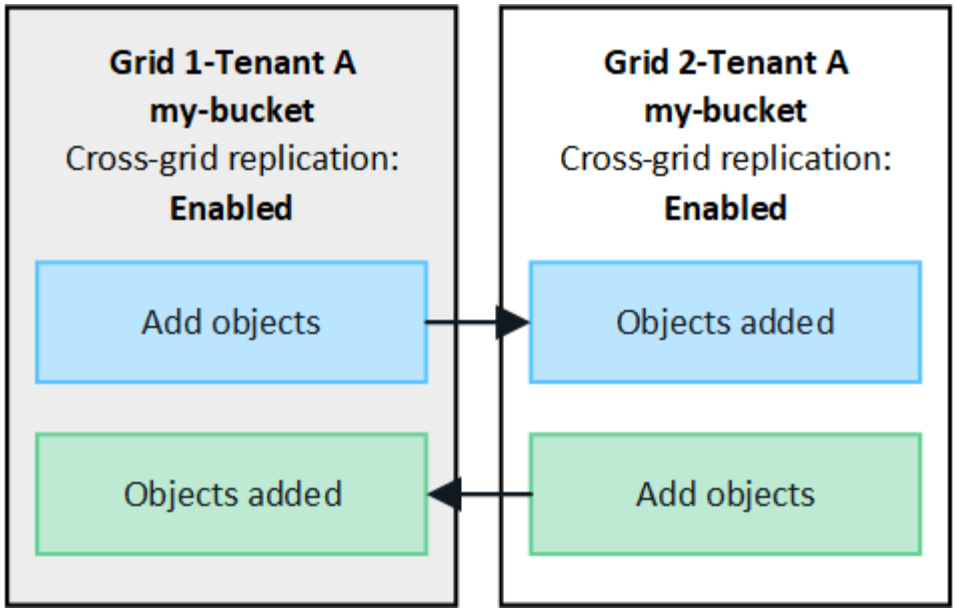
Réplication dans une direction

Si vous activez la réplication inter-grid pour un compartiment sur une seule grille, les objets ajoutés à ce compartiment (le compartiment source) sont répliqués dans le compartiment correspondant de l'autre grille (le compartiment de destination). Toutefois, les objets ajoutés au compartiment de destination ne sont pas répliqués à nouveau vers la source. Dans la figure, la réplication inter-grid est activée pour `my-bucket` De la grille 1 à la grille 2, mais elle n'est pas activée dans l'autre sens.



Réplication dans les deux sens

Si vous activez la réplication inter-grid pour le même compartiment sur les deux grilles, les objets ajoutés à l'un des compartiments sont répliqués sur l'autre grille. Dans la figure, la réplication inter-grid est activée pour `my-bucket` dans les deux sens.



Que se passe-t-il lorsque des objets sont ingérés ?

Lorsqu'un client S3 ajoute un objet à un compartiment pour lequel la réplication inter-grid est activée, les événements suivants se produisent :

1. StorageGRID réplique automatiquement l'objet depuis le compartiment source vers le compartiment de destination. Le temps nécessaire pour effectuer cette opération de réplication en arrière-plan dépend de plusieurs facteurs, dont le nombre d'autres opérations de réplication en attente.

   Le client S3 peut vérifier l'état de réplication d'un objet en émettant une requête GET Object ou HEAD Object. La réponse inclut un élément spécifique à StorageGRID `x-ntap-sg-cgr-replication-status` En-tête de réponse, qui aura l'une des valeurs suivantes : le client S3 peut vérifier l'état de réplication d'un objet en émettant une requête GET Object ou HEAD Object. La réponse inclut un élément spécifique à StorageGRID `x-ntap-sg-cgr-replication-status` en-tête de réponse, qui aura l'une des valeurs suivantes :

Grille	État de la réplication
Source	• **SUCCÈS** : la réplication a réussi pour toutes les connexions de grille. • **EN ATTENTE** : l'objet n'a pas été répliqué vers au moins une connexion de grille. • **ÉCHEC** : la réplication n'est pas en attente pour une connexion de grille et au moins une a échoué avec une défaillance permanente. L'utilisateur doit résoudre l'erreur.
Destination	**RÉPLIQUE** : l'objet a été répliqué à partir de la grille source.

   > StorageGRID ne prend pas en charge le `x-amz-replication-status` en-tête.

2. StorageGRID utilise la règle ILM active de chaque grid pour gérer les objets, comme n'importe quel autre objet. Par exemple, l'objet A sur la grille 1 peut être stocké sous forme de deux copies répliquées et conservé indéfiniment, tandis que la copie de l'objet A répliqué sur la grille 2 peut être stockée avec un

code d'effacement 2+1 et supprimée après trois ans.

Que se passe-t-il lorsque des objets sont supprimés ?

Comme décrit dans "Supprimer le flux de données", StorageGRID peut supprimer un objet pour l'une des raisons suivantes :

- Le client S3 émet une demande de suppression.
- Un utilisateur tenant Manager sélectionne le "Supprime les objets du compartiment" option permettant de supprimer tous les objets d'un compartiment.
- Le compartiment dispose d'une configuration en cycle de vie, qui expire.
- La dernière période de la règle ILM pour l'objet se termine et aucun autre placement n'est spécifié.

Lorsque StorageGRID supprime un objet en raison d'une opération de suppression d'objets dans un compartiment, d'expiration du cycle de vie du compartiment ou d'expiration du placement ILM, l'objet répliqué n'est jamais supprimé d'une autre grille d'une connexion de fédération de grid. Toutefois, les marqueurs de suppression ajoutés au compartiment source par les suppressions du client S3 peuvent éventuellement être répliqués dans le compartiment de destination.

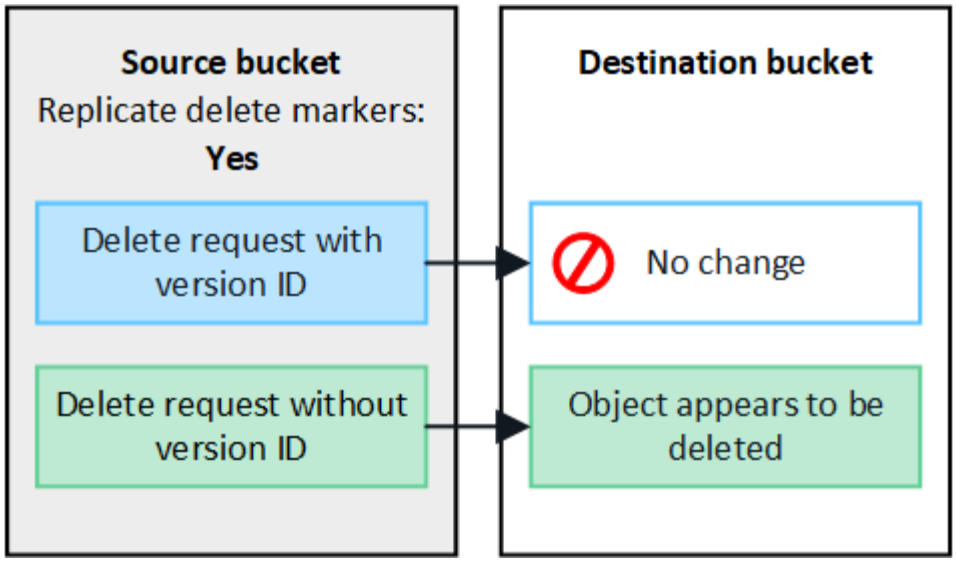
Pour comprendre ce qui se passe lorsqu'un client S3 supprime des objets d'un compartiment dans lequel la réplication inter-grid est activée, vérifiez comment les clients S3 suppriment des objets des compartiments pour lesquels la gestion de version est activée, comme suit :

- Si un client S3 émet une demande de suppression qui inclut un ID de version, cette version de l'objet est définitivement supprimée. Aucun marqueur de suppression n'est ajouté au godet.
- Si un client S3 émet une demande de suppression qui n'inclut pas d'ID de version, StorageGRID ne supprime aucune version d'objet. Au lieu de cela, il ajoute un marqueur de suppression au godet. Avec le marqueur de suppression, StorageGRID agit comme si l'objet avait été supprimé :
  - Une demande GET sans ID de version échoue avec `404 No Object Found`
  - Une demande GET avec un ID de version valide réussit et renvoie la version d'objet demandée.

Lorsqu'un client S3 supprime un objet d'un compartiment pour lequel la réplication inter-grid est activée, StorageGRID détermine s'il faut répliquer la demande de suppression vers la destination, comme suit :

- Si la demande de suppression inclut un ID de version, cette version d'objet est définitivement supprimée de la grille source. Cependant, StorageGRID ne réplique pas les demandes de suppression qui incluent un ID de version, de sorte que la même version d'objet n'est pas supprimée de la destination.
- Si la demande de suppression n'inclut pas d'ID de version, StorageGRID peut éventuellement répliquer le marqueur de suppression en fonction de la configuration de la réplication inter-grid pour le compartiment :
  - Si vous choisissez de répliquer les marqueurs de suppression (par défaut), un marqueur de suppression est ajouté au compartiment source et répliqué vers le compartiment de destination. En effet, l'objet semble être supprimé sur les deux grilles.
  - Si vous choisissez de ne pas répliquer les marqueurs de suppression, un marqueur de suppression est ajouté au compartiment source, mais il n'est pas répliqué vers le compartiment de destination. En effet, les objets supprimés de la grille source ne sont pas supprimés de la grille de destination.

Dans la figure, **replicate delete marqueurs** a été défini sur **Yes** quand "la réplication inter-grid a été activée". Les demandes de suppression du compartiment source qui incluent un ID de version ne supprimera pas les objets du compartiment de destination. Les demandes de suppression pour le compartiment source qui n'incluent pas d'ID de version apparaissent pour supprimer des objets dans le compartiment de destination.



Si vous souhaitez garder les suppressions d'objets synchronisées entre les grilles, créez les éléments correspondants "Configurations de cycle de vie S3" pour les compartiments des deux grilles.

Mode de réplication des objets chiffrés

Lorsque vous répliquez les objets entre les grilles à l'aide de la réplication multigrille, vous pouvez chiffrer des objets individuels, utiliser le chiffrement de compartiment par défaut ou configurer le chiffrement au niveau de la grille. Vous pouvez ajouter, modifier ou supprimer les paramètres de chiffrement de compartiment ou de grille par défaut avant ou après l'activation de la réplication entre plusieurs grilles pour un compartiment.

Pour chiffrer des objets individuels, vous pouvez utiliser SSE (chiffrement côté serveur avec des clés gérées par StorageGRID) lors de l'ajout des objets au compartiment source. Utilisez le `x-amz-server-side-encryption` demandez l'en-tête et spécifiez `AES256`. Voir "Utilisez le cryptage côté serveur".

L'utilisation de SSE-C (chiffrement côté serveur avec clés fournies par le client) n'est pas prise en charge pour la réplication inter-grille. L'opération d'acquisition échoue.

Pour utiliser le chiffrement par défaut pour un compartiment, utilisez une demande DE chiffrement DE compartiment PUT et définissez le `SSEAlgorithm` paramètre à `AES256`. Le chiffrement au niveau du compartiment s'applique à tous les objets ingérés sans le `x-amz-server-side-encryption` en-tête de demande. Voir "Opérations sur les compartiments".

Pour utiliser le cryptage au niveau de la grille, définissez l'option **Stored object Encryption** sur **AES-256**. Le chiffrement au niveau du grid s'applique aux objets qui ne sont pas chiffrés au niveau du compartiment ou qui sont ingérés sans le `x-amz-server-side-encryption` en-tête de demande. Voir "Configurez les options réseau et objet".

SSE ne prend pas en charge AES-128. Si l'option **Stored object Encryption** est activée pour la grille source à l'aide de l'option **AES-128**, l'utilisation de l'algorithme AES-128 ne sera pas propagée à l'objet répliqué. À la place, l'objet répliqué utilisera le paramètre de chiffrement par défaut du compartiment ou de la grille de destination, le cas échéant.

Lors de la détermination du mode de chiffrement des objets source, StorageGRID applique les règles suivantes :

1. Utilisez le `x-amz-server-side-encryption` récupérer l'en-tête, le cas échéant.
2. Si aucun en-tête d'ingestion n'est présent, utilisez le paramètre de chiffrement par défaut du compartiment, s'il est configuré.
3. Si aucun paramètre de compartiment n'est configuré, utilisez le paramètre de chiffrement au niveau de la grille, si celui-ci est configuré.
4. Si aucun paramètre de grille n'est présent, ne chiffrez pas l'objet source.

Pour déterminer comment chiffrer les objets répliqués, StorageGRID applique les règles suivantes dans l'ordre suivant :

1. Utilisez le même chiffrement que l'objet source, sauf si cet objet utilise le chiffrement AES-128.
2. Si l'objet source n'est pas chiffré ou utilise la norme AES-128, utilisez le paramètre de chiffrement par défaut du compartiment de destination, s'il est configuré.
3. Si le compartiment de destination ne possède pas de paramètre de chiffrement, utilisez le paramètre de chiffrement de la grille de destination, si celui-ci est configuré.
4. Si aucun paramètre de grille n'est présent, ne chiffrez pas l'objet de destination.

LE balisage PUT Object et le balisage DELETE Object ne sont pas pris en charge

LES demandes DE balisage ET de SUPPRESSION D'objets PUT ne sont pas prises en charge pour les objets situés dans des compartiments pour lesquels la réplication entre les grilles est activée.

Si un client S3 émet une requête DE balisage D'objets PUT ou DE SUPPRESSION d'objets, `501 Not Implemented` est renvoyé. Le message est `Put(Delete) ObjectTagging is not available for buckets that have cross-grid replication configured`.

Comment les objets segmentés sont répliqués

La taille de segment maximale de la grille source s'applique aux objets répliqués sur la grille de destination. Lorsque des objets sont répliqués dans une autre grille, le paramètre **taille de segment maximale** (**CONFIGURATION** > **système** > **Options de stockage**) de la grille source sera utilisé sur les deux grilles. Par exemple, supposons que la taille de segment maximale de la grille source soit de 1 Go, alors que la taille de segment maximale de la grille de destination est de 50 Mo. Si vous ingérer un objet de 2 Go sur la grille source, cet objet est enregistré en tant que deux segments de 1 Go. Il sera également répliqué sur la grille de destination sous forme de deux segments de 1 Go, même si la taille maximale de segment de cette grille est de 50 Mo.

Comparez la réplication entre les grilles et la réplication CloudMirror

Lorsque vous commencez à utiliser la fédération de grille, examinez les similitudes et les différences entre "réplication entre plusieurs grilles" et le "Service de réplication StorageGRID CloudMirror".

	Réplication entre plusieurs grilles	Service de réplication CloudMirror
Quel est l'objectif principal ?	Un système StorageGRID agit comme un système de reprise après incident. Les objets d'un compartiment peuvent être répliqués entre les grilles dans une ou les deux directions.	Permet à un locataire de répliquer automatiquement les objets à partir d'un compartiment dans StorageGRID (source) vers un compartiment S3 externe (destination). La réplication CloudMirror crée une copie indépendante d'un objet dans une infrastructure S3 indépendante. Cette copie indépendante n'est pas utilisée comme sauvegarde, mais elle est souvent traitée dans le cloud.
Comment est-il configuré ?	1. Configurer une connexion de fédération de grille entre deux grilles. 2. Ajoutez de nouveaux comptes de locataires, qui sont automatiquement clonés dans l'autre grid. 3. Ajoutez de nouveaux groupes de locataires et utilisateurs qui sont également clonés. 4. Créez les compartiments correspondants sur chaque grille et activez la réplication inter-grille dans une ou les deux directions.	1. Un utilisateur de locataire configure la réplication CloudMirror en définissant un terminal CloudMirror (adresse IP, identifiants, etc.) à l'aide du Gestionnaire des locataires ou de l'API S3. 2. Tout compartiment appartenant à ce compte de locataire peut être configuré de manière à pointer vers le terminal CloudMirror.
Qui est responsable de sa configuration ?	• Un administrateur du grid configure la connexion et les locataires. • Les utilisateurs locataires configurent les groupes, les utilisateurs, les clés et les compartiments.	Généralement, un utilisateur locataire.
Quelle est la destination ?	Un compartiment S3 correspondant et identique sur l'autre système StorageGRID dans la connexion de fédération du grid.	• Toute infrastructure S3 compatible (y compris Amazon S3) • Google Cloud Platform (GCP)
La gestion des versions d'objets est-elle requise ?	Oui, la gestion des versions d'objet doit être activée dans les compartiments source et de destination.	Non, la réplication CloudMirror prend en charge toute combinaison de compartiments sans version et avec version sur la source et la destination.

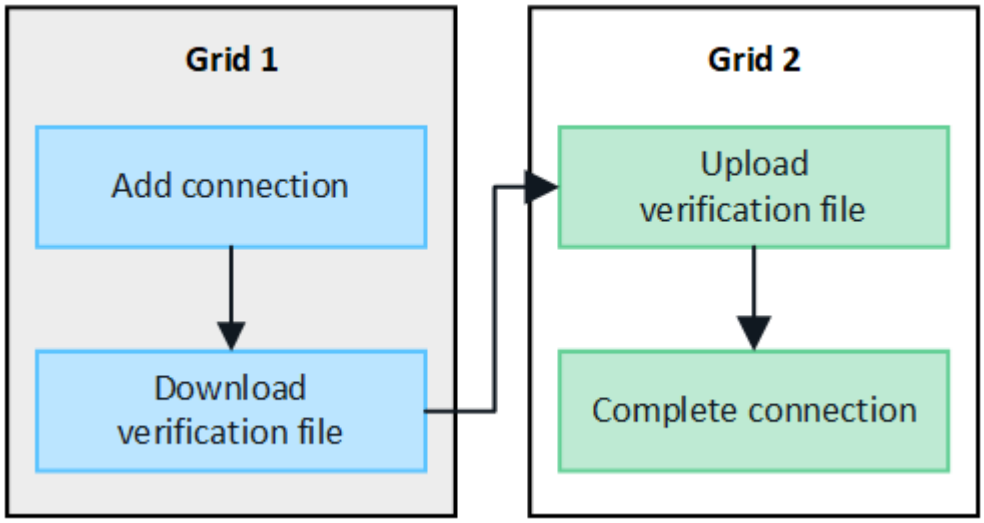
	Réplication entre plusieurs grilles	Service de réplication CloudMirror
Pourquoi déplacer des objets vers la destination ?	Les objets sont automatiquement répliqués lorsque ceux-ci sont ajoutés à un compartiment sur lequel la réplication inter-grid est activée.	Les objets sont automatiquement répliqués lorsqu'ils sont ajoutés à un compartiment qui a été configuré avec un terminal CloudMirror. Les objets qui existaient dans le compartiment source avant la configuration du compartiment avec le point de terminaison CloudMirror ne sont pas répliqués, sauf s'ils ont été modifiés.
Comment les objets sont-ils répliqués ?	La réplication inter-grid crée des objets versionnés et réplique l'ID de version du compartiment source vers le compartiment de destination. Cela permet de maintenir l'ordre des versions sur les deux grilles.	La réplication CloudMirror ne nécessite pas de compartiments prenant en charge la gestion des versions. CloudMirror peut donc uniquement gérer les commandes d'une clé au sein d'un site. Il n'y a aucune garantie que la commande sera maintenue pour les demandes à un objet sur un site différent.
Que se passe-t-il si un objet ne peut pas être répliqué ?	L'objet est placé dans la file d'attente de réplication, en fonction des limites de stockage des métadonnées.	L'objet est mis en file d'attente pour la réplication, sous réserve des limites des services de plate-forme (voir "Recommandations relatives à l'utilisation des services de plate-forme").
Les métadonnées système de l'objet sont-elles répliquées ?	Oui, lorsqu'un objet est répliqué sur l'autre grille, les métadonnées de son système sont également répliquées. Les métadonnées seront identiques sur les deux grilles.	Non. Lorsqu'un objet est répliqué vers un compartiment externe, les métadonnées de son système sont mises à jour. Les métadonnées diffèrent d'un emplacement à l'autre, selon le moment de l'ingestion et le comportement de l'infrastructure S3 indépendante.
Comment les objets sont-ils récupérés ?	Les applications peuvent récupérer ou lire les objets en faisant une demande au compartiment sur les deux grilles.	Les applications peuvent récupérer ou lire les objets en faisant une requête vers StorageGRID ou vers la destination S3. Supposons, par exemple, que vous utilisiez la réplication CloudMirror pour mettre en miroir les objets dans une organisation partenaire. Le partenaire peut utiliser ses propres applications pour lire ou mettre à jour les objets directement à partir de la destination S3. Utiliser StorageGRID n'est pas nécessaire.

	Réplication entre plusieurs grilles	Service de réplication CloudMirror
Que se passe-t-il si un objet est supprimé ?	• Les demandes de suppression comprenant un ID de version ne sont jamais répliquées dans la grille de destination. • Les demandes de suppression qui n'incluent pas d'ID de version ajoutent un marqueur de suppression au compartiment source, qui peut éventuellement être répliqué vers la grille de destination. • Si la réplication inter-grid est configurée pour une seule direction, les objets du compartiment de destination peuvent être supprimés sans affecter la source.	Les résultats varient en fonction de l'état de gestion des versions des compartiments source et destination (qui ne doivent pas nécessairement être identiques) : • Si les deux compartiments sont versionnés, une demande de suppression ajoute un marqueur de suppression aux deux emplacements. • Si seul le compartiment source est versionné, une demande de suppression ajoute un marqueur de suppression à la source, mais pas à la destination. • Si aucun compartiment n'est versionné, une demande de suppression supprime l'objet de la source mais pas de la destination. De même, les objets du compartiment de destination peuvent être supprimés sans affecter la source.

Créer des connexions de fédération de grille

Vous pouvez créer une connexion de fédération de grille entre deux systèmes StorageGRID si vous souhaitez cloner les détails du locataire et répliquer les données d'objet.

Comme illustré dans la figure, la création d'une connexion de fédération de grille inclut des étapes sur les deux grilles. Vous ajoutez la connexion sur une grille et la remplissez sur l'autre grille. Vous pouvez commencer à partir de n'importe quelle grille.



Avant de commencer

- Vous avez passé en revue le "considérations et exigences" pour configurer les connexions de fédération de grille.
- Si vous prévoyez d'utiliser des noms de domaine complets (FQDN) pour chaque grille au lieu d'adresses IP ou VIP, vous savez quels noms utiliser et vous avez confirmé que le serveur DNS de chaque grille contient les entrées appropriées.
- Vous utilisez un "navigateur web pris en charge".
- Vous devez disposer des droits d'accès racine et de la phrase de passe de provisionnement pour les deux grilles.

Ajouter une connexion

Effectuez ces étapes sur l'un des deux systèmes StorageGRID.

Étapes

1. Connectez-vous au Grid Manager à partir du nœud d'administration principal de l'une des grilles.
2. Sélectionnez **CONFIGURATION** > **système** > **fédération de grille**.
3. Sélectionnez **Ajouter une connexion**.
4. Entrez les détails de la connexion.

Champ	Description
Nom de la connexion	Un nom unique pour vous aider à reconnaître cette connexion, par exemple « grille 1-grille 2 ».
FQDN ou IP pour cette grille	L'une des options suivantes : • Nom de domaine complet de la grille dans laquelle vous êtes actuellement connecté • Adresse VIP d'un groupe haute disponibilité sur cette grille • Adresse IP d'un nœud d'administration ou d'un nœud de passerelle sur cette grille. L'adresse IP peut se trouver sur n'importe quel réseau que la grille de destination peut atteindre.
Port	Le port que vous souhaitez utiliser pour cette connexion. Vous pouvez entrer n'importe quel numéro de port inutilisé compris entre 23000 et 23999. Les deux grilles de cette connexion utilisent le même port. Vous devez vous assurer qu'aucun nœud d'une grille n'utilise ce port pour d'autres connexions.
Jours de validité du certificat pour cette grille	Nombre de jours pendant lesquels vous souhaitez que les certificats de sécurité pour cette grille dans la connexion soient valides. La valeur par défaut est 730 jours (2 ans), mais vous pouvez entrer une valeur comprise entre 1 et 762 jours. StorageGRID génère automatiquement des certificats client et serveur pour chaque grille lorsque vous enregistrez la connexion.

Champ	Description
Phrase secrète de provisionnement pour cette grille	Phrase secrète de provisionnement de la grille à laquelle vous êtes connecté.
FQDN ou IP pour l'autre grille	L'une des options suivantes : • Nom de domaine complet de la grille à laquelle vous souhaitez vous connecter • Adresse VIP d'un groupe HA sur l'autre grid • Adresse IP d'un nœud d'administration ou d'un nœud de passerelle sur l'autre grille. L'adresse IP peut se trouver sur n'importe quel réseau que la grille source peut atteindre.

5. Sélectionnez **Enregistrer et continuer**.
6. Pour l'étape Télécharger le fichier de vérification, sélectionnez **Télécharger le fichier de vérification**.

   Une fois la connexion terminée sur l'autre grille, vous ne pouvez plus télécharger le fichier de vérification depuis l'une ou l'autre grille.

7. Localisez le fichier téléchargé (*connection-name*`.grid-federation`), et enregistrez-le dans un endroit sûr.

   > ⚠ Ce fichier contient des secrets (masqués en tant que *****) et d'autres détails sensibles et doivent être stockés et transmis en toute sécurité.

8. Sélectionnez **Fermer** pour revenir à la page de fédération de grille.
9. Vérifiez que la nouvelle connexion est affichée et que son **état de connexion** est **en attente de connexion**.
10. Fournir le *connection-name*`.grid-federation` vers l'administrateur grid de l'autre grid.

Connexion complète

Procédez comme suit sur le système StorageGRID auquel vous vous connectez (l'autre grille).

Étapes

1. Connectez-vous au Grid Manager à partir du nœud d'administration principal.
2. Sélectionnez **CONFIGURATION** > **système** > **fédération de grille**.
3. Sélectionnez **Télécharger le fichier de vérification** pour accéder à la page Télécharger.
4. Sélectionnez **Télécharger le fichier de vérification**. Ensuite, recherchez et sélectionnez le fichier téléchargé à partir de la première grille (*connection-name*`.grid-federation`).

   Les détails de la connexion sont affichés.

5. Vous pouvez également saisir un nombre différent de jours valides pour les certificats de sécurité de cette grille. Par défaut, l'entrée **Certificate valid Days** correspond à la valeur que vous avez entrée sur la première grille, mais chaque grille peut utiliser des dates d'expiration différentes.

   En général, utilisez le même nombre de jours pour les certificats des deux côtés de la connexion.

Si les certificats à l'une des extrémités de la connexion expirent, la connexion cesse de fonctionner et les réplications sont en attente jusqu'à ce que les certificats soient mis à jour.

6. Saisissez la phrase de passe de provisionnement pour la grille à laquelle vous êtes actuellement connecté.
7. Sélectionnez **Enregistrer et tester**.

   Les certificats sont générés et la connexion est testée. Si la connexion est valide, un message de réussite s'affiche et la nouvelle connexion apparaît sur la page de fédération de grille. **État de la connexion** sera **connecté**.

   Si un message d'erreur s'affiche, résoudre les problèmes éventuels. Voir "Dépanner les erreurs de fédération de grille".

8. Accédez à la page grid federation sur la première grille et actualisez le navigateur. Vérifiez que l'état de la **connexion** est maintenant **connecté**.
9. Une fois la connexion établie, supprimez de manière sécurisée toutes les copies du fichier de vérification.

   Si vous modifiez cette connexion, un nouveau fichier de vérification sera créé. Le fichier d'origine ne peut pas être réutilisé.

Une fois que vous avez terminé

- Consultez les éléments à prendre en compte pour "gestion des locataires autorisés".
- "Créez un ou plusieurs nouveaux comptes de locataire", Attribuez l'autorisation **utiliser la connexion de fédération de grille** et sélectionnez la nouvelle connexion.
- "Gérer la connexion" selon les besoins. Vous pouvez modifier les valeurs de connexion, tester une connexion, faire pivoter les certificats de connexion ou supprimer une connexion.
- "Surveiller la connexion" Dans le cadre de vos activités de surveillance StorageGRID normales.
- "Dépanner la connexion", y compris la résolution des alertes et erreurs liées au clone de compte et à la réplication inter-grille.

Gérer les connexions de fédération de grille

La gestion des connexions de fédération de grille entre les systèmes StorageGRID inclut la modification des détails de connexion, la rotation des certificats, la suppression des autorisations de locataire et la suppression des connexions inutilisées.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille sur l'une des grilles à l'aide d'un "navigateur web pris en charge".
- Vous disposez de l'autorisation d'accès racine pour la grille à laquelle vous êtes connecté.

modifiez une connexion de fédération de grille

Vous pouvez modifier une connexion de fédération de grille en vous connectant au nœud d'administration principal sur l'une des grilles de la connexion. Après avoir apporté des modifications à la première grille, vous devez télécharger un nouveau fichier de vérification et le télécharger sur l'autre grille.

Pendant la modification de la connexion, les demandes de réplication de clone de compte ou de grille croisée continueront à utiliser les paramètres de connexion existants. Toutes les modifications apportées à la première grille sont enregistrées localement, mais ne sont utilisées qu'après avoir été téléchargées sur la deuxième grille, enregistrées et testées.

Commencez à modifier la connexion

Étapes

1. Connectez-vous au Grid Manager à partir du nœud d'administration principal de l'une des grilles.
2. Sélectionnez **NODES** et confirmez que tous les autres noeuds Admin de votre système sont en ligne.

   Lorsque vous modifiez une connexion de fédération grid, StorageGRID tente d'enregistrer un fichier « configuration candidate » sur tous les nœuds d'administration de la première grille. Si ce fichier ne peut pas être enregistré sur tous les nœuds d'administration, un message d'avertissement s'affiche lorsque vous sélectionnez **Enregistrer et tester**.

3. Sélectionnez **CONFIGURATION** > **système** > **fédération de grille**.
4. Modifiez les détails de la connexion à l'aide du menu **actions** de la page de fédération de la grille ou de la page de détails d'une connexion spécifique. Voir "Créer des connexions de fédération de grille" pour quoi participer.

   Menu actions

   a. Sélectionnez le bouton radio de la connexion.
   b. Sélectionnez **actions** > **Modifier**.
   c. Entrez les nouvelles informations.

   Page de détails

   a. Sélectionnez un nom de connexion pour afficher ses détails.
   b. Sélectionnez **Modifier**.
   c. Entrez les nouvelles informations.

5. Saisissez la phrase de passe de provisionnement pour la grille à laquelle vous êtes connecté.
6. Sélectionnez **Enregistrer et continuer**.

   Les nouvelles valeurs sont enregistrées, mais elles ne seront pas appliquées à la connexion tant que vous n'aurez pas téléchargé le nouveau fichier de vérification sur l'autre grille.

7. Sélectionnez **Télécharger le fichier de vérification**.

   Pour télécharger ce fichier ultérieurement, rendez-vous sur la page de détails de la connexion.

8. Localisez le fichier téléchargé (*`connection-name`*`.grid-federation`), et enregistrez-le dans un endroit sûr.

   Le fichier de vérification contient des secrets et doit être stocké et transmis en toute sécurité.

9. Sélectionnez **Fermer** pour revenir à la page de fédération de grille.
10. Vérifiez que l'état de la **connexion** est **en attente de modification**.

> Si l'état de la connexion était autre que **connecté** lorsque vous avez commencé à modifier la connexion, il ne passera pas à **modification en attente**.

11. Fournir le *`connection-name`*`.grid-federation` vers l'administrateur grid de l'autre grid.

Terminer la modification de la connexion

Terminez la modification de la connexion en téléchargeant le fichier de vérification sur l'autre grille.

Étapes

1. Connectez-vous au Grid Manager à partir du nœud d'administration principal.
2. Sélectionnez **CONFIGURATION** > **système** > **fédération de grille**.
3. Sélectionnez **Télécharger le fichier de vérification** pour accéder à la page de téléchargement.
4. Sélectionnez **Télécharger le fichier de vérification**. Ensuite, recherchez et sélectionnez le fichier téléchargé à partir de la première grille.
5. Saisissez la phrase de passe de provisionnement pour la grille à laquelle vous êtes actuellement connecté.
6. Sélectionnez **Enregistrer et tester**.

   Si la connexion peut être établie à l'aide des valeurs modifiées, un message de réussite s'affiche. Sinon, un message d'erreur s'affiche. Passez en revue le message et répondez à tout problème.

7. Fermez l'assistant pour revenir à la page de fédération de grille.
8. Vérifiez que l'état de la **connexion** est **connecté**.
9. Accédez à la page grid federation sur la première grille et actualisez le navigateur. Vérifiez que l'état de la **connexion** est maintenant **connecté**.
10. Une fois la connexion établie, supprimez de manière sécurisée toutes les copies du fichier de vérification.

Tester une connexion de fédération de grille

Étapes

1. Connectez-vous au Grid Manager à partir du nœud d'administration principal.
2. Sélectionnez **CONFIGURATION** > **système** > **fédération de grille**.
3. Testez la connexion à l'aide du menu **actions** de la page de fédération de la grille ou de la page de détails d'une connexion spécifique.

   Menu actions

   a. Sélectionnez le bouton radio de la connexion.
   b. Sélectionnez **actions** > **Test**.

   Page de détails

   a. Sélectionnez un nom de connexion pour afficher ses détails.
   b. Sélectionnez **Tester la connexion**.

4. Vérifiez l'état de la connexion :

État de la connexion	Description
Connecté	Les deux grilles sont connectées et communiquent normalement.
Erreur	La connexion est en état d'erreur. Par exemple, un certificat a expiré ou une valeur de configuration n'est plus valide.
Modification en attente	Vous avez modifié la connexion sur cette grille, mais la connexion utilise toujours la configuration existante. Pour terminer la modification, téléchargez le nouveau fichier de vérification sur l'autre grille.
En attente de connexion	Vous avez configuré la connexion sur cette grille, mais la connexion n'a pas été effectuée sur l'autre grille. Téléchargez le fichier de vérification à partir de cette grille et téléchargez-le sur l'autre grille.
Inconnu	La connexion est dans un état inconnu, probablement en raison d'un problème de mise en réseau ou d'un nœud hors ligne.

5. Si l'état de la connexion est **Error**, résolvez les problèmes éventuels. Ensuite, sélectionnez de nouveau **Tester la connexion** pour confirmer que le problème a été résolu.

faire pivoter les certificats de connexion

Chaque connexion de fédération de grille utilise quatre certificats SSL générés automatiquement pour sécuriser la connexion. Lorsque les deux certificats de chaque grille sont proches de leur date d'expiration, l'alerte **expiration du certificat de fédération GRID** vous rappelle de faire pivoter les certificats.

> ⚠ Si les certificats à l'une des extrémités de la connexion expirent, la connexion cesse de fonctionner et les réplications sont en attente jusqu'à ce que les certificats soient mis à jour.

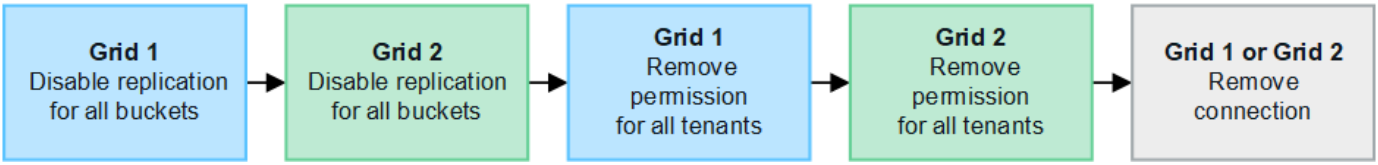
Étapes

1. Connectez-vous au Grid Manager à partir du nœud d'administration principal de l'une des grilles.
2. Sélectionnez **CONFIGURATION** > **système** > **fédération de grille**.
3. Dans l'un des onglets de la page fédération de grille, sélectionnez le nom de la connexion pour afficher ses détails.
4. Sélectionnez l'onglet **certificats**.
5. Sélectionnez **faire pivoter les certificats**.
6. Spécifiez le nombre de jours pendant lesquels les nouveaux certificats doivent être valides.
7. Saisissez la phrase de passe de provisionnement pour la grille à laquelle vous êtes connecté.
8. Sélectionnez **faire pivoter les certificats**.
9. Si nécessaire, répétez ces étapes sur l'autre grille de la connexion.

   En général, utilisez le même nombre de jours pour les certificats des deux côtés de la connexion.

supprime une connexion de fédération de grille

Vous pouvez supprimer une connexion de fédération de grille de l'une des grilles de la connexion. Comme indiqué dans la figure, vous devez effectuer les étapes préalables sur les deux grilles pour confirmer que la connexion n'est pas utilisée par un locataire sur l'une ou l'autre des grilles.



Avant de supprimer une connexion, notez les points suivants :

- La suppression d'une connexion ne supprime pas les éléments qui ont déjà été copiés entre les grilles. Par exemple, les utilisateurs de tenant, les groupes et les objets qui existent sur les deux grilles ne sont pas supprimés de l'une ou l'autre de ces grilles lorsque l'autorisation du tenant est supprimée. Si vous souhaitez supprimer ces éléments, vous devez les supprimer manuellement des deux grilles.
- Lorsque vous supprimez une connexion, la réplication de tous les objets en attente de réplication (ingérés mais pas encore répliqués sur l'autre grille) échouera définitivement.

Désactivez la réplication pour tous les compartiments de locataires

Étapes

1. À partir de l'une des grilles, connectez-vous au Gestionnaire de grille à partir du nœud d'administration principal.
2. Sélectionnez **CONFIGURATION** > **système** > **fédération de grille**.
3. Sélectionnez le nom de la connexion pour afficher ses détails.
4. Dans l'onglet **locataires autorisés**, déterminez si la connexion est utilisée par un locataire.
5. Si des locataires sont répertoriés, demandez à tous les locataires de le faire "désactiver la réplication entre les grilles" pour tous leurs compartiments sur les deux grilles dans la connexion.

> Vous ne pouvez pas supprimer l'autorisation **utiliser la connexion de fédération de grille** si une réplication de type cross-grid est activée dans des compartiments de tenant. Chaque compte de locataire doit désactiver la réplication inter-grid pour ses compartiments sur les deux grilles.

Supprimer l'autorisation pour chaque locataire

Une fois la réplication multigrille désactivée pour tous les compartiments de tenant, supprimez l'autorisation **utiliser la fédération de grid** de tous les locataires sur les deux grilles.

Étapes

1. Sélectionnez **CONFIGURATION** > **système** > **fédération de grille**.
2. Sélectionnez le nom de la connexion pour afficher ses détails.
3. Pour chaque locataire de l'onglet **locataires autorisés**, supprimez l'autorisation **utiliser la connexion de fédération de grille** de chaque locataire. Voir "Gérer les locataires autorisés".
4. Répétez ces étapes pour les locataires autorisés sur l'autre grille.

Déposer la connexion

Étapes

1. Lorsqu'aucun locataire de l'une ou l'autre grille n'utilise la connexion, sélectionnez **Supprimer**.
2. Vérifiez le message de confirmation et sélectionnez **Supprimer**.
   - Si la connexion peut être supprimée, un message de réussite s'affiche. La connexion de fédération de grille est maintenant supprimée des deux grilles.
   - Si la connexion ne peut pas être supprimée (par exemple, elle est toujours en cours d'utilisation ou si une erreur de connexion s'est produite), un message d'erreur s'affiche. Vous pouvez effectuer l'une des opérations suivantes :
     - Résolvez l'erreur (recommandé). Voir "Dépanner les erreurs de fédération de grille".
     - Déposer la connexion par la force. Voir la section suivante.

supprime une connexion de fédération de grille par force

Si nécessaire, vous pouvez forcer la suppression d'une connexion qui n'a pas l'état **Connected**.

La suppression forcée supprime uniquement la connexion de la grille locale. Pour supprimer complètement la connexion, effectuez les mêmes étapes sur les deux grilles.

Étapes

1. Dans la boîte de dialogue de confirmation, sélectionnez **forcer la suppression**.

   Un message de réussite s'affiche. Cette connexion de fédération de grille ne peut plus être utilisée. Cependant, la réplication entre les compartiments de locataires peut toujours être activée et certaines copies d'objet peuvent avoir déjà été répliquées entre les grilles dans la connexion.

2. À partir de l'autre grille de la connexion, connectez-vous au Gestionnaire de grille à partir du nœud d'administration principal.
3. Sélectionnez **CONFIGURATION** > **système** > **fédération de grille**.
4. Sélectionnez le nom de la connexion pour afficher ses détails.
5. Sélectionnez **Supprimer** et **Oui**.
6. Sélectionnez **forcer la suppression** pour supprimer la connexion de cette grille.

Gérer les locataires autorisés pour la fédération dans le grid

Vous pouvez autoriser les nouveaux comptes de locataires S3 à utiliser une connexion de fédération grid entre deux systèmes StorageGRID. Lorsque les locataires sont autorisés à utiliser une connexion, des étapes spéciales sont requises pour modifier les détails du locataire ou pour supprimer définitivement l'autorisation d'un locataire d'utiliser la connexion.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille sur l'une des grilles à l'aide d'un "navigateur web pris en charge".
- Vous disposez de l'autorisation d'accès racine pour la grille à laquelle vous êtes connecté.
- Vous avez "créé une connexion de fédération de grille" entre deux grilles.

- Vous avez examiné les flux de travail pour "clone de compte" et "réplication entre plusieurs grilles".
- Si nécessaire, vous avez déjà configuré l'authentification unique (SSO) ou la fédération d'identification pour les deux grilles de la connexion. Voir "Qu'est-ce que le clone de compte".

Créez un locataire autorisé

Si vous souhaitez autoriser un compte de locataire à utiliser une connexion de fédération de grille pour le clone de compte et la réplication entre les grilles, suivez les instructions générales à "Créer un locataire S3" et notez ce qui suit :

- Vous pouvez créer le locataire à partir de l'une ou l'autre grille dans la connexion. La grille dans laquelle un locataire est créé est la *grille source du locataire*.
- L'état de la connexion doit être **connecté**.
- Vous ne pouvez sélectionner l'autorisation **utiliser la connexion de fédération de grille** que lorsque vous créez un nouveau locataire S3. Vous ne pouvez pas activer cette autorisation lorsque vous modifiez un locataire existant.
- Lorsque le nouveau locataire est enregistré sur la première grille, un locataire identique est automatiquement répliqué sur l'autre grille. La grille dans laquelle le locataire est répliqué est la grille de destination du locataire_.
- Les locataires des deux grilles auront les mêmes ID de compte, nom, description, quota et autorisations à 20 chiffres. Vous pouvez également utiliser le champ **Description** pour identifier le locataire source et le locataire de destination. Par exemple, cette description pour un locataire créé sur la grille 1 s'affiche également pour le locataire répliqué sur la grille 2 : « ce locataire a été créé sur la grille 1 ».
- Pour des raisons de sécurité, le mot de passe d'un utilisateur root local n'est pas copié dans la grille de destination.

> Pour qu'un utilisateur root local puisse se connecter au tenant répliqué sur la grille de destination, un administrateur de grille pour cette grille doit "modifiez le mot de passe de l'utilisateur root local".

- Une fois le nouveau tenant disponible sur les deux grilles, les utilisateurs de tenant peuvent effectuer les opérations suivantes :
  - Dans la grille source du locataire, créez des groupes et des utilisateurs locaux qui sont automatiquement clonés dans la grille de destination du locataire. Voir "Cloner des groupes de locataires et des utilisateurs".
  - Créez de nouvelles clés d'accès S3, qui peuvent être clonées sur la grille de destination du locataire. Voir "Cloner les clés d'accès S3 à l'aide de l'API".
  - Créez des compartiments identiques sur les deux grilles dans la connexion et activez la réplication de type grille dans une direction ou dans les deux directions. Voir "Gérer la réplication entre les grilles".

Afficher un locataire autorisé

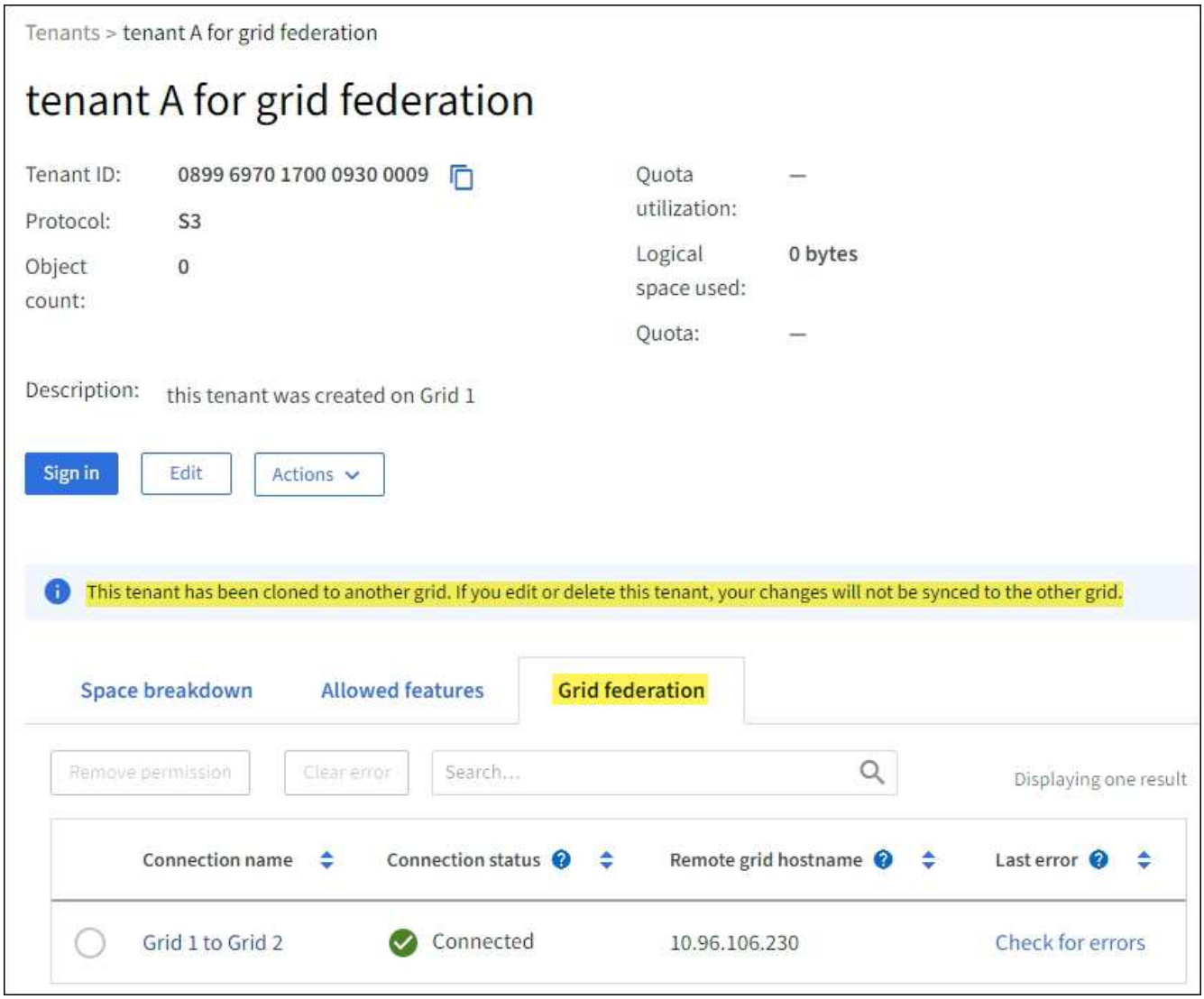
Vous pouvez afficher les détails d'un locataire autorisé à utiliser une connexion de fédération de grille.

Étapes

1. Sélectionnez **LOCATAIRES**.
2. Sur la page tenants, sélectionnez le nom du locataire pour afficher la page des détails du locataire.

   S'il s'agit de la grille source du locataire (c'est-à-dire si le locataire a été créé sur cette grille), une bannière

apparaît pour vous rappeler que le locataire a été cloné dans une autre grille. Si vous modifiez ou supprimez ce locataire, vos modifications ne seront pas synchronisées avec l'autre grille.



3. Sélectionnez éventuellement l'onglet **grid federation** pour "surveillez la connexion de fédération de grille".

Modifier un locataire autorisé

Si vous devez modifier un locataire doté de l'autorisation **utiliser la connexion de fédération de grille**, suivez les instructions générales de "modification d'un compte de locataire" et notez ce qui suit :

- Si un locataire dispose de l'autorisation **utiliser la connexion de fédération de grille**, vous pouvez modifier les détails du locataire à partir de l'une des grilles de la connexion. Toutefois, les modifications que vous apportez ne seront pas copiées dans l'autre grille. Si vous souhaitez que les détails du locataire restent synchronisés entre les grilles, vous devez effectuer les mêmes modifications sur les deux grilles.
- Vous ne pouvez pas effacer l'autorisation **utiliser la connexion de fédération de grille** lorsque vous modifiez un locataire.
- Vous ne pouvez pas sélectionner une autre connexion de fédération de grille lorsque vous modifiez un locataire.

Supprimer un locataire autorisé

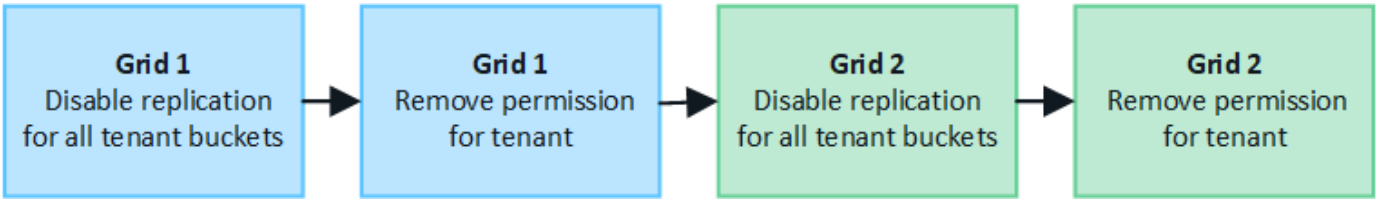
Si vous devez supprimer un locataire doté de l'autorisation **utiliser la connexion de fédération de grille**, suivez les instructions générales pour "suppression d'un compte de locataire" et notez ce qui suit :

- Avant de pouvoir supprimer le locataire d'origine sur la grille source, vous devez supprimer toutes les rubriques du compte sur la grille source.
- Avant de supprimer le locataire cloné sur la grille de destination, vous devez supprimer tous les compartiments du compte de la grille de destination.
- Si vous supprimez le locataire d'origine ou cloné, le compte ne peut plus être utilisé pour la réplication entre les grilles.
- Si vous supprimez le locataire d'origine sur la grille source, tous les groupes de locataires, utilisateurs ou clés clonés dans la grille de destination ne seront pas affectés. Vous pouvez soit supprimer le locataire cloné, soit lui permettre de gérer ses propres groupes, utilisateurs, clés d'accès et compartiments.
- Si vous supprimez le locataire cloné sur la grille de destination, des erreurs de clonage se produisent si de nouveaux groupes ou utilisateurs sont ajoutés au locataire d'origine.

  Pour éviter ces erreurs, supprimez l'autorisation du locataire d'utiliser la connexion de fédération de grille avant de supprimer le locataire de cette grille.

Supprimer l'autorisation de connexion utiliser la fédération de grille

Pour empêcher un locataire d'utiliser une connexion de fédération de grille, vous devez supprimer l'autorisation **utiliser la connexion de fédération de grille**.



Avant de supprimer l'autorisation d'un locataire d'utiliser une connexion de fédération de grille, notez ce qui suit :

- La suppression de l'autorisation **utiliser la connexion de fédération de grille** d'un locataire est une action permanente. Vous ne pouvez pas réactiver l'autorisation pour ce locataire.
- Vous ne pouvez pas supprimer l'autorisation **utiliser la connexion de fédération de grille** si la réplication inter-grille est activée pour l'un des compartiments du locataire. Le compte de locataire doit d'abord désactiver la réplication inter-grid pour tous ses compartiments.
- La suppression de l'autorisation **utiliser la connexion de fédération de grille** ne supprime pas les éléments qui ont déjà été répliqués entre les grilles. Par exemple, les utilisateurs, groupes et objets de tenant qui existent sur les deux grilles ne sont pas supprimés de l'une ou l'autre des grilles lorsque l'autorisation du tenant est supprimée. Si vous souhaitez supprimer ces éléments, vous devez les supprimer manuellement des deux grilles.

Avant de commencer

- Vous utilisez un "navigateur web pris en charge".
- Vous disposez de l'autorisation d'accès racine pour les deux grilles.

Désactivez la réplication pour les compartiments de locataires

Dans un premier temps, désactivez la réplication inter-grid pour tous les compartiments de locataires.

Étapes

1. À partir de l'une des grilles, connectez-vous au Gestionnaire de grille à partir du nœud d'administration principal.
2. Sélectionnez **CONFIGURATION** > **système** > **fédération de grille**.
3. Sélectionnez le nom de la connexion pour afficher ses détails.
4. Dans l'onglet **locataires autorisés**, déterminez si le locataire utilise la connexion.
5. Si le locataire est répertorié, demandez-lui de le faire "désactiver la réplication entre les grilles" pour tous leurs compartiments sur les deux grilles dans la connexion.

> Vous ne pouvez pas supprimer l'autorisation **utiliser la connexion de fédération de grille** si une réplication de type cross-grid est activée dans des compartiments de tenant. Le locataire doit désactiver la réplication inter-grid pour ses compartiments sur les deux grilles.

Supprimer l'autorisation pour le locataire

Une fois la réplication multigrille désactivée pour les compartiments de tenant, vous pouvez supprimer l'autorisation du locataire d'utiliser la connexion de fédération GRID.

Étapes

1. Connectez-vous au Grid Manager à partir du nœud d'administration principal.
2. Supprimez l'autorisation de la page grid federation ou de la page tenants.

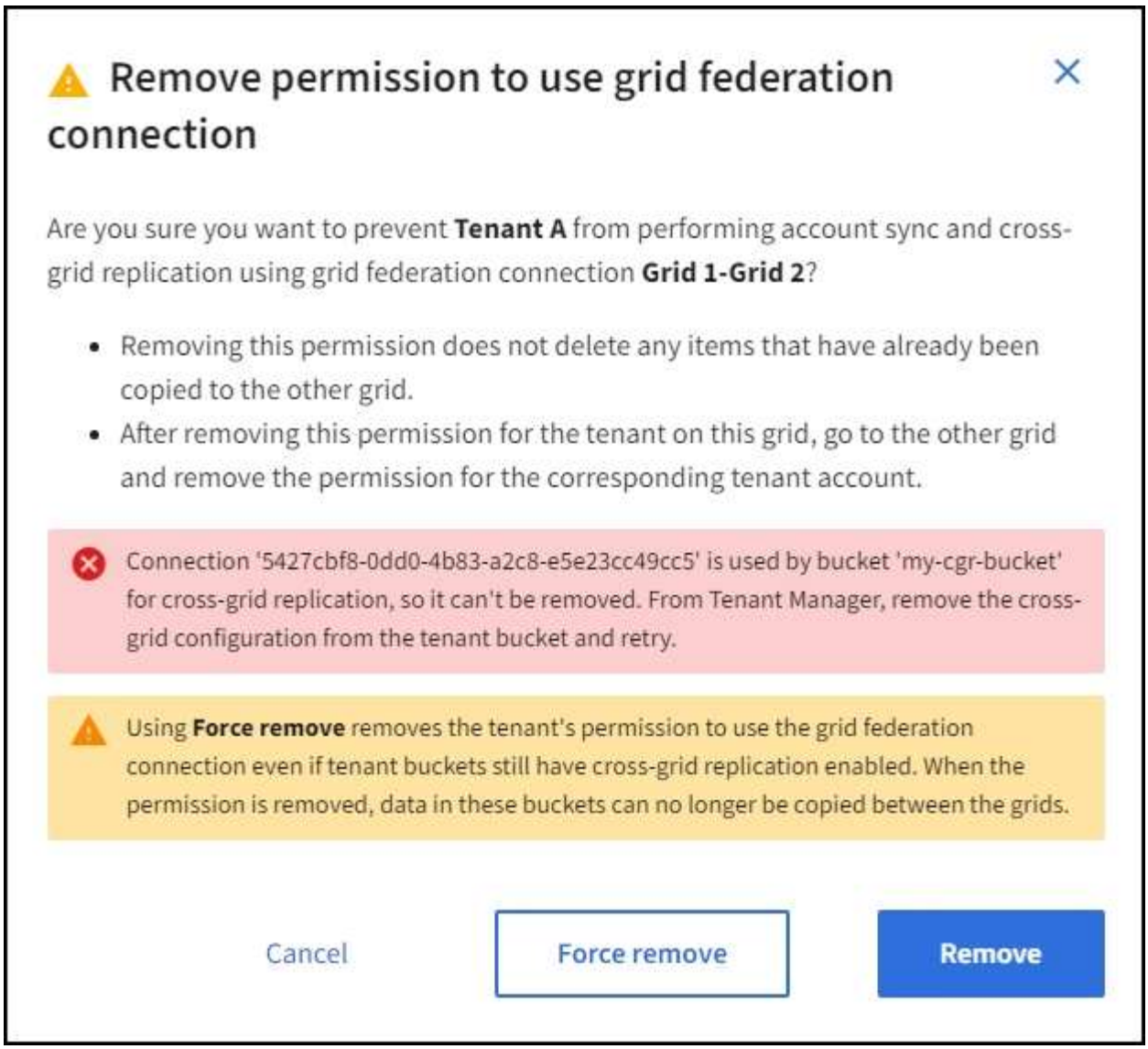
Page de fédération de grille

a. Sélectionnez **CONFIGURATION** > **système** > **fédération de grille**.
b. Sélectionnez le nom de la connexion pour afficher sa page de détails.
c. Dans l'onglet **locataires autorisés**, sélectionnez le bouton radio du locataire.
d. Sélectionnez **Supprimer l'autorisation**.

Page locataires

a. Sélectionnez **LOCATAIRES**.
b. Sélectionnez le nom du locataire pour afficher la page de détails.
c. Dans l'onglet **grid federation**, sélectionnez le bouton radio de la connexion.
d. Sélectionnez **Supprimer l'autorisation**.

3. Passez en revue les avertissements dans la boîte de dialogue de confirmation et sélectionnez **Supprimer**.
   - Si l'autorisation peut être supprimée, vous êtes renvoyé à la page des détails et un message de réussite s'affiche. Ce locataire ne peut plus utiliser la connexion de fédération de grille.
   - Si la réplication entre plusieurs compartiments de tenant est toujours activée, une erreur s'affiche.



Vous pouvez effectuer l'une des opérations suivantes :

- (Recommandé.) Connectez-vous au gestionnaire de locataires et désactivez la réplication pour chaque compartiments du locataire. Voir "Gérer la réplication entre les grilles". Répétez ensuite les étapes pour supprimer l'autorisation **utiliser la connexion grille**.
- Supprimez l'autorisation par force. Voir la section suivante.

4. Accédez à l'autre grille et répétez ces étapes pour supprimer l'autorisation pour le même locataire sur l'autre grille.

supprimez l'autorisation par la force

Si nécessaire, vous pouvez forcer la suppression de l'autorisation d'un locataire à utiliser une connexion de fédération de grille, même si la réplication inter-grid est activée dans les compartiments de locataires.

Avant de supprimer l'autorisation d'un locataire par la force, notez les considérations générales de suppression de l'autorisation ainsi que les considérations suivantes :

- Si vous supprimez l'autorisation **utiliser la connexion de fédération de grille** par force, tous les objets en attente de réplication vers l'autre grille (ingérés mais pas encore répliqués) continueront d'être répliqués. Pour empêcher ces objets en cours d'exécution d'atteindre le compartiment de destination, vous devez

également supprimer l'autorisation du locataire sur l'autre grille.

- Tous les objets ingérés dans le compartiment source après la suppression de l'autorisation **utiliser la connexion de fédération de grille** ne seront jamais répliqués dans le compartiment de destination.

Étapes

1. Connectez-vous au Grid Manager à partir du nœud d'administration principal.
2. Sélectionnez **CONFIGURATION** > **système** > **fédération de grille**.
3. Sélectionnez le nom de la connexion pour afficher sa page de détails.
4. Dans l'onglet **locataires autorisés**, sélectionnez le bouton radio du locataire.
5. Sélectionnez **Supprimer l'autorisation**.
6. Passez en revue les avertissements dans la boîte de dialogue de confirmation et sélectionnez **forcer la suppression**.

   Un message de réussite s'affiche. Ce locataire ne peut plus utiliser la connexion de fédération de grille.

7. Si nécessaire, accédez à l'autre grille et répétez ces étapes pour forcer la suppression de l'autorisation pour le même compte de tenant sur l'autre grille. Par exemple, vous devez répéter ces étapes sur l'autre grille pour empêcher les objets en cours d'atteindre le compartiment de destination.

Dépanner les erreurs de fédération de grille

Vous devrez peut-être résoudre les problèmes liés aux alertes et aux erreurs liées aux connexions de fédération du grid, au clone de compte et à la réplication intergrille.

alertes et erreurs de connexion de fédération de grille

Vous pouvez recevoir des alertes ou rencontrer des erreurs avec vos connexions de fédération de grille.

Après avoir effectué des modifications pour résoudre un problème de connexion, testez la connexion pour vous assurer que l'état de la connexion revient à **connecté**. Pour obtenir des instructions, reportez-vous à la section "Gérer les connexions de fédération de grille".

Alerte d'échec de la connexion de fédération de grille

Problème

L'alerte **échec de la connexion de fédération de grille** a été déclenchée.

Détails

Cette alerte indique que la connexion de fédération de grille entre les grilles ne fonctionne pas.

Actions recommandées

1. Vérifiez les paramètres de la page de fédération de grille pour les deux grilles. Vérifier que toutes les valeurs sont correctes. Voir "Gérer les connexions de fédération de grille".
2. Vérifiez les certificats utilisés pour la connexion. Assurez-vous qu'il n'y a pas d'alertes pour les certificats de fédération de grille expirés et que les détails de chaque certificat sont valides. Reportez-vous aux instructions relatives aux certificats de connexion rotatifs de la section "Gérer les connexions de fédération de grille".
3. Vérifiez que tous les nœuds d'administration et de passerelle des deux grilles sont en ligne et disponibles. Résolvez les alertes susceptibles d'affecter ces nœuds et réessayez.

4. Si vous avez fourni un nom de domaine complet (FQDN) pour la grille locale ou distante, vérifiez que le serveur DNS est en ligne et disponible. Voir "Qu'est-ce que la fédération de grille ?" Pour la mise en réseau, l'adresse IP et les exigences DNS.

Expiration de l'alerte de certificat de fédération de grille

Problème

L'alerte **expiration du certificat de fédération de grille** a été déclenchée.

Détails

Cette alerte indique qu'un ou plusieurs certificats de fédération de grille sont sur le point d'expirer.

Actions recommandées

Reportez-vous aux instructions relatives aux certificats de connexion rotatifs de la section "Gérer les connexions de fédération de grille".

Erreur lors de la modification d'une connexion de fédération de grille

Problème

Lors de la modification d'une connexion de fédération de grille, le message d'avertissement suivant s'affiche lorsque vous sélectionnez **Enregistrer et tester** : "Echec de la création d'un fichier de configuration de candidat sur un ou plusieurs nœuds."

Détails

Lorsque vous modifiez une connexion de fédération de grille, StorageGRID tente d'enregistrer un fichier de configuration de candidat sur tous les nœuds d'administration de la première grille. Un message d'avertissement s'affiche si ce fichier ne peut pas être enregistré sur tous les nœuds d'administration, par exemple, parce qu'un nœud d'administration est hors ligne.

Actions recommandées

1. Dans la grille que vous utilisez pour modifier la connexion, sélectionnez **NODES**.
2. Vérifiez que tous les nœuds d'administration de ce grid sont en ligne.
3. Si des nœuds sont hors ligne, remettez-les en ligne et réessayez de modifier la connexion.

Erreurs de clonage de compte

Impossible de se connecter à un compte de locataire cloné

Problème

Vous ne pouvez pas vous connecter à un compte de locataire cloné. Le message d'erreur sur la page de connexion du gestionnaire de locataires est « vos informations d'identification pour ce compte n'étaient pas valides. Veuillez réessayer.»

Détails

Pour des raisons de sécurité, lorsqu'un compte de locataire est cloné depuis la grille source du locataire vers la grille de destination du locataire, le mot de passe que vous définissez pour l'utilisateur root local du locataire n'est pas cloné. De même, lorsqu'un locataire crée des utilisateurs locaux dans sa grille source, les mots de passe des utilisateurs locaux ne sont pas clonés dans la grille de destination.

Actions recommandées

Pour que l'utilisateur root puisse se connecter à la grille de destination du locataire, un administrateur de la

grille doit d'abord se connecter "modifiez le mot de passe de l'utilisateur root local" sur la grille de destination.

Pour qu'un utilisateur local cloné puisse se connecter à la grille de destination du locataire, l'utilisateur root du locataire cloné doit ajouter un mot de passe pour l'utilisateur sur la grille de destination. Pour obtenir des instructions, reportez-vous à la section "Gérez les utilisateurs locaux" Dans les instructions d'utilisation du Gestionnaire de locataires.

Locataire créé sans clone

Problème

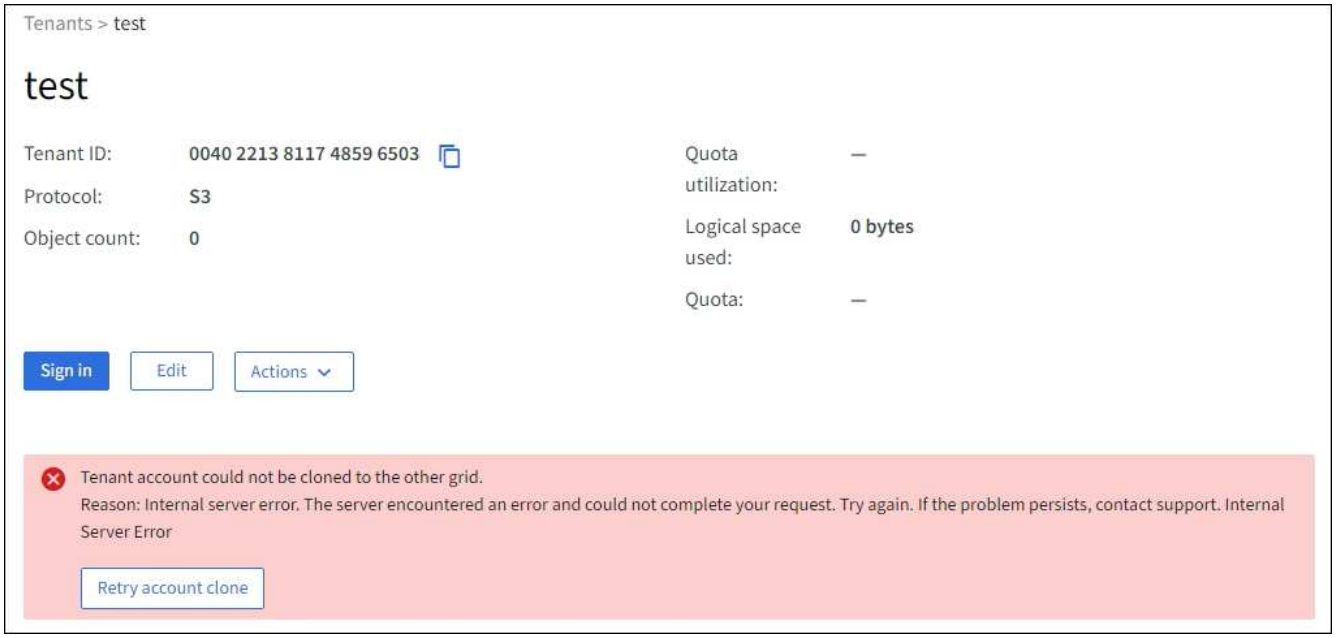
Vous voyez le message « tenant créé sans clone » après avoir créé un nouveau locataire avec l'autorisation **Use grid federation connection**.

Détails

Ce problème peut se produire si les mises à jour de l'état de la connexion sont retardées, ce qui peut entraîner la liste d'une connexion défectueuse sous le nom **connectée**.

Actions recommandées

1. Vérifiez la raison indiquée dans le message d'erreur et résolvez tout problème de réseau ou autre qui pourrait empêcher la connexion de fonctionner. Voir Alertes et erreurs de connexion de fédération de grille.
2. Suivez les instructions pour tester une connexion de fédération de grille dans "Gérer les connexions de fédération de grille" pour confirmer que le problème a été résolu.
3. Dans la grille source du locataire, sélectionnez **TENANTS**.
4. Recherchez le compte de locataire qui n'a pas pu être cloné.
5. Sélectionnez le nom du locataire pour afficher la page de détails.
6. Sélectionnez **Réessayer le clone de compte**.



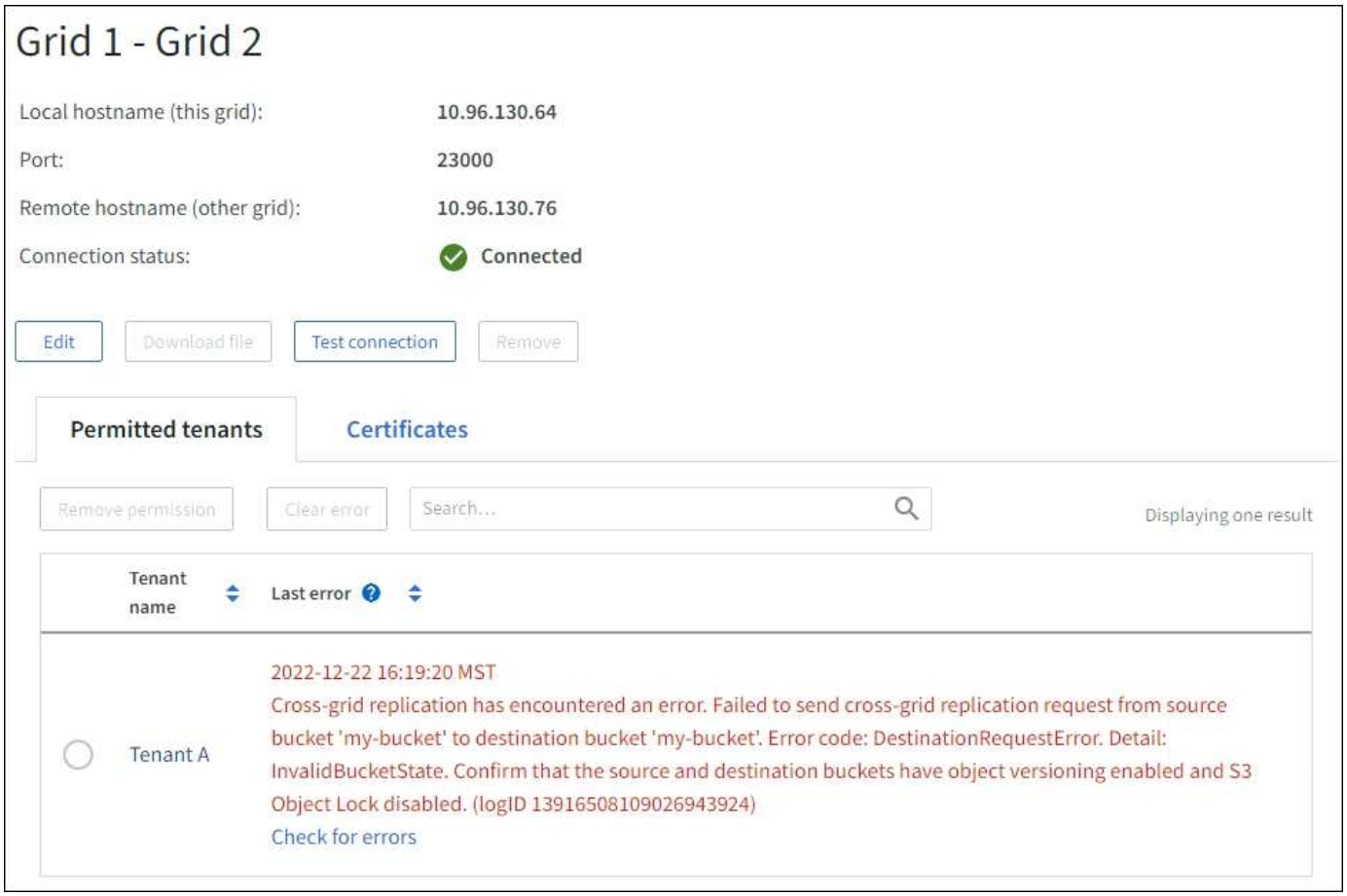
Si l'erreur a été résolue, le compte locataire sera cloné dans l'autre grille.

Alertes et erreurs de réplication intergrid

Dernière erreur affichée pour la connexion ou le locataire

Problème

Quand "affichage d'une connexion de fédération de grille" (ou quand "gestion des locataires autorisés" Pour une connexion), vous remarquez une erreur dans la colonne **dernière erreur** de la page de détails de la connexion. Par exemple :



Détails

Pour chaque connexion de fédération de grille, la colonne **dernière erreur** indique l'erreur la plus récente à se produire, le cas échéant, lors de la réplication des données d'un locataire vers l'autre grille. Cette colonne affiche uniquement la dernière erreur de réplication inter-grille à se produire ; les erreurs précédentes qui se sont peut-être produites ne seront pas affichées. Une erreur dans cette colonne peut se produire pour l'une des raisons suivantes :

- La version de l'objet source est introuvable.
- Le compartiment source est introuvable.
- Le compartiment de destination a été supprimé.
- Le compartiment de destination a été recréé par un autre compte.
- La gestion des versions du compartiment de destination est suspendue.
- Le compartiment de destination a été recréé par le même compte, mais il n'est plus versionné.

Actions recommandées

Si un message d'erreur apparaît dans la colonne **dernière erreur**, procédez comme suit :

1. Vérifiez le texte du message.
2. Effectuez toutes les actions recommandées. Par exemple, si la gestion des versions a été suspendue dans le compartiment de destination pour la réplication inter-grid, réactivez la gestion des versions pour ce compartiment.
3. Sélectionnez le compte de connexion ou de locataire dans le tableau.
4. Sélectionnez **Effacer erreur**.
5. Sélectionnez **Oui** pour effacer le message et mettre à jour l'état du système.
6. Patientez 5-6 minutes, puis ingérer un nouvel objet dans le compartiment. Vérifiez que le message d'erreur ne réapparaît pas.

   Pour vous assurer que le message d'erreur est effacé, attendez au moins 5 minutes après l'horodatage dans le message avant d'ingérer un nouvel objet.

   Après avoir dégagé l'erreur, une nouvelle **dernière erreur** peut apparaître si des objets sont ingérés dans un autre compartiment qui présente également une erreur.

7. Pour déterminer si des objets n'ont pas pu être répliqués en raison d'une erreur de compartiment, reportez-vous à la section "Identifier et réessayer les opérations de réplication ayant échoué".

Alerte de défaillance permanente de la réplication multi-grid

Problème

L'alerte **échec permanent de la réplication Cross-grid** a été déclenchée.

Détails

Cette alerte indique que les objets tenant ne peuvent pas être répliqués entre les compartiments de deux grilles pour une raison qui nécessite une intervention de l'utilisateur. Cette alerte est généralement causée par une modification du compartiment source ou de destination.

Actions recommandées

1. Connectez-vous à la grille dans laquelle l'alerte a été déclenchée.
2. Accédez à **CONFIGURATION** > **système** > **fédération de grille** et localisez le nom de connexion indiqué dans l'alerte.
3. Dans l'onglet locataires autorisés, consultez la colonne **dernière erreur** pour déterminer quels comptes de locataires ont des erreurs.
4. Pour en savoir plus sur l'échec, reportez-vous aux instructions de la section "Surveiller les connexions de fédération de grille" pour vérifier les metrics de réplication entre les grilles.
5. Pour chaque compte de locataire concerné :
   a. Reportez-vous aux instructions de la section "Surveillez l'activité des locataires" pour confirmer que le locataire n'a pas dépassé son quota sur la grille de destination pour la réplication inter-grid.
   b. Si nécessaire, augmentez le quota du locataire sur la grille de destination pour permettre l'enregistrement de nouveaux objets.
6. Pour chaque locataire concerné, connectez-vous au Gestionnaire de locataires sur les deux grilles afin de comparer la liste des compartiments.
7. Pour chaque compartiment pour lequel la réplication inter-grid est activée, vérifiez les points suivants :
   - Il existe un compartiment correspondant pour le même locataire sur l'autre grille (doit utiliser le nom

exact).

- La gestion des versions des objets est activée dans les deux compartiments (la gestion des versions ne peut pas être suspendue sur les deux grilles).
- Le verrouillage d'objet S3 est désactivé dans les deux compartiments.
- Aucun compartiment n'est à l'état **Suppression d'objets : lecture seule**.

8. Pour confirmer que le problème a été résolu, reportez-vous aux instructions de la section "Surveiller les connexions de fédération de grille" pour vérifier les mesures de réplication inter-grid ou effectuer les étapes suivantes :

   a. Retournez à la page Grid federation.
   b. Sélectionnez le locataire affecté et sélectionnez **Effacer erreur** dans la colonne **dernière erreur**.
   c. Sélectionnez **Oui** pour effacer le message et mettre à jour l'état du système.
   d. Patientez 5-6 minutes, puis ingérer un nouvel objet dans le compartiment. Vérifiez que le message d'erreur ne réapparaît pas.

   > Pour vous assurer que le message d'erreur est effacé, attendez au moins 5 minutes après l'horodatage dans le message avant d'ingérer un nouvel objet.

   > Une fois l'alerte résolue, il peut s'écouler jusqu'à un jour avant que l'alerte ne s'efface.

   a. Accédez à "Identifier et réessayer les opérations de réplication ayant échoué" pour identifier les objets ou supprimer les marqueurs qui n'ont pas pu être répliqués sur l'autre grille et pour relancer la réplication si nécessaire.

Alerte de ressource de réplication inter-grid indisponible

Problème

L'alerte **ressource de réplication multigrille indisponible** a été déclenchée.

Détails

Cette alerte indique que les demandes de réplication inter-grid sont en attente car une ressource n'est pas disponible. Par exemple, une erreur réseau peut se produire.

Actions recommandées

1. Surveillez l'alerte pour voir si le problème se résout de lui-même.
2. Si le problème persiste, déterminez si l'une des grilles a une alerte **échec de la connexion de fédération de grille** pour la même connexion ou une alerte **Impossible de communiquer avec le nœud** pour un nœud. Cette alerte peut être résolue lorsque vous résolvez ces alertes.
3. Pour en savoir plus sur l'échec, reportez-vous aux instructions de la section "Surveiller les connexions de fédération de grille" pour vérifier les metrics de réplication entre les grilles.
4. Si vous ne parvenez pas à résoudre l'alerte, contactez le support technique.

La réplication inter-grid se poursuivra normalement une fois le problème résolu.

Identifier et réessayer les opérations de réplication ayant échoué

Après avoir résolu l'alerte **échec permanent de la réplication Cross-grid**, vous devez déterminer si des objets ou des marqueurs de suppression n'ont pas pu être répliqués

sur l'autre grille. Vous pouvez ensuite réingérer ces objets ou utiliser l'API de gestion de grille pour réessayer la réplication.

L'alerte **échec permanent de la réplication multigrille** indique que les objets tenant ne peuvent pas être répliqués entre les compartiments de deux grilles pour une raison qui nécessite une intervention de l'utilisateur pour la résoudre. Cette alerte est généralement causée par une modification du compartiment source ou de destination. Pour plus de détails, voir "Dépanner les erreurs de fédération de grille".

Déterminez si des objets n'ont pas pu être répliqués

Pour déterminer si des objets ou des marqueurs de suppression n'ont pas été répliqués sur l'autre grille, vous pouvez rechercher dans le journal d'audit "CGRR (demande de réplication multigrille)" messages. Ce message est ajouté au journal lorsque StorageGRID ne parvient pas à répliquer un objet, un objet en plusieurs parties ou un marqueur de suppression vers le compartiment de destination.

Vous pouvez utiliser le "outil d'audit-explication" pour traduire les résultats dans un format plus facile à lire.

Avant de commencer

- Vous disposez de l'autorisation d'accès racine.
- Vous avez le `Passwords.txt` fichier.
- Vous connaissez l'adresse IP du nœud d'administration principal.

Étapes

1. Connectez-vous au nœud d'administration principal :
   a. Saisissez la commande suivante : `ssh admin@primary_Admin_Node_IP`
   b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
   c. Entrez la commande suivante pour passer à la racine : `su -`
   d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

   Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

2. Recherchez les messages du CRGR sur le site audit.log et utilisez l'outil audit-explication pour formater les résultats.

   Par exemple, cette commande gronde tous les messages CGRR au cours des 30 dernières minutes et utilise l'outil audit-Explain.

```
# awk -vdate=$(date -d "30 minutes ago" '+%Y-%m-%dT%H:%M:%S') '$1$2 >= date { print }' audit.log | grep CGRR | audit-explain
```

Les résultats de la commande ressemblent à cet exemple, qui contient des entrées pour six messages CGRR. Dans l'exemple, toutes les demandes de réplication inter-grid ont renvoyé une erreur générale car l'objet n'a pas pu être répliqué. Les trois premières erreurs concernent les opérations « Replicate object » et les trois dernières sont pour les opérations « Replicate delete marker ».

```
CGRR Cross-Grid Replication Request tenant:5073644526962743774 8
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
object" bucket:bucket123 object:"audit-0"
version:QjRBNDIzODAtNjQ3My0xMUVELTg2QjEtODJBMjAwQkI3NEM4 error:general
error
CGRR Cross-Grid Replication Request tenant:5073644526962743774 8
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
object" bucket:bucket123 object:"audit-3"
version:QjRDOTRCOUMtNjQ3My0xMUVELTkzM0YtOTg1MTAwQkI3NEM4 error:general
error
CGRR Cross-Grid Replication Request tenant:5073644526962743774 8
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
delete marker" bucket:bucket123 object:"audit-1"
version:NUQ0OEYxMDAtNjQ3NC0xMUVELTg2NjMtOTY5NzAwQkI3NEM4 error:general
error
CGRR Cross-Grid Replication Request tenant:5073644526962743774 8
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
delete marker" bucket:bucket123 object:"audit-5"
version:NUQ1ODUwQkUtNjQ3NC0xMUVELTg1NTItRDkwNzAwQkI3NEM4 error:general
error
```

Chaque entrée contient les informations suivantes :

Champ	Description
Demande de réplication croisée CGRR	Nom de la demande
locataire	ID de compte du locataire
connexion	ID de la connexion de fédération de grille
fonctionnement	Type d'opération de réplication en cours de tentative : • répliquer l'objet • répliquer le marqueur de suppression • répliquer un objet multipièce
godet	Nom du compartiment
objet	Nom de l'objet
version	ID de version de l'objet

Champ	Description
erreur	Type d'erreur. Si la réplication de la grille croisée a échoué, l'erreur est « erreur générale ».

Réessayer les réplications ayant échoué

Après avoir généré une liste d'objets et supprimé des marqueurs qui n'ont pas été répliqués dans le compartiment de destination et résolu les problèmes sous-jacents, vous pouvez réessayer la réplication de l'une des deux manières suivantes :

- Réintégrez chaque objet dans le compartiment source.
- Utilisez l'API privée Grid Management, comme décrit.

Étapes

1. En haut du Gestionnaire de grille, sélectionnez l'icône d'aide et sélectionnez **documentation API**.
2. Sélectionnez **aller à la documentation privée de l'API**.

> Les terminaux de l'API StorageGRID marqués « privé » sont susceptibles d'être modifiés sans préavis. Les terminaux privés StorageGRID ignorent également la version API de la demande.

3. Dans la section **cross-grid-Replication-Advanced**, sélectionnez le noeud final suivant :

   ```
   POST /private/cross-grid-replication-retry-failed
   ```

4. Sélectionnez **essayez-le**.
5. Dans la zone de texte **body**, remplacez l'exemple de **versionID** par un ID de version du fichier audit.log correspondant à une demande de réplication croisée ayant échoué.

   Veillez à conserver les guillemets doubles autour de la chaîne.

6. Sélectionnez **Exécuter**.
7. Vérifiez que le code de réponse du serveur est **204**, indiquant que l'objet ou le marqueur de suppression a été marqué comme en attente pour la réplication de la grille transversale vers l'autre grille.

> En attente signifie que la demande de réplication inter-grille a été ajoutée à la file d'attente interne pour traitement.

Surveiller les nouvelles tentatives de réplication

Vous devez surveiller les opérations de nouvelle tentative de réplication pour vous assurer qu'elles sont terminées.

> La réplication d'un objet ou d'un marqueur de suppression vers une autre grille peut prendre plusieurs heures, voire plus.

Vous pouvez surveiller les nouvelles tentatives de deux manières :

- Utiliser un S3 "Objet TÊTE" ou "OBTENIR l'objet" demande. La réponse inclut la réponse spécifique à

StorageGRID `x-ntap-sg-cgr-replication-status` en-tête de réponse, qui aura l'une des valeurs suivantes :

Grille	État de la réplication
Source	• **SUCCÈS** : la réplication a réussi. • **EN ATTENTE** : l'objet n'a pas encore été répliqué. • **ÉCHEC** : la réplication a échoué avec une défaillance permanente. L'utilisateur doit résoudre l'erreur.
Destination	**RÉPLIQUE** : l'objet a été répliqué à partir de la grille source.

- Utilisez l'API privée Grid Management, comme décrit.

Étapes

1. Dans la section **cross-grid-Replication-Advanced** de la documentation de l'API privée, sélectionnez le noeud final suivant :

   `GET /private/cross-grid-replication-object-status/{id}`

2. Sélectionnez **essayez-le**.
3. Dans la section paramètre, entrez l'ID de version que vous avez utilisé dans l' `cross-grid-replication-retry-failed` demande.
4. Sélectionnez **Exécuter**.
5. Vérifiez que le code de réponse du serveur est **200**.
6. Vérifiez l'état de la réplication, qui sera l'un des suivants :
   - **EN ATTENTE** : l'objet n'a pas encore été répliqué.
   - **TERMINÉ** : la réplication a réussi.
   - **ÉCHEC** : la réplication a échoué avec une défaillance permanente. L'utilisateur doit résoudre l'erreur.

Gérer la sécurité

Gérer la sécurité : présentation

Vous pouvez configurer différents paramètres de sécurité à partir du Gestionnaire de grille pour sécuriser votre système StorageGRID.

Gestion du chiffrement

StorageGRID propose plusieurs options pour le chiffrement des données. Vous devriez "consultez les méthodes de cryptage disponibles" afin d'identifier celles qui répondent à vos exigences en matière de protection des données.

Gérer les certificats

C'est possible "configurer et gérer les certificats de serveur" Utilisé pour les connexions HTTP ou les certificats client utilisés pour authentifier l'identité d'un client ou d'un utilisateur sur le serveur.

Configurer les serveurs de gestion des clés

À l'aide d'un "serveur de gestion des clés" Vous permet de protéger vos données StorageGRID même si une appliance est retirée du data Center. Une fois les volumes de l'appliance chiffrés, vous ne pouvez accéder aux données de l'appliance que si le nœud peut communiquer avec le KMS.

> Pour utiliser la gestion des clés de chiffrement, vous devez activer le paramètre **Node Encryption** pour chaque appliance au cours de l'installation, avant d'ajouter l'appliance à la grille.

Gérer les paramètres proxy

Si vous utilisez les services de plateforme S3 ou les pools de stockage cloud, vous pouvez configurer un "Serveur proxy de stockage" Entre les nœuds de stockage et les terminaux S3 externes. Si vous envoyez des messages AutoSupport via HTTPS ou HTTP, vous pouvez configurer un "Serveur proxy d'administration" Entre les nœuds d'administration et le support technique.

Contrôle des pare-feu

Pour améliorer la sécurité de votre système, vous pouvez contrôler l'accès aux nœuds d'administration StorageGRID en ouvrant ou en fermant des ports spécifiques sur le "pare-feu externe". Vous pouvez également contrôler l'accès réseau à chaque nœud en configurant son "pare-feu interne". Vous pouvez empêcher l'accès à tous les ports, à l'exception de ceux nécessaires à votre déploiement.

Étudiez les méthodes de cryptage StorageGRID

StorageGRID propose plusieurs options pour le chiffrement des données. Consultez les méthodes disponibles pour identifier les méthodes qui répondent à vos exigences en matière de protection des données.

Le tableau fournit un récapitulatif détaillé des méthodes de cryptage disponibles dans StorageGRID.

Option de chiffrement	Comment cela fonctionne	S'applique à
Serveur de gestion des clés (KMS) dans Grid Manager	Vous "configurer un serveur de gestion des clés" Pour le site StorageGRID et "activez le chiffrement des nœuds pour l'appliance". Ensuite, un nœud d'appliance se connecte au KMS pour demander une clé de chiffrement (KEK). Cette clé chiffre et décrypte la clé de chiffrement des données (DEK) sur chaque volume.	Nœuds d'appliance sur lesquels **Node Encryption** est activé pendant l'installation. Toutes les données de l'appliance sont protégées contre les pertes ou les suppressions physiques du data Center. La gestion des clés de chiffrement avec un KMS n'est prise en charge que pour les nœuds de stockage et les appliances de services.

Option de chiffrement	Comment cela fonctionne	S'applique à
Sécurité des disques dans SANtricity System Manager	Si la fonctionnalité Drive Security est activée pour une appliance de stockage SG5700 ou SG6000, vous pouvez utiliser "SANtricity System Manager" pour créer et gérer la clé de sécurité. La clé est requise pour accéder aux données sur les disques sécurisés.	Dispositifs de stockage équipés de disques Full Disk Encryption (FDE) ou de disques FIPS. Toutes les données des disques sécurisés sont protégées contre les pertes ou suppressions physiques du data Center. Utilisation avec certaines appliances de stockage ou avec des appliances de service impossible.
Chiffrement des objets stockés	Vous activez le "Chiffrement des objets stockés" Dans le Gestionnaire de grille. Lorsqu'il est activé, tout nouvel objet non chiffré au niveau du compartiment ou de l'objet est chiffré lors de l'ingestion.	Ingestion récente des données d'objet S3 et Swift. Les objets stockés existants ne sont pas chiffrés. Les métadonnées d'objet et les autres données sensibles ne sont pas chiffrées.
Chiffrement de compartiment S3	Vous émettez une demande de chiffrement Put bucket pour activer le chiffrement du compartiment. Tout nouvel objet non chiffré au niveau de l'objet est chiffré lors de l'ingestion.	Données d'objet S3 récemment ingérées uniquement. Le chiffrement doit être spécifié pour le compartiment. Les objets de compartiment existants ne sont pas chiffrés. Les métadonnées d'objet et les autres données sensibles ne sont pas chiffrées. "Opérations sur les compartiments"
Chiffrement côté serveur d'objets S3 (SSE)	Vous émettez une demande S3 pour stocker un objet et inclure le `x-amz-server-side-encryption` en-tête de demande.	Données d'objet S3 récemment ingérées uniquement. Le chiffrement doit être spécifié pour l'objet. Les métadonnées d'objet et les autres données sensibles ne sont pas chiffrées. StorageGRID gère les clés. "Utilisez le cryptage côté serveur"

Option de chiffrement	Comment cela fonctionne	S'applique à
Chiffrement côté serveur objet S3 avec clés fournies par le client (SSE-C)	Vous émettez une demande S3 pour stocker un objet et incluez trois en-têtes de requête. • `x-amz-server-side-encryption-customer-algorithm` • `x-amz-server-side-encryption-customer-key` • `x-amz-server-side-encryption-customer-key-MD5`	Données d'objet S3 récemment ingérées uniquement. Le chiffrement doit être spécifié pour l'objet. Les métadonnées d'objet et les autres données sensibles ne sont pas chiffrées. Les clés sont gérées en dehors du StorageGRID. "Utilisez le cryptage côté serveur"
Chiffrement de volume ou de datastore externe	Vous utilisez une méthode de chiffrement autres que StorageGRID pour chiffrer un volume ou un datastore entier, si votre plateforme de déploiement le prend en charge.	Toutes les données d'objet, de métadonnées et de configuration du système, en supposant que chaque volume ou datastore est chiffré. Une méthode de chiffrement externe permet un contrôle plus précis des clés et des algorithmes de chiffrement. Peut être combiné avec les autres méthodes répertoriées.
Chiffrement d'objet en dehors de StorageGRID	Vous utilisez une méthode de chiffrement à l'extérieur de StorageGRID pour chiffrer les données d'objet et les métadonnées avant leur ingestion dans StorageGRID.	Données et métadonnées d'objet uniquement (les données de configuration du système ne sont pas chiffrées). Une méthode de chiffrement externe permet un contrôle plus précis des clés et des algorithmes de chiffrement. Peut être combiné avec les autres méthodes répertoriées. "Amazon simple Storage Service - Guide des développeurs : protection des données à l'aide du chiffrement côté client"

Utilisez plusieurs méthodes de chiffrement

Selon vos besoins, vous pouvez utiliser plusieurs méthodes de chiffrement à la fois. Par exemple :

- Vous pouvez utiliser un KMS pour protéger les nœuds d'appliance et utiliser également la fonctionnalité de sécurité des disques de SANtricity System Manager pour « déchiffrer » les données présentes sur les

disques à autocryptage des mêmes dispositifs.

- Vous pouvez utiliser un KMS pour sécuriser les données des nœuds de l'appliance et utiliser l'option de chiffrement des objets stockés pour chiffrer tous les objets lors de leur ingestion.

Si seule une petite partie de vos objets doit être cryptée, pensez à contrôler le chiffrement au niveau du compartiment ou de l'objet au niveau individuel. L'activation de plusieurs niveaux de chiffrement a un coût supplémentaire en termes de performance.

Gérer les certificats

Gérer les certificats de sécurité : présentation

Les certificats de sécurité sont de petits fichiers de données utilisés pour créer des connexions sécurisées et fiables entre les composants StorageGRID et entre les composants StorageGRID et les systèmes externes.

StorageGRID utilise deux types de certificats de sécurité :

- **Les certificats de serveur** sont requis lorsque vous utilisez des connexions HTTPS. Les certificats de serveur permettent d'établir des connexions sécurisées entre les clients et les serveurs, d'authentifier l'identité d'un serveur pour ses clients et de fournir un chemin de communication sécurisé pour les données. Le serveur et le client ont chacun une copie du certificat.
- **Certificats client** authentifiez une identité client ou utilisateur au serveur, fournissant une authentification plus sécurisée que les mots de passe seuls. Les certificats client ne chiffrent pas les données.

Lorsqu'un client se connecte au serveur via HTTPS, le serveur répond avec le certificat du serveur, qui contient une clé publique. Le client vérifie ce certificat en comparant la signature du serveur à la signature figurant sur sa copie du certificat. Si les signatures correspondent, le client démarre une session avec le serveur en utilisant la même clé publique.

StorageGRID fonctionne comme serveur pour certaines connexions (par exemple, le point de terminaison de l'équilibreur de charge) ou comme client pour d'autres connexions (par exemple, le service de réplication CloudMirror).

Certificat CA grille par défaut

StorageGRID inclut une autorité de certification intégrée qui génère un certificat d'autorité de certification interne Grid lors de l'installation du système. Par défaut, le certificat de l'autorité de certification Grid est utilisé pour sécuriser le trafic StorageGRID interne. Une autorité de certification externe peut émettre des certificats personnalisés qui sont entièrement conformes aux politiques de sécurité des informations de votre entreprise. Bien que vous puissiez utiliser le certificat d'autorité de certification Grid pour un environnement non productif, la meilleure pratique pour un environnement de production consiste à utiliser des certificats personnalisés signés par une autorité de certification externe. Les connexions non sécurisées sans certificat sont également prises en charge, mais ne sont pas recommandées.

- Les certificats d'autorité de certification personnalisée ne suppriment pas les certificats internes ; cependant, les certificats personnalisés doivent être ceux spécifiés pour vérifier les connexions au serveur.
- Tous les certificats personnalisés doivent être conformes au "instructions de renforcement du système pour les certificats de serveur".
- StorageGRID prend en charge le regroupement de certificats d'une autorité de certification dans un seul fichier (appelé bundle de certificats d'autorité de certification).

StorageGRID inclut également des certificats CA du système d'exploitation identiques sur toutes les grilles. Dans les environnements de production, assurez-vous de spécifier un certificat personnalisé signé par une autorité de certification externe à la place du certificat d'autorité de certification du système d'exploitation.

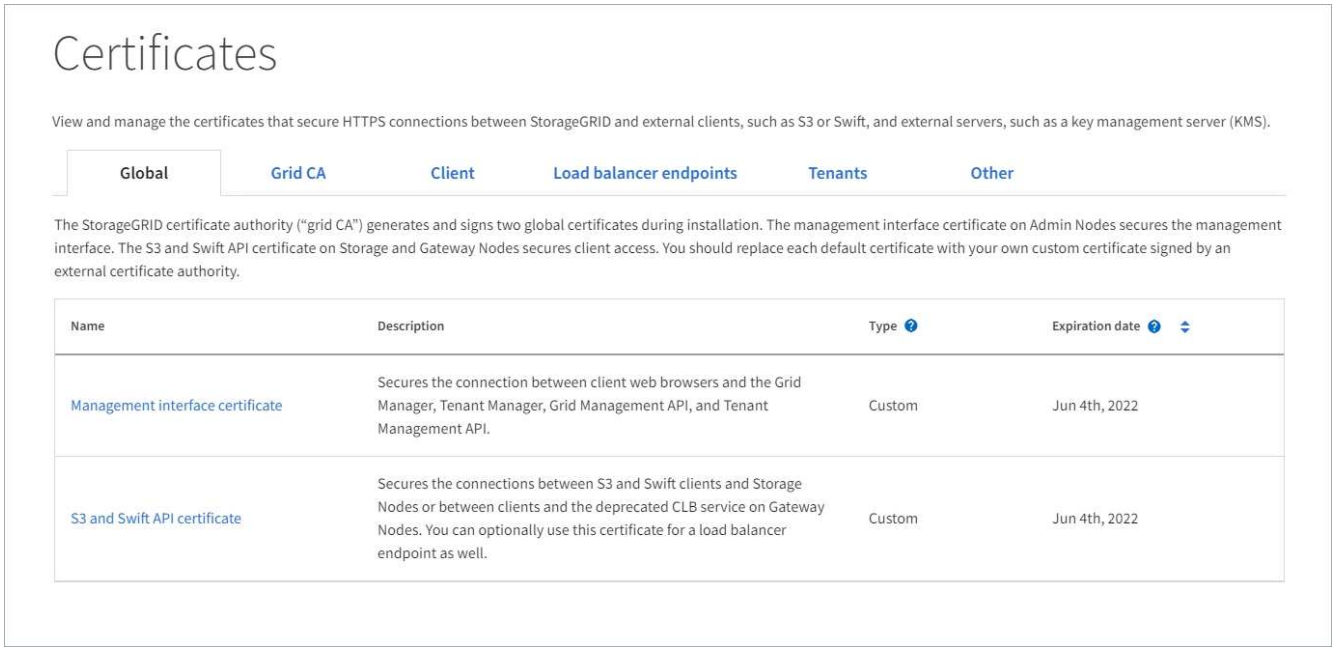
Les variantes du serveur et des types de certificats client sont mises en œuvre de plusieurs façons. Avant de configurer le système, tous les certificats nécessaires à votre configuration StorageGRID spécifique doivent être prêts.

Accéder aux certificats de sécurité

Vous pouvez accéder aux informations relatives à tous les certificats StorageGRID dans un seul emplacement, ainsi qu'aux liens vers le flux de travail de configuration de chaque certificat.

Étapes

1. Dans Grid Manager, sélectionnez **CONFIGURATION** > **sécurité** > **certificats**.



2. Sélectionnez un onglet sur la page certificats pour obtenir des informations sur chaque catégorie de certificat et pour accéder aux paramètres du certificat. Vous ne pouvez accéder à un onglet que si vous disposez de l'autorisation appropriée.

   - **Global** : sécurise l'accès à StorageGRID à partir de navigateurs Web et de clients API externes.
   - **Grid CA** : sécurise le trafic StorageGRID interne.
   - **Client** : sécurise les connexions entre les clients externes et la base de données StorageGRID Prometheus.
   - **Points d'extrémité de l'équilibreur de charge** : sécurise les connexions entre les clients S3 et Swift et l'équilibreur de charge StorageGRID.
   - **Locataires** : sécurise les connexions aux serveurs de fédération d'identités ou des terminaux de service de plate-forme aux ressources de stockage S3.
   - **Autre** : sécurise les connexions StorageGRID nécessitant des certificats spécifiques.

   Chaque onglet est décrit ci-dessous avec des liens vers des détails de certificat supplémentaires.

Mondial

Les certificats globaux sécurisent l'accès StorageGRID à partir de navigateurs Web et de clients API S3 et Swift externes. Deux certificats globaux sont initialement générés par l'autorité de certification StorageGRID lors de l'installation. La meilleure pratique pour un environnement de production consiste à utiliser des certificats personnalisés signés par une autorité de certification externe.

- Certificat de l'interface de gestion: Sécurise les connexions du navigateur Web client aux interfaces de gestion StorageGRID.
- Certificat API S3 et Swift: Sécurise les connexions API client aux nœuds de stockage, aux nœuds d'administration et aux nœuds de passerelle, que les applications client S3 et Swift utilisent pour télécharger et télécharger les données d'objet.

Les informations sur les certificats globaux installés comprennent :

- **Nom** : nom du certificat avec lien vers la gestion du certificat.
- **Description**
- **Type** : personnalisé ou par défaut. + vous devez toujours utiliser un certificat personnalisé pour améliorer la sécurité de la grille.
- **Date d'expiration** : si vous utilisez le certificat par défaut, aucune date d'expiration n'est affichée.

Vous pouvez :

- Remplacez les certificats par défaut par des certificats personnalisés signés par une autorité de certification externe pour améliorer la sécurité de la grille :
  - "Remplacez le certificat d'interface de gestion généré par défaut par StorageGRID" Utilisé pour les connexions Grid Manager et tenant Manager.
  - "Remplacez le certificat API S3 et Swift" Utilisé pour les connexions de nœuds de stockage et de terminaux d'équilibrage de la charge (en option).
- "Restaurez le certificat de l'interface de gestion par défaut."
- "Restaurez le certificat API S3 et Swift par défaut."
- "Utilisez un script pour générer un nouveau certificat d'interface de gestion auto-signé."
- Copiez ou téléchargez le "certificat de l'interface de gestion" ou "Certificat API S3 et Swift".

CA grille

Le Certificat CA de la grille, Généré par l'autorité de certification StorageGRID lors de l'installation de StorageGRID, sécurise tout le trafic StorageGRID interne.

Les informations sur le certificat comprennent la date d'expiration du certificat et son contenu.

C'est possible "Copiez ou téléchargez le certificat d'autorité de certification Grid", mais vous ne pouvez pas le modifier.

Client

Certificats client, Généré par une autorité de certification externe, sécurisez les connexions entre les outils de contrôle externes et la base de données StorageGRID Prometheus.

La table de certificats possède une ligne pour chaque certificat client configuré et indique si le certificat peut être utilisé pour l'accès à la base de données Prometheus, ainsi que la date d'expiration du certificat.

Vous pouvez :

- "Téléchargez ou générez un nouveau certificat client."
- Sélectionnez un nom de certificat pour afficher les détails du certificat où vous pouvez :
  - "Modifiez le nom du certificat client."
  - "Définissez l'autorisation d'accès Prometheus."
  - "Téléchargez et remplacez le certificat client."
  - "Copiez ou téléchargez le certificat client."
  - "Supprimez le certificat client."
- Sélectionnez **actions** pour accélérer "modifier", "attacher", ou "déposer" un certificat client. Vous pouvez sélectionner jusqu'à 10 certificats client et les supprimer en une seule fois en utilisant **actions** > **Supprimer**.

Terminaux d'équilibrage de charge

Certificats de noeud final de l'équilibreur de charge Sécurisez les connexions entre les clients S3 et Swift et le service StorageGRID Load Balancer sur les nœuds de passerelle et les nœuds d'administration.

La table des noeuds finaux de l'équilibreur de charge comporte une ligne pour chaque noeud final de l'équilibreur de charge configuré et indique si le certificat API S3 et Swift global ou un certificat de point final d'équilibreur de charge personnalisé est utilisé pour le noeud final. La date d'expiration de chaque certificat s'affiche également.

> Les modifications apportées à un certificat de point final peuvent prendre jusqu'à 15 minutes pour être appliquées à tous les nœuds.

Vous pouvez :

- "Afficher un point d'extrémité d'équilibreur de charge", y compris les détails de son certificat.
- "Spécifiez un certificat de noeud final de l'équilibreur de charge pour FabricPool."
- "Utilisez le certificat global d'API S3 et Swift" au lieu de générer un nouveau certificat de terminal de l'équilibreur de charge.

Locataires

Les locataires peuvent utiliser certificats de serveur de fédération des identités ou certificats de terminal du service de plate-forme Pour sécuriser leurs connexions avec StorageGRID.

La table de tenant dispose d'une ligne pour chaque locataire et indique si chaque locataire a l'autorisation d'utiliser ses propres services de référentiel d'identité ou de plate-forme.

Vous pouvez :

- "Sélectionnez un nom de locataire pour vous connecter au Gestionnaire de tenant"
- "Sélectionnez un nom de locataire pour afficher les détails de la fédération des identités du locataire"
- "Sélectionnez un nom de locataire pour afficher les détails des services de plateforme du locataire"
- "Spécifiez un certificat de noeud final du service de plate-forme pendant la création du noeud final"

Autre

StorageGRID utilise d'autres certificats de sécurité pour des fins spécifiques. Ces certificats sont

répertoriés par leur nom fonctionnel. Voici d'autres certificats de sécurité :

- Certificats de pool de stockage cloud
- Certificats de notification d'alerte par e-mail
- Certificats de serveur syslog externe
- Certificats de connexion de fédération de grille
- Certificats de fédération des identités
- Certificats de serveur de gestion des clés (KMS)
- Certificats d'authentification unique

Informations indique le type de certificat utilisé par une fonction et ses dates d'expiration de certificat de serveur et de client, le cas échéant. La sélection d'un nom de fonction ouvre un onglet de navigateur dans lequel vous pouvez afficher et modifier les détails du certificat.

> Vous ne pouvez afficher et accéder aux informations d'autres certificats que si vous disposez de l'autorisation appropriée.

Vous pouvez :

- "Spécification d'un certificat de pool de stockage cloud pour S3, C2S S3 ou Azure"
- "Spécifiez un certificat pour les notifications par e-mail d'alerte"
- "Spécifiez un certificat de serveur syslog externe"
- "Faire pivoter les certificats de connexion de fédération de grille"
- "Afficher et modifier un certificat de fédération d'identités"
- "Télécharger les certificats du serveur de gestion des clés (KMS) et du client"
- "Spécifiez manuellement un certificat SSO pour une confiance de partie utilisatrice"

Détails du certificat de sécurité

Chaque type de certificat de sécurité est décrit ci-dessous, avec des liens vers les instructions d'implémentation.

Certificat de l'interface de gestion

Type de certificat	Description	Emplacement de navigation	Détails
Serveur	Authentifie la connexion entre les navigateurs Web client et l'interface de gestion StorageGRID, permettant aux utilisateurs d'accéder à Grid Manager et au gestionnaire de locataires sans avertissement de sécurité. Ce certificat authentifie également les connexions de l'API de gestion du grid et de l'API de gestion des locataires. Vous pouvez utiliser le certificat par défaut créé lors de l'installation ou télécharger un certificat personnalisé.	**CONFIGURATION** > **sécurité** > **certificats**, sélectionnez l'onglet **Global**, puis **certificat d'interface de gestion**	"Configurer les certificats d'interface de gestion"

Certificat API S3 et Swift

Type de certificat	Description	Emplacement de navigation	Détails
Serveur	Authentifie les connexions client S3 ou Swift sécurisées auprès d'un nœud de stockage et les terminaux d'équilibrage de la charge (facultatif).	**CONFIGURATION** > **sécurité** > **certificats**, sélectionnez l'onglet **Global**, puis **S3 et Swift API certificates**	"Configurez les certificats API S3 et Swift"

Certificat CA de la grille

Voir la Description du certificat CA de la grille par défaut.

Certificat du client administrateur

Type de certificat	Description	Emplacement de navigation	Détails
Client	Installé sur chaque client, permettant à StorageGRID d'authentifier l'accès client externe. • Permet aux clients externes autorisés d'accéder à la base de données StorageGRID Prometheus. • Contrôle sécurisé de StorageGRID à l'aide d'outils externes.	**CONFIGURATION** > **sécurité** > **certificats**, puis sélectionnez l'onglet **client**	"Configurer les certificats client"

Certificat de terminal de l'équilibreur de charge

Type de certificat	Description	Emplacement de navigation	Détails
Serveur	Authentifie la connexion entre les clients S3 ou Swift et le service StorageGRID Load Balancer sur les nœuds de passerelle et les nœuds d'administration. Vous pouvez télécharger ou générer un certificat d'équilibreur de charge lorsque vous configurez un noeud final d'équilibreur de charge. Les applications client utilisent le certificat d'équilibreur de charge lors de la connexion à StorageGRID pour enregistrer et récupérer les données d'objet. Vous pouvez également utiliser une version personnalisée de Global Certificat API S3 et Swift Certificat permettant d'authentifier les connexions au service Load Balancer. Si le certificat global est utilisé pour authentifier les connexions de l'équilibreur de charge, vous n'avez pas besoin de télécharger ou de générer un certificat distinct pour chaque noeud final de l'équilibreur de charge. **Remarque :** le certificat utilisé pour l'authentification de l'équilibreur de charge est le certificat le plus utilisé pendant le fonctionnement normal de l'StorageGRID.	**CONFIGURATION** > **réseau** > **points d'extrémité de l'équilibreur de charge**	• "Configurer les terminaux de l'équilibreur de charge" • "Créez un noeud final d'équilibrage de charge pour FabricPool"

Certificat de terminal Cloud Storage Pool

Type de certificat	Description	Emplacement de navigation	Détails
Serveur	Authentifie la connexion à partir d'un pool de stockage cloud StorageGRID vers un emplacement de stockage externe, tel que S3 Glacier ou Microsoft Azure Blob Storage. Un certificat différent est requis pour chaque type de fournisseur cloud.	**ILM** > **pools de stockage**	"Création d'un pool de stockage cloud"

Certificat de notification d'alerte par e-mail

Type de certificat	Description	Emplacement de navigation	Détails
Serveur et client	Authentifie la connexion entre un serveur de messagerie SMTP et StorageGRID utilisé pour les notifications d'alerte. • Si les communications avec le serveur SMTP nécessitent TLS (transport Layer Security), vous devez spécifier le certificat AC du serveur de messagerie. • Spécifiez un certificat client uniquement si le serveur de messagerie SMTP nécessite des certificats client pour l'authentification.	**ALERTES** > **Configuration de la messagerie**	"Configurez les notifications par e-mail pour les alertes"

Certificat de serveur syslog externe

Type de certificat	Description	Emplacement de navigation	Détails
Serveur	Authentifie la connexion TLS ou RELP/TLS entre un serveur syslog externe qui consigne les événements dans StorageGRID. **Remarque :** un certificat de serveur syslog externe n'est pas requis pour les connexions TCP, RELP/TCP et UDP à un serveur syslog externe.	**CONFIGURATION** > **surveillance** > **Audit et serveur syslog**, puis sélectionnez **configurer serveur syslog externe**	"Configurer un serveur syslog externe"

certificat de connexion de fédération de grille

Type de certificat	Description	Emplacement de navigation	Détails
Serveur et client	Authentifier et crypter les informations envoyées entre le système StorageGRID actuel et une autre grille dans une connexion de fédération de grille.	**CONFIGURATION** > **système** > **fédération de grille**	• "Créer des connexions de fédération de grille" • "Faire pivoter les certificats de connexion"

Certificat de fédération des identités

Type de certificat	Description	Emplacement de navigation	Détails
Serveur	Authentifie la connexion entre StorageGRID et un fournisseur d'identité externe, tel qu'Active Directory, OpenLDAP ou Oracle Directory Server. Utilisé pour la fédération des identités, ce qui permet de gérer les groupes et les utilisateurs d'administration par un système externe.	**CONFIGURATION** > **contrôle d'accès** > **fédération d'identités**	"Utiliser la fédération des identités"

Certificat de serveur de gestion des clés (KMS)

Type de certificat	Description	Emplacement de navigation	Détails
Serveur et client	Authentifie la connexion entre StorageGRID et un serveur de gestion des clés (KMS) externe qui fournit les clés de chiffrement aux nœuds d'appliance StorageGRID.	**CONFIGURATION** > **sécurité** > **serveur de gestion des clés**	"Ajout d'un serveur de gestion des clés (KMS)"

Certificat de terminal des services de plate-forme

Type de certificat	Description	Emplacement de navigation	Détails
Serveur	Authentification de la connexion depuis le service de la plateforme StorageGRID vers une ressource de stockage S3	**Tenant Manager** > **STORAGE (S3)** > **Platform services Endpoints**	"Créer un terminal de services de plate-forme" "Modifier le point final des services de plate-forme"

Certificat SSO (Single Sign-on)

Type de certificat	Description	Emplacement de navigation	Détails
Serveur	Authentifie la connexion entre les services de fédération d'identités, tels que Active Directory Federation Services (AD FS) et StorageGRID utilisés pour les demandes SSO (Single Sign-on).	**CONFIGURATION** > **contrôle d'accès** > **Single Sign-on**	"Configurer l'authentification unique"

Exemples de certificats

Exemple 1 : service Load Balancer

Dans cet exemple, StorageGRID sert de serveur.

1. Vous configurez un noeud final de l'équilibreur de charge et téléchargez ou générez un certificat de serveur dans StorageGRID.
2. Vous configurez une connexion client S3 ou Swift au point de terminaison de l'équilibreur de charge et téléchargez le même certificat au client.
3. Lorsque le client souhaite enregistrer ou récupérer des données, il se connecte au point de terminaison de l'équilibreur de charge à l'aide de HTTPS.
4. StorageGRID répond avec le certificat du serveur, qui contient une clé publique, et une signature basée

sur la clé privée.

5. Le client vérifie ce certificat en comparant la signature du serveur à la signature figurant sur sa copie du certificat. Si les signatures correspondent, le client lance une session à l'aide de la même clé publique.
6. Le client envoie des données d'objet à StorageGRID.

Exemple 2 : serveur de gestion externe des clés (KMS)

Dans cet exemple, StorageGRID agit comme client.

1. À l'aide du logiciel serveur de gestion de clés externe, vous configurez StorageGRID en tant que client KMS et obtenez un certificat de serveur signé par l'autorité de certification, un certificat de client public et la clé privée pour le certificat client.
2. À l'aide de Grid Manager, vous configurez un serveur KMS et téléchargez les certificats du serveur et du client ainsi que la clé privée du client.
3. Lorsqu'un nœud StorageGRID a besoin d'une clé de chiffrement, il envoie une requête au serveur KMS qui inclut les données du certificat et une signature basée sur la clé privée.
4. Le serveur KMS valide la signature du certificat et décide qu'il peut faire confiance à StorageGRID.
5. Le serveur KMS répond à l'aide de la connexion validée.

Configurer les certificats de serveur

Types de certificat de serveur pris en charge

Le système StorageGRID prend en charge les certificats personnalisés chiffrés avec RSA ou ECDSA (algorithme de signature numérique de courbe elliptique).

> Le type de chiffrement de la stratégie de sécurité doit correspondre au type de certificat du serveur. Par exemple, les chiffrements RSA nécessitent des certificats RSA et les chiffrements ECDSA requièrent des certificats ECDSA. Voir "Gérer les certificats de sécurité". Si vous configurez une stratégie de sécurité personnalisée qui n'est pas compatible avec le certificat de serveur, vous pouvez le faire "rétablir temporairement la stratégie de sécurité par défaut".

Pour plus d'informations sur la façon dont StorageGRID sécurise les connexions client pour l'API REST, reportez-vous à la section "Configuration de la sécurité pour l'API REST S3" ou "Configuration de la sécurité pour l'API REST Swift".

Configurer les certificats d'interface de gestion

Vous pouvez remplacer le certificat de l'interface de gestion par défaut par un certificat personnalisé unique qui permet aux utilisateurs d'accéder à Grid Manager et au Gestionnaire de locataires sans rencontrer d'avertissement de sécurité. Vous pouvez également revenir au certificat d'interface de gestion par défaut ou en générer un nouveau.

Description de la tâche

Par défaut, chaque nœud d'administration est doté d'un certificat signé par l'autorité de certification de la grille. Ces certificats signés par l'autorité de certification peuvent être remplacés par un seul certificat d'interface de gestion personnalisée commun et une clé privée correspondante.

Étant donné qu'un seul certificat d'interface de gestion personnalisée est utilisé pour tous les nœuds

d'administration, vous devez spécifier le certificat en tant que certificat générique ou multidomaine si les clients doivent vérifier le nom d'hôte lors de la connexion à Grid Manager et au tenant Manager. Définissez le certificat personnalisé de sorte qu'il corresponde à tous les nœuds d'administration de la grille.

Vous devez terminer la configuration sur le serveur et, en fonction de l'autorité de certification racine (AC) que vous utilisez, les utilisateurs peuvent également avoir besoin d'installer le certificat d'autorité de certification Grid dans le navigateur Web qu'ils utiliseront pour accéder au Grid Manager et au Gestionnaire de locataires.

Pour garantir que les opérations ne sont pas interrompues par un certificat de serveur défaillant, l'alerte **expiration du certificat de serveur pour l'interface de gestion** est déclenchée lorsque ce certificat de serveur est sur le point d'expirer. Si nécessaire, vous pouvez afficher le moment où le certificat en cours expire en sélectionnant **CONFIGURATION** > **sécurité** > **certificats** et en consultant la date d'expiration du certificat de l'interface de gestion dans l'onglet Global.

Si vous accédez à Grid Manager ou au Gestionnaire de locataires à l'aide d'un nom de domaine au lieu d'une adresse IP, le navigateur affiche une erreur de certificat sans option de contournement si l'un des cas suivants se produit :

- Votre certificat d'interface de gestion personnalisée expire.
- Vous restaurez le certificat de serveur par défaut à partir d'un certificat d'interface de gestion personnalisée.

Ajoutez un certificat d'interface de gestion personnalisée

Pour ajouter un certificat d'interface de gestion personnalisée, vous pouvez fournir votre propre certificat ou en générer un à l'aide de Grid Manager.

Étapes

1. Sélectionnez **CONFIGURATION** > **sécurité** > **certificats**.
2. Dans l'onglet **Global**, sélectionnez **Management interface certificate**.
3. Sélectionnez **utiliser le certificat personnalisé**.
4. Chargez ou générez le certificat.

Télécharger le certificat

Téléchargez les fichiers de certificat de serveur requis.

a. Sélectionnez **Télécharger le certificat**.

b. Téléchargez les fichiers de certificat de serveur requis :

- **Certificat de serveur** : fichier de certificat de serveur personnalisé (codé PEM).
- **Clé privée de certificat** : fichier de clé privée de certificat de serveur personnalisé (`.key`).

> Les clés privées EC doivent être de 224 bits ou plus. Les clés privées RSA doivent être de 2048 bits ou plus.

- **Paquet CA** : un fichier facultatif unique contenant les certificats de chaque autorité de certification intermédiaire (AC). Le fichier doit contenir chacun des fichiers de certificat d'autorité de certification codés au PEM, concaténés dans l'ordre de la chaîne de certificats.

c. Développez **Détails du certificat** pour afficher les métadonnées de chaque certificat que vous avez téléchargé. Si vous avez téléchargé un bundle CA facultatif, chaque certificat s'affiche sur son propre onglet.

- Sélectionnez **Télécharger le certificat** pour enregistrer le fichier de certificat ou sélectionnez **Télécharger le paquet CA** pour enregistrer le lot de certificats.

  Spécifiez le nom du fichier de certificat et l'emplacement de téléchargement. Enregistrez le fichier avec l'extension `.pem`.

  Par exemple : `storagegrid_certificate.pem`

- Sélectionnez **Copy certificate PEM** ou **Copy CA bundle PEM** pour copier le contenu du certificat pour le coller ailleurs.

d. Sélectionnez **Enregistrer**. + le certificat d'interface de gestion personnalisée est utilisé pour toutes les nouvelles connexions ultérieures à Grid Manager, tenant Manager, l'API Grid Manager ou l'API tenant Manager.

Générez un certificat

Générez les fichiers de certificat du serveur.

> La meilleure pratique pour un environnement de production consiste à utiliser un certificat d'interface de gestion personnalisée signé par une autorité de certification externe.

a. Sélectionnez **générer certificat**.

b. Spécifiez les informations de certificat :

Champ	Description
Nom de domaine	Un ou plusieurs noms de domaine complets à inclure dans le certificat. Utilisez un * comme caractère générique pour représenter plusieurs noms de domaine.

Champ	Description
IP	Une ou plusieurs adresses IP à inclure dans le certificat.
Objet (facultatif)	Objet X.509 ou nom distinctif (DN) du propriétaire du certificat. Si aucune valeur n'est saisie dans ce champ, le certificat généré utilise le premier nom de domaine ou l'adresse IP comme nom commun de l'objet (CN).
Jours valides	Nombre de jours après la création, pendant lesquels le certificat expire.
Ajouter des extensions d'utilisation de clé	Si cette option est sélectionnée (par défaut et recommandée), l'utilisation des clés et les extensions d'utilisation des clés étendues sont ajoutées au certificat généré. Ces extensions définissent l'objectif de la clé contenue dans le certificat. **Remarque** : ne cochez pas cette case si vous rencontrez des problèmes de connexion avec des clients plus anciens lorsque les certificats incluent ces extensions.

c. Sélectionnez **generate**.

d. Sélectionnez **Détails du certificat** pour afficher les métadonnées du certificat généré.

   - Sélectionnez **Télécharger le certificat** pour enregistrer le fichier de certificat.

     Spécifiez le nom du fichier de certificat et l'emplacement de téléchargement. Enregistrez le fichier avec l'extension `.pem`.

   Par exemple : `storagegrid_certificate.pem`

   - Sélectionnez **Copier le certificat PEM** pour copier le contenu du certificat pour le coller ailleurs.

e. Sélectionnez **Enregistrer**. + le certificat d'interface de gestion personnalisée est utilisé pour toutes les nouvelles connexions ultérieures à Grid Manager, tenant Manager, l'API Grid Manager ou l'API tenant Manager.

5. Actualisez la page pour vous assurer que le navigateur Web est mis à jour.

   Après avoir téléchargé ou généré un nouveau certificat, autorisez jusqu'à un jour l'effacement des alertes d'expiration de certificat associées.

6. Une fois que vous avez ajouté un certificat d'interface de gestion personnalisé, la page de certificat de l'interface de gestion affiche des informations détaillées sur le certificat pour les certificats en cours d'utilisation. + vous pouvez télécharger ou copier le certificat PEM selon vos besoins.

Restaurez le certificat de l'interface de gestion par défaut

Vous pouvez revenir à l'utilisation du certificat d'interface de gestion par défaut pour les connexions Grid

Manager et tenant Manager.

Étapes

1. Sélectionnez **CONFIGURATION** > **sécurité** > **certificats**.
2. Dans l'onglet **Global**, sélectionnez **Management interface certificate**.
3. Sélectionnez **utiliser le certificat par défaut**.

   Lorsque vous restaurez le certificat d'interface de gestion par défaut, les fichiers de certificat de serveur personnalisés que vous avez configurés sont supprimés et ne peuvent pas être récupérés du système. Le certificat d'interface de gestion par défaut est utilisé pour toutes les nouvelles connexions client suivantes.

4. Actualisez la page pour vous assurer que le navigateur Web est mis à jour.

Utilisez un script pour générer un nouveau certificat d'interface de gestion auto-signé

Si une validation stricte du nom d'hôte est requise, vous pouvez utiliser un script pour générer le certificat de l'interface de gestion.

Avant de commencer

- Vous disposez d'autorisations d'accès spécifiques.
- Vous avez le `Passwords.txt` fichier.

Description de la tâche

La meilleure pratique pour un environnement de production consiste à utiliser un certificat signé par une autorité de certification externe.

Étapes

1. Obtenez le nom de domaine complet (FQDN) de chaque nœud d'administration.
2. Connectez-vous au nœud d'administration principal :
   a. Saisissez la commande suivante : `ssh admin@primary_Admin_Node_IP`
   b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
   c. Entrez la commande suivante pour passer à la racine : `su -`
   d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

      Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

3. Configurez StorageGRID avec un nouveau certificat auto-signé.

   ```
   $ sudo make-certificate --domains wildcard-admin-node-fqdn --type management
   ```

   - Pour `--domains`, Utilisez des caractères génériques pour représenter les noms de domaine complets de tous les nœuds d'administration. Par exemple : `*.ui.storagegrid.example.com` utilise le caractère générique * pour représenter `admin1.ui.storagegrid.example.com` et `admin2.ui.storagegrid.example.com`.
   - Réglez `--type` à `management` Pour configurer le certificat de l'interface de gestion, utilisé par Grid Manager et tenant Manager.
   - Par défaut, les certificats générés sont valables pendant un an (365 jours) et doivent être recréés avant leur expiration. Vous pouvez utiliser le `--days` argument pour remplacer la période de validité par

défaut.

> La période de validité d'un certificat commence quand `make-certificate` est exécuté. Vous devez vous assurer que le client de gestion est synchronisé avec la même source horaire que StorageGRID ; sinon, le client peut rejeter le certificat.

```
$ sudo make-certificate --domains *.ui.storagegrid.example.com --type
management --days 720
```

Le résultat contient le certificat public requis par votre client de l'API de gestion.

4. Sélectionnez et copiez le certificat.

   Incluez les étiquettes DE DÉBUT et DE FIN dans votre sélection.

5. Déconnectez-vous du shell de commande. `$ exit`
6. Vérifiez que le certificat a été configuré :
   a. Accédez au Grid Manager.
   b. Sélectionnez **CONFIGURATION** > **sécurité** > **certificats**
   c. Dans l'onglet **Global**, sélectionnez **Management interface certificate**.
7. Configurez votre client de gestion pour utiliser le certificat public que vous avez copié. Incluez les balises DE DÉBUT et DE FIN.

Téléchargez ou copiez le certificat de l'interface de gestion

Vous pouvez enregistrer ou copier le contenu du certificat de l'interface de gestion pour l'utiliser ailleurs.

Étapes

1. Sélectionnez **CONFIGURATION** > **sécurité** > **certificats**.
2. Dans l'onglet **Global**, sélectionnez **Management interface certificate**.
3. Sélectionnez l'onglet **Server** ou **CA bundle**, puis téléchargez ou copiez le certificat.

Téléchargez le fichier de certificat ou le bundle CA

Téléchargez le certificat ou le bundle CA `.pem` fichier. Si vous utilisez un bundle CA facultatif, chaque certificat du bundle s'affiche dans son propre sous-onglet.

a. Sélectionnez **Télécharger le certificat** ou **Télécharger le paquet CA**.

   Si vous téléchargez un bundle CA, tous les certificats des onglets secondaires de l'offre CA sont téléchargés en un seul fichier.

b. Spécifiez le nom du fichier de certificat et l'emplacement de téléchargement. Enregistrez le fichier avec l'extension `.pem`.

   Par exemple : `storagegrid_certificate.pem`

Copie du certificat ou pack CA PEM

Copiez le texte du certificat pour le coller ailleurs. Si vous utilisez un bundle CA facultatif, chaque certificat du bundle s'affiche dans son propre sous-onglet.

a. Sélectionnez **Copy Certificate PEM** ou **Copy CA bundle PEM**.

   Si vous copiez un bundle CA, tous les certificats des onglets secondaires de l'offre CA sont copiés ensemble.

b. Collez le certificat copié dans un éditeur de texte.

c. Enregistrez le fichier texte avec l'extension `.pem`.

   Par exemple : `storagegrid_certificate.pem`

Configurez les certificats API S3 et Swift

Vous pouvez remplacer ou restaurer le certificat du serveur utilisé pour les connexions des clients S3 ou Swift aux nœuds de stockage ou pour équilibreur de charge des terminaux. Le certificat de serveur personnalisé de remplacement est spécifique à votre organisation.

Description de la tâche

Par défaut, chaque nœud de stockage est doté d'un certificat de serveur X.509 signé par l'autorité de certification de la grille. Ces certificats signés par l'autorité de certification peuvent être remplacés par un seul certificat de serveur personnalisé commun et une clé privée correspondante.

Un seul certificat de serveur personnalisé est utilisé pour tous les nœuds de stockage. Vous devez donc spécifier le certificat comme un certificat générique ou multidomaine si les clients doivent vérifier le nom d'hôte lors de la connexion au noeud final de stockage. Définissez le certificat personnalisé de sorte qu'il corresponde à tous les nœuds de stockage de la grille.

Une fois la configuration terminée sur le serveur, vous devrez également installer le certificat d'autorité de certification Grid dans le client API S3 ou Swift que vous utiliserez pour accéder au système, en fonction de l'autorité de certification racine (CA) que vous utilisez.

Pour garantir que les opérations ne sont pas interrompues par un certificat de serveur défaillant, l'alerte **expiration du certificat de serveur global pour S3 et Swift API** est déclenchée lorsque le certificat de serveur racine est sur le point d'expirer. Si nécessaire, vous pouvez afficher le moment où le certificat en cours expire en sélectionnant **CONFIGURATION** > **sécurité** > **certificats** et en consultant la date d'expiration du certificat API S3 et Swift dans l'onglet Global.

Vous pouvez charger ou générer un certificat API S3 et Swift personnalisé.

Ajoutez un certificat S3 et Swift personnalisé

Étapes

1. Sélectionnez **CONFIGURATION** > **sécurité** > **certificats**.
2. Dans l'onglet **Global**, sélectionnez **S3 et certificat API Swift**.
3. Sélectionnez **utiliser le certificat personnalisé**.
4. Chargez ou générez le certificat.

Télécharger le certificat

Téléchargez les fichiers de certificat de serveur requis.

a. Sélectionnez **Télécharger le certificat**.

b. Téléchargez les fichiers de certificat de serveur requis :

- **Certificat de serveur** : fichier de certificat de serveur personnalisé (codé PEM).
- **Clé privée de certificat** : fichier de clé privée de certificat de serveur personnalisé (`.key`).

> Les clés privées EC doivent être de 224 bits ou plus. Les clés privées RSA doivent être de 2048 bits ou plus.

- **Paquet CA** : un fichier facultatif unique contenant les certificats de chaque autorité de délivrance de certificat intermédiaire. Le fichier doit contenir chacun des fichiers de certificat d'autorité de certification codés au PEM, concaténés dans l'ordre de la chaîne de certificats.

c. Sélectionnez les détails du certificat pour afficher les métadonnées et le PEM pour chaque certificat API S3 et Swift personnalisé chargé. Si vous avez téléchargé un bundle CA facultatif, chaque certificat s'affiche sur son propre onglet.

- Sélectionnez **Télécharger le certificat** pour enregistrer le fichier de certificat ou sélectionnez **Télécharger le paquet CA** pour enregistrer le lot de certificats.

  Spécifiez le nom du fichier de certificat et l'emplacement de téléchargement. Enregistrez le fichier avec l'extension `.pem`.

  Par exemple : `storagegrid_certificate.pem`

- Sélectionnez **Copy certificate PEM** ou **Copy CA bundle PEM** pour copier le contenu du certificat pour le coller ailleurs.

d. Sélectionnez **Enregistrer**.

Le certificat de serveur personnalisé est utilisé pour les nouvelles connexions client S3 et Swift suivantes.

Générez un certificat

Générez les fichiers de certificat du serveur.

a. Sélectionnez **générer certificat**.

b. Spécifiez les informations de certificat :

Champ	Description
Nom de domaine	Un ou plusieurs noms de domaine complets à inclure dans le certificat. Utilisez un * comme caractère générique pour représenter plusieurs noms de domaine.
IP	Une ou plusieurs adresses IP à inclure dans le certificat.

Champ	Description
Objet (facultatif)	Objet X.509 ou nom distinctif (DN) du propriétaire du certificat. Si aucune valeur n'est saisie dans ce champ, le certificat généré utilise le premier nom de domaine ou l'adresse IP comme nom commun de l'objet (CN).
Jours valides	Nombre de jours après la création, pendant lesquels le certificat expire.
Ajouter des extensions d'utilisation de clé	Si cette option est sélectionnée (par défaut et recommandée), l'utilisation des clés et les extensions d'utilisation des clés étendues sont ajoutées au certificat généré. Ces extensions définissent l'objectif de la clé contenue dans le certificat. **Remarque** : ne cochez pas cette case si vous rencontrez des problèmes de connexion avec des clients plus anciens lorsque les certificats incluent ces extensions.

c. Sélectionnez **generate**.

d. Sélectionnez **Détails du certificat** pour afficher les métadonnées et PEM pour le certificat d'API S3 et Swift personnalisé qui a été généré.

- Sélectionnez **Télécharger le certificat** pour enregistrer le fichier de certificat.

  Spécifiez le nom du fichier de certificat et l'emplacement de téléchargement. Enregistrez le fichier avec l'extension `.pem`.

  Par exemple : `storagegrid_certificate.pem`

- Sélectionnez **Copier le certificat PEM** pour copier le contenu du certificat pour le coller ailleurs.

e. Sélectionnez **Enregistrer**.

Le certificat de serveur personnalisé est utilisé pour les nouvelles connexions client S3 et Swift suivantes.

5. Sélectionnez un onglet pour afficher les métadonnées du certificat de serveur StorageGRID par défaut, un certificat signé par l'autorité de certification qui a été chargé ou un certificat personnalisé qui a été généré.

> Après avoir téléchargé ou généré un nouveau certificat, autorisez jusqu'à un jour l'effacement des alertes d'expiration de certificat associées.

6. Actualisez la page pour vous assurer que le navigateur Web est mis à jour.
7. Après avoir ajouté un certificat d'API S3 et Swift personnalisé, la page de certificats d'API S3 et Swift affiche des informations détaillées sur le certificat d'API S3 et Swift personnalisé utilisé. + vous pouvez télécharger ou copier le certificat PEM selon vos besoins.

Restaurez le certificat API S3 et Swift par défaut

Vous pouvez revenir à l'utilisation du certificat d'API S3 et Swift par défaut pour les connexions des clients S3 et Swift aux nœuds de stockage. Toutefois, vous ne pouvez pas utiliser le certificat par défaut des API S3 et Swift pour un terminal d'équilibrage des charges.

Étapes

1. Sélectionnez **CONFIGURATION** > **sécurité** > **certificats**.
2. Dans l'onglet **Global**, sélectionnez **S3 et certificat API Swift**.
3. Sélectionnez **utiliser le certificat par défaut**.

   Lorsque vous restaurez la version par défaut du certificat d'API S3 et Swift global, les fichiers de certificat de serveur personnalisé que vous avez configurés sont supprimés et ne peuvent pas être récupérés du système. Le certificat par défaut des API S3 et Swift sera utilisé pour les nouvelles connexions clientes S3 et Swift suivantes aux nœuds de stockage.

4. Sélectionnez **OK** pour confirmer l'avertissement et restaurer le certificat API S3 et Swift par défaut.

   Si vous disposez de l'autorisation d'accès racine et que le certificat d'API S3 et Swift personnalisé a été utilisé pour les connexions de terminal de l'équilibreur de charge, une liste de terminaux d'équilibreur de charge qui ne seront plus accessibles via le certificat d'API S3 et Swift par défaut s'affiche. Accédez à "Configurer les terminaux de l'équilibreur de charge" pour modifier ou supprimer les points finaux affectés.

5. Actualisez la page pour vous assurer que le navigateur Web est mis à jour.

Téléchargez ou copiez le certificat API S3 et Swift

Vous pouvez enregistrer ou copier le contenu du certificat de l'API S3 et Swift pour l'utiliser ailleurs.

Étapes

1. Sélectionnez **CONFIGURATION** > **sécurité** > **certificats**.
2. Dans l'onglet **Global**, sélectionnez **S3 et certificat API Swift**.
3. Sélectionnez l'onglet **Server** ou **CA bundle**, puis téléchargez ou copiez le certificat.

Téléchargez le fichier de certificat ou le bundle CA

Téléchargez le certificat ou le bundle CA `.pem` fichier. Si vous utilisez un bundle CA facultatif, chaque certificat du bundle s'affiche dans son propre sous-onglet.

a. Sélectionnez **Télécharger le certificat** ou **Télécharger le paquet CA**.

   Si vous téléchargez un bundle CA, tous les certificats des onglets secondaires de l'offre CA sont téléchargés en un seul fichier.

b. Spécifiez le nom du fichier de certificat et l'emplacement de téléchargement. Enregistrez le fichier avec l'extension `.pem`.

   Par exemple : `storagegrid_certificate.pem`

Copie du certificat ou pack CA PEM

Copiez le texte du certificat pour le coller ailleurs. Si vous utilisez un bundle CA facultatif, chaque certificat du bundle s'affiche dans son propre sous-onglet.

a. Sélectionnez **Copy Certificate PEM** ou **Copy CA bundle PEM**.

   Si vous copiez un bundle CA, tous les certificats des onglets secondaires de l'offre CA sont copiés ensemble.

b. Collez le certificat copié dans un éditeur de texte.

c. Enregistrez le fichier texte avec l'extension `.pem`.

   Par exemple : `storagegrid_certificate.pem`

Informations associées

- "UTILISEZ L'API REST S3"
- "Utilisez l'API REST de Swift"
- "Configuration des noms de domaine de terminaux S3"

Copiez le certificat de l'autorité de certification Grid

StorageGRID utilise une autorité de certification interne pour sécuriser le trafic interne, Ce certificat ne change pas si vous téléchargez vos propres certificats.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous disposez d'autorisations d'accès spécifiques.

Description de la tâche

Si un certificat de serveur personnalisé a été configuré, les applications client doivent vérifier le serveur à l'aide du certificat de serveur personnalisé. Ils ne doivent pas copier le certificat de l'autorité de certification depuis le système StorageGRID.

Étapes

1. Sélectionnez **CONFIGURATION** > **sécurité** > **certificats**, puis sélectionnez l'onglet **Grid CA**.
2. Dans la section **Certificate PEM**, téléchargez ou copiez le certificat.

Téléchargez le fichier de certificat

Téléchargez le certificat `.pem` fichier.

a. Sélectionnez **Télécharger le certificat**.
b. Spécifiez le nom du fichier de certificat et l'emplacement de téléchargement. Enregistrez le fichier avec l'extension `.pem`.

   Par exemple : `storagegrid_certificate.pem`

Copie du certificat PEM

Copiez le texte du certificat pour le coller ailleurs.

a. Sélectionnez **Copier le certificat PEM**.
b. Collez le certificat copié dans un éditeur de texte.
c. Enregistrez le fichier texte avec l'extension `.pem`.

   Par exemple : `storagegrid_certificate.pem`

Configurez les certificats StorageGRID pour FabricPool

Pour les clients S3 qui valident rigoureusement le nom d'hôte et ne prennent pas en charge la désactivation de la validation stricte du nom d'hôte, comme les clients ONTAP qui utilisent FabricPool, vous pouvez générer ou télécharger un certificat de serveur lorsque vous configurez le terminal de l'équilibreur de charge.

Avant de commencer

- Vous disposez d'autorisations d'accès spécifiques.
- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".

Description de la tâche

Lorsque vous créez un noeud final d'équilibreur de charge, vous pouvez générer un certificat de serveur auto-signé ou télécharger un certificat signé par une autorité de certification connue. Dans les environnements de production, vous devez utiliser un certificat signé par une autorité de certification connue. Les certificats signés par une autorité de certification peuvent être pivotés sans interruption. Elles sont également plus sécurisées parce qu'elles offrent une meilleure protection contre les attaques de l'homme au milieu.

Les étapes suivantes fournissent des instructions d'ordre général pour les clients S3 qui utilisent FabricPool. Pour plus d'informations et de procédures, reportez-vous à la section "Configuration de StorageGRID pour FabricPool".

Étapes

1. Configurez également un groupe haute disponibilité (HA) pour FabricPool à utiliser.
2. Créez un terminal d'équilibrage de charge S3 pour FabricPool.

Lorsque vous créez un noeud final d'équilibreur de charge HTTPS, vous êtes invité à télécharger votre certificat de serveur, votre clé privée de certificat et votre bundle CA facultatif.

3. Association de StorageGRID en tant que Tier cloud dans ONTAP

   Spécifiez le port de point final de l'équilibreur de charge et le nom de domaine complet utilisé dans le certificat de l'autorité de certification que vous avez téléchargé. Ensuite, indiquez le certificat de l'autorité de certification.

   > Si une autorité de certification intermédiaire a émis le certificat StorageGRID, vous devez fournir le certificat CA intermédiaire. Si le certificat StorageGRID a été émis directement par l'autorité de certification racine, vous devez fournir le certificat d'autorité de certification racine.

Configurer les certificats client

Les certificats client permettent aux clients externes autorisés d'accéder à la base de données StorageGRID Prometheus, ce qui fournit un moyen sécurisé aux outils externes de surveillance StorageGRID.

Si vous devez accéder à StorageGRID à l'aide d'un outil de surveillance externe, vous devez télécharger ou générer un certificat client à l'aide de Grid Manager et copier les informations de certificat dans l'outil externe.

Voir "Gérer les certificats de sécurité" et "Configurer des certificats de serveur personnalisés".

> Pour garantir que les opérations ne sont pas interrompues par un certificat de serveur défaillant, l'alerte **expiration des certificats client configurés sur la page certificats** est déclenchée lorsque ce certificat de serveur est sur le point d'expirer. Si nécessaire, vous pouvez afficher le moment où le certificat en cours expire en sélectionnant **CONFIGURATION** > **sécurité** > **certificats** et en consultant la date d'expiration du certificat client dans l'onglet client.

> Si vous utilisez un serveur de gestion des clés (KMS) pour protéger les données sur les nœuds d'appliance spécialement configurés, consultez les informations spécifiques à propos de "Téléchargement d'un certificat client KMS".

Avant de commencer

- Vous disposez de l'autorisation d'accès racine.
- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Pour configurer un certificat client :
  - Vous disposez de l'adresse IP ou du nom de domaine du nœud d'administration.
  - Si vous avez configuré le certificat de l'interface de gestion StorageGRID, l'autorité de certification, le certificat client et la clé privée sont utilisés pour configurer le certificat de l'interface de gestion.
  - Pour télécharger votre propre certificat, la clé privée du certificat est disponible sur votre ordinateur local.
  - La clé privée doit avoir été enregistrée ou enregistrée au moment de sa création. Si vous ne possédez pas la clé privée d'origine, vous devez en créer une nouvelle.
- Pour modifier un certificat client :
  - Vous disposez de l'adresse IP ou du nom de domaine du nœud d'administration.

- Pour télécharger votre propre certificat ou un nouveau certificat, la clé privée, le certificat client et l'autorité de certification (si utilisée) sont disponibles sur votre ordinateur local.

Ajouter des certificats client

Pour ajouter le certificat client, utilisez l'une des procédures suivantes :

- Certificat d'interface de gestion déjà configuré
- CERTIFICAT client émis
- Certificat généré par Grid Manager

Certificat d'interface de gestion déjà configuré

Utilisez cette procédure pour ajouter un certificat client si un certificat d'interface de gestion est déjà configuré à l'aide d'une autorité de certification fournie par le client, d'un certificat client et d'une clé privée.

Étapes

1. Dans le Gestionnaire de grille, sélectionnez **CONFIGURATION** > **sécurité** > **certificats**, puis sélectionnez l'onglet **client**.
2. Sélectionnez **Ajouter**.
3. Entrez un nom de certificat.
4. Pour accéder aux metrics Prometheus à l'aide de votre outil de surveillance externe, sélectionnez **Autoriser prometheus**.
5. Sélectionnez **Continuer**.
6. Pour l'étape **Attach certificates**, téléchargez le certificat de l'interface de gestion.
   a. Sélectionnez **Télécharger le certificat**.
   b. Sélectionnez **Browse** et sélectionnez le fichier de certificat de l'interface de gestion (`.pem`).
      - Sélectionnez **Détails du certificat client** pour afficher les métadonnées du certificat et le certificat PEM.
      - Sélectionnez **Copier le certificat PEM** pour copier le contenu du certificat pour le coller ailleurs.
   c. Sélectionnez **Créer** pour enregistrer le certificat dans le gestionnaire de grille.

      Le nouveau certificat apparaît sur l'onglet client.
7. Configurer un outil de surveillance externe, Comme Grafana.

CERTIFICAT client émis

Utilisez cette procédure pour ajouter un certificat client d'administrateur si un certificat d'interface de gestion n'a pas été configuré et que vous prévoyez d'ajouter un certificat client pour Prometheus qui utilise un certificat client émis par l'autorité de certification et une clé privée.

Étapes

1. Effectuez les étapes à "configurez un certificat d'interface de gestion".
2. Dans le Gestionnaire de grille, sélectionnez **CONFIGURATION** > **sécurité** > **certificats**, puis sélectionnez l'onglet **client**.
3. Sélectionnez **Ajouter**.

4. Entrez un nom de certificat.
5. Pour accéder aux metrics Prometheus à l'aide de votre outil de surveillance externe, sélectionnez **Autoriser prometheus**.
6. Sélectionnez **Continuer**.
7. Pour l'étape **joindre des certificats**, téléchargez le certificat client, la clé privée et les fichiers de bundle CA :
   a. Sélectionnez **Télécharger le certificat**.
   b. Sélectionnez **Browse** et sélectionnez le certificat client, la clé privée et les fichiers de bundle CA (`.pem`).
      - Sélectionnez **Détails du certificat client** pour afficher les métadonnées du certificat et le certificat PEM.
      - Sélectionnez **Copier le certificat PEM** pour copier le contenu du certificat pour le coller ailleurs.
   c. Sélectionnez **Créer** pour enregistrer le certificat dans le gestionnaire de grille.

      Les nouveaux certificats apparaissent sur l'onglet client.
8. Configurer un outil de surveillance externe, Comme Grafana.

Certificat généré par Grid Manager

Utilisez cette procédure pour ajouter un certificat client d'administrateur si un certificat d'interface de gestion n'a pas été configuré et que vous prévoyez d'ajouter un certificat client pour Prometheus qui utilise la fonction générer certificat dans Grid Manager.

Étapes

1. Dans le Gestionnaire de grille, sélectionnez **CONFIGURATION** > **sécurité** > **certificats**, puis sélectionnez l'onglet **client**.
2. Sélectionnez **Ajouter**.
3. Entrez un nom de certificat.
4. Pour accéder aux metrics Prometheus à l'aide de votre outil de surveillance externe, sélectionnez **Autoriser prometheus**.
5. Sélectionnez **Continuer**.
6. Pour l'étape **joindre des certificats**, sélectionnez **générer un certificat**.
7. Spécifiez les informations de certificat :
   - **Sujet** (facultatif) : sujet X.509 ou nom distinctif (DN) du propriétaire du certificat.
   - **Jours valides** : nombre de jours pendant lesquels le certificat généré est valide, à partir du moment où il est généré.
   - **Ajouter des extensions d'utilisation de clé** : si cette option est sélectionnée (par défaut et recommandée), l'utilisation de clé et les extensions d'utilisation de clé étendue sont ajoutées au certificat généré.

     Ces extensions définissent l'objectif de la clé contenue dans le certificat.

     Laissez cette case cochée sauf si vous rencontrez des problèmes de connexion avec des clients plus anciens lorsque les certificats incluent ces extensions.

8. Sélectionnez **generate**.
9. sélectionnez **Détails du certificat client** pour afficher les métadonnées du certificat et le certificat PEM.

   Vous ne pourrez pas afficher la clé privée du certificat après avoir fermé la boîte de dialogue. Copiez ou téléchargez la clé dans un endroit sûr.

   - Sélectionnez **Copier le certificat PEM** pour copier le contenu du certificat pour le coller ailleurs.
   - Sélectionnez **Télécharger le certificat** pour enregistrer le fichier de certificat.

     Spécifiez le nom du fichier de certificat et l'emplacement de téléchargement. Enregistrez le fichier avec l'extension `.pem`.

   Par exemple : `storagegrid_certificate.pem`

   - Sélectionnez **Copier la clé privée** pour copier la clé privée de certificat pour coller ailleurs.
   - Sélectionnez **Télécharger la clé privée** pour enregistrer la clé privée en tant que fichier.

     Spécifiez le nom du fichier de clé privée et l'emplacement de téléchargement.

10. Sélectionnez **Créer** pour enregistrer le certificat dans le gestionnaire de grille.

    Le nouveau certificat apparaît sur l'onglet client.

11. Dans le Gestionnaire de grille, sélectionnez **CONFIGURATION** > **sécurité** > **certificats**, puis sélectionnez l'onglet **Global**.
12. Sélectionnez **certificat d'interface de gestion**.
13. Sélectionnez **utiliser le certificat personnalisé**.
14. Téléchargez les fichiers Certificate.pem et private_key.pem à partir du détails du certificat client étape. Il n'est pas nécessaire de télécharger le pack CA.
    a. Sélectionnez **Télécharger le certificat**, puis **Continuer**.
    b. Téléchargez chaque fichier de certificat (`.pem`).
    c. Sélectionnez **Créer** pour enregistrer le certificat dans le gestionnaire de grille.

       Le nouveau certificat apparaît sur l'onglet client.

15. Configurer un outil de surveillance externe, Comme Grafana.

configurez un outil de surveillance externe

Étapes

1. Configurez les paramètres suivants sur votre outil de surveillance externe, tels que Grafana.
   a. **Nom** : saisissez un nom pour la connexion.

      StorageGRID ne requiert pas ces informations, mais vous devez fournir un nom pour tester la connexion.

   b. **URL** : saisissez le nom de domaine ou l'adresse IP du noeud d'administration. Spécifiez HTTPS et le port 9091.

Par exemple : `https://admin-node.example.com:9091`

c. Activez **TLS client Auth** et **avec CA Cert**.

d. Sous TLS/SSL Auth Details, copiez et collez : +

- Le certificat CA de l'interface de gestion à **CA Cert**
- Le certificat client à **Cert client**
- La clé privée pour **clé client**

e. **NomServeur** : saisissez le nom de domaine du noeud d'administration.

Le nom de serveur doit correspondre au nom de domaine tel qu'il apparaît dans le certificat de l'interface de gestion.

2. Enregistrez et testez le certificat et la clé privée que vous avez copiés à partir de StorageGRID ou d'un fichier local.

Vous avez désormais accès aux metrics Prometheus à partir de StorageGRID grâce à votre outil de surveillance externe.

Pour plus d'informations sur les mesures, reportez-vous à la section "Instructions de surveillance de StorageGRID".

Modifier les certificats client

Vous pouvez modifier un certificat de client d'administrateur pour changer son nom, activer ou désactiver l'accès Prometheus, ou télécharger un nouveau certificat lorsque le certificat actuel a expiré.

Étapes

1. Sélectionnez **CONFIGURATION** > **sécurité** > **certificats**, puis sélectionnez l'onglet **client**.

Les dates d'expiration des certificats et les autorisations d'accès Prometheus sont répertoriées dans le tableau. Si un certificat expire bientôt ou est déjà expiré, un message apparaît dans le tableau et une alerte est déclenchée.

2. Sélectionnez le certificat à modifier.
3. Sélectionnez **Modifier**, puis **Modifier le nom et l'autorisation**
4. Entrez un nom de certificat.
5. Pour accéder aux metrics Prometheus à l'aide de votre outil de surveillance externe, sélectionnez **Autoriser prometheus**.
6. Sélectionnez **Continuer** pour enregistrer le certificat dans Grid Manager.

Le certificat mis à jour s'affiche dans l'onglet client.

Joindre un nouveau certificat client

Vous pouvez télécharger un nouveau certificat lorsque celui actuel a expiré.

Étapes

1. Sélectionnez **CONFIGURATION** > **sécurité** > **certificats**, puis sélectionnez l'onglet **client**.

Les dates d’expiration des certificats et les autorisations d’accès Prometheus sont répertoriées dans le tableau. Si un certificat expire bientôt ou est déjà expiré, un message apparaît dans le tableau et une alerte est déclenchée.

2. Sélectionnez le certificat à modifier.
3. Sélectionnez **Modifier**, puis sélectionnez une option d’édition.

Télécharger le certificat

Copiez le texte du certificat pour le coller ailleurs.

a. Sélectionnez **Télécharger le certificat**, puis **Continuer**.

b. Téléchargez le nom du certificat client (`.pem`).

   Sélectionnez **Détails du certificat client** pour afficher les métadonnées du certificat et le certificat PEM.

   - Sélectionnez **Télécharger le certificat** pour enregistrer le fichier de certificat.

     Spécifiez le nom du fichier de certificat et l'emplacement de téléchargement. Enregistrez le fichier avec l'extension `.pem`.

   Par exemple : `storagegrid_certificate.pem`

   - Sélectionnez **Copier le certificat PEM** pour copier le contenu du certificat pour le coller ailleurs.

c. Sélectionnez **Créer** pour enregistrer le certificat dans le gestionnaire de grille.

   Le certificat mis à jour s'affiche dans l'onglet client.

Générez un certificat

Générez le texte du certificat pour le coller ailleurs.

a. Sélectionnez **générer certificat**.

b. Spécifiez les informations de certificat :

   - **Sujet** (facultatif) : sujet X.509 ou nom distinctif (DN) du propriétaire du certificat.
   - **Jours valides** : nombre de jours pendant lesquels le certificat généré est valide, à partir du moment où il est généré.
   - **Ajouter des extensions d'utilisation de clé** : si cette option est sélectionnée (par défaut et recommandée), l'utilisation de clé et les extensions d'utilisation de clé étendue sont ajoutées au certificat généré.

     Ces extensions définissent l'objectif de la clé contenue dans le certificat.

     Laissez cette case cochée sauf si vous rencontrez des problèmes de connexion avec des clients plus anciens lorsque les certificats incluent ces extensions.

c. Sélectionnez **generate**.

d. Sélectionnez **Détails du certificat client** pour afficher les métadonnées du certificat et le certificat PEM.

   Vous ne pourrez pas afficher la clé privée du certificat après avoir fermé la boîte de dialogue. Copiez ou téléchargez la clé dans un endroit sûr.

   - Sélectionnez **Copier le certificat PEM** pour copier le contenu du certificat pour le coller ailleurs.

- Sélectionnez **Télécharger le certificat** pour enregistrer le fichier de certificat.

  Spécifiez le nom du fichier de certificat et l'emplacement de téléchargement. Enregistrez le fichier avec l'extension `.pem`.

  Par exemple : `storagegrid_certificate.pem`

- Sélectionnez **Copier la clé privée** pour copier la clé privée de certificat pour coller ailleurs.
- Sélectionnez **Télécharger la clé privée** pour enregistrer la clé privée en tant que fichier.

  Spécifiez le nom du fichier de clé privée et l'emplacement de téléchargement.

e. Sélectionnez **Créer** pour enregistrer le certificat dans le gestionnaire de grille.

Le nouveau certificat apparaît sur l'onglet client.

Téléchargez ou copiez les certificats client

Vous pouvez télécharger ou copier un certificat client pour l'utiliser ailleurs.

Étapes

1. Sélectionnez **CONFIGURATION** > **sécurité** > **certificats**, puis sélectionnez l'onglet **client**.
2. Sélectionnez le certificat que vous souhaitez copier ou télécharger.
3. Téléchargez ou copiez le certificat.

Téléchargez le fichier de certificat

Téléchargez le certificat `.pem` fichier.

a. Sélectionnez **Télécharger le certificat**.
b. Spécifiez le nom du fichier de certificat et l'emplacement de téléchargement. Enregistrez le fichier avec l'extension `.pem`.

   Par exemple : `storagegrid_certificate.pem`

Copier le certificat

Copiez le texte du certificat pour le coller ailleurs.

a. Sélectionnez **Copier le certificat PEM**.
b. Collez le certificat copié dans un éditeur de texte.
c. Enregistrez le fichier texte avec l'extension `.pem`.

   Par exemple : `storagegrid_certificate.pem`

Supprimer les certificats client

Si vous n'avez plus besoin d'un certificat de client administrateur, vous pouvez le supprimer.

Étapes

1. Sélectionnez **CONFIGURATION** > **sécurité** > **certificats**, puis sélectionnez l'onglet **client**.
2. Sélectionnez le certificat à supprimer.
3. Sélectionnez **Supprimer**, puis confirmez.

> Pour supprimer jusqu'à 10 certificats, sélectionnez chaque certificat à supprimer dans l'onglet client, puis sélectionnez **actions** > **Supprimer**.

Après la suppression d'un certificat, les clients qui ont utilisé le certificat doivent spécifier un nouveau certificat client pour accéder à la base de données StorageGRID Prometheus.

Configurez les paramètres de sécurité

Gestion des règles TLS et SSH

La règle TLS et SSH détermine les protocoles et les chiffrements utilisés pour établir des connexions TLS sécurisées avec les applications client et des connexions SSH sécurisées avec les services StorageGRID internes.

La règle de sécurité contrôle la façon dont TLS et SSH chiffrent les données en mouvement. En général, utilisez la règle de compatibilité moderne (par défaut), sauf si votre système doit être conforme aux critères communs ou si vous devez utiliser d'autres chiffrements.

> Certains services StorageGRID n'ont pas été mis à jour pour utiliser le chiffrement inclus dans ces règles.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous avez le "Autorisation d'accès racine".

Sélectionnez une stratégie de sécurité

Étapes

1. Sélectionnez **CONFIGURATION** > **sécurité** > **Paramètres de sécurité**.

   L'onglet **TLS et SSH policies** affiche les stratégies disponibles. La règle actuellement active est indiquée par une coche verte sur la vignette de la police.

2. Consultez les vignettes pour en savoir plus sur les stratégies disponibles.

Politique	Description
Compatibilité moderne (par défaut)	Utilisez la stratégie par défaut si vous avez besoin d'un cryptage fort et si vous ne disposez pas d'exigences particulières. Cette règle est compatible avec la plupart des clients TLS et SSH.
Compatibilité avec les systèmes existants	Utilisez cette stratégie si vous avez besoin d'options de compatibilité supplémentaires pour les anciens clients. Les options supplémentaires de cette politique pourraient la rendre moins sécurisée que la politique de compatibilité moderne.
Critères communs	Utilisez cette règle si vous avez besoin de la certification critères communs.
Norme FIPS stricte	Utilisez cette règle si vous avez besoin de la certification critères communs et que vous devez utiliser NetApp Cryptographic Security module 3.0.0 pour les connexions de clients externes vers les terminaux d'équilibrage de charge, le gestionnaire de locataires et Grid Manager. L'utilisation de cette règle peut réduire les performances.
Personnalisées	Créez une stratégie personnalisée si vous devez appliquer vos propres chiffrements.

3. Pour afficher des détails sur les chiffrements, les protocoles et les algorithmes de chaque stratégie, sélectionnez **Afficher les détails**.
4. Pour modifier la stratégie actuelle, sélectionnez **utiliser la stratégie**.

   Une coche verte apparaît en regard de **police actuelle** sur la mosaïque de police.

Créez une stratégie de sécurité personnalisée

Vous pouvez créer une stratégie personnalisée si vous devez appliquer vos propres chiffrements.

Étapes

1. Dans la mosaïque de la stratégie la plus similaire à la stratégie personnalisée que vous souhaitez créer, sélectionnez **Afficher les détails**.
2. Sélectionnez **Copier dans le presse-papiers**, puis sélectionnez **Annuler**.

3. Dans la mosaïque **Personnaliser la stratégie**, sélectionnez **configurer et utiliser**.
4. Collez le fichier JSON que vous avez copié et apportez les modifications nécessaires.
5. Sélectionnez **utiliser la stratégie**.

   Une coche verte apparaît en regard de **politique actuelle** sur la mosaïque de stratégie personnalisée.

6. Si vous le souhaitez, sélectionnez **Modifier la configuration** pour apporter d'autres modifications à la nouvelle stratégie personnalisée.

Rétablir temporairement la stratégie de sécurité par défaut

Si vous avez configuré une stratégie de sécurité personnalisée, il se peut que vous ne puissiez pas vous connecter au gestionnaire de grille si la stratégie TLS configurée est incompatible avec le "certificat de serveur configuré".

Vous pouvez rétablir temporairement la stratégie de sécurité par défaut.

Étapes

1. Connectez-vous à un nœud d'administration :
   a. Saisissez la commande suivante : `ssh admin@Admin_Node_IP`
   b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
   c. Entrez la commande suivante pour passer à la racine : `su -`
   d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

      Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

2. Exécutez la commande suivante :

   ```
   restore-default-cipher-configurations
   ```

3. À partir d'un navigateur Web, accédez à Grid Manager sur le même nœud d'administration.
4. Suivez les étapes de la section Sélectionnez une stratégie de sécurité pour reconfigurer la stratégie.

Vous pouvez configurer la sécurité du réseau et des objets pour chiffrer les objets stockés, empêcher certaines requêtes S3 et Swift, ou autoriser les connexions client aux nœuds de stockage à utiliser le protocole HTTP au lieu du protocole HTTPS.

Chiffrement des objets stockés

Le chiffrement des objets stockés permet de chiffrer toutes les données d'objet lors de leur ingestion via S3. Par défaut, les objets stockés ne sont pas chiffrés, mais vous pouvez choisir de chiffrer les objets à l'aide de l'algorithme de cryptage AES-128 ou AES-256. Lorsque vous activez le paramètre, tous les objets récemment acquis sont chiffrés, mais aucun changement n'est apporté aux objets stockés existants. Si vous désactivez le chiffrement, les objets actuellement chiffrés restent chiffrés, mais les objets nouvellement ingérés ne sont pas chiffrés.

Le paramètre de chiffrement des objets stockés s'applique uniquement aux objets S3 qui n'ont pas été chiffrés par chiffrement au niveau du compartiment ou de l'objet.

Pour plus d'informations sur les méthodes de cryptage StorageGRID, reportez-vous à la section "Étudiez les méthodes de cryptage StorageGRID".

Empêcher toute modification du client

Empêcher la modification du client est un paramètre à l'échelle du système. Lorsque l'option **empêcher la modification du client** est sélectionnée, les demandes suivantes sont refusées.

L'API REST S3

- Supprimer les demandes de compartiment
- Toute demande de modification des données d'un objet existant, des métadonnées définies par l'utilisateur ou du balisage d'objets S3

API REST Swift

- Supprimer les demandes de conteneur
- Demande de modifier tout objet existant. Par exemple, les opérations suivantes sont refusées : remplacement, suppression, mise à jour des métadonnées, etc.

Activez HTTP pour les connexions de nœud de stockage

Par défaut, les applications clientes utilisent le protocole réseau HTTPS pour toutes les connexions directes aux nœuds de stockage. Vous pouvez éventuellement activer HTTP pour ces connexions, par exemple lors du test d'une grille autre que la production.

Utilisez HTTP pour les connexions de nœuds de stockage uniquement si les clients S3 et Swift doivent établir des connexions HTTP directement aux nœuds de stockage. Vous n'avez pas besoin d'utiliser cette option pour les clients qui utilisent uniquement des connexions HTTPS ou pour les clients qui se connectent au service Load Balancer (parce que vous le pouvez) "configurez chaque point d'extrémité de l'équilibreur de charge" Pour utiliser HTTP ou HTTPS).

Voir "Résumé : adresses IP et ports pour les connexions client" Pour savoir quels ports les clients S3 et Swift utilisent lors de la connexion aux nœuds de stockage via HTTP ou HTTPS.

Sélectionnez les options

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous disposez de l'autorisation d'accès racine.

Étapes

1. Sélectionnez **CONFIGURATION** > **sécurité** > **Paramètres de sécurité**.
2. Sélectionnez l'onglet **réseau et objets**.
3. Pour le chiffrement des objets stockés, utilisez le paramètre **None** (par défaut) si vous ne souhaitez pas que les objets stockés soient cryptés, ou sélectionnez **AES-128** ou **AES-256** pour crypter les objets stockés.
4. Vous pouvez également sélectionner **empêcher la modification du client** si vous souhaitez empêcher les clients S3 et Swift de faire des demandes spécifiques.

   Si vous modifiez ce paramètre, il faudra environ une minute pour appliquer le nouveau paramètre. La valeur configurée est mise en cache pour les performances et l'évolutivité.

5. Sélectionnez **Activer HTTP pour les connexions de noeud de stockage** si les clients se connectent directement aux noeuds de stockage et que vous souhaitez utiliser les connexions HTTP.

   Soyez prudent lorsque vous activez HTTP pour une grille de production car les requêtes seront envoyées de manière non chiffrée.

6. Sélectionnez **Enregistrer**.

Modifier le délai d'inactivité du navigateur

Vous pouvez contrôler si les utilisateurs de Grid Manager et de tenant Manager sont déconnectés s'ils sont inactifs pendant plus d'un certain temps.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous disposez de l'autorisation d'accès racine.

Description de la tâche

Par défaut, le délai d'inactivité du navigateur est de 15 minutes. Si le navigateur d'un utilisateur n'est pas actif pendant cette période, l'utilisateur est déconnecté.

Si nécessaire, vous pouvez augmenter ou diminuer le délai d'expiration en définissant l'option **déconnecter les utilisateurs inactifs après**.

Le délai d'inactivité du navigateur est également contrôlé par les éléments suivants :

- Un minuteur StorageGRID séparé non configurable, inclus pour la sécurité du système. Par défaut, le jeton d'authentification de chaque utilisateur expire 16 heures après la connexion de l'utilisateur. Lorsque l'authentification d'un utilisateur expire, cet utilisateur est automatiquement déconnecté, même si le délai d'inactivité du navigateur est désactivé ou si la valeur du délai d'inactivité du navigateur n'a pas été atteinte. Pour renouveler le jeton, l'utilisateur doit se reconnecter.
- Paramètres de délai d'expiration pour le fournisseur d'identité, en supposant que l'authentification unique

(SSO) est activée pour StorageGRID.

Si la fonction SSO est activée et que le navigateur d'un utilisateur arrive à expiration, l'utilisateur doit saisir à nouveau ses informations d'identification SSO pour accéder à StorageGRID à nouveau. Voir "Configurer l'authentification unique".

Étapes

1. Sélectionnez **CONFIGURATION** > **sécurité** > **Paramètres de sécurité**.
2. Sélectionnez l'onglet **délai d'inactivité du navigateur**.
3. Dans le champ **déconnecter les utilisateurs inactifs après**, spécifiez un délai d'expiration du navigateur compris entre 60 secondes et 7 jours.

   Vous pouvez spécifier le délai d'expiration du navigateur en secondes, minutes, heures ou jours.

4. Sélectionnez **Enregistrer**. Si un navigateur est inactif pendant la durée spécifiée, l'utilisateur est déconnecté du Gestionnaire de grille ou du Gestionnaire de locataires.

   Le nouveau paramètre n'affecte pas les utilisateurs actuellement connectés. Les utilisateurs doivent se reconnecter ou actualiser leur navigateur pour que le nouveau paramètre de délai d'expiration prenne effet.

Configurer les serveurs de gestion des clés

Configurer les serveurs de gestion des clés : présentation

Vous pouvez configurer un ou plusieurs serveurs de gestion externe des clés (KMS) afin de protéger les données sur les nœuds d'appliance spécialement configurés.

Qu'est-ce qu'un serveur de gestion des clés (KMS) ?

Un serveur de gestion des clés (KMS) est un système externe tiers qui fournit des clés de chiffrement aux nœuds d'appliance StorageGRID sur le site StorageGRID associé à l'aide du protocole KMIP (Key Management Interoperability Protocol).

Vous pouvez utiliser un ou plusieurs serveurs de gestion des clés pour gérer les clés de cryptage de nœud pour tous les nœuds d'appliance StorageGRID dont le paramètre **Node Encryption** est activé pendant l'installation. L'utilisation de serveurs de gestion des clés avec ces nœuds de dispositif permet de protéger vos données même en cas de retrait d'une appliance du data Center. Une fois les volumes de l'appliance chiffrés, vous ne pouvez accéder aux données de l'appliance que si le nœud peut communiquer avec le KMS.

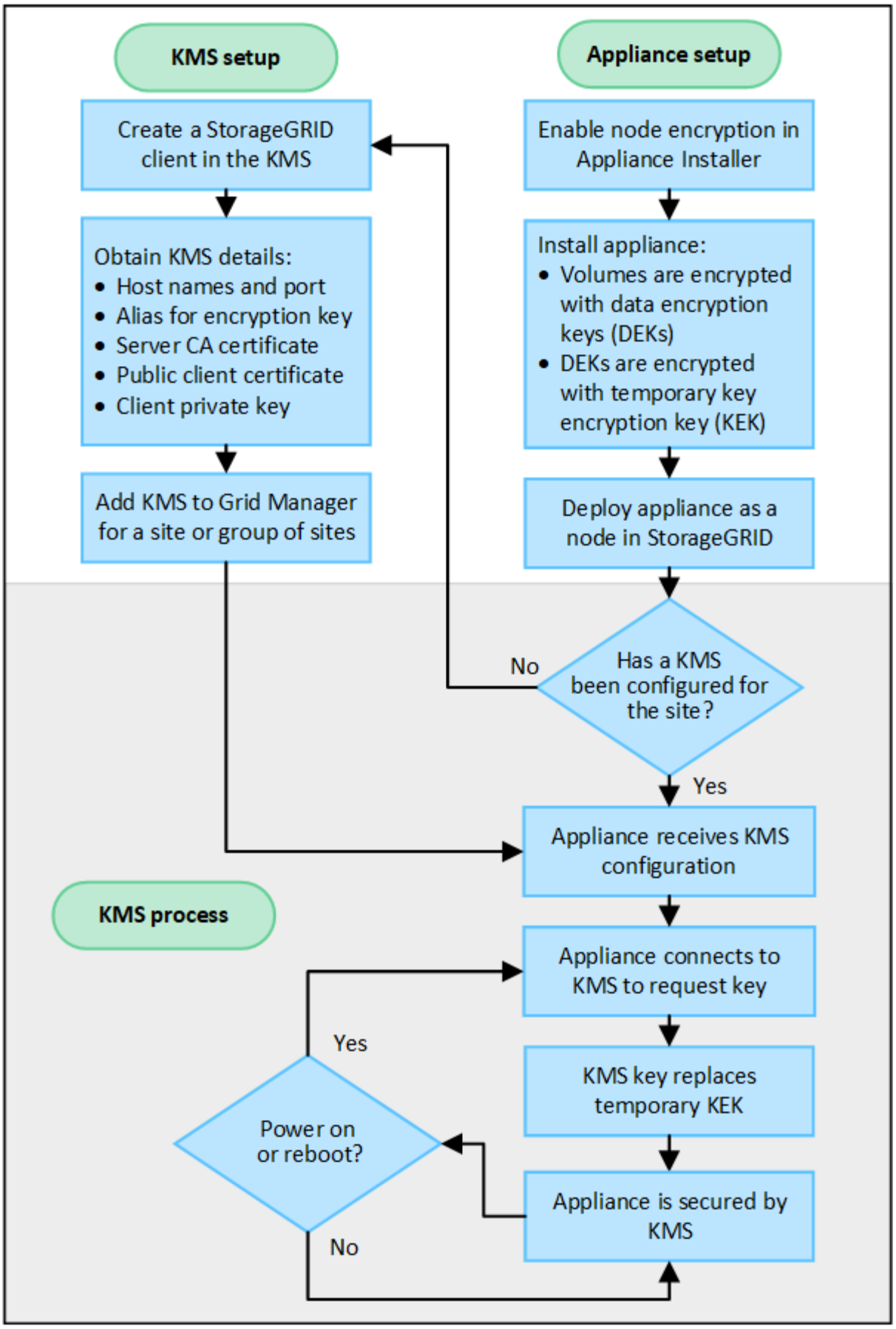
> StorageGRID ne crée ni ne gère pas les clés externes utilisées pour chiffrer et décrypter les nœuds des systèmes. Si vous prévoyez d'utiliser un serveur de gestion externe des clés pour protéger les données StorageGRID, vous devez comprendre comment configurer ce serveur et savoir comment gérer les clés de cryptage. Ces instructions ne sont pas uniquement destinées à effectuer des tâches de gestion clés. Si vous avez besoin d'aide, consultez la documentation de votre serveur de gestion des clés ou contactez le support technique.

Présentation de la configuration des appliances et KMS

Avant d'utiliser un serveur de gestion des clés (KMS) afin de sécuriser les données StorageGRID sur les nœuds de l'appliance, vous devez effectuer deux tâches de configuration : configurer un ou plusieurs serveurs KMS et activer le chiffrement des

nœuds pour les nœuds de l’appliance. Une fois ces deux tâches de configuration terminées, le processus de gestion des clés est automatique.

L’organigramme présente les étapes générales permettant d’utiliser un KMS pour sécuriser les données StorageGRID sur les nœuds du dispositif.



L’organigramme présente la configuration du KMS et l’appliance en parallèle. Toutefois, vous pouvez

configurer les serveurs de gestion des clés avant ou après avoir activé le chiffrement des nœuds pour les nouveaux nœuds d'appliance, selon vos besoins.

Configuration du serveur de gestion des clés (KMS)

La configuration d'un serveur de gestion des clés comprend les étapes générales suivantes.

Étape	Reportez-vous à la section
Accédez au logiciel KMS et ajoutez un client pour StorageGRID à chaque cluster KMS ou KMS.	"Configurer StorageGRID en tant que client dans le KMS"
Obtenir les informations requises pour le client StorageGRID sur le KMS.	"Configurer StorageGRID en tant que client dans le KMS"
Ajoutez le KMS à Grid Manager, attribuez-le à un seul site ou à un groupe de sites par défaut, téléchargez les certificats requis et enregistrez la configuration KMS.	"Ajout d'un serveur de gestion des clés (KMS)"

Configurez l'appareil

La configuration d'un nœud d'appliance pour l'utilisation de KMS comprend les étapes générales suivantes.

1. Pendant l'étape de configuration matérielle de l'installation de l'appliance, utilisez le programme d'installation de l'appliance StorageGRID pour activer le paramètre **Node Encryption** pour l'appliance.

   > Vous ne pouvez pas activer le paramètre **Node Encryption** après l'ajout d'une appliance à la grille, et vous ne pouvez pas utiliser la gestion de clés externe pour les appliances pour lesquelles le chiffrement de nœud n'est pas activé.

2. Exécutez le programme d'installation de l'appliance StorageGRID. Lors de l'installation, une clé de chiffrement aléatoire des données (DEK) est attribuée à chaque volume de dispositif, comme suit :
   - Les clés de licence sont utilisées pour chiffrer les données sur chaque volume. Ces clés sont générées à l'aide du chiffrement de disque LUKS (Unified Key Setup) Linux dans le système d'exploitation de l'appliance et ne peuvent pas être modifiées.
   - Chaque DEK individuel est chiffré par une clé de cryptage principale (KEK). La KEK initiale est une clé temporaire qui chiffre les clés de fin de séjour jusqu'à ce que l'appareil puisse se connecter au KMS.
3. Ajoutez le nœud d'appliance à StorageGRID.

Voir "Activez le chiffrement de nœud" pour plus d'informations.

Processus de chiffrement de la gestion des clés (automatique)

Le chiffrement de la gestion des clés inclut les étapes générales suivantes qui sont automatiquement effectuées.

1. Lorsque vous installez une appliance sur laquelle le chiffrement de nœud est activé dans le grid, StorageGRID détermine si une configuration KMS existe pour le site qui contient le nouveau nœud.
   - Si un KMS a déjà été configuré pour le site, l'appliance reçoit la configuration KMS.

- Si un KMS n'a pas encore été configuré pour le site, les données de l'appliance continuent d'être cryptées par le KEK temporaire jusqu'à ce que vous configuriez un KMS pour le site et que l'appliance reçoive la configuration KMS.

2. L'appliance utilise la configuration KMS pour vous connecter au KMS et demander une clé de chiffrement.
3. Le KMS envoie une clé de chiffrement à l'appliance. La nouvelle clé du KMS remplace la KEK temporaire et est maintenant utilisée pour crypter et décrypter les clés de fin de séjour des volumes d'appliance.

> Toutes les données qui existent avant que le nœud d'appliance chiffré ne se connecte au KMS configuré sont chiffrées à l'aide d'une clé temporaire. Cependant, les volumes de l'appliance ne doivent pas être considérés comme protégés de leur retrait du data Center tant que la clé temporaire n'est pas remplacée par la clé de cryptage KMS.

4. Si l'appliance est sous tension ou redémarrée, elle se reconnecte au KMS pour demander la clé. La clé, enregistrée dans la mémoire volatile, ne peut pas survivre à une perte de puissance ou à un redémarrage.

Considérations et conditions requises pour l'utilisation d'un serveur de gestion des clés

Avant de configurer un serveur de gestion des clés externe (KMS), vous devez connaître les considérations et les exigences requises.

Quelles sont les exigences du protocole KMIP ?

StorageGRID prend en charge KMIP version 1.4.

"Spécification du protocole d'interopérabilité de gestion des clés version 1.4"

Les communications entre les nœuds d'appliance et le KMS configuré utilisent des connexions TLS sécurisées. StorageGRID prend en charge le chiffrement TLS v1.2 suivant pour KMIP :

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

Vous devez vous assurer que chaque nœud d'appliance qui utilise le chiffrement de nœud dispose d'un accès réseau au cluster KMS ou KMS que vous avez configuré pour le site.

Les paramètres de pare-feu réseau doivent permettre à chaque nœud de l'appliance de communiquer via le port utilisé pour les communications KMIP (Key Management Interoperability Protocol). Le port KMIP par défaut est 5696.

Quels dispositifs sont pris en charge ?

Vous pouvez utiliser un serveur de gestion des clés (KMS) pour gérer les clés de cryptage de n'importe quelle appliance StorageGRID de la grille dont le paramètre **Node Encryption** est activé. Ce paramètre ne peut être activé que lors de l'étape de configuration matérielle de l'installation de l'appliance à l'aide du programme d'installation de l'appliance StorageGRID.

> Le chiffrement des nœuds ne peut pas être activé après l'ajout d'une appliance à la grille. De plus, vous ne pouvez pas utiliser la gestion externe des clés pour les appliances pour lesquelles le chiffrement des nœuds n'est pas activé.

Vous pouvez utiliser le KMS configuré pour les appliances et les nœuds StorageGRID.

Vous ne pouvez pas utiliser le KMS configuré pour les nœuds logiciels (non liés à l'appliance) :

- Nœuds déployés en tant que machines virtuelles
- Nœuds déployés dans les moteurs de mise en conteneurs sur les hôtes Linux

Les nœuds déployés sur ces autres plateformes peuvent utiliser le cryptage en dehors de StorageGRID au niveau du datastore ou du disque.

Quand dois-je configurer les serveurs de gestion des clés ?

Dans le cadre d'une nouvelle installation, vous devez généralement configurer un ou plusieurs serveurs de gestion des clés dans Grid Manager avant de créer des locataires. Cette commande garantit que les nœuds sont protégés avant que des données d'objet ne soient stockées sur ces nœuds.

Vous pouvez configurer les serveurs de gestion des clés dans Grid Manager avant ou après l'installation des nœuds de l'appliance.

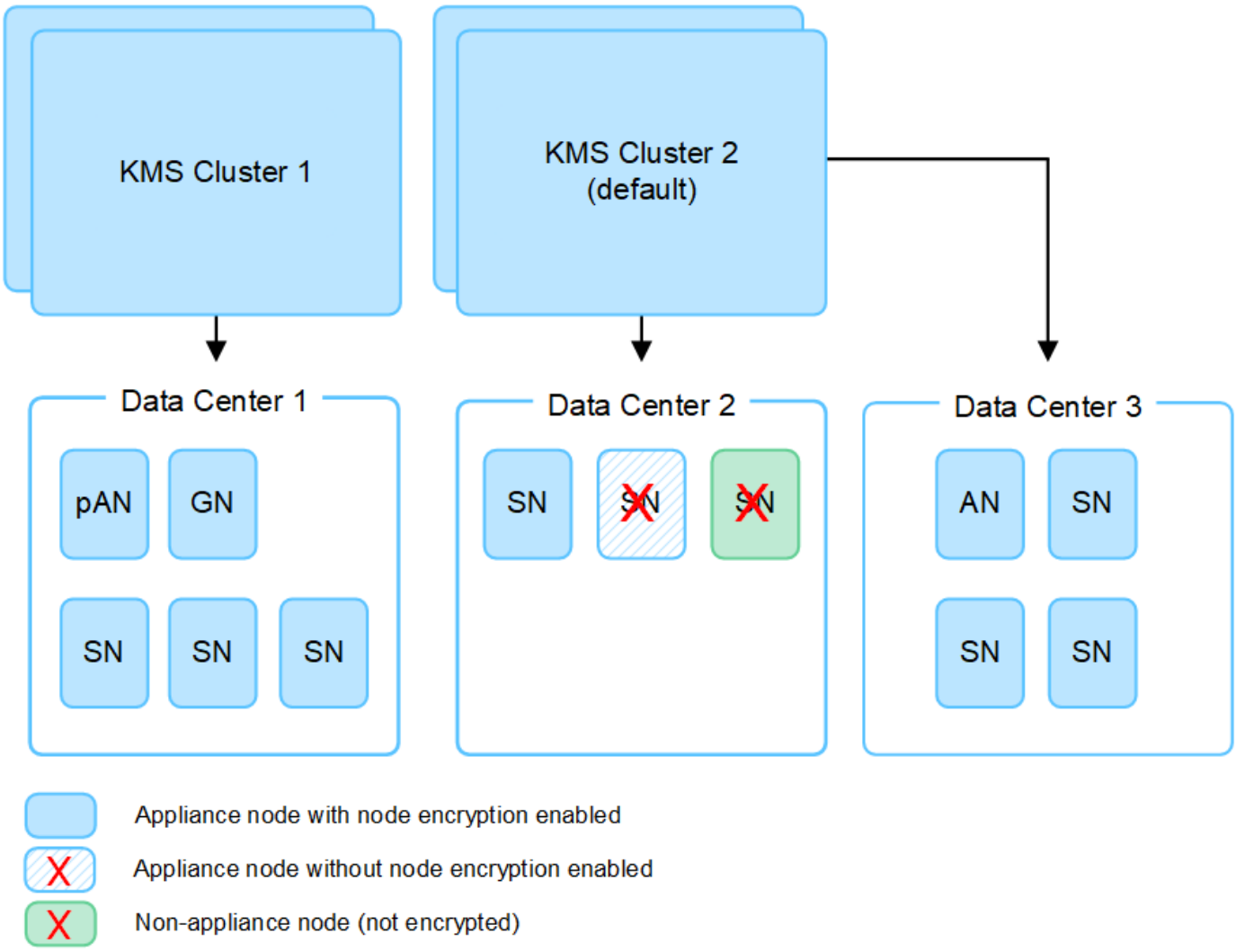
Combien de serveurs de gestion des clés ai-je besoin ?

Vous pouvez configurer un ou plusieurs serveurs de gestion externe des clés de chiffrement pour les nœuds d'appliance de votre système StorageGRID. Chaque KMS fournit une clé de chiffrement unique aux nœuds d'appliance StorageGRID sur un seul site ou dans un groupe de sites.

StorageGRID prend en charge l'utilisation des clusters KMS. Chaque cluster KMS contient plusieurs serveurs de gestion des clés répliqués qui partagent les paramètres de configuration et les clés de chiffrement. L'utilisation de clusters KMS pour la gestion des clés est recommandée, car il améliore les fonctionnalités de basculement d'une configuration haute disponibilité.

Supposons par exemple que votre système StorageGRID possède trois sites de data Center. Vous pouvez configurer un cluster KMS pour que tous les nœuds d'appliance soient essentiels dans le Data Center 1 et un second cluster KMS pour que ces derniers soient essentiels pour que tous les nœuds d'appliance soient disponibles sur les autres sites. Lorsque vous ajoutez le second cluster KMS, vous pouvez configurer un KMS par défaut pour Data Center 2 et Data Center 3.

Notez que vous ne pouvez pas utiliser de KMS pour les nœuds non liés à l'appliance ou pour les nœuds d'appliance sur lesquels le paramètre **Node Encryption** n'a pas été activé lors de l'installation.



Que se passe-t-il lorsqu'une clé est tournée ?

Dans le cadre de nos meilleures pratiques en matière de sécurité, vous devez régulièrement faire tourner la clé de chiffrement utilisée par chaque KMS configuré.

Lors de la rotation de la clé de chiffrement, utilisez le logiciel KMS pour faire pivoter la dernière version utilisée de la clé vers une nouvelle version de la même clé. Ne tournez pas vers une clé complètement différente.

> Ne tentez jamais de faire pivoter une clé en modifiant le nom de clé (alias) du KMS dans Grid Manager. Faites plutôt pivoter la clé en mettant à jour la version de clé dans le logiciel KMS. Utilisez le même alias de clé pour les nouvelles clés que celles utilisées pour les touches précédentes. Si vous modifiez l'alias de clé pour un KMS configuré, StorageGRID risque de ne pas être en mesure de décrypter vos données.

Lorsque la nouvelle version de clé est disponible :

- Elle est automatiquement distribuée aux nœuds d'appliance chiffrés sur le site ou les sites associés au KMS. La distribution doit se produire dans une heure après la rotation de la clé.
- Si le nœud d'appliance chiffré est hors ligne lorsque la nouvelle version de clé est distribuée, le nœud reçoit la nouvelle clé dès le redémarrage.

- Si la nouvelle version de clé ne peut pas être utilisée pour chiffrer les volumes de l'appliance pour une raison quelconque, l'alerte **Echec de la rotation de la clé de chiffrement KMS** est déclenchée pour le nœud de l'appliance. Vous devrez peut-être contacter le support technique pour obtenir de l'aide afin de résoudre cette alerte.

Puis-je réutiliser un nœud d'appliance après chiffrement ?

Si vous devez installer une appliance chiffrée dans un autre système StorageGRID, vous devez d'abord désactiver le nœud de grille pour déplacer les données d'objet vers un autre nœud. Vous pouvez ensuite utiliser le programme d'installation de l'appliance StorageGRID pour "Effacez la configuration KMS". L'effacement de la configuration KMS désactive le paramètre **Node Encryption** et supprime l'association entre le nœud de l'appliance et la configuration KMS pour le site StorageGRID.

> Étant donnée l'accès à la clé de chiffrement KMS, toutes les données conservées sur l'appliance ne sont plus accessibles et sont verrouillées en permanence.

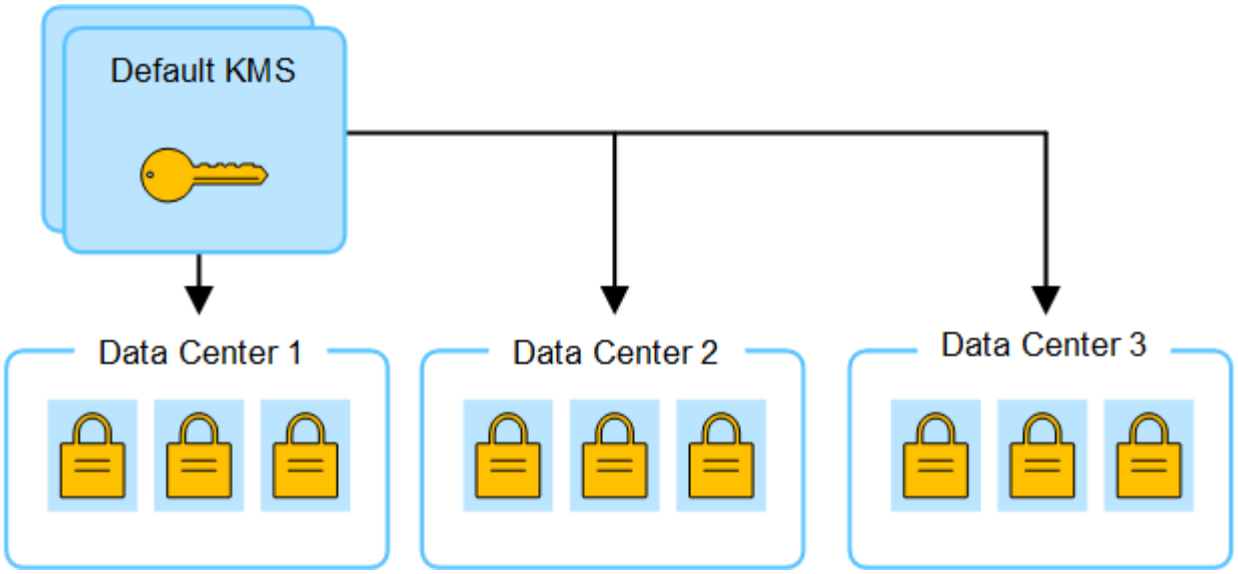
Considérations relatives à la modification du KMS pour un site

Chaque cluster de serveur de gestion des clés (KMS) ou KMS fournit une clé de chiffrement à tous les nœuds d'appliance sur un site unique ou dans un groupe de sites. Si vous devez modifier le KMS utilisé pour un site, vous devrez peut-être copier la clé de chiffrement d'un KMS vers un autre.

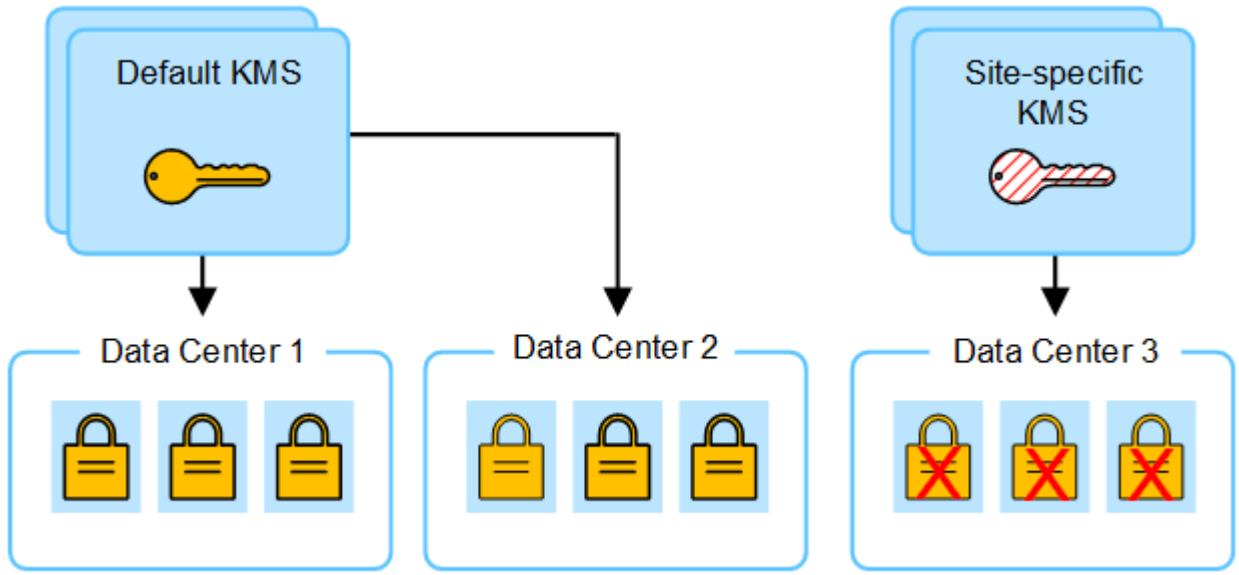
Si vous modifiez le KMS utilisé pour un site, vous devez vous assurer que les nœuds d'appliance précédemment cryptés de ce site peuvent être déchiffrés à l'aide de la clé stockée sur le nouveau KMS. Dans certains cas, vous devrez peut-être copier la version actuelle de la clé de chiffrement à partir du KMS d'origine vers le nouveau KMS. Vous devez vous assurer que le KMS dispose de la clé correcte pour décrypter les nœuds de l'appliance chiffrée sur le site.

Par exemple :

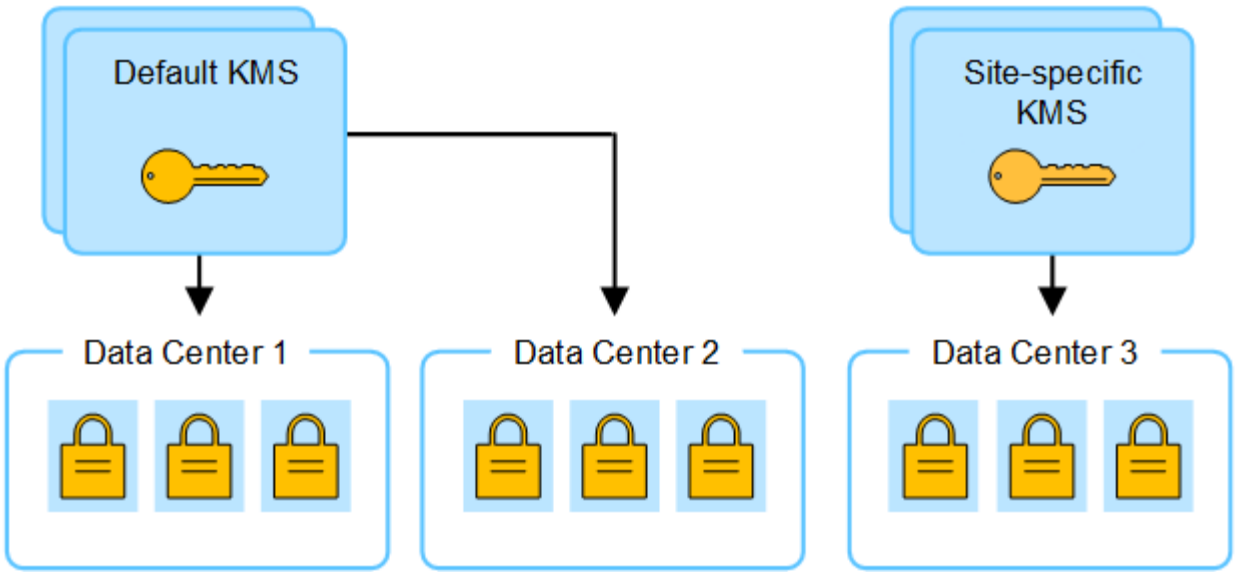
1. Vous configurez initialement un KMS par défaut qui s'applique à tous les sites qui ne disposent pas d'un KMS dédié.
2. Lorsque le KMS est enregistré, tous les nœuds de l'appliance dont le paramètre **Node Encryption** est activé se connectent au KMS et demandent la clé de chiffrement. Cette clé est utilisée pour chiffrer les nœuds de l'appliance sur tous les sites. Cette même clé doit également être utilisée pour décrypter ces dispositifs.



3. Vous décidez d'ajouter un KMS spécifique au site pour un site (Data Center 3 dans la figure). Toutefois, les nœuds d'appliance sont déjà chiffrés. Une erreur de validation se produit lorsque vous tentez d'enregistrer la configuration du KMS spécifique au site. L'erreur se produit car le KMS spécifique au site ne dispose pas de la clé correcte pour décrypter les nœuds de ce site.



4. Pour résoudre ce problème, vous copiez la version actuelle de la clé de chiffrement à partir du KMS par défaut vers le nouveau KMS. (Techniquement, vous copiez la clé d'origine dans une nouvelle clé avec le même alias. La clé d'origine devient une version antérieure de la nouvelle clé.) Le KMS spécifique au site dispose désormais de la clé correcte pour décrypter les nœuds d'appliance sur Data Center 3, afin qu'ils puissent être sauvegardés sur StorageGRID.



Cas d'utilisation pour changer quel KMS est utilisé pour un site

Le tableau résume les étapes requises pour les cas les plus courants de modification du KMS pour un site.

Cas d'utilisation lors de la modification du KMS d'un site	Étapes requises
Vous avez une ou plusieurs entrées KMS spécifiques au site, et vous souhaitez utiliser l'une d'entre elles comme étant le KMS par défaut.	Modifiez le KMS spécifique au site. Dans le champ **gère clés pour**, sélectionnez **sites non gérés par un autre KMS (KMS par défaut)**. Le KMS spécifique au site sera maintenant utilisé comme KMS par défaut. Il s'appliquera à tous les sites qui n'ont pas de KMS dédié. "Modification d'un serveur de gestion des clés (KMS)"
Vous avez un KMS par défaut et vous ajoutez un nouveau site dans une extension. Vous ne souhaitez pas utiliser le KMS par défaut pour le nouveau site.	1. Si les nœuds d'appliance du nouveau site ont déjà été chiffrés par le KMS par défaut, utilisez le logiciel KMS pour copier la version actuelle de la clé de chiffrement à partir du KMS par défaut vers un nouveau KMS. 2. À l'aide de Grid Manager, ajoutez le nouveau KMS et sélectionnez le site. "Ajout d'un serveur de gestion des clés (KMS)"
Vous souhaitez que le KMS pour un site utilise un serveur différent.	1. Si les nœuds d'appliance du site ont déjà été chiffrés par le KMS existant, utilisez le logiciel KMS pour copier la version actuelle de la clé de chiffrement à partir du KMS existant vers le nouveau KMS. 2. À l'aide de Grid Manager, modifiez la configuration KMS existante et entrez le nouveau nom d'hôte ou l'adresse IP. "Ajout d'un serveur de gestion des clés (KMS)"

Configurer StorageGRID en tant que client dans le KMS

Vous devez configurer StorageGRID en tant que client pour chaque serveur de gestion

externe des clés ou cluster KMS avant de pouvoir ajouter le KMS à StorageGRID.

Description de la tâche

Ces instructions s'appliquent au gestionnaire Thales CipherTrust. Pour obtenir la liste des versions prises en charge, utilisez le "Matrice d'interopérabilité NetApp (IMT)".

Étapes

1. À partir du logiciel KMS, créez un client StorageGRID pour chaque cluster KMS ou KMS que vous souhaitez utiliser.

   Chaque KMS gère une clé de chiffrement unique pour les nœuds d'appliances StorageGRID dans un seul site ou dans un groupe de sites.

2. Depuis le logiciel KMS, créez une clé de chiffrement AES pour chaque cluster KMS ou KMS.

   La clé de chiffrement doit être de 2,048 bits ou plus et doit être exportable.

3. Notez les informations suivantes pour chaque cluster KMS ou KMS.

   Vous avez besoin de ces informations lorsque vous ajoutez le KMS à StorageGRID.

   - Nom d'hôte ou adresse IP pour chaque serveur.
   - Port KMIP utilisé par le KMS.
   - Alias de clé pour la clé de cryptage dans le KMS.

     > La clé de chiffrement doit déjà exister dans le KMS. StorageGRID ne crée ni ne gère pas de clés KMS.

4. Pour chaque cluster KMS ou KMS, procurez-vous un certificat de serveur signé par une autorité de certification (CA) ou un bundle de certificats contenant chacun des fichiers de certificat d'autorité de certification codés au PEM, concaténés dans l'ordre de la chaîne de certificats.

   Le certificat du serveur permet au KMS externe de s'authentifier auprès de StorageGRID.

   - Le certificat doit utiliser le format X.509 encodé au format PEM (Privacy Enhanced Mail) Base-64.
   - Le champ Subject alternative Name (SAN) de chaque certificat de serveur doit inclure le nom de domaine complet (FQDN) ou l'adresse IP à laquelle StorageGRID se connectera.

     > Lorsque vous configurez le KMS dans StorageGRID, vous devez entrer les mêmes FQDN ou adresses IP dans le champ **Hostname**.

   - Le certificat du serveur doit correspondre au certificat utilisé par l'interface KMIP du KMS, qui utilise généralement le port 5696.

5. Obtenir le certificat du client public délivré à StorageGRID par le KMS externe et la clé privée du certificat du client.

   Le certificat client permet à StorageGRID de s'authentifier auprès du KMS.

Ajout d'un serveur de gestion des clés (KMS)

L'assistant de serveur de gestion des clés StorageGRID vous permet d'ajouter chaque

cluster KMS ou KMS.

Avant de commencer

- Vous avez passé en revue le "considérations et conditions requises pour l'utilisation d'un serveur de gestion des clés".
- Vous avez "Configuration de StorageGRID en tant que client dans le KMS", Et vous disposez des informations requises pour chaque cluster KMS ou KMS.
- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous disposez de l'autorisation d'accès racine.

Description de la tâche

Si possible, configurez tous les serveurs de gestion de clés spécifiques au site avant de configurer un KMS par défaut qui s'applique à tous les sites non gérés par un autre KMS. Si vous créez d'abord le KMS par défaut, toutes les appliances chiffrées par nœud dans le grid seront chiffrées par le KMS par défaut. Si vous souhaitez créer ultérieurement un KMS spécifique au site, vous devez d'abord copier la version actuelle de la clé de chiffrement à partir du KMS par défaut vers le nouveau KMS. Voir "Considérations relatives à la modification du KMS pour un site" pour plus d'informations.

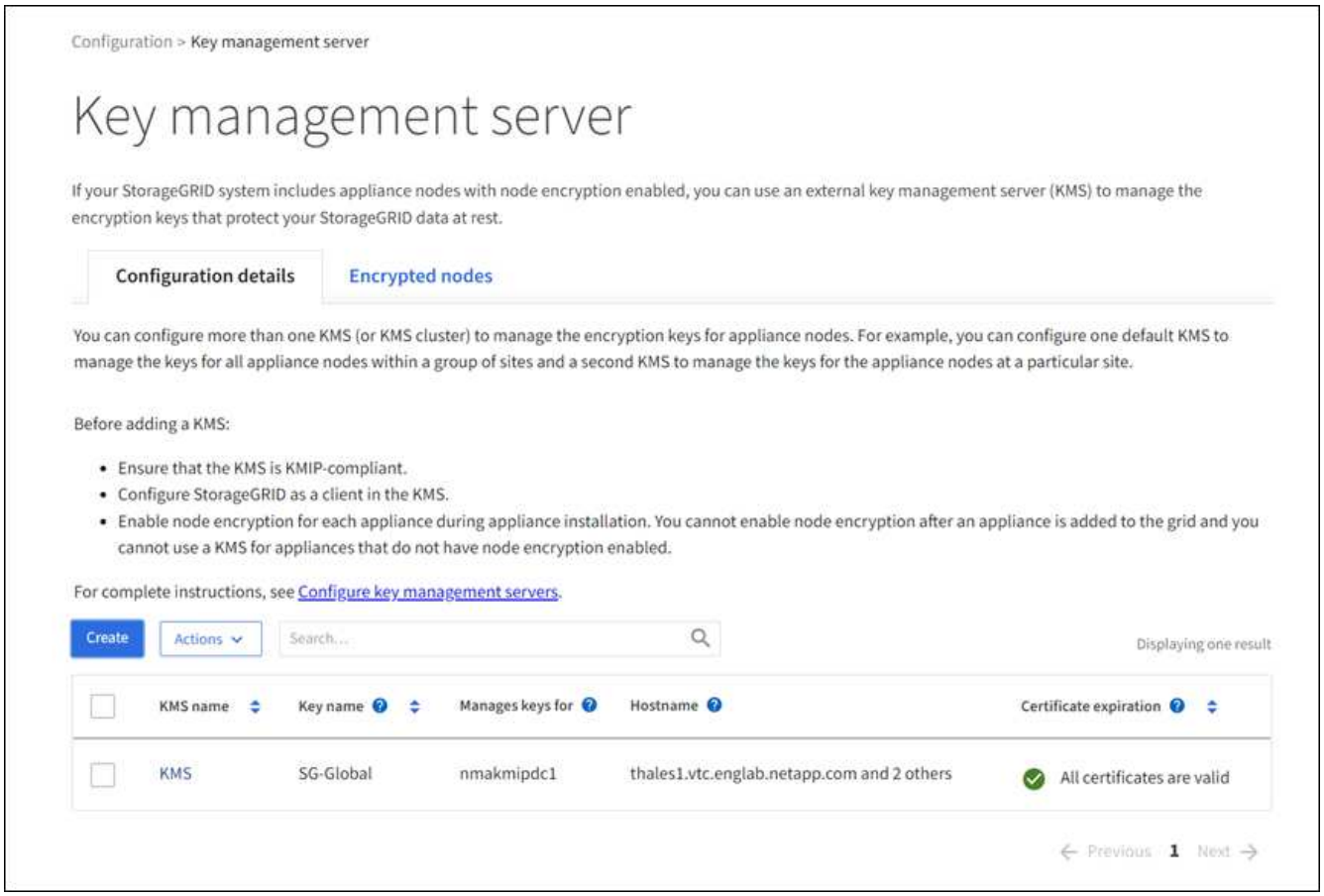
Étape 1 : détails KM

À l'étape 1 (détails KMS) de l'assistant Add a Key Management Server (Ajouter un serveur de gestion des clés), vous fournissez des informations sur le cluster KMS ou KMS.

Étapes

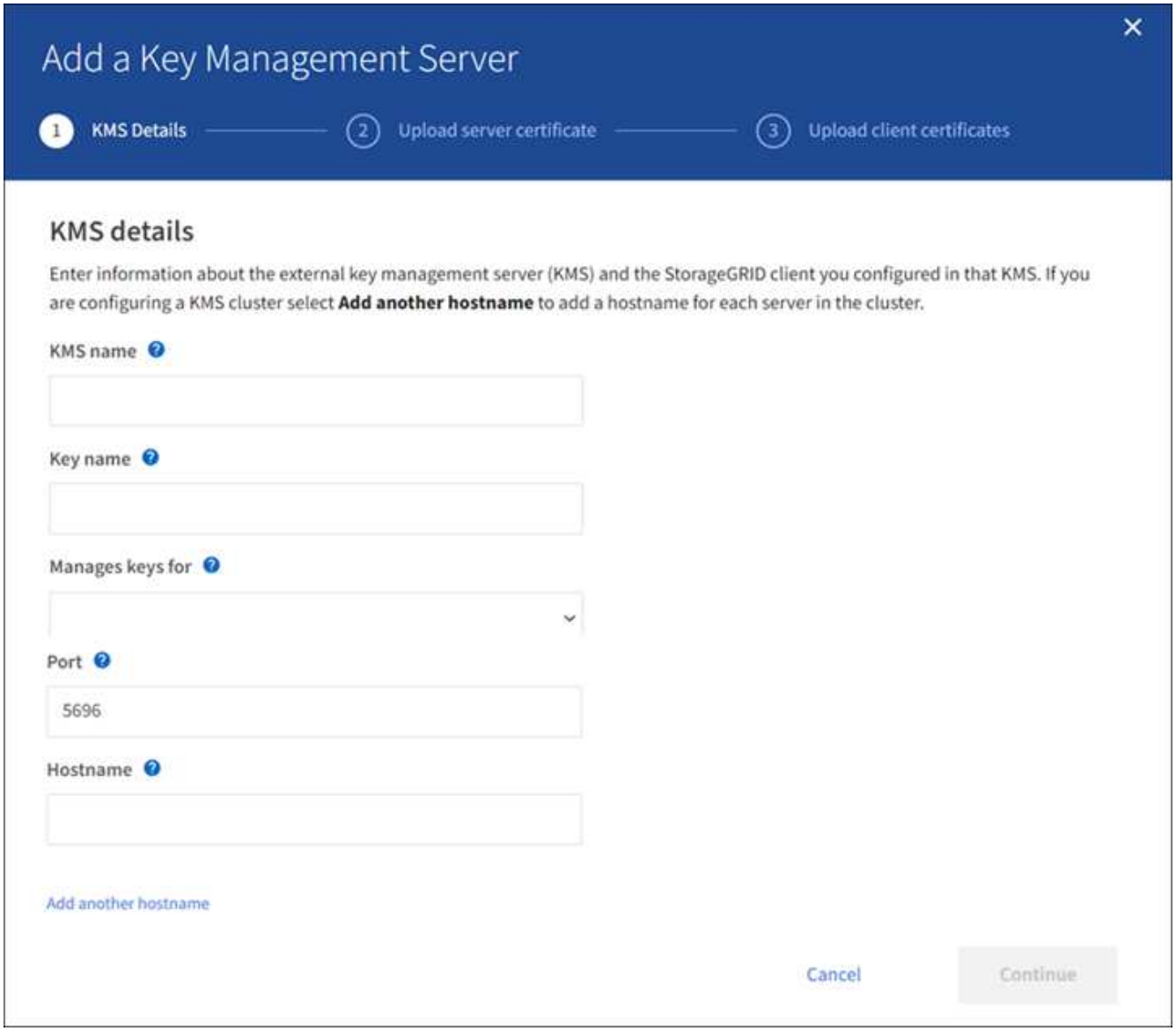
1. Sélectionnez **CONFIGURATION** > **sécurité** > **serveur de gestion des clés**.

   La page serveur de gestion des clés s'affiche avec l'onglet Détails de la configuration sélectionné.



2. Sélectionnez **Créer**.

   L'étape 1 (détails KMS) de l'assistant Add a Key Management Server (Ajouter un serveur de gestion des clés) s'affiche.



3. Entrez les informations suivantes pour le KMS et le client StorageGRID que vous avez configuré dans ce KMS.

Champ	Description
Nom KM	Un nom descriptif pour vous aider à identifier ce KMS. Doit comporter entre 1 et 64 caractères.
Nom de la clé	Alias de clé exact pour le client StorageGRID dans le KMS. Doit comporter entre 1 et 255 caractères.

Champ	Description
Gère les clés pour	Le site StorageGRID qui sera associé à ce KMS. Si possible, vous devez configurer des serveurs de gestion de clés spécifiques au site avant de configurer un KMS par défaut qui s'applique à tous les sites non gérés par un autre KMS. • Sélectionnez un site si ce KMS gère les clés de chiffrement pour les nœuds d'appliance sur un site spécifique. • Sélectionnez **sites non gérés par un autre KMS (KMS par défaut)** pour configurer un KMS par défaut qui s'appliquera à tous les sites qui n'ont pas de KMS dédié et à tous les sites que vous ajoutez dans les extensions suivantes. **Remarque :** Une erreur de validation se produit lorsque vous enregistrez la configuration KMS si vous sélectionnez un site qui a été précédemment crypté par le KMS par défaut, mais que vous n'avez pas fourni la version actuelle de la clé de cryptage d'origine au nouveau KMS.
Port	Le port utilisé par le serveur KMS pour les communications KMIP (Key Management Interoperability Protocol). La valeur par défaut est 5696, qui est le port standard KMIP.
Nom d'hôte	Le nom de domaine complet ou l'adresse IP du KMS. **Remarque :** le champ Subject alternative Name (SAN) du certificat de serveur doit inclure le nom de domaine complet ou l'adresse IP que vous entrez ici. Dans le cas contraire, StorageGRID ne pourra pas se connecter au KMS ou à tous les serveurs d'un cluster KMS.

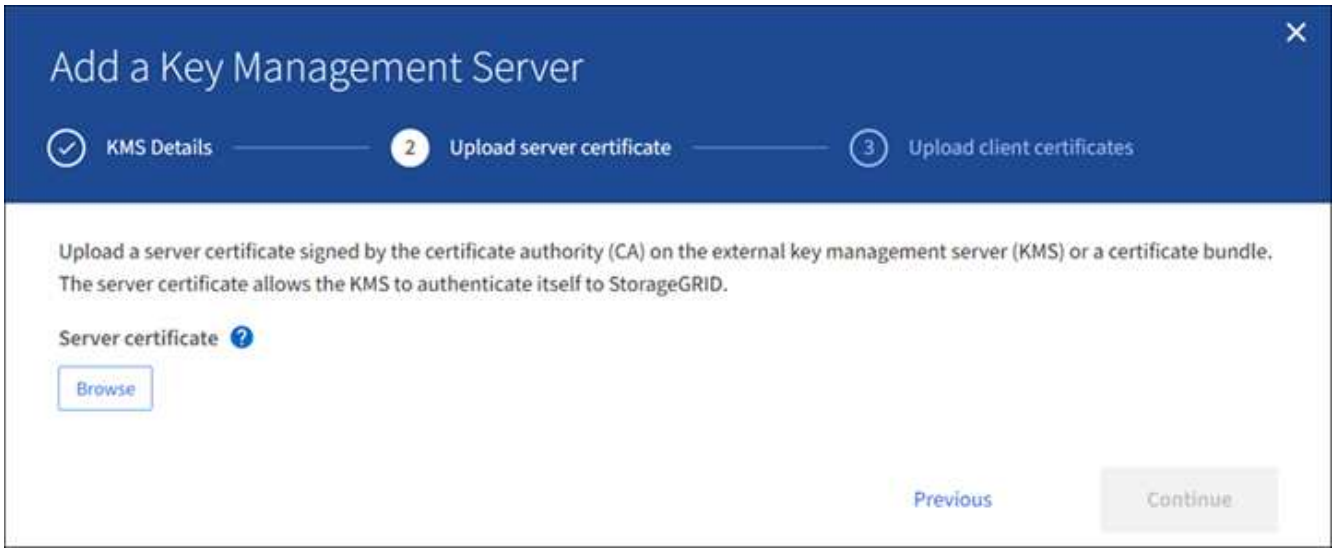
4. Si vous configurez un cluster KMS, sélectionnez **Ajouter un autre nom d'hôte** pour ajouter un nom d'hôte pour chaque serveur du cluster.
5. Sélectionnez **Continuer**.

Étape 2 : télécharger le certificat du serveur

À l'étape 2 (Télécharger le certificat de serveur) de l'assistant Ajouter un serveur de gestion des clés, vous téléchargez le certificat de serveur (ou le paquet de certificats) pour le KMS. Le certificat du serveur permet au KMS externe de s'authentifier auprès de StorageGRID.

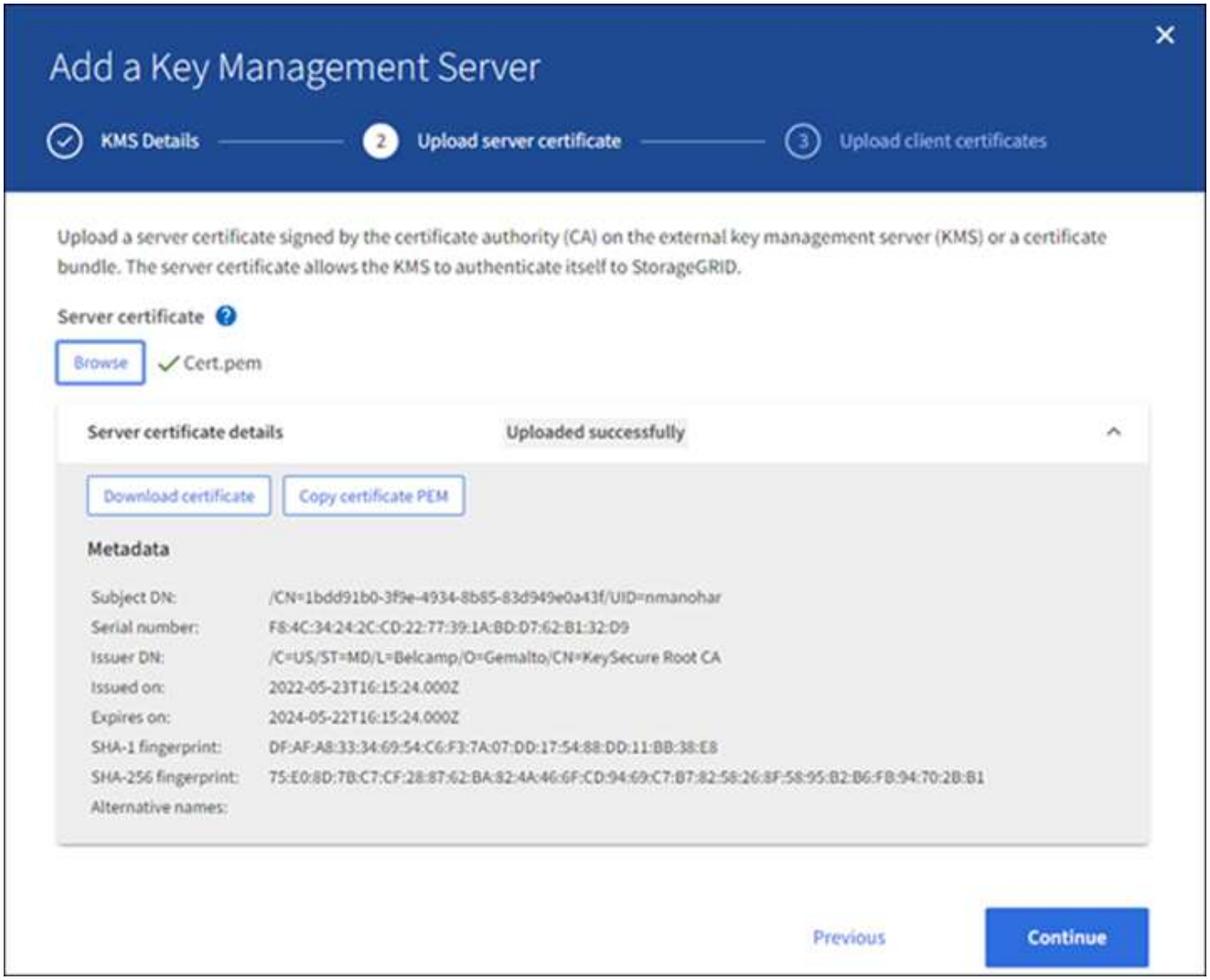
Étapes

1. A partir de **Etape 2 (Télécharger le certificat de serveur)**, accédez à l'emplacement du certificat de serveur ou du paquet de certificats enregistré.



2. Téléchargez le fichier de certificat.

   Les métadonnées du certificat de serveur s'affichent.



Si vous avez téléchargé un ensemble de certificats, les métadonnées de chaque certificat s'affichent sur son propre onglet.

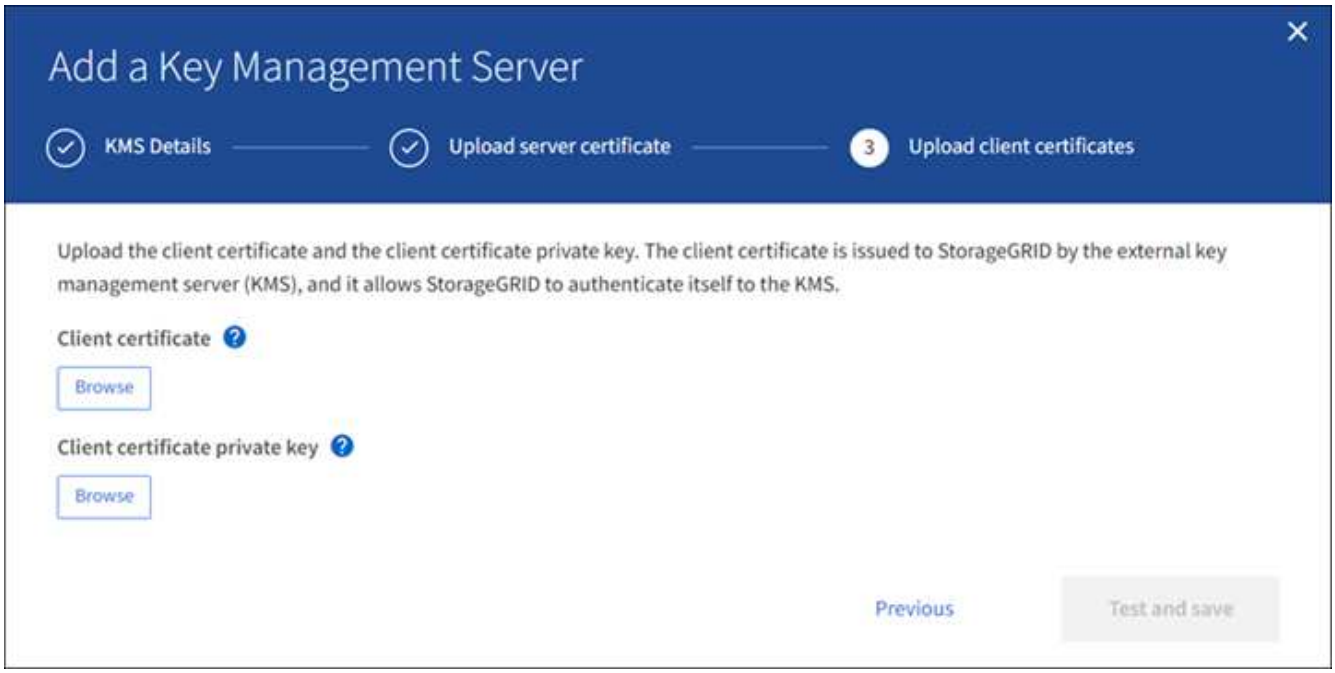
3. Sélectionnez **Continuer**.

Étape 3 : téléchargement des certificats client

À l'étape 3 (Téléchargement de certificats client) de l'assistant Ajouter un serveur de gestion des clés, vous téléchargez le certificat client et la clé privée du certificat client. Le certificat client permet à StorageGRID de s'authentifier auprès du KMS.

Étapes

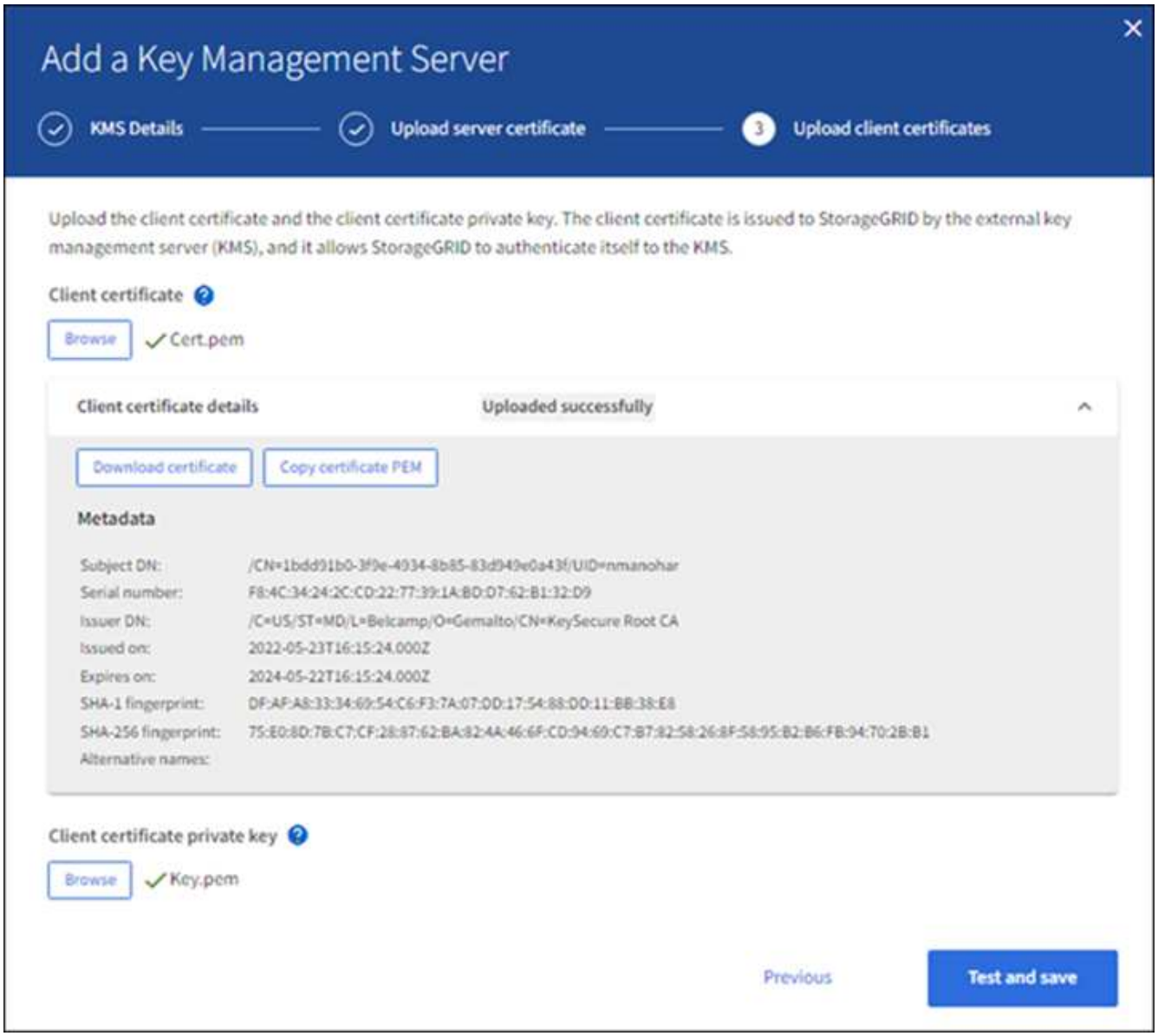
1. A partir de **Etape 3 (Téléchargement de certificats client)**, naviguez jusqu'à l'emplacement du certificat client.



2. Téléchargez le fichier de certificat client.

   Les métadonnées du certificat client s'affichent.

3. Accédez à l'emplacement de la clé privée pour le certificat client.
4. Téléchargez le fichier de clé privée.



5. Sélectionnez **Tester et enregistrer**.

   Les connexions entre le serveur de gestion des clés et les nœuds de dispositif sont testées. Si toutes les connexions sont valides et que la clé correcte est trouvée sur le KMS, le nouveau serveur de gestion des clés est ajouté à la table de la page serveur de gestion des clés.

   > Immédiatement après l'ajout d'un KMS, l'état du certificat sur la page Key Management Server apparaît comme inconnu. Le statut réel de chaque certificat peut prendre jusqu'à 30 minutes pour StorageGRID. Vous devez actualiser votre navigateur Web pour voir l'état actuel.

6. Si un message d'erreur s'affiche lorsque vous sélectionnez **Test and save**, vérifiez les détails du message, puis sélectionnez **OK**.

   Par exemple, vous pourriez recevoir une erreur 422 : entité impossible à traiter si un test de connexion a échoué.

7. Si vous devez enregistrer la configuration actuelle sans tester la connexion externe, sélectionnez **forcer l'enregistrement**.

La sélection de **forcer l'enregistrement** enregistre la configuration KMS, mais elle ne teste pas la connexion externe de chaque appliance à ce KMS. En cas de problème avec la configuration, vous ne pouvez pas redémarrer les nœuds d'appliance pour lesquels le chiffrement de nœud est activé sur le site affecté. L'accès à vos données risque d'être perdu jusqu'à la résolution des problèmes.

8. Vérifiez l'avertissement de confirmation et sélectionnez **OK** si vous êtes sûr de vouloir forcer l'enregistrement de la configuration.

   La configuration KMS est enregistrée mais la connexion au KMS n'est pas testée.

Afficher les détails du KMS

Vous pouvez afficher des informations sur chaque serveur de gestion des clés (KMS) de votre système StorageGRID, notamment l'état actuel des certificats serveur et client.

Étapes

1. Sélectionnez **CONFIGURATION** > **sécurité** > **serveur de gestion des clés**.

   La page serveur de gestion des clés s'affiche. L'onglet Détails de la configuration affiche tous les serveurs de gestion des clés configurés.

2. Examinez les informations du tableau pour chaque KMS.

Champ	Description
Nom KM	Nom descriptif du KMS.
Nom de la clé	Alias de clé pour le client StorageGRID dans le KMS.
Gère les clés pour	Site StorageGRID associé au KMS Ce champ affiche le nom d'un site StorageGRID spécifique ou **sites non gérés par un autre KMS (KMS par défaut).**
Nom d'hôte	Le nom de domaine complet ou l'adresse IP du KMS. S'il existe un cluster de deux serveurs de gestion des clés, le nom de domaine complet ou l'adresse IP des deux serveurs sont répertoriés. S'il y a plus de deux serveurs de gestion des clés dans un cluster, le nom de domaine complet ou l'adresse IP du premier KMS est répertorié avec le nombre de serveurs de gestion des clés supplémentaires dans le cluster. Par exemple : `10.10.10.10 and 10.10.10.11` ou `10.10.10.10 and 2 others`. Pour afficher tous les noms d'hôtes d'un cluster, ouvrez un KMS et sélectionnez **Modifier** ou **actions** > **Modifier**.

Champ	Description
Expiration du certificat	État actuel du certificat de serveur, du certificat d'autorité de certification facultatif et du certificat client : valide, expiré, proche de l'expiration ou inconnu. **Note:** il peut prendre StorageGRID jusqu'à 30 minutes pour obtenir les mises à jour de l'expiration du certificat. Vous devez actualiser votre navigateur Web pour voir les valeurs actuelles.

3. Si l'expiration du certificat est inconnue, attendez jusqu'à 30 minutes, puis actualisez votre navigateur Web.

> Immédiatement après l'ajout d'un KMS, l'expiration du certificat sur la page Key Management Server apparaît comme Inconnu. Le statut réel de chaque certificat peut prendre jusqu'à 30 minutes pour StorageGRID. Vous devez actualiser votre navigateur Web pour voir l'état réel.

4. Si la colonne expiration du certificat indique qu'un certificat a expiré ou qu'il est sur le point d'expirer, répondez au problème dès que possible.

   Lorsque les alertes **KMS CA Certificate expiration**, **KMS client Certificate expiration** et **KMS Server Certificate expiration** sont déclenchées, notez la description de chaque alerte et effectuez les actions recommandées.

> Vous devez corriger tout problème de certificat dès que possible pour maintenir l'accès aux données.

5. Pour afficher les détails du certificat pour ce KMS, sélectionnez le nom KMS dans le tableau.
6. Sur la page de résumé KMS, examinez les métadonnées et le certificat PEM pour le certificat du serveur et le certificat du client. Si nécessaire, sélectionnez **Modifier le certificat** pour remplacer un certificat par un nouveau.

Afficher les nœuds chiffrés

Vous pouvez afficher des informations sur les nœuds d'appliance de votre système StorageGRID sur lesquels le paramètre **Node Encryption** est activé.

Étapes

1. Sélectionnez **CONFIGURATION** > **sécurité** > **serveur de gestion des clés**.

   La page Key Management Server s'affiche. L'onglet Détails de la configuration affiche tous les serveurs de gestion des clés qui ont été configurés.

2. En haut de la page, sélectionnez l'onglet **encrypted nodes**.

   L'onglet noeuds cryptés répertorie les noeuds de l'appliance de votre système StorageGRID sur lesquels le paramètre **chiffrement de noeud** est activé.

3. Vérifiez les informations du tableau pour chaque nœud d'appliance.

Colonne	Description
Nom du nœud	Nom du nœud d'appliance.
Type de nœud	Le type de nœud : stockage, Administrateur ou passerelle.
Le site	Nom du site StorageGRID sur lequel le nœud est installé.
Nom KM	Nom descriptif du KMS utilisé pour le nœud. Si aucun KMS n'est répertorié, sélectionnez l'onglet Détails de la configuration pour ajouter un KMS. "Ajout d'un serveur de gestion des clés (KMS)"
UID de clé	ID unique de la clé de cryptage utilisée pour crypter et décrypter les données sur le nœud de l'appliance. Pour afficher un UID de clé entier, placez le curseur sur la cellule. Un tiret (--) indique que l'UID de clé est inconnu, peut-être en raison d'un problème de connexion entre le nœud de l'appliance et le KMS.
État	L'état de la connexion entre le KMS et le nœud de l'appliance. Si le nœud est connecté, l'horodatage est mis à jour toutes les 30 minutes. La mise à jour de l'état de connexion peut prendre plusieurs minutes après la modification de la configuration KMS. **Remarque :** vous devez actualiser votre navigateur Web pour voir les nouvelles valeurs.

4. Si la colonne État indique un problème KMS, répondez immédiatement au problème.

   Pendant les opérations KMS normales, l'état sera **connecté à KMS**. Si un nœud est déconnecté de la grille, l'état de connexion du nœud est affiché (administrativement arrêté ou inconnu).

   Les autres messages d'état correspondent aux alertes StorageGRID portant le même nom :

   - Echec du chargement de la configuration DES KMS
   - Erreur de connectivité KMS
   - Nom de la clé de cryptage KMS introuvable
   - Echec de la rotation de la clé de chiffrement KMS
   - La clé KMS n'a pas réussi à décrypter un volume d'appliance
   - LES KMS ne sont pas configurés

   Effectuez les actions recommandées pour ces alertes.

   Vous devez immédiatement résoudre tout problème pour assurer la protection intégrale de vos données.

Modification d'un serveur de gestion des clés (KMS)

Vous devrez peut-être modifier la configuration d'un serveur de gestion des clés, par exemple si un certificat est sur le point d'expirer.

Avant de commencer

- Vous avez passé en revue le "considérations et conditions requises pour l'utilisation d'un serveur de gestion des clés".
- Si vous prévoyez de mettre à jour le site sélectionné pour un KMS, vous avez examiné le "Considérations relatives à la modification du KMS pour un site".
- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous disposez de l'autorisation d'accès racine.

Étapes

1. Sélectionnez **CONFIGURATION** > **sécurité** > **serveur de gestion des clés**.

   La page serveur de gestion des clés s'affiche et affiche tous les serveurs de gestion des clés qui ont été configurés.

2. Sélectionnez le KMS à modifier, puis sélectionnez **actions** > **Modifier**.

   Vous pouvez également modifier un KMS en sélectionnant le nom KMS dans la table et en sélectionnant **Modifier** sur la page de détails KMS.

3. Vous pouvez également mettre à jour les détails dans **Etape 1 (détails KMS)** de l'assistant Modifier un serveur de gestion des clés.

Champ	Description
Nom KM	Un nom descriptif pour vous aider à identifier ce KMS. Doit comporter entre 1 et 64 caractères.
Nom de la clé	Alias de clé exact pour le client StorageGRID dans le KMS. Doit comporter entre 1 et 255 caractères. Il vous suffit de modifier le nom de la clé dans de rares cas. Par exemple, vous devez modifier le nom de la clé si l'alias est renommé dans le KMS ou si toutes les versions de la clé précédente ont été copiées dans l'historique des versions du nouvel alias. Ne tentez jamais de faire pivoter une clé en modifiant le nom de clé (alias) du KMS. Faites plutôt pivoter la clé en mettant à jour la version de clé dans le logiciel KMS. StorageGRID nécessite que toutes les versions de clés déjà utilisées (ainsi que toutes les versions à venir) soient accessibles depuis le KMS avec le même alias de clé. Si vous modifiez l'alias de clé pour un KMS configuré, StorageGRID risque de ne pas être en mesure de décrypter vos données. "Considérations et conditions requises pour l'utilisation d'un serveur de gestion des clés"

Champ	Description
Gère les clés pour	Si vous modifiez un KMS spécifique à un site et que vous ne disposez pas déjà d'un KMS par défaut, sélectionnez éventuellement **sites non gérés par un autre KMS (KMS par défaut)**. Cette sélection convertit un KMS spécifique au site en KMS par défaut, qui s'appliquera à tous les sites qui n'ont pas de KMS dédié et à tous les sites ajoutés dans une extension. **Remarque :** si vous modifiez un KMS spécifique à un site, vous ne pouvez pas sélectionner un autre site. Si vous modifiez le KMS par défaut, vous ne pouvez pas sélectionner un site spécifique.
Port	Le port utilisé par le serveur KMS pour les communications KMIP (Key Management Interoperability Protocol). La valeur par défaut est 5696, qui est le port standard KMIP.
Nom d'hôte	Le nom de domaine complet ou l'adresse IP du KMS. **Remarque :** le champ Subject alternative Name (SAN) du certificat de serveur doit inclure le nom de domaine complet ou l'adresse IP que vous entrez ici. Dans le cas contraire, StorageGRID ne pourra pas se connecter au KMS ou à tous les serveurs d'un cluster KMS.

4. Si vous configurez un cluster KMS, sélectionnez **Ajouter un autre nom d'hôte** pour ajouter un nom d'hôte pour chaque serveur du cluster.
5. Sélectionnez **Continuer**.

   L'étape 2 (Télécharger le certificat de serveur) de l'assistant Modifier un serveur de gestion des clés s'affiche.

6. Si vous devez remplacer le certificat de serveur, sélectionnez **Parcourir** et téléchargez le nouveau fichier.
7. Sélectionnez **Continuer**.

   L'étape 3 (Téléchargement de certificats client) de l'assistant Modifier un serveur de gestion des clés s'affiche.

8. Si vous devez remplacer le certificat client et la clé privée du certificat client, sélectionnez **Parcourir** et téléchargez les nouveaux fichiers.
9. Sélectionnez **Tester et enregistrer**.

   Les connexions entre le serveur de gestion des clés et tous les nœuds d'appliance chiffrés sur les sites affectés sont testées. Si toutes les connexions de nœud sont valides et que la clé correcte est trouvée sur le KMS, le serveur de gestion des clés est ajouté à la table de la page Key Management Server.

10. Si un message d'erreur s'affiche, vérifiez les détails du message et sélectionnez **OK**.

    Par exemple, vous pouvez recevoir une erreur 422 : entité impossible à traiter si le site que vous avez sélectionné pour ce KMS est déjà géré par un autre KMS, ou si un test de connexion a échoué.

11. Si vous devez enregistrer la configuration actuelle avant de résoudre les erreurs de connexion, sélectionnez **forcer l'enregistrement**.

La sélection de **forcer l'enregistrement** enregistre la configuration KMS, mais elle ne teste pas la connexion externe de chaque appliance à ce KMS. En cas de problème avec la configuration, vous ne pouvez pas redémarrer les nœuds d'appliance pour lesquels le chiffrement de nœud est activé sur le site affecté. L'accès à vos données risque d'être perdu jusqu'à la résolution des problèmes.

La configuration KMS est enregistrée.

12. Vérifiez l'avertissement de confirmation et sélectionnez **OK** si vous êtes sûr de vouloir forcer l'enregistrement de la configuration.

    La configuration KMS est enregistrée mais la connexion au KMS n'est pas testée.

Suppression d'un serveur de gestion des clés (KMS)

Dans certains cas, vous pouvez supprimer un serveur de gestion des clés. Par exemple, vous pouvez vouloir supprimer un KMS spécifique au site si vous avez désactivé le site.

Avant de commencer

- Vous avez passé en revue le "considérations et conditions requises pour l'utilisation d'un serveur de gestion des clés".
- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous disposez de l'autorisation d'accès racine.

Description de la tâche

Vous pouvez supprimer un KMS dans les cas suivants :

- Vous pouvez supprimer un KMS spécifique au site si le site a été désactivé ou si le site ne contient aucun nœud d'appliance lorsque le chiffrement de nœud est activé.
- Vous pouvez supprimer le KMS par défaut si un KMS spécifique au site existe déjà pour chaque site sur lequel des nœuds d'appliance sont activés pour que le chiffrement des nœuds soit activé.

Étapes

1. Sélectionnez **CONFIGURATION** > **sécurité** > **serveur de gestion des clés**.

   La page serveur de gestion des clés s'affiche et affiche tous les serveurs de gestion des clés qui ont été configurés.

2. Sélectionnez le KMS à supprimer, puis sélectionnez **actions** > **Supprimer**.

   Vous pouvez également supprimer un KMS en sélectionnant le nom KMS dans la table et en sélectionnant **Supprimer** dans la page de détails KMS.

3. Vérifiez que ce qui suit est vrai :
   - Vous supprimez un KMS spécifique au site pour un site qui n'a aucun nœud d'appliance pour lequel le chiffrement des nœuds est activé.
   - Vous supprimez le KMS par défaut, mais un KMS spécifique au site existe déjà pour chaque site avec chiffrement des nœuds.
4. Sélectionnez **Oui**.

La configuration KMS est supprimée.

Gérer les paramètres proxy

Configurez les paramètres du proxy de stockage

Si vous utilisez des services de plateforme ou des pools de stockage cloud, vous pouvez configurer un proxy non transparent entre les nœuds de stockage et les terminaux S3 externes. Par exemple, vous aurez peut-être besoin d'un proxy non transparent pour permettre l'envoi de messages de services de plate-forme vers des noeuds finaux externes, tels qu'un noeud final sur Internet.

Avant de commencer

- Vous disposez d'autorisations d'accès spécifiques.
- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".

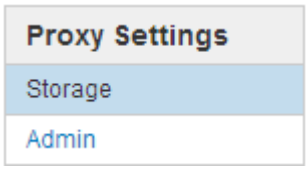
Description de la tâche

Vous pouvez configurer les paramètres d'un proxy de stockage unique.

Étapes

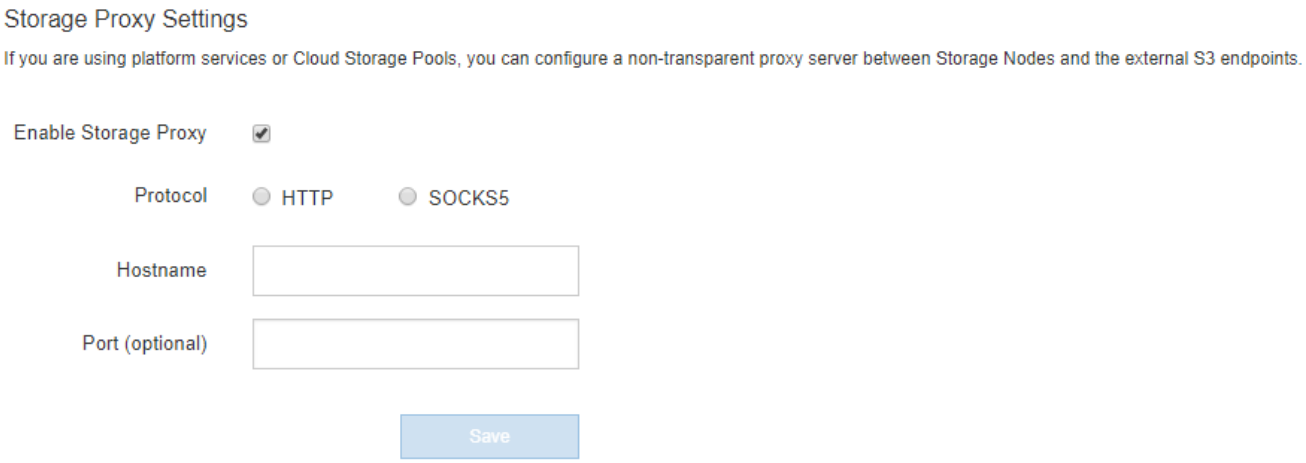
1. Sélectionnez **CONFIGURATION** > **sécurité** > **Paramètres proxy**.

   La page Paramètres du proxy de stockage s'affiche. Par défaut, **Storage** est sélectionné dans le menu de la barre latérale.

2. Cochez la case **Activer le proxy de stockage**.

   Les champs de configuration d'un proxy de stockage s'affichent.

3. Sélectionnez le protocole du proxy de stockage non transparent.
4. Entrez le nom d'hôte ou l'adresse IP du serveur proxy.

5. Vous pouvez également saisir le port utilisé pour vous connecter au serveur proxy.

   Vous pouvez laisser ce champ vide si vous utilisez le port par défaut pour le protocole : 80 pour HTTP ou 1080 pour SOCKS5.

6. Sélectionnez **Enregistrer**.

   Une fois le proxy de stockage enregistré, de nouveaux terminaux pour les services de plateforme ou les pools de stockage cloud peuvent être configurés et testés.

   > Les modifications de proxy peuvent prendre jusqu'à 10 minutes.

7. Vérifiez les paramètres de votre serveur proxy pour vous assurer que les messages relatifs au service de la plate-forme de StorageGRID ne seront pas bloqués.

Une fois que vous avez terminé

Si vous devez désactiver un proxy de stockage, décochez la case **Activer le proxy de stockage** et sélectionnez **Enregistrer**.

Informations associées

- "Réseau et ports pour les services de plate-forme"
- "Gestion des objets avec ILM"

Configurez les paramètres du proxy d'administration

Si vous envoyez des messages AutoSupport via HTTP ou HTTPS (reportez-vous à la section "Configurez AutoSupport"), vous pouvez configurer un serveur proxy non transparent entre les nœuds d'administration et le support technique (AutoSupport).

Avant de commencer

- Vous disposez d'autorisations d'accès spécifiques.
- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".

Description de la tâche

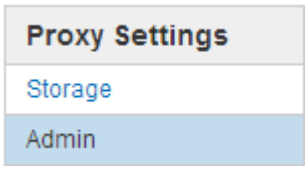
Vous pouvez configurer les paramètres d'un proxy d'administration unique.

Étapes

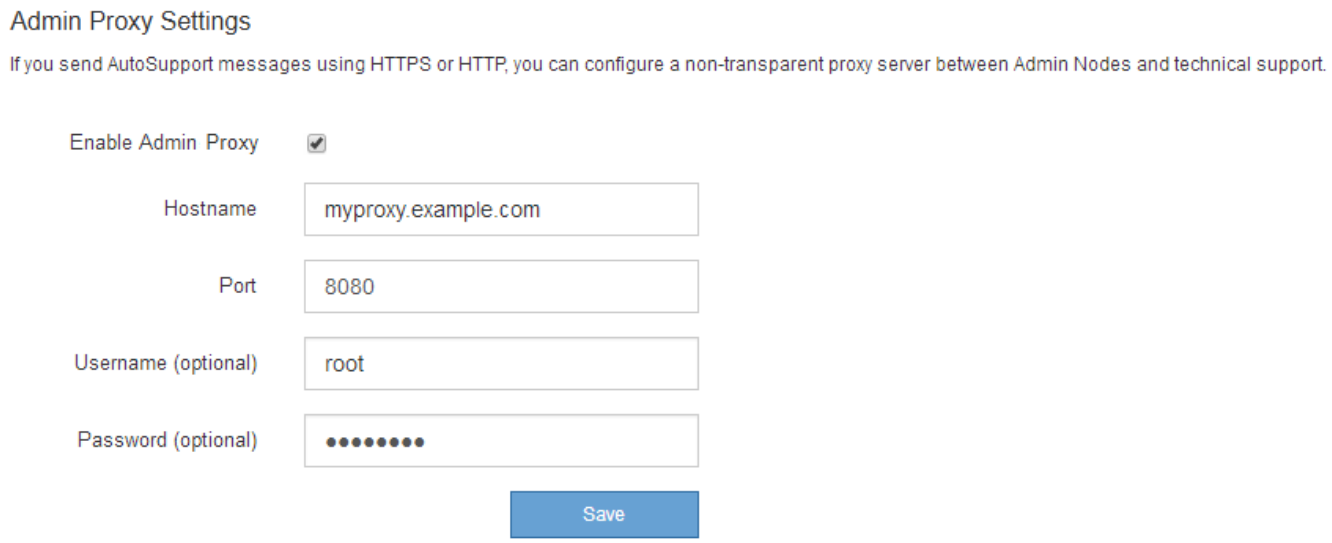
1. Sélectionnez **CONFIGURATION** > **sécurité** > **Paramètres proxy**.

   La page Paramètres du proxy administrateur s'affiche. Par défaut, **Storage** est sélectionné dans le menu de la barre latérale.

2. Dans le menu barre latérale, sélectionnez **Admin**.



3. Cochez la case **Activer le proxy Admin**.



4. Entrez le nom d'hôte ou l'adresse IP du serveur proxy.
5. Entrez le port utilisé pour se connecter au serveur proxy.
6. Vous pouvez également saisir le nom d'utilisateur du proxy.

   Laissez ce champ vide si votre serveur proxy ne nécessite pas de nom d'utilisateur.

7. Vous pouvez également saisir le mot de passe du proxy.

   Laissez ce champ vide si votre serveur proxy ne nécessite pas de mot de passe.

8. Sélectionnez **Enregistrer**.

   Une fois le proxy d'administration enregistré, le serveur proxy entre les nœuds d'administration et le support technique est configuré.

   > Les modifications de proxy peuvent prendre jusqu'à 10 minutes.

9. Si vous devez désactiver le proxy, décochez la case **Activer le proxy Admin** et sélectionnez **Enregistrer**.

Contrôle des pare-feu

Contrôler l'accès au niveau du pare-feu externe

Vous pouvez ouvrir ou fermer des ports spécifiques au niveau du pare-feu externe.

Vous pouvez contrôler l'accès aux interfaces utilisateur et aux API des nœuds d'administration StorageGRID en ouvrant ou en fermant des ports spécifiques au pare-feu externe. Par exemple, vous pouvez empêcher les locataires de se connecter à Grid Manager au niveau du pare-feu, en plus d'utiliser d'autres méthodes pour contrôler l'accès au système.

Si vous souhaitez configurer le pare-feu interne StorageGRID, reportez-vous à la section "Configurer le pare-feu interne".

Port	Description	Si le port est ouvert…
443	Port HTTPS par défaut pour les nœuds d'administration	Les navigateurs Web et les clients d'API de gestion peuvent accéder à Grid Manager, à l'API de gestion du grid, au gestionnaire des locataires et à l'API de gestion des locataires. **Remarque :** le port 443 est également utilisé pour un trafic interne.
8443	Port restreint de Grid Manager sur les nœuds d'administration	• Les navigateurs Web et les clients d'API de gestion peuvent accéder à Grid Manager et à l'API de gestion Grid via HTTPS. • Les navigateurs Web et les clients de l'API de gestion ne peuvent pas accéder au gestionnaire de locataires ou à l'API de gestion des locataires. • Les demandes de contenu interne seront rejetées.
9443	Port de gestionnaire de locataires restreint sur les nœuds d'administration	• Les navigateurs Web et les clients d'API de gestion peuvent accéder au Gestionnaire de locataires et à l'API de gestion des locataires via HTTPS. • Les navigateurs Web et les clients API de gestion ne peuvent pas accéder à Grid Manager ou à l'API Grid Management. • Les demandes de contenu interne seront rejetées.

L'authentification unique (SSO) n'est pas disponible sur les ports du gestionnaire de grille restreinte ou du gestionnaire de locataires. Vous devez utiliser le port HTTPS par défaut (443) si vous souhaitez que les utilisateurs s'authentifient avec une connexion unique.

Informations associées

- "Connectez-vous au Grid Manager"
- "Créer un compte de locataire"
- "Communications externes"

Gérer les contrôles de pare-feu internes

StorageGRID comprend un pare-feu interne sur chaque nœud qui améliore la sécurité de votre grille en vous permettant de contrôler l'accès réseau au nœud. Utilisez le pare-feu pour empêcher l'accès au réseau sur tous les ports, à l'exception de ceux nécessaires à votre déploiement de grille spécifique. Les modifications de configuration effectuées sur la page de contrôle du pare-feu sont déployées sur chaque nœud.

Utilisez les trois onglets de la page de contrôle du pare-feu pour personnaliser l'accès dont vous avez besoin pour votre grille.

- **Liste d'adresses privilégiées** : utilisez cet onglet pour autoriser l'accès sélectionné aux ports fermés. Vous pouvez ajouter des adresses IP ou des sous-réseaux en notation CIDR qui peuvent accéder aux ports fermés à l'aide de l'onglet gérer l'accès externe.
- **Gérer l'accès externe** : utilisez cet onglet pour fermer les ports ouverts par défaut ou rouvrir les ports précédemment fermés.
- **Réseau client non approuvé** : utilisez cet onglet pour indiquer si un nœud approuve le trafic entrant provenant du réseau client.

  Cet onglet offre également l'option permettant de spécifier des ports supplémentaires que vous souhaitez ouvrir lorsque le réseau client non sécurisé est configuré. Ces ports permettent d'accéder au gestionnaire de grille, au gestionnaire de locataires ou aux deux.

  Les paramètres de cet onglet remplacent les paramètres de l'onglet gérer l'accès externe.

  - Un nœud avec un réseau client non approuvé accepte uniquement les connexions sur les ports de point final de l'équilibreur de charge configurés sur ce nœud (points finaux globaux, liés à l'interface de nœud et au type de nœud).
  - Les ports supplémentaires ouverts sous l'onglet réseau client non approuvé sont ouverts sur tous les réseaux client non approuvés, même si aucun point final d'équilibreur de charge n'est configuré.
  - Les ports de point final de l'équilibreur de charge et les ports supplémentaires sélectionnés *sont les seuls ports ouverts* sur les réseaux clients non approuvés, quels que soient les paramètres de l'onglet gérer les réseaux externes.
  - Une fois approuvés, tous les ports ouverts sous l'onglet gérer l'accès externe sont accessibles, ainsi que tous les noeuds finaux d'équilibrage de charge ouverts sur le réseau client.

> Les paramètres que vous effectuez sur un onglet peuvent affecter les modifications d'accès que vous effectuez sur un autre onglet. Vérifiez les paramètres de tous les onglets pour vous assurer que votre réseau se comporte comme vous le souhaitez.

Pour configurer les contrôles de pare-feu internes, reportez-vous à la section "Configurer les contrôles de pare-feu".

Pour plus d'informations sur les pare-feu externes et la sécurité réseau, reportez-vous à la section "Contrôler l'accès au niveau du pare-feu externe".

Liste d'adresses privilégiées et onglets gérer les accès externes

L'onglet liste d'adresses privilégiées vous permet d'enregistrer une ou plusieurs adresses IP qui ont accès aux ports de la grille fermés. L'onglet gérer l'accès externe vous permet de fermer l'accès externe aux ports externes sélectionnés ou à tous les ports externes ouverts (les ports externes sont des ports accessibles par défaut par les nœuds non-grid). Ces deux onglets peuvent souvent être utilisés ensemble pour personnaliser l'accès réseau exact dont vous avez besoin pour votre grille.

> Par défaut, les adresses IP privilégiées n'ont pas d'accès au port de la grille interne.

Exemple 1 : utilisez un hôte de secours pour les tâches de maintenance

Supposons que vous souhaitiez utiliser un hôte de secours (un hôte renforcé par la sécurité) pour l'administration du réseau. Vous pouvez utiliser les étapes générales suivantes :

1. Utilisez l'onglet liste d'adresses privilégiées pour ajouter l'adresse IP de l'hôte de saut.

2. Utilisez l'onglet gérer l'accès externe pour bloquer tous les ports.

> Ajoutez l'adresse IP privilégiée avant de bloquer les ports 443 et 8443. Tous les utilisateurs actuellement connectés sur un port bloqué, y compris vous, perdront l'accès à Grid Manager à moins que leur adresse IP n'ait été ajoutée à la liste d'adresses privilégiées.

Après avoir enregistré votre configuration, tous les ports externes du nœud d'administration de votre grille seront bloqués pour tous les hôtes, à l'exception de l'hôte de saut. Vous pouvez ensuite utiliser l'hôte de secours pour effectuer des tâches de maintenance sur votre grille de manière plus sécurisée.

Exemple 2 : limiter l'accès au gestionnaire de grille et au gestionnaire de locataires

Supposons que vous souhaitiez limiter l'accès au gestionnaire de grille et au gestionnaire de locataires pour des raisons de sécurité. Vous pouvez utiliser les étapes générales suivantes :

1. Utilisez le bouton bascule de l'onglet gérer l'accès externe pour bloquer le port 443.
2. Utilisez la bascule de l'onglet gérer l'accès externe pour autoriser l'accès au port 8443.
3. Utilisez la bascule de l'onglet gérer l'accès externe pour autoriser l'accès au port 9443.

Une fois la configuration enregistrée, les hôtes ne pourront pas accéder au port 443, mais ils pourront toujours accéder au Grid Manager via le port 8443 et le tenant Manager via le port 9443.

Exemple 3 : verrouiller les ports sensibles

Supposons que vous souhaitez verrouiller les ports sensibles et le service sur ce port (par exemple, SSH sur le port 22). Vous pouvez utiliser les étapes générales suivantes :

1. Utilisez l'onglet liste d'adresses privilégiées pour accorder l'accès uniquement aux hôtes qui ont besoin d'accéder au service.
2. Utilisez l'onglet gérer l'accès externe pour bloquer tous les ports.

> Ajoutez l'adresse IP privilégiée avant de bloquer les ports 443 et 8443. Tous les utilisateurs actuellement connectés sur un port bloqué, y compris vous, perdront l'accès à Grid Manager à moins que leur adresse IP n'ait été ajoutée à la liste d'adresses privilégiées.

Après avoir enregistré votre configuration, le port 22 et le service SSH seront disponibles pour les hôtes de la liste d'adresses privilégiées. Tous les autres hôtes se verront refuser l'accès au service, quelle que soit l'interface d'origine de la demande.

Exemple 4 : désactiver l'accès aux services inutilisés

Au niveau du réseau, vous pouvez désactiver certains services que vous n'avez pas l'intention d'utiliser. Par exemple, si vous ne souhaitez pas fournir l'accès Swift, vous devez effectuer les étapes générales suivantes :

1. Utilisez le bouton bascule de l'onglet gérer l'accès externe pour bloquer le port 18083.
2. Utilisez le bouton bascule de l'onglet gérer l'accès externe pour bloquer le port 18085.

Une fois la configuration enregistrée, le nœud de stockage n'autorise plus la connectivité Swift, mais continue d'autoriser l'accès à d'autres services sur les ports débloqués.

Onglet réseaux de clients non approuvés

Si vous utilisez un réseau client, vous pouvez aider à protéger StorageGRID contre les attaques hostiles en acceptant le trafic client entrant uniquement sur les points finaux explicitement configurés ou sur les ports supplémentaires sélectionnés dans cet onglet.

Par défaut, le réseau client sur chaque nœud de la grille est *Trusted*. Par défaut, StorageGRID approuve les connexions entrantes à chaque nœud de grid sur tous "ports externes disponibles".

Vous pouvez réduire la menace d'attaques hostiles sur votre système StorageGRID en spécifiant que le réseau client sur chaque nœud est *non fiable*. Si le réseau client d'un nœud n'est pas fiable, le nœud accepte uniquement les connexions entrantes sur les ports explicitement configurés comme points finaux d'équilibrage de charge et tous les ports supplémentaires que vous désignez à l'aide de l'onglet réseau client non approuvé de la page de contrôle du pare-feu. Voir "Configurer les terminaux de l'équilibreur de charge" et "Configurer les contrôles de pare-feu".

Exemple 1 : le nœud de passerelle n'accepte que les requêtes HTTPS S3

Supposons que vous souhaitiez qu'un nœud de passerelle refuse tout trafic entrant sur le réseau client, à l'exception des requêtes HTTPS S3. Vous devez effectuer les étapes générales suivantes :

1. À partir du "Terminaux d'équilibrage de charge" Configurez un terminal d'équilibreur de charge pour S3 sur HTTPS sur le port 443.
2. Sur la page de contrôle du pare-feu, sélectionnez non approuvé pour indiquer que le réseau client sur le nœud passerelle n'est pas fiable.

Après avoir enregistré votre configuration, tout le trafic entrant sur le réseau client du nœud passerelle est supprimé, sauf pour les requêtes HTTPS S3 sur le port 443 et les requêtes ICMP Echo (ping).

Exemple 2 : le nœud de stockage envoie des demandes de services de plateforme S3

Supposons que vous souhaitiez activer le trafic sortant des services de la plateforme S3 à partir d'un nœud de stockage, mais que vous souhaitiez empêcher toute connexion entrante à ce nœud de stockage sur le réseau client. Vous devez effectuer cette étape générale :

- Dans l'onglet réseaux de clients non approuvés de la page de contrôle du pare-feu, indiquez que le réseau client sur le nœud de stockage n'est pas fiable.

Une fois la configuration enregistrée, le nœud de stockage n'accepte plus le trafic entrant sur le réseau client, mais continue à autoriser les requêtes sortantes vers les destinations de services de plate-forme configurées.

Exemple 3 : limitation de l'accès à Grid Manager à un sous-réseau

Supposons que vous souhaitiez autoriser l'accès à Grid Manager uniquement sur un sous-réseau spécifique. Procédez comme suit :

1. Connectez le réseau client de vos nœuds d'administration au sous-réseau.
2. Utilisez l'onglet réseau client non approuvé pour configurer le réseau client comme non fiable.
3. Dans la section **ports supplémentaires ouverts sur le réseau client non approuvé** de l'onglet, ajoutez le port 443 ou 8443.
4. Utilisez l'onglet gérer l'accès externe pour bloquer tous les ports externes (avec ou sans adresses IP privilégiées définies pour les hôtes situés en dehors de ce sous-réseau).

Après avoir enregistré votre configuration, seuls les hôtes du sous-réseau que vous avez spécifié peuvent accéder à Grid Manager. Tous les autres hôtes sont bloqués.

Configurer le pare-feu interne

Vous pouvez configurer le pare-feu StorageGRID pour contrôler l'accès réseau à des ports spécifiques sur vos nœuds StorageGRID.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous avez "autorisations d'accès spécifiques".
- Vous avez examiné les informations dans "Gérer les contrôles de pare-feu" et "Instructions de mise en réseau".
- Si vous souhaitez qu'un nœud d'administration ou un nœud de passerelle accepte le trafic entrant uniquement sur des noeuds finaux configurés explicitement, vous avez défini les noeuds finaux de l'équilibreur de charge.

> ⓘ Lors de la modification de la configuration du réseau client, les connexions client existantes peuvent échouer si les noeuds finaux de l'équilibreur de charge n'ont pas été configurés.

Description de la tâche

StorageGRID comprend un pare-feu interne sur chaque nœud qui vous permet d'ouvrir ou de fermer certains ports sur les nœuds de votre grille. Vous pouvez utiliser les onglets de contrôle du pare-feu pour ouvrir ou fermer des ports ouverts par défaut sur le réseau Grid, le réseau Admin et le réseau client. Vous pouvez également créer une liste d'adresses IP privilégiées pouvant accéder aux ports de la grille fermés. Si vous utilisez un réseau client, vous pouvez spécifier si un nœud approuve le trafic entrant à partir du réseau client et configurer l'accès à des ports spécifiques sur le réseau client.

Limiter le nombre de ports ouverts aux adresses IP en dehors de votre grille à ceux qui sont absolument nécessaires améliore la sécurité de votre grille. Vous utilisez les paramètres de chacun des trois onglets de contrôle du pare-feu pour vous assurer que seuls les ports nécessaires sont ouverts.

Pour plus d'informations sur l'utilisation des contrôles de pare-feu, notamment des exemples, reportez-vous à la section "Gérer les contrôles de pare-feu".

Pour plus d'informations sur les pare-feu externes et la sécurité réseau, reportez-vous à la section "Contrôler l'accès au niveau du pare-feu externe".

Accès aux contrôles de pare-feu

Étapes

1. Sélectionnez **CONFIGURATION** > **sécurité** > **contrôle du pare-feu**.

   Les trois onglets de cette page sont décrits dans "Gérer les contrôles de pare-feu".

2. Sélectionnez n'importe quel onglet pour configurer les contrôles du pare-feu.

   Vous pouvez utiliser ces onglets dans n'importe quel ordre. Les configurations que vous définissez sur un onglet ne limitent pas ce que vous pouvez faire sur les autres onglets. Cependant, les modifications de configuration effectuées sur un onglet peuvent modifier le comportement des ports configurés sur d'autres onglets.

Liste d'adresses privilégiées

Vous utilisez l'onglet liste d'adresses privilégiées pour accorder aux hôtes l'accès aux ports fermés par défaut ou fermés par des paramètres de l'onglet gérer l'accès externe.

Par défaut, les adresses IP privilégiées et les sous-réseaux ne disposent pas d'un accès au grid interne. En outre, les noeuds finaux d'équilibrage de charge et les ports supplémentaires ouverts dans l'onglet liste d'adresses privilégiées sont accessibles même si bloqués dans l'onglet gérer l'accès externe.

> Les paramètres de l'onglet liste d'adresses privilégiées ne peuvent pas remplacer les paramètres de l'onglet réseau client non approuvé.

Étapes

1. Dans l'onglet liste d'adresses privilégiées, entrez l'adresse ou le sous-réseau IP que vous souhaitez accorder à l'accès aux ports fermés.
2. Si vous le souhaitez, sélectionnez **Ajouter une autre adresse IP ou un autre sous-réseau en notation CIDR** pour ajouter des clients privilégiés supplémentaires.

   > Ajoutez autant d'adresses que possible à la liste privilégiée.

3. Vous pouvez également sélectionner **Autoriser les adresses IP privilégiées à accéder aux ports internes StorageGRID**. Voir "Ports internes StorageGRID".

   > Cette option supprime certaines protections pour les services internes. Laissez-le désactivé si possible.

4. Sélectionnez **Enregistrer**.

Gérer l'accès externe

Lorsqu'un port est fermé dans l'onglet gérer l'accès externe, il est impossible d'accéder au port par une adresse IP non grille à moins que vous n'ajoutiez l'adresse IP à la liste d'adresses privilégiées. Vous ne pouvez fermer que les ports ouverts par défaut et vous ne pouvez ouvrir que les ports que vous avez fermés.

> Les paramètres de l'onglet gérer l'accès externe ne peuvent pas remplacer les paramètres de l'onglet réseau client non approuvé. Par exemple, si un nœud n'est pas approuvé, le port SSH/22 est bloqué sur le réseau client même s'il est ouvert dans l'onglet gérer l'accès externe. Les paramètres de l'onglet réseau client non approuvé remplacent les ports fermés (tels que 443, 8443, 9443) sur le réseau client.

Étapes

1. Sélectionnez **gérer l'accès externe**. L'onglet affiche un tableau contenant tous les ports externes (ports accessibles par défaut par les nœuds non GRID) pour les nœuds de votre grille.
2. Configurez les ports que vous souhaitez ouvrir et fermer à l'aide des options suivantes :
   - Utilisez la bascule située en regard de chaque port pour ouvrir ou fermer le port sélectionné.
   - Sélectionnez **Ouvrir tous les ports affichés** pour ouvrir tous les ports répertoriés dans le tableau.
   - Sélectionnez **Fermer tous les ports affichés** pour fermer tous les ports répertoriés dans le tableau.

Si vous fermez les ports Grid Manager 443 ou 8443, tous les utilisateurs actuellement connectés sur un port bloqué, y compris vous, perdront l'accès à Grid Manager, sauf si leur adresse IP a été ajoutée à la liste d'adresses privilégiées.

Utilisez la barre de défilement située à droite du tableau pour vous assurer que vous avez affiché tous les ports disponibles. Utilisez le champ de recherche pour trouver les paramètres de n'importe quel port externe en entrant un numéro de port. Vous pouvez entrer un numéro de port partiel. Par exemple, si vous entrez un **2**, tous les ports dont le nom contient la chaîne "2" s'affichent.

3. Sélectionnez **Enregistrer**

Réseau client non fiable

Si le réseau client d'un nœud n'est pas approuvé, le nœud accepte uniquement le trafic entrant sur les ports configurés comme points finaux de l'équilibreur de charge et, éventuellement, les ports supplémentaires que vous sélectionnez dans cet onglet. Vous pouvez également utiliser cet onglet pour spécifier le paramètre par défaut pour les nouveaux nœuds ajoutés dans une extension.

Les connexions client existantes peuvent échouer si les points de terminaison de l'équilibreur de charge n'ont pas été configurés.

Les modifications de configuration effectuées dans l'onglet **réseau client non approuvé** remplacent les paramètres de l'onglet **gérer l'accès externe**.

Étapes

1. Sélectionnez **réseau client non approuvé**.
2. Dans la section définir les nouveaux nœuds par défaut, spécifiez le paramètre par défaut lorsque de nouveaux nœuds sont ajoutés à la grille dans une procédure d'extension.
   - **Approuvé** (par défaut) : lorsqu'un nœud est ajouté dans une extension, son réseau client est approuvé.
   - **Non fiable** : lorsqu'un nœud est ajouté dans une extension, son réseau client n'est pas fiable.

     Si nécessaire, vous pouvez revenir à cet onglet pour modifier le paramètre d'un nouveau nœud spécifique.

     Ce paramètre n'affecte pas les nœuds existants du système StorageGRID.
3. Utilisez les options suivantes pour sélectionner les nœuds qui doivent autoriser les connexions client uniquement sur les terminaux d'équilibrage de charge configurés explicitement ou sur les ports sélectionnés supplémentaires :
   - Sélectionnez **ne pas faire confiance aux nœuds affichés** pour ajouter tous les nœuds affichés dans le tableau à la liste réseau client non approuvé.
   - Sélectionnez **confiance sur les nœuds affichés** pour supprimer tous les nœuds affichés dans le tableau de la liste réseau client non approuvé.
   - Utilisez le commutateur situé en regard de chaque port pour définir le réseau client comme approuvé ou non fiable pour le nœud sélectionné.

     Par exemple, vous pouvez sélectionner **ne plus faire confiance aux nœuds affichés** pour ajouter

tous les nœuds à la liste réseau client non approuvé, puis utiliser la bascule à côté d'un nœud individuel pour ajouter ce nœud à la liste réseau client approuvé.

> Utilisez la barre de défilement située à droite du tableau pour vous assurer que vous avez affiché tous les nœuds disponibles. Utilisez le champ de recherche pour rechercher les paramètres d'un nœud en saisissant son nom. Vous pouvez entrer un nom partiel. Par exemple, si vous entrez un **GW**, tous les nœuds qui ont la chaîne "GW" comme partie de leur nom sont affichés.

4. Vous pouvez également sélectionner les ports supplémentaires que vous souhaitez ouvrir sur le réseau client non approuvé. Ces ports permettent d'accéder au gestionnaire de grille, au gestionnaire de locataires ou aux deux.

   Par exemple, vous pouvez utiliser cette option pour vous assurer que le gestionnaire de grille est accessible sur le réseau client à des fins de maintenance.

   > Ces ports supplémentaires sont ouverts sur le réseau client, qu'ils soient fermés ou non dans l'onglet gérer l'accès externe.

5. Sélectionnez **Enregistrer**.

   Les nouveaux paramètres de pare-feu sont immédiatement appliqués et appliqués. Les connexions client existantes peuvent échouer si les points de terminaison de l'équilibreur de charge n'ont pas été configurés.

Gérer les locataires

Gestion des locataires : présentation

En tant qu'administrateur grid, vous créez et gérez les comptes de locataire utilisés par les clients S3 et Swift pour stocker et récupérer des objets.

> La prise en charge des applications du client Swift a été obsolète et sera supprimée dans une prochaine version.

Qu'est-ce qu'un compte de locataire ?

Un compte de locataire vous permet d'utiliser l'API REST S3 (simple Storage Service) ou l'API REST Swift pour stocker et récupérer des objets dans un système StorageGRID.

Chaque compte de locataire comprend des groupes, utilisateurs, compartiments S3 ou conteneurs Swift et objets fédérés ou locaux.

Les comptes de tenant peuvent être utilisés pour isoler les objets stockés par des entités différentes. Par exemple, vous pouvez utiliser plusieurs comptes locataires pour l'une de ces utilisations :

- **Cas d'utilisation entreprise :** si vous gérez un système StorageGRID dans une application d'entreprise, vous pourriez vouloir isoler le stockage objet de la grille par les différents départements de votre organisation. Dans ce cas, vous pouvez créer des comptes de tenant pour le département Marketing, le service Customer support, le service des ressources humaines, etc.

Si vous utilisez le protocole client S3, vous pouvez utiliser des compartiments S3 et des règles de compartiments pour isoler les objets entre les services d'une entreprise. Vous n'avez pas besoin d'utiliser de comptes de locataire. Voir les instructions de mise en œuvre "Compartiments S3 et règles de compartiments" pour en savoir plus.

- **Cas d'utilisation de fournisseur de services :** si vous gérez un système StorageGRID en tant que fournisseur de services, vous pouvez isoler le stockage objet de la grille par les différentes entités qui loueront le stockage sur votre grille. Dans ce cas, vous créeriez des comptes de tenant pour la société A, la société B, la société C, etc.

Pour plus d'informations, voir "Utilisez un compte de locataire".

Comment créer un compte de locataire ?

Lorsque vous créez un compte de locataire, vous spécifiez les informations suivantes :

- Informations de base comprenant le nom du locataire, le type de client (S3 ou Swift) et le quota de stockage facultatif.
- Autorisations pour le compte de locataire, par exemple si le compte de locataire peut utiliser les services de la plateforme S3, configurer son propre référentiel d'identité, utiliser S3 Select ou utiliser une connexion de fédération grid.
- Accès racine initial pour le locataire, selon que le système StorageGRID utilise des groupes et utilisateurs locaux, la fédération des identités ou l'authentification unique (SSO).

En outre, vous pouvez activer le paramètre de verrouillage des objets S3 pour le système StorageGRID si les comptes de locataires S3 doivent se conformer aux exigences réglementaires. Lorsque le verrouillage des objets S3 est activé, tous les comptes de locataires S3 peuvent créer et gérer des compartiments conformes.

À quoi sert le gestionnaire de locataires ?

Une fois le compte de tenant créé, les utilisateurs de tenant peuvent se connecter au gestionnaire de tenant pour effectuer les tâches suivantes :

- Configurer la fédération des identités (sauf si le référentiel d'identité est partagé avec la grille)
- Gestion des groupes et des utilisateurs
- Utilisez la fédération grid pour le clone de compte et la réplication inter-grid
- Gestion des clés d'accès S3
- Création et gestion de compartiments S3
- Utilisez les services de plateforme S3
- Utiliser S3 Select
- Contrôle de l'utilisation du stockage

Les locataires S3 peuvent créer et gérer des clés d'accès S3 et des compartiments avec le gestionnaire de locataires. Ils doivent utiliser une application client S3 pour ingérer et gérer les objets. Voir "UTILISEZ L'API REST S3" pour plus d'informations.

Les utilisateurs Swift doivent disposer de l'autorisation d'accès racine pour accéder au Gestionnaire de locataires. Toutefois, l'autorisation d'accès racine ne permet pas aux utilisateurs de s'authentifier auprès de l'API REST Swift pour créer des conteneurs et ingérer des objets. Les utilisateurs doivent disposer de l'autorisation Administrateur Swift pour s'authentifier dans l'API REST de Swift.

Créez un compte de locataire

Vous devez créer au moins un compte de locataire pour contrôler l'accès au stockage dans votre système StorageGRID.

Les étapes de création d'un compte de locataire varient selon que "fédération des identités" et "authentification unique" Sont configurés et si le compte Grid Manager que vous utilisez pour créer le compte de tenant appartient à un groupe d'administration disposant de l'autorisation d'accès racine.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous disposez de l'autorisation accès racine ou comptes de tenant.
- Si le compte de tenant utilise le référentiel d'identité qui a été configuré pour Grid Manager et que vous souhaitez accorder l'autorisation d'accès racine au compte de tenant à un groupe fédéré, vous avez importé ce groupe fédéré dans Grid Manager. Vous n'avez pas besoin d'affecter d'autorisations Grid Manager à ce groupe d'administration. Voir "Gérez les groupes d'administration".
- Si vous souhaitez autoriser un locataire S3 à cloner les données de compte et à répliquer les objets de compartiment vers une autre grille à l'aide d'une connexion de fédération de grille :
  - Vous avez "configurez la connexion de fédération de grille - effectué".
  - L'état de la connexion est **connecté**.
  - Vous disposez de l'autorisation d'accès racine.
  - Vous avez examiné les éléments à prendre en compte pour "gestion des locataires autorisés pour la fédération dans le grid".
  - Si le compte de tenant utilise le référentiel d'identité configuré pour Grid Manager, vous avez importé le même groupe fédéré dans Grid Manager sur les deux grilles.

    Lorsque vous créez le tenant, vous sélectionnez ce groupe pour obtenir l'autorisation d'accès racine initiale pour les comptes de tenant source et de destination.

    Si ce groupe d'administration n'existe pas sur les deux grilles avant la création du tenant, celui-ci n'est pas répliqué vers la destination.

Accéder à l'assistant

Étapes

1. Sélectionnez **LOCATAIRES**.
2. Sélectionnez **Créer**.

Entrez les détails

Étapes

1. Entrez les détails du locataire.

Champ	Description
Nom	Nom du compte de locataire. Les noms de locataires n'ont pas besoin d'être uniques. Lorsque le compte de locataire est créé, il reçoit un ID de compte unique à 20 chiffres.
Description (facultatif)	Une description pour aider à identifier le locataire. Si vous créez un locataire qui utilisera une connexion de fédération de grille, vous pouvez utiliser ce champ pour identifier le locataire source et le locataire de destination. Par exemple, cette description pour un locataire créé sur la grille 1 s'affiche également pour le locataire répliqué dans la grille 2 : « ce locataire a été créé sur la grille 1 ».
Type de client	Le type de protocole client que ce locataire utilisera, soit **S3** soit **Swift**. **Remarque** : la prise en charge des applications clientes Swift a été obsolète et sera supprimée dans une version ultérieure.
Quota de stockage (facultatif)	Si vous souhaitez que ce locataire ait un quota de stockage, une valeur numérique pour le quota et les unités.

2. Sélectionnez **Continuer**.

Sélectionnez les autorisations

Étapes

1. Si vous le souhaitez, sélectionnez les autorisations dont ce locataire doit disposer.

> Certaines de ces autorisations ont des exigences supplémentaires. Pour plus de détails, sélectionnez l'icône d'aide pour chaque autorisation.

Autorisations	Si cette option est sélectionnée…
Autoriser les services de plate-forme	Le locataire peut utiliser des services de plateforme S3 tels que CloudMirror. Voir "Gestion des services de plateforme pour les comptes de locataires S3".
Utiliser son propre référentiel d'identité	Le locataire peut configurer et gérer son propre référentiel d'identité pour les groupes et utilisateurs fédérés. Cette option est désactivée si vous l'avez "SSO configuré" De votre système StorageGRID.

Autorisations	Si cette option est sélectionnée…
Autoriser la sélection S3	Le locataire peut émettre des requêtes d'API S3 SelectObjectContent pour filtrer et récupérer des données d'objet. Voir "Gérez S3 Select pour les comptes de locataires". **Important** : les requêtes SelectObjectContent peuvent réduire les performances de l'équilibreur de charge pour tous les clients S3 et tous les locataires. Activez cette fonctionnalité uniquement lorsque cela est nécessaire et uniquement pour les locataires de confiance.
Utiliser la connexion de fédération de grille	Le locataire peut utiliser une connexion de fédération de grille. Sélection de cette option : • Provoque le clonage de ce locataire et de tous les groupes de locataires et utilisateurs ajoutés au compte à partir de cette grille (la *grille source*) vers l'autre grille de la connexion sélectionnée (la *grille de destination*). • Permet à ce locataire de configurer la réplication entre les compartiments correspondants sur chaque grille. Voir "Gérer les locataires autorisés pour la fédération dans le grid". **Remarque** : vous ne pouvez sélectionner **utiliser la connexion de fédération de grille** que lorsque vous créez un nouveau locataire S3 ; vous ne pouvez pas sélectionner cette autorisation pour un locataire existant.

2. Si vous avez sélectionné **utiliser la connexion de fédération de grille**, sélectionnez l'une des connexions de fédération de grille disponibles.

3. Sélectionnez **Continuer**.

Définissez l'accès racine et créez un locataire

Étapes

1. Définissez l'accès racine pour le compte de locataire, selon que votre système StorageGRID utilise ou non la fédération des identités, l'authentification unique (SSO), ou les deux.

Option	Faites ça
Si la fédération des identités n'est pas activée	Spécifiez le mot de passe à utiliser lors de la connexion au tenant en tant qu'utilisateur root local.

Option	Faites ça
Si la fédération des identités est activée	a. Sélectionnez un groupe fédéré existant pour obtenir l'autorisation d'accès racine pour le tenant. b. Vous pouvez également spécifier le mot de passe à utiliser lors de la connexion au tenant en tant qu'utilisateur root local.
Si la fédération des identités et l'authentification unique (SSO) sont toutes deux activées	Sélectionnez un groupe fédéré existant pour obtenir l'autorisation d'accès racine pour le tenant. Aucun utilisateur local ne peut se connecter.

2. Sélectionnez **Créer locataire**.

   Un message de réussite s'affiche et le nouveau locataire apparaît sur la page locataires. Pour savoir comment afficher les détails des locataires et surveiller l'activité des locataires, reportez-vous à la section "Surveillez l'activité des locataires".

3. Si vous avez sélectionné l'autorisation **utiliser la connexion de fédération de grille** pour le locataire :
   a. Confirmez qu'un locataire identique a été répliqué sur l'autre grille de la connexion. Les locataires des deux grilles auront les mêmes ID de compte, nom, description, quota et autorisations à 20 chiffres.

      Si le message d'erreur « tenant créé sans clone » s'affiche, reportez-vous aux instructions de la section "Dépanner les erreurs de fédération de grille".

   b. Si vous avez fourni un mot de passe d'utilisateur root local lors de la définition de l'accès root, "modifiez le mot de passe de l'utilisateur root local" pour le tenant répliqué.

      Un utilisateur root local ne peut pas se connecter au gestionnaire de locataires sur la grille de destination tant que le mot de passe n'est pas modifié.

Se connecter au locataire (facultatif)

Si nécessaire, vous pouvez vous connecter au nouveau locataire maintenant pour terminer la configuration ou vous pouvez vous connecter ultérieurement au locataire. Les étapes de connexion dépendent si vous êtes connecté à Grid Manager à l'aide du port par défaut (443) ou d'un port restreint. Voir "Contrôler l'accès au niveau du pare-feu externe".

Connectez-vous dès maintenant

Si vous utilisez…	Procédez comme ça…
Le port 443 et vous définissez un mot de passe pour l'utilisateur root local	1. Sélectionnez **se connecter en tant que root**. Lorsque vous vous connectez, des liens s'affichent pour la configuration des compartiments, de la fédération des identités, des groupes et des utilisateurs. 2. Sélectionnez les liens pour configurer le compte de tenant. Chaque lien ouvre la page correspondante dans le Gestionnaire de locataires. Pour terminer la page, reportez-vous à la section "instructions d'utilisation des comptes de tenant".
Le port 443 et vous n'avez pas défini de mot de passe pour l'utilisateur root local	Sélectionnez **se connecter** et entrez les informations d'identification d'un utilisateur dans le groupe fédéré d'accès racine.
Un port restreint	1. Sélectionnez **Terminer** 2. Sélectionnez **Restricted** dans la table tenant pour en savoir plus sur l'accès à ce compte de tenant. L'URL du Gestionnaire de locataires a le format suivant : `https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id/` ◦ *`FQDN_or_Admin_Node_IP`* Est un nom de domaine complet ou l'adresse IP d'un nœud d'administration ◦ *`port`* est le port locataire uniquement ◦ *`20-digit-account-id`* Est l'ID de compte unique du locataire

Connectez-vous plus tard

Si vous utilisez…	Effectuez l'une d'entre elles…
Orifice 443	• Dans Grid Manager, sélectionnez **TENANTS**, puis **connexion** à droite du nom du locataire. • Entrez l'URL du locataire dans un navigateur Web : `https://FQDN_or_Admin_Node_IP/?accountId=20-digit-account-id/` ◦ *`FQDN_or_Admin_Node_IP`* Est un nom de domaine complet ou l'adresse IP d'un nœud d'administration ◦ *`20-digit-account-id`* Est l'ID de compte unique du locataire

Si vous utilisez…	Effectuez l'une d'entre elles…
Un port restreint	• Dans le Gestionnaire de grille, sélectionnez **TENANTS** et sélectionnez **restreint**. • Entrez l'URL du locataire dans un navigateur Web : `https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id` ◦ *FQDN_or_Admin_Node_IP* Est un nom de domaine complet ou l'adresse IP d'un nœud d'administration ◦ *port* est le port réservé aux locataires ◦ *20-digit-account-id* Est l'ID de compte unique du locataire

Configurez le tenant

Suivez les instructions de la section "Utilisez un compte de locataire" Pour gérer les groupes et utilisateurs de locataires, les clés d'accès S3, les compartiments, les services de plateforme, le clone de compte et la réplication inter-grid.

Modifiez le compte de tenant

Vous pouvez modifier un compte de locataire pour modifier le nom d'affichage, le quota de stockage ou les autorisations de locataire.

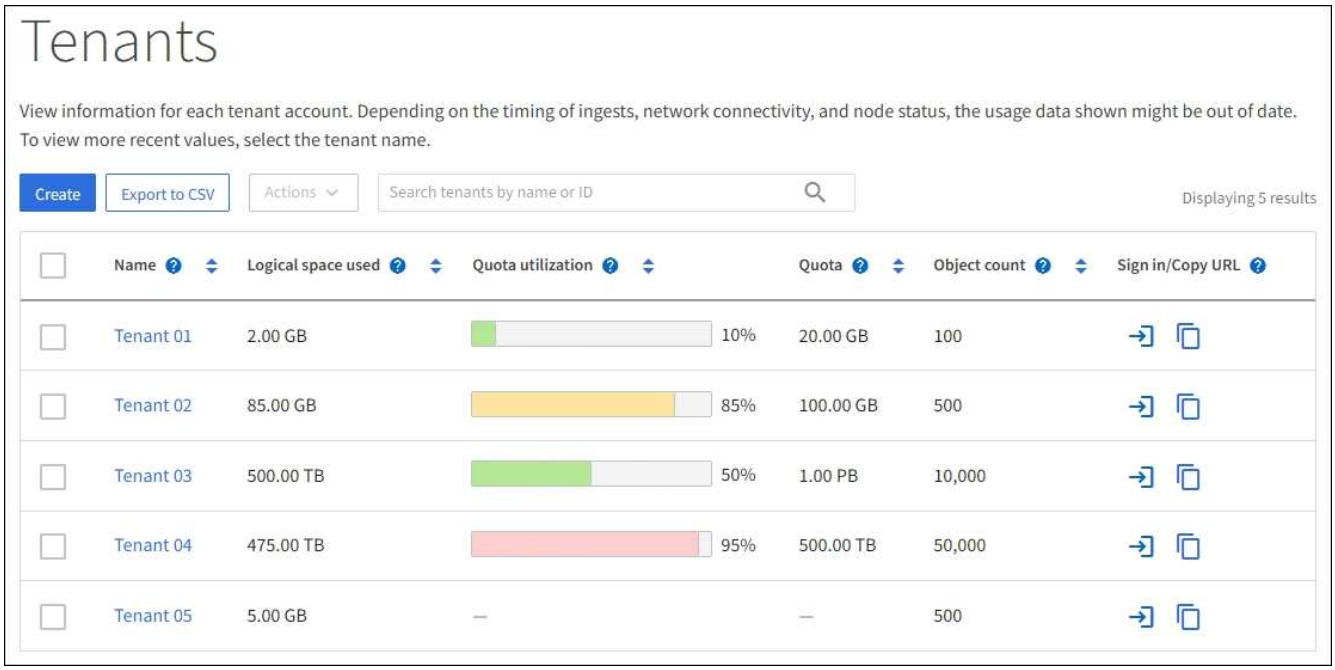
> Si un locataire dispose de l'autorisation **utiliser la connexion de fédération de grille**, vous pouvez modifier les détails du locataire à partir de l'une des grilles de la connexion. Toutefois, toute modification apportée à une grille dans la connexion ne sera pas copiée dans l'autre grille. Si vous souhaitez que les détails du locataire soient synchronisés exactement entre les grilles, effectuez les mêmes modifications sur les deux grilles. Voir "Gérez les locataires autorisés pour la connexion de fédération de grille".

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous disposez de l'autorisation accès racine ou comptes de tenant.

Étapes

1. Sélectionnez **LOCATAIRES**.



2. Recherchez le compte de locataire à modifier.

   Utilisez la zone de recherche pour rechercher un locataire par nom ou ID locataire.

3. Sélectionnez le locataire. Vous pouvez effectuer l'une des opérations suivantes :
   - Cochez la case du locataire, puis sélectionnez **actions** > **Modifier**.
   - Sélectionnez le nom du locataire pour afficher la page des détails, puis sélectionnez **Modifier**.
4. Si vous le souhaitez, modifiez les valeurs de ces champs :
   - **Nom**
   - **Description**
   - **Quota de stockage**
5. Sélectionnez **Continuer**.
6. Sélectionnez ou désélectionnez les autorisations pour le compte de tenant.
   - Si vous désactivez **Platform Services** pour un locataire qui les utilise déjà, les services qu'ils ont configurés pour leurs compartiments S3 cessent de fonctionner. Aucun message d'erreur n'est envoyé au locataire. Par exemple, si le locataire a configuré la réplication CloudMirror pour un compartiment S3, il peut toujours stocker les objets dans le compartiment, mais les copies de ces objets ne sont plus effectuées dans le compartiment S3 externe qu'ils ont configuré en tant que terminal. Voir "Gestion des services de plateforme pour les comptes de locataires S3".
   - Modifiez le paramètre de **utilise son propre référentiel d'identité** pour déterminer si le compte de tenant utilisera son propre référentiel d'identité ou le référentiel d'identité configuré pour le gestionnaire de grille.

     Si **utilise son propre référentiel d'identité** est :

     - Désactivé et sélectionné, le locataire a déjà activé son propre référentiel d'identité. Un locataire doit désactiver son référentiel d'identité avant de pouvoir utiliser le référentiel d'identité configuré pour Grid Manager.
     - Désactivé et non sélectionné, SSO est activé pour le système StorageGRID. Le locataire doit

utiliser le référentiel d'identité qui a été configuré pour Grid Manager.

- Sélectionnez ou désélectionnez l'autorisation **Autoriser S3 Select** selon les besoins. Voir "Gérez S3 Select pour les comptes de locataires".
- Pour supprimer l'autorisation **utiliser la connexion de fédération de grille**, suivez les instructions de "suppression de l'autorisation d'un locataire pour utiliser la fédération de grille".

Modifiez le mot de passe de l'utilisateur racine local du locataire

Vous devrez peut-être modifier le mot de passe de l'utilisateur root local d'un locataire si celui-ci est verrouillé hors du compte.

Avant de commencer

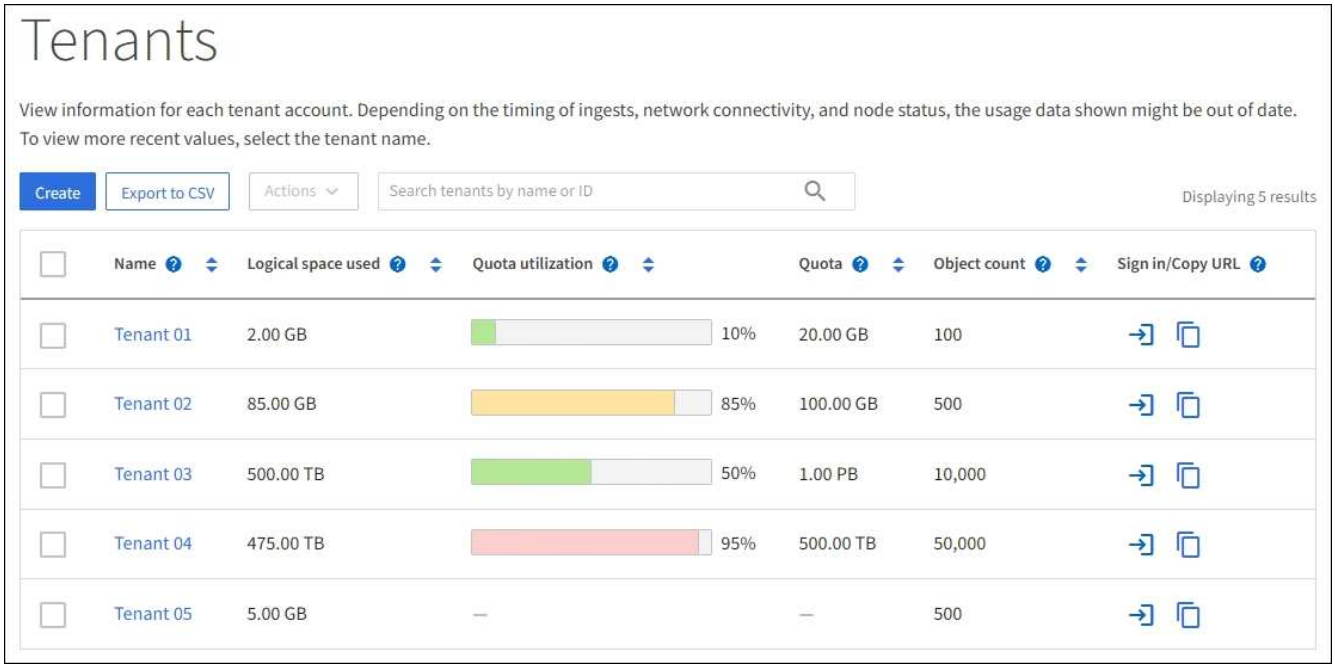
- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous disposez d'autorisations d'accès spécifiques.

Description de la tâche

Si l'authentification unique (SSO) est activée pour votre système StorageGRID, l'utilisateur root local ne peut pas se connecter au compte de locataire. Pour effectuer des tâches utilisateur racine, les utilisateurs doivent appartenir à un groupe fédéré disposant de l'autorisation d'accès racine pour le locataire.

Étapes

1. Sélectionnez **LOCATAIRES**.



2. Sélectionnez le compte locataire. Vous pouvez effectuer l'une des opérations suivantes :
   - Cochez la case du locataire, puis sélectionnez **actions** > **Modifier le mot de passe root**.
   - Sélectionnez le nom du locataire pour afficher la page de détails, puis sélectionnez **actions** > **Modifier le mot de passe root**.
3. Saisissez le nouveau mot de passe du compte de tenant.
4. Sélectionnez **Enregistrer**.

Supprimer le compte de locataire

Vous pouvez supprimer un compte de tenant si vous souhaitez supprimer définitivement l'accès du tenant au système.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous disposez d'autorisations d'accès spécifiques.
- Vous avez supprimé tous les compartiments (S3), conteneurs (Swift) et objets associés au compte de locataire.
- Si le locataire est autorisé à utiliser une connexion de fédération de grille, vous avez examiné les considérations de "Suppression d'un locataire avec l'autorisation utiliser la connexion de fédération de grille".

Étapes

1. Sélectionnez **LOCATAIRES**.
2. Recherchez le ou les comptes de tenant que vous souhaitez supprimer.

   Utilisez la zone de recherche pour rechercher un locataire par nom ou ID locataire.

3. Pour supprimer plusieurs locataires, cochez les cases et sélectionnez **actions** > **Supprimer**.
4. Pour supprimer un seul locataire, effectuez l'une des opérations suivantes :
   - Cochez la case et sélectionnez **actions** > **Supprimer**.
   - Sélectionnez le nom du locataire pour afficher la page des détails, puis sélectionnez **actions** > **Supprimer**.
5. Sélectionnez **Oui**.

Gestion des services de plateforme

Gestion des services de plateforme pour les locataires : présentation

Si vous activez des services de plateforme pour les comptes de locataires S3, vous devez configurer votre grid de manière à ce que les locataires puissent accéder aux ressources externes nécessaires à l'utilisation de ces services.

Qu'est-ce que les services de plateforme ?

Les services de plateforme incluent la réplication CloudMirror, les notifications d'événement et le service d'intégration de la recherche.

Ces services permettent aux locataires d'utiliser les fonctionnalités suivantes avec leurs compartiments S3 :

- **Réplication CloudMirror** : le service de réplication StorageGRID CloudMirror permet la mise en miroir d'objets spécifiques d'un compartiment StorageGRID vers une destination externe spécifiée.

  Vous pouvez, par exemple, utiliser la réplication CloudMirror pour mettre en miroir des enregistrements client spécifiques dans Amazon S3, puis exploiter les services AWS pour analyser vos données.

La réplication CloudMirror présente des similarités et des différences importantes avec la fonction de réplication multigrille. Pour en savoir plus, voir "Comparez la réplication entre les grilles et la réplication CloudMirror".

La réplication CloudMirror n'est pas prise en charge si le compartiment source est activé pour le verrouillage objet S3.

- **Notifications** : les notifications d'événements par compartiment sont utilisées pour envoyer des notifications sur des actions spécifiques effectuées sur des objets à un service Amazon simple notification Service™ (Amazon SNS) externe spécifié.

  Par exemple, vous pouvez configurer l'envoi d'alertes aux administrateurs pour chaque objet ajouté à un compartiment, où les objets représentent les fichiers de journal associés à un événement système critique.

  Bien que la notification d'événement puisse être configurée sur un compartiment avec l'option de verrouillage d'objet S3 activée, les métadonnées S3 Object Lock (conservation jusqu'à la date et état de conservation légale) des objets ne seront pas incluses dans les messages de notification.

- **Service d'intégration de recherche** : le service d'intégration de recherche est utilisé pour envoyer des métadonnées d'objet S3 à un index Elasticsearch spécifié où les métadonnées peuvent être recherchées ou analysées à l'aide du service externe.

  Vous pouvez, par exemple, configurer des compartiments pour envoyer les métadonnées d'objet S3 vers un service Elasticsearch distant. Vous pouvez ensuite utiliser Elasticsearch pour effectuer des recherches dans des compartiments et effectuer des analyses sophistiquées des modèles présents dans les métadonnées de l'objet.

  Bien que l'intégration avec Elasticsearch puisse être configurée sur un compartiment avec l'option S3 Object Lock activée, les métadonnées S3 Object Lock (conservation jusqu'à la date et état de conservation légale) des objets ne seront pas incluses dans les messages de notification.

Les services de plateforme permettent aux locataires d'utiliser des ressources de stockage externes, des services de notification et des services de recherche ou d'analyse avec leurs données. Étant donné que l'emplacement cible des services de plateforme ne fait généralement pas partie de votre déploiement StorageGRID, vous devez décider si vous souhaitez autoriser les locataires à utiliser ces services. Dans ce cas, vous devez activer l'utilisation des services de plateforme lorsque vous créez ou modifiez des comptes de tenant. Vous devez également configurer votre réseau de sorte que les messages de services de plate-forme générés par les locataires puissent atteindre leurs destinations.

Recommandations relatives à l'utilisation des services de plate-forme

Avant d'utiliser les services de plate-forme, tenez compte des recommandations suivantes :

- Si le contrôle de versions et la réplication CloudMirror sont activés pour un compartiment S3 dans le système StorageGRID, vous devez également activer la gestion des versions du compartiment S3 pour le terminal de destination. Cela permet à la réplication CloudMirror de générer des versions d'objet similaires sur le noeud final.
- Vous ne devez pas utiliser plus de 100 locataires actifs avec les demandes S3 nécessitant la réplication CloudMirror, les notifications et l'intégration de la recherche. Avec plus de 100 locataires actifs, les performances des clients S3 sont plus lentes.

- Les demandes adressées à un point final qui ne peut pas être terminé seront mises en file d'attente pour un maximum de 500,000 demandes. Cette limite est également partagée entre les locataires actifs. Les nouveaux locataires sont autorisés à dépasser temporairement cette limite de 500,000 afin que les locataires nouvellement créés ne soient pas pénalisés injustement.

Informations associées

- "Utilisez un compte de locataire"
- "Configurez les paramètres du proxy de stockage"
- "Surveillez StorageGRID"

Réseau et ports pour les services de plate-forme

Si vous autorisez un locataire S3 à utiliser des services de plateforme, vous devez configurer la mise en réseau pour le grid de manière à ce que les messages des services de plateforme puissent être envoyés vers leur destination.

Lorsque vous créez ou mettez à jour le compte de locataire, vous pouvez activer des services de plateforme pour un compte de locataire S3. Si les services de plateforme sont activés, le locataire peut créer des terminaux qui servent de destination à la réplication CloudMirror, à la notification d'événement ou aux messages d'intégration de recherche à partir de ses compartiments S3. Ces messages de services de plateforme sont envoyés depuis les nœuds de stockage qui exécutent le service ADC vers les terminaux de destination.

Par exemple, les locataires peuvent configurer les types de terminaux de destination suivants :

- Un cluster Elasticsearch hébergé localement
- Application locale qui prend en charge la réception de messages Amazon SNS (simple notification Service)
- Un compartiment S3 hébergé localement sur la même instance d'StorageGRID ou sur une autre instance
- Un terminal externe, tel qu'un terminal sur Amazon Web Services.

Pour vous assurer que les messages des services de plate-forme peuvent être envoyés, vous devez configurer le réseau ou les réseaux contenant les nœuds de stockage ADC. Vous devez vous assurer que les ports suivants peuvent être utilisés pour envoyer des messages de services de plate-forme aux noeuds finaux de destination.

Par défaut, les messages des services de plate-forme sont envoyés sur les ports suivants :

- **80**: Pour les URI de point final commençant par http
- **443**: Pour les URI de point final qui commencent par https

Les locataires peuvent spécifier un port différent lorsqu'ils créent ou modifient un noeud final.

> Si un déploiement StorageGRID est utilisé comme destination pour la réplication CloudMirror, des messages de réplication peuvent être reçus sur un port autre que 80 ou 443. Vérifiez que le port utilisé pour S3 par le déploiement StorageGRID de destination est spécifié dans le terminal.

Si vous utilisez un serveur proxy non transparent, vous devez également "Configurez les paramètres du proxy de stockage" pour permettre l'envoi de messages vers des points de terminaison externes, tels qu'un point de terminaison sur internet.

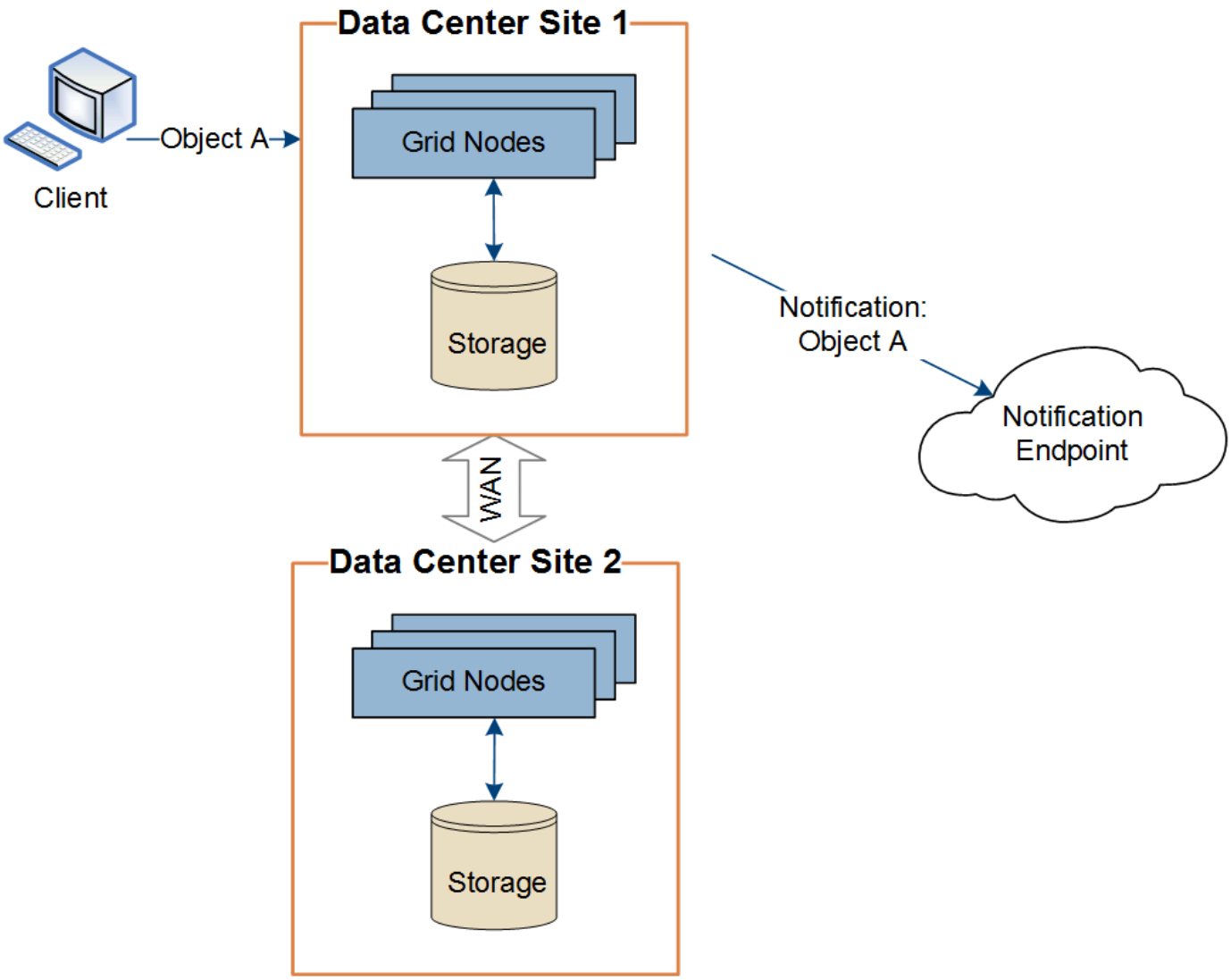
Informations associées

- "Utilisez un compte de locataire"

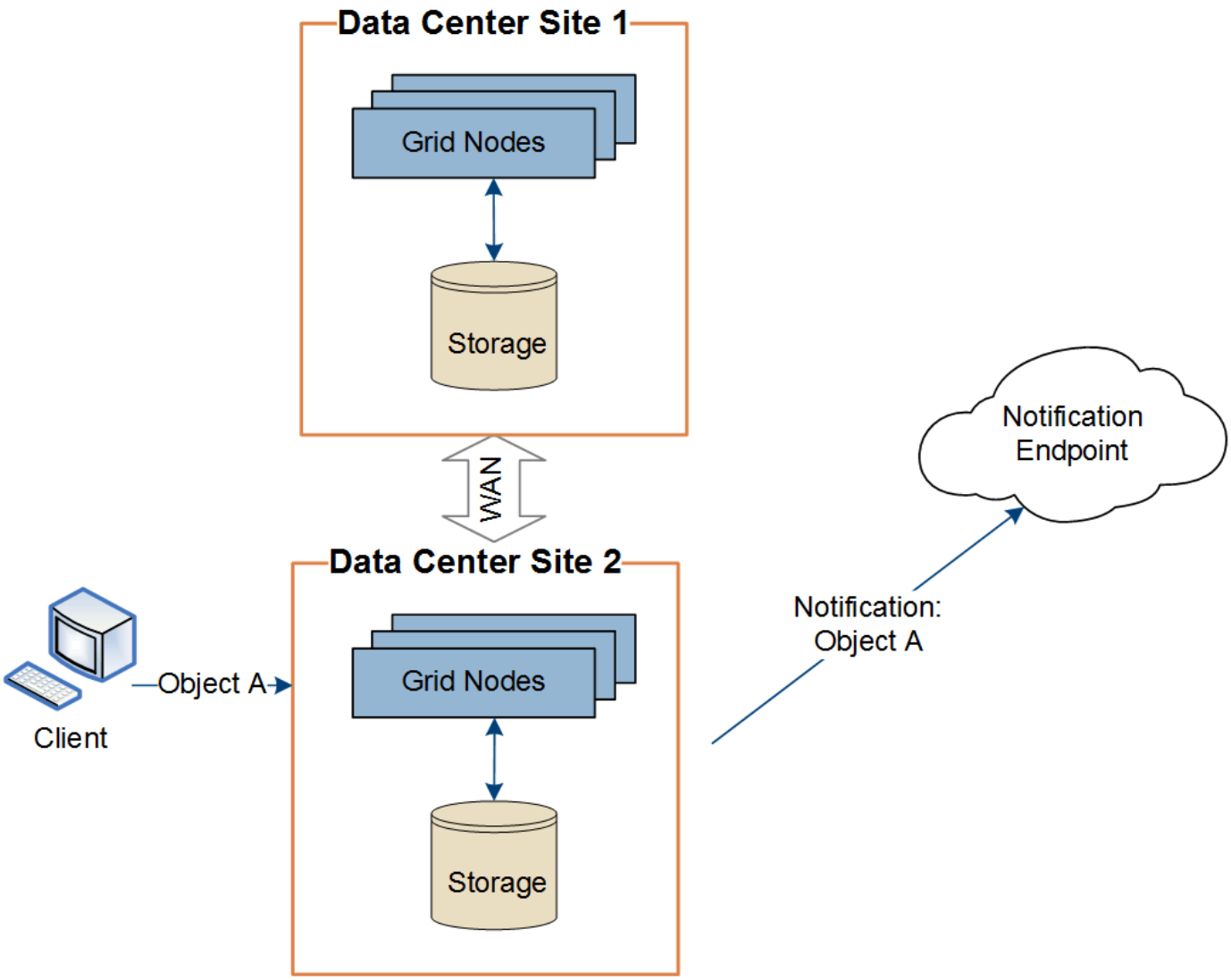
Livraison par site de messages de services de plate-forme

Toutes les opérations de services de plateforme sont réalisées sur une base par site.

C'est-à-dire que si un locataire utilise un client pour effectuer une opération de création d'API S3 sur un objet en se connectant à un nœud de passerelle sur le site de Data Center 1, la notification concernant cette action est déclenchée et envoyée depuis le site de Data Center 1.



Si le client exécute ensuite une opération de suppression d'API S3 sur ce même objet à partir du site du centre de données 2, la notification concernant l'action de suppression est déclenchée et envoyée depuis le site du centre de données 2.



Assurez-vous que le réseau de chaque site est configuré de manière à ce que les messages des services de plate-forme puissent être transmis à leurs destinations.

Résoudre les problèmes liés aux services de plateforme

Les terminaux utilisés dans les services de plateforme sont créés et gérés par les utilisateurs locataires dans le Gestionnaire de locataires. Toutefois, si un locataire a des problèmes de configuration ou d'utilisation des services de plateforme, vous pouvez utiliser le Gestionnaire de grille pour résoudre le problème.

Problèmes liés aux nouveaux terminaux

Avant qu'un locataire ne puisse utiliser les services de plateforme, il doit créer un ou plusieurs terminaux à l'aide du Gestionnaire des locataires. Chaque terminal représente une destination externe pour un service de plateforme unique, par exemple un compartiment StorageGRID S3, un compartiment Amazon Web Services, un thème simple Service de notification ou un cluster Elasticsearch hébergé localement ou sur AWS. Chaque noeud final comprend à la fois l'emplacement de la ressource externe et les informations d'identification nécessaires pour accéder à cette ressource.

Lorsqu'un locataire crée un noeud final, le système StorageGRID valide que ce dernier existe et qu'il peut être atteint à l'aide des identifiants spécifiés. La connexion au noeud final est validée à partir d'un nœud sur chaque

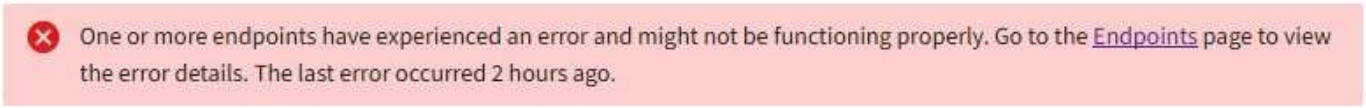
site.

Si la validation du noeud final échoue, un message d'erreur explique pourquoi la validation du noeud final a échoué. L'utilisateur locataire doit résoudre le problème, puis essayer de créer à nouveau le noeud final.

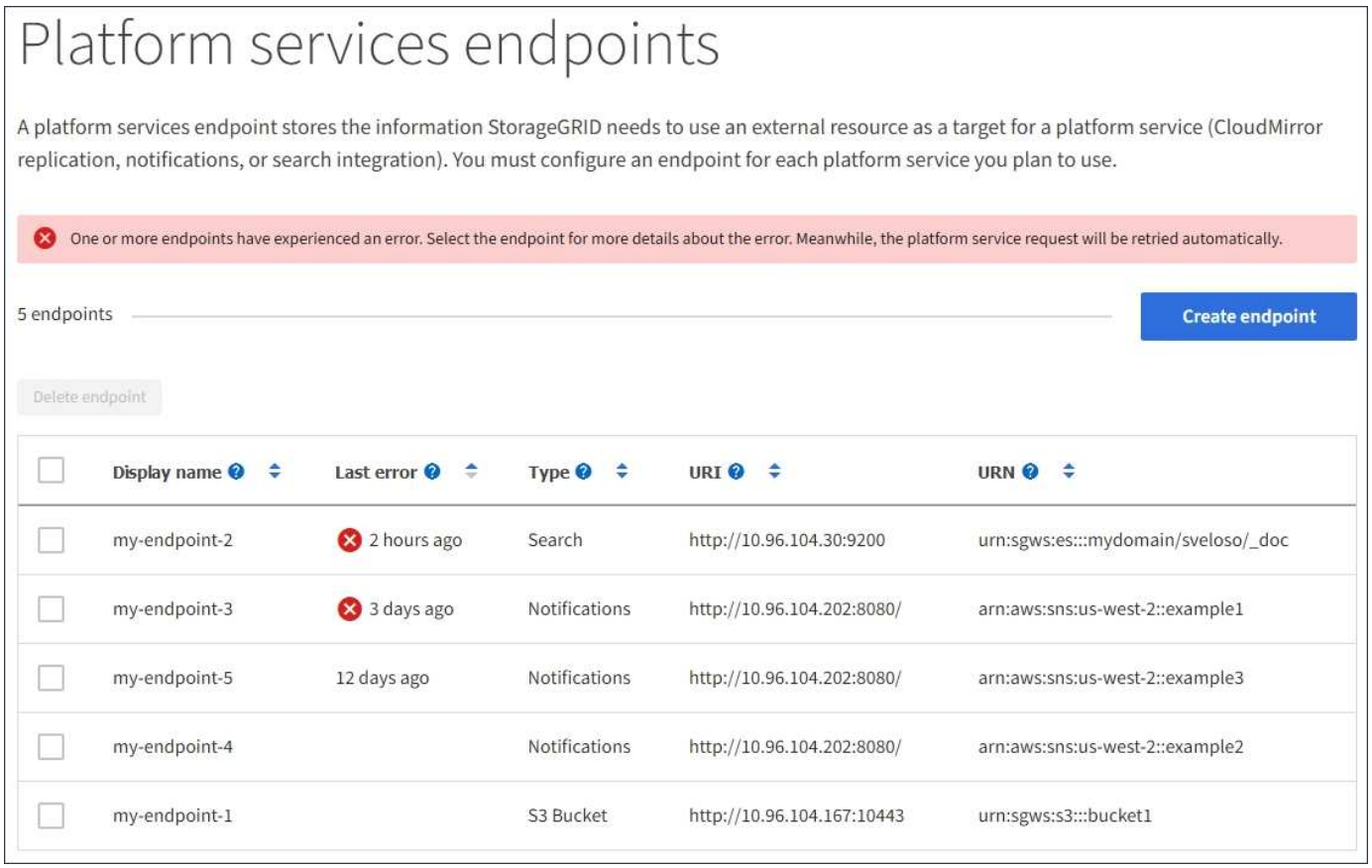
La création du terminal échoue si les services de plateforme ne sont pas activés pour le compte de locataire.

Problèmes avec les terminaux existants

Si une erreur se produit lorsque StorageGRID tente d'atteindre un noeud final existant, un message s'affiche sur le tableau de bord dans le Gestionnaire de locataires.



Les utilisateurs locataires peuvent accéder à la page noeuds finaux pour consulter le message d'erreur le plus récent pour chaque noeud final et déterminer la durée de l'erreur. La colonne **dernière erreur** affiche le message d'erreur le plus récent pour chaque noeud final et indique la durée de l'erreur. Erreurs incluant le l'icône s'est produite au cours des 7 derniers jours.



Certains messages d'erreur dans la colonne **dernière erreur** peuvent inclure un LogId entre parenthèses. Un administrateur de grille ou le support technique peut utiliser cet ID pour trouver des informations plus détaillées sur l'erreur dans bycast.log.

Problèmes liés aux serveurs proxy

Si vous avez configuré un "Proxy de stockage" Entre les noeuds de stockage et les noeuds finaux du service de plate-forme, des erreurs peuvent se produire si votre service proxy n'autorise pas les messages de StorageGRID. Pour résoudre ces problèmes, vérifiez les paramètres de votre serveur proxy pour vous assurer que les messages liés au service de plate-forme ne sont pas bloqués.

Déterminez si une erreur s'est produite

Si des erreurs de noeud final se sont produites au cours des 7 derniers jours, le tableau de bord du gestionnaire de locataires affiche un message d'alerte. Vous pouvez accéder à la page noeuds finaux pour obtenir plus de détails sur l'erreur.

Échec des opérations client

Certains problèmes de service de plateforme peuvent entraîner l'échec des opérations client dans le compartiment S3. Par exemple, les opérations client S3 échouent si le service RSM (Replicated State machine) interne s'arrête ou s'il y a trop de messages de services de plate-forme en file d'attente pour la livraison.

Pour vérifier l'état des services :

1. Sélectionnez **SUPPORT** > **Outils** > **topologie de grille**.
2. Sélectionnez ***site*** > ***Storage Node*** > **SSM** > **Services**.

Erreurs récupérables et récupérables du point final

Une fois les noeuds finaux créés, des erreurs de demande de service de plate-forme peuvent se produire pour diverses raisons. Certaines erreurs peuvent être récupérées avec l'intervention de l'utilisateur. Par exemple, des erreurs récupérables peuvent se produire pour les raisons suivantes :

- Les informations d'identification de l'utilisateur ont été supprimées ou ont expiré.
- Le compartiment de destination n'existe pas.
- La notification ne peut pas être remise.

Si StorageGRID rencontre une erreur récupérable, la demande de service de plate-forme sera relancée jusqu'à ce qu'elle réussisse.

D'autres erreurs sont irrécupérables. Par exemple, une erreur irrécupérable se produit si le noeud final est supprimé.

Si StorageGRID rencontre une erreur de point final irrécupérable, l'alarme d'événements totaux (SMTT) héritée est déclenchée dans le Gestionnaire de grille. Pour afficher l'alarme Total Events hérité :

1. Sélectionnez **SUPPORT** > **Outils** > **topologie de grille**.
2. Sélectionnez ***site*** > ***node*** > **SSM** > **Events**.
3. Afficher le dernier événement en haut du tableau.

   Les messages d'événement sont également répertoriés dans le `/var/local/log/bycast-err.log`.

4. Suivez les instructions fournies dans le contenu de l'alarme SMTT pour corriger le problème.
5. Sélectionnez l'onglet **Configuration** pour réinitialiser le nombre d'événements.

6. Notifier le locataire des objets dont les messages de services de plate-forme n'ont pas été livrés.
7. Demandez au locataire de déclencher à nouveau la réplication ou la notification ayant échoué en mettant à jour les métadonnées ou balises de l'objet.

   Le locataire peut soumettre de nouveau les valeurs existantes afin d'éviter toute modification non souhaitée.

Les messages des services de plateforme ne peuvent pas être transmis

Si la destination rencontre un problème qui l'empêche d'accepter des messages de services de plate-forme, l'opération client sur le compartiment réussit, mais le message des services de plate-forme n'est pas livré. Par exemple, cette erreur peut se produire si les informations d'identification sont mises à jour sur la destination de sorte que StorageGRID ne puisse plus s'authentifier auprès du service de destination.

Si les messages des services de plate-forme ne peuvent pas être transmis en raison d'une erreur irrécupérable, l'alarme héritée Total Events (SMTT) est déclenchée dans le gestionnaire de grille.

Des performances plus lentes pour les demandes de services de plateforme

Le logiciel StorageGRID peut canaliser les demandes S3 entrantes pour un compartiment si le taux d'envoi des demandes dépasse le taux à partir duquel le terminal de destination peut recevoir les demandes. La restriction ne se produit que lorsqu'il existe un arriéré de demandes en attente d'envoi vers le noeud final de destination.

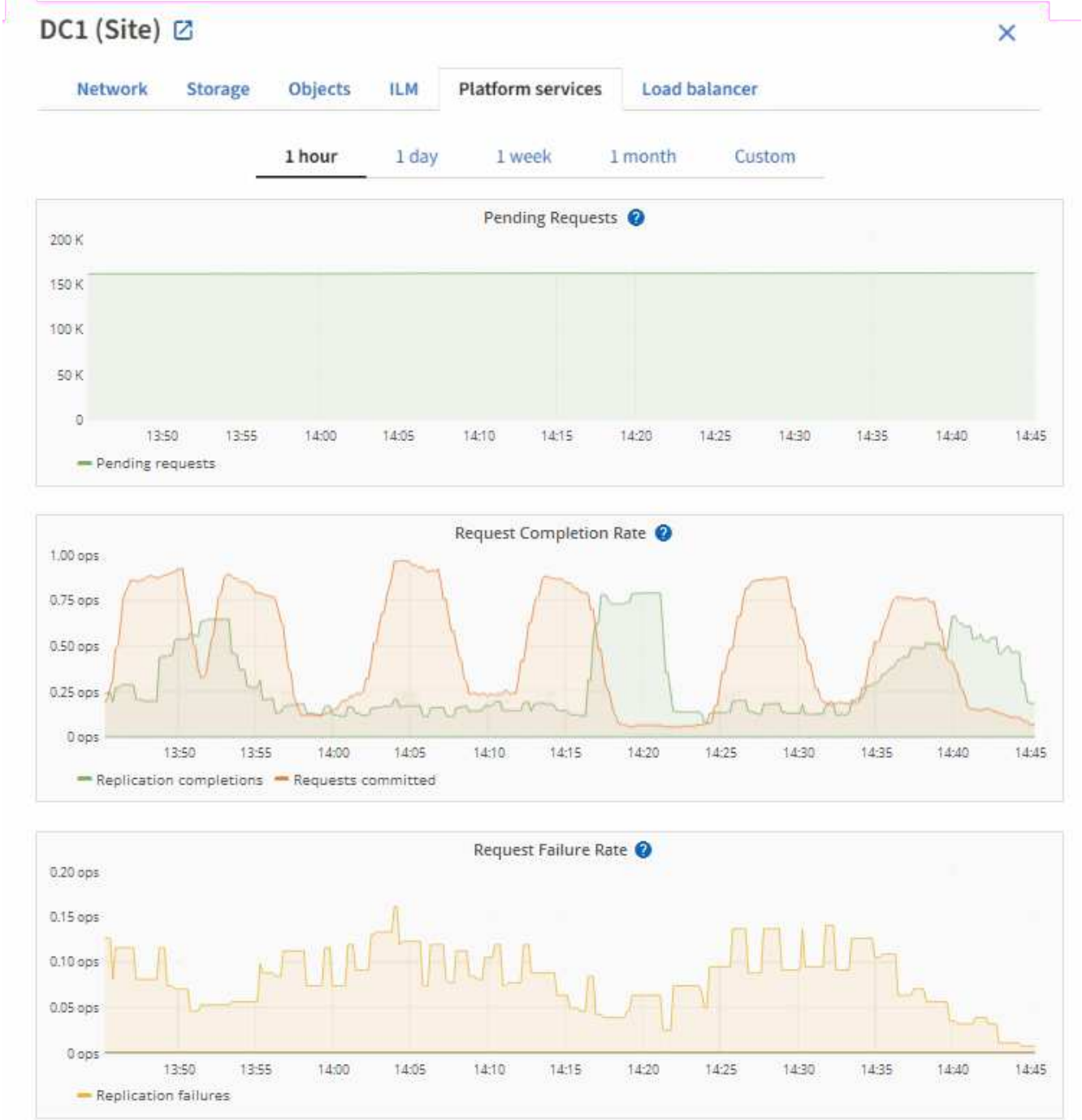
Le seul effet visible est que les requêtes S3 entrantes prennent plus de temps à s'exécuter. Si vous commencez à détecter les performances beaucoup plus lentes, vous devez réduire le taux d'entrée ou utiliser un terminal avec une capacité plus élevée. Si l'carnet de commandes des requêtes continue d'augmenter, les opérations S3 des clients (par EXEMPLE, LES requêtes PUT) finiront par échouer.

Les demandes CloudMirror sont plus susceptibles d'être affectées par les performances du terminal de destination, car ces demandes impliquent généralement plus de transfert de données que les demandes d'intégration de recherche ou de notification d'événements.

Les demandes de service de la plateforme échouent

Pour afficher le taux d'échec de la demande pour les services de plate-forme :

1. Sélectionnez **NOEUDS**.
2. Sélectionnez ***site*** > **Platform Services**.
3. Afficher le tableau des taux d'erreur de demande.



Alerte de services de plate-forme non disponibles

L'alerte **Platform services unavailable** indique qu'aucune opération de service de plate-forme ne peut être effectuée sur un site car trop de nœuds de stockage avec le service RSM sont en cours d'exécution ou disponibles.

Le service RSM garantit que les demandes de service de plate-forme sont envoyées à leurs points de terminaison respectifs.

Pour résoudre cette alerte, déterminez quels nœuds de stockage du site incluent le service RSM. (Le service RSM est présent sur les nœuds de stockage qui incluent également le service ADC.) Ensuite, assurez-vous que la plupart de ces nœuds de stockage sont exécutés et disponibles.

Si plusieurs nœuds de stockage contenant le service RSM échouent sur un site, vous perdez toute demande de service de plateforme en attente pour ce site.

Conseils de dépannage supplémentaires pour les terminaux des services de plateforme

Pour plus d'informations, voir "Utiliser un compte locataire ; dépanner les terminaux des services de plateforme".

Informations associées

- "Dépanner le système StorageGRID"

Gérez S3 Select pour les comptes de locataires

Vous pouvez autoriser certains locataires S3 à utiliser S3 Select pour émettre des demandes SelectObjectContent sur des objets individuels.

S3 Select constitue un moyen efficace d'effectuer des recherches dans de vastes volumes de données sans avoir à déployer une base de données et les ressources associées pour activer les recherches. Il réduit également le coût et la latence liés à la récupération des données.

Qu'est-ce que S3 Select ?

S3 Select permet aux clients S3 d'utiliser les requêtes SelectObjectContent pour filtrer et récupérer uniquement les données nécessaires à partir d'un objet. L'implémentation d'StorageGRID de S3 Select inclut un sous-ensemble de commandes et de fonctionnalités S3 Select.

Considérations et configuration requise pour l'utilisation de S3 Select

Exigences d'administration du grid

L'administrateur du grid doit autoriser les locataires S3 Select. Sélectionnez **Autoriser sélection S3** quand "création d'un locataire" ou "modification d'un locataire".

Exigences de format d'objet

L'objet que vous souhaitez interroger doit être dans l'un des formats suivants :

- **CSV**. Peut être utilisé tel qu'il est ou compressé dans des archives GZIP ou BZIP2.
- **Parquet**. Exigences supplémentaires pour les objets parquet :
  - S3 Select prend uniquement en charge la compression par colonne à l'aide de GZIP ou de Snappy. S3 Select ne prend pas en charge la compression d'objets entiers pour les objets parquet.
  - S3 Select ne prend pas en charge la sortie parquet. Vous devez spécifier le format de sortie au format CSV ou JSON.
  - La taille maximale du groupe de lignes non compressées est de 512 Mo.
  - Vous devez utiliser les types de données spécifiés dans le schéma de l'objet.
  - Vous ne pouvez pas utiliser de types logiques D'INTERVALLE, de JSON, DE LISTE, DE TEMPS ou d'UUID.

Exigences relatives aux terminaux

La requête SelectObjectContent doit être envoyée à un "Terminal d'équilibrage de charge StorageGRID".

Les nœuds d'administration et de passerelle utilisés par le noeud final doivent être l'un des suivants :

- Nœud d'appliance SG100 ou SG1000
- Nœud logiciel basé sur VMware
- Nœud bare Metal exécutant un noyau avec cgroup v2 activé

Considérations générales

Les requêtes ne peuvent pas être envoyées directement aux nœuds de stockage.

> SelectObjectContent les demandes peuvent réduire les performances d'équilibrage de charge pour tous les clients S3 et tous les locataires. Activez cette fonctionnalité uniquement lorsque cela est nécessaire et uniquement pour les locataires de confiance.

Voir la "Instructions d'utilisation de S3 Select".

Pour afficher "Graphiques Grafana" Pour les opérations S3 Select dans le temps, sélectionnez **SUPPORT** > **Outils** > **métriques** dans le Gestionnaire de grille.

Configurer les connexions client

Présentation de la configuration des connexions client S3 et Swift

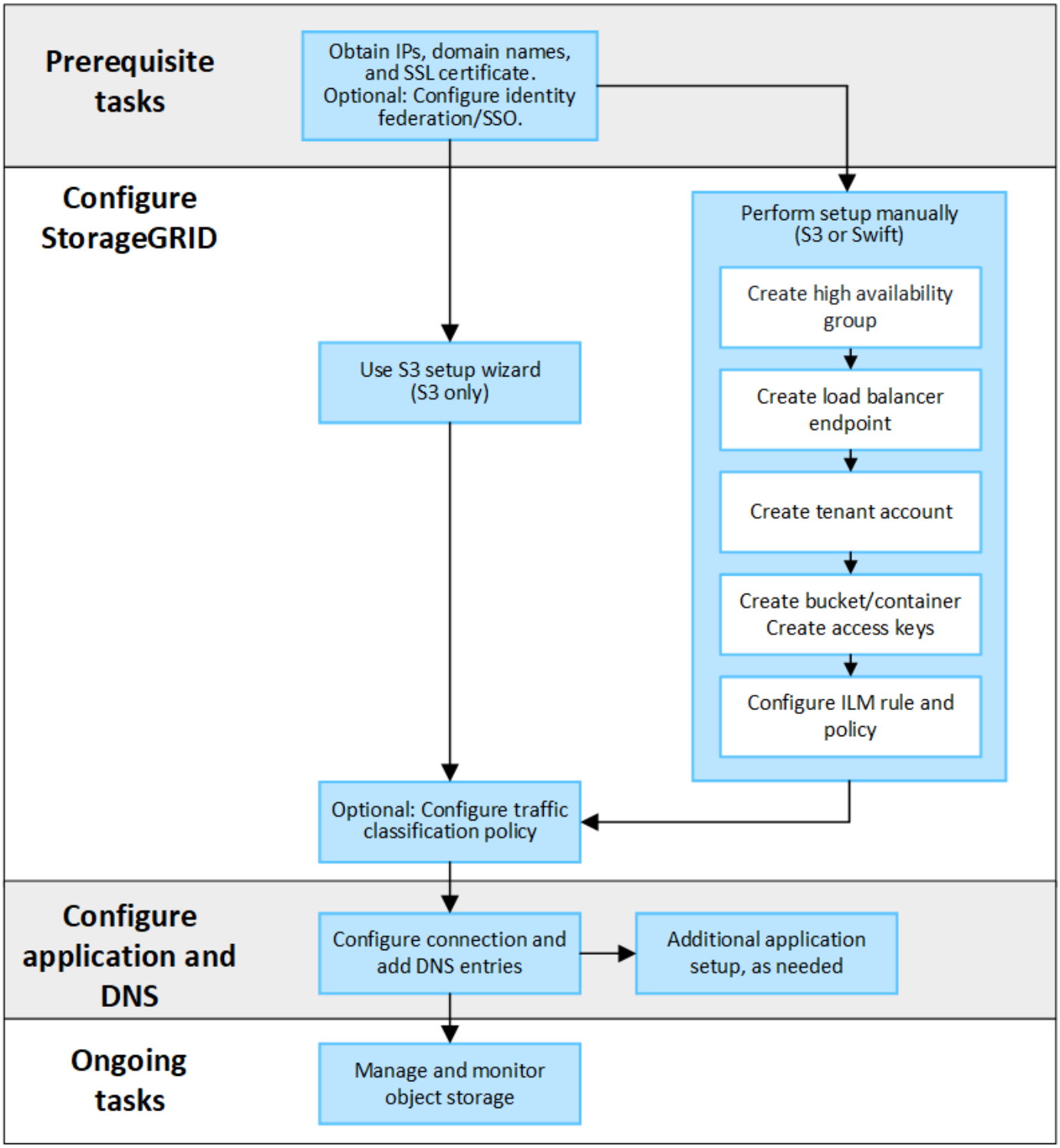
En tant qu'administrateur du grid, vous gérez les options de configuration qui contrôlent la façon dont les applications clientes S3 et Swift se connectent au système StorageGRID pour stocker et récupérer les données.

> La prise en charge des applications du client Swift a été obsolète et sera supprimée dans une prochaine version.

Flux de travail de configuration

Comme illustré dans le schéma de workflow, il existe quatre étapes principales pour connecter StorageGRID à une application S3 ou Swift :

1. Effectuez les tâches requises dans StorageGRID, en fonction de la façon dont l'application client se connecte à StorageGRID.
2. Utilisez StorageGRID pour obtenir les valeurs dont l'application a besoin pour se connecter à la grille. Vous pouvez utiliser l'assistant d'installation S3 ou configurer chaque entité StorageGRID manuellement.
3. Utilisez l'application S3 ou Swift pour terminer la connexion à StorageGRID. Créez des entrées DNS pour associer des adresses IP à tous les noms de domaine que vous prévoyez d'utiliser.
4. Effectuez des tâches continues dans l'application et dans StorageGRID afin de gérer et de surveiller le stockage objet au fil du temps.



Informations nécessaires pour joindre StorageGRID à une application client

Avant de connecter StorageGRID à une application client S3 ou Swift, vous devez effectuer les étapes de configuration dans StorageGRID et obtenir une certaine valeur.

Quelles valeurs ai-je besoin ?

Le tableau suivant présente les valeurs que vous devez configurer dans StorageGRID et où ces valeurs sont utilisées par l'application S3 ou Swift et le serveur DNS.

Valeur	Où la valeur est configurée	Où la valeur est utilisée
Adresses IP virtuelles (VIP)	Groupe StorageGRID > HA	Entrée DNS
Port	StorageGRID > terminal de l'équilibreur de charge	Application client
Certificat SSL	StorageGRID > terminal de l'équilibreur de charge	Application client
Nom du serveur (FQDN)	StorageGRID > terminal de l'équilibreur de charge	• Application client • Entrée DNS
ID de clé d'accès S3 et clé d'accès secrète	StorageGRID > locataire et compartiment	Application client
Nom du compartiment/conteneur	StorageGRID > locataire et compartiment	Application client

Comment obtenir ces valeurs ?

Selon vos besoins, vous pouvez effectuer l'une des opérations suivantes pour obtenir les informations dont vous avez besoin :

- **Utilisez le "Assistant d'installation S3"**. L'assistant d'installation S3 vous aide à configurer rapidement les valeurs requises dans StorageGRID et génère un ou deux fichiers que vous pouvez utiliser pour configurer l'application S3. L'assistant vous guide tout au long des étapes requises et vous aide à vous assurer que vos paramètres sont conformes aux bonnes pratiques de StorageGRID.

  Si vous configurez une application S3, il est recommandé d'utiliser l'assistant d'installation S3, sauf si vous savez que vous disposez d'exigences spéciales, faute de quoi votre implémentation nécessitera une personnalisation importante.

- **Utilisez le "Assistant d'installation FabricPool"**. À l'instar de l'assistant d'installation de S3, l'assistant d'installation de FabricPool vous aide à configurer rapidement les valeurs requises et génère un fichier que vous pouvez utiliser pour configurer un Tier cloud FabricPool dans ONTAP.

  Si vous prévoyez d'utiliser StorageGRID en tant que système de stockage objet pour un niveau cloud FabricPool, il est recommandé d'utiliser l'assistant d'installation FabricPool, sauf si vous disposez d'une configuration spécifique ou si votre implémentation nécessite une personnalisation importante.

- **Configurer les éléments manuellement**. Si vous vous connectez à une application Swift (ou si vous vous connectez à une application S3 et que vous préférez ne pas utiliser l'assistant d'installation S3), vous pouvez obtenir les valeurs requises en effectuant la configuration manuellement. Voici la procédure à suivre :

  a. Configurez le groupe haute disponibilité (HA) que vous souhaitez utiliser pour l'application S3 ou Swift. Voir "Configurez les groupes haute disponibilité".

  b. Créez le terminal d'équilibrage de charge que l'application S3 ou Swift utilisera. Voir "Configurer les

terminaux de l'équilibreur de charge".

c. Créez le compte de locataire que l'application S3 ou Swift utilisera. Voir "Créez un compte de locataire".

d. Pour un locataire S3, connectez-vous au compte du locataire et générez un ID de clé d'accès et une clé d'accès secrète pour chaque utilisateur qui accérera à l'application. Voir "Créez vos propres clés d'accès".

e. Créez un ou plusieurs compartiments S3 ou conteneurs Swift dans le compte de locataire. Pour S3, voir "Créer un compartiment S3". Pour Swift, utilisez le "METTRE la demande de conteneur".

f. Pour ajouter des instructions de placement spécifiques pour les objets appartenant au nouveau locataire ou compartiment/conteneur, créez une règle ILM et activez une nouvelle règle ILM pour utiliser cette règle. Voir "Création d'une règle ILM" et "Création de la règle ILM".

Utilisation de l'assistant d'installation S3

Assistant d'installation S3 : considérations et configuration requise

À l'aide de l'assistant d'installation S3, vous pouvez configurer StorageGRID en tant que système de stockage objet d'une application S3.

Utilisation de l'assistant d'installation S3

L'assistant d'installation S3 vous guide à chaque étape de la configuration d'StorageGRID pour une utilisation avec une application S3. Dans le cadre de l'assistant, vous téléchargez des fichiers que vous pouvez utiliser pour saisir des valeurs dans l'application S3. Utilisez l'assistant pour configurer votre système plus rapidement et pour vous assurer que vos paramètres sont conformes aux meilleures pratiques de StorageGRID.

Si vous disposez de l'autorisation d'accès racine, vous pouvez compléter l'assistant d'installation S3 lorsque vous commencez à utiliser le Gestionnaire de grille StorageGRID, ou vous pouvez accéder à l'assistant et l'exécuter ultérieurement. Selon vos besoins, vous pouvez également configurer une partie ou la totalité des éléments requis manuellement, puis utiliser l'assistant pour assembler les valeurs dont une application S3 a besoin.

Avant d'utiliser l'assistant

Avant d'utiliser l'assistant, vérifiez que vous avez terminé ces conditions préalables.

Obtenir des adresses IP et configurer des interfaces VLAN

Si vous configurez un groupe haute disponibilité, vous savez à quels nœuds l'application S3 se connectera et à quel réseau StorageGRID sera utilisé. Vous savez également quelles valeurs entrer pour le CIDR de sous-réseau, l'adresse IP de la passerelle et les adresses IP virtuelles (VIP).

Si vous prévoyez d'utiliser un réseau local virtuel pour isoler le trafic de l'application S3, vous avez déjà configuré l'interface VLAN. Voir "Configurez les interfaces VLAN".

Configurer la fédération des identités et SSO

Si vous prévoyez d'utiliser la fédération des identités ou l'authentification unique (SSO) pour votre système StorageGRID, vous avez activé ces fonctionnalités. Vous savez également quel groupe fédéré doit disposer d'un accès racine pour le compte locataire utilisé par l'application S3. Voir "Utiliser la fédération des identités" et "Configurer l'authentification unique".

Obtenir et configurer des noms de domaine

Vous savez quel nom de domaine complet (FQDN) utiliser pour StorageGRID. Les entrées de serveur de noms de domaine (DNS) mapperont ce FQDN aux adresses IP virtuelles (VIP) du groupe haute disponibilité que vous créez à l'aide de l'assistant.

Si vous prévoyez d'utiliser des requêtes de type hébergement virtuel S3, vous devriez le faire "Noms de domaine de terminaux S3 configurés". Il est recommandé d'utiliser des demandes de type hébergement virtuel.

Examinez les exigences en matière d'équilibreur de charge et de certificat de sécurité

Si vous envisagez d'utiliser l'équilibreur de charge StorageGRID, vous avez examiné les considérations générales relatives à l'équilibrage de la charge. Vous disposez des certificats que vous allez télécharger ou des valeurs dont vous avez besoin pour générer un certificat.

Si vous prévoyez d'utiliser un noeud final externe (tiers) d'équilibreur de charge, vous disposez du nom de domaine complet (FQDN), du port et du certificat pour cet équilibreur de charge.

Configurez toutes les connexions de fédération de grille

Si vous souhaitez permettre au locataire S3 de cloner les données de compte et de répliquer les objets de compartiment vers une autre grille à l'aide d'une connexion de fédération de grille, vérifiez les points suivants avant de démarrer l'assistant :

- Vous avez "configurez la connexion de fédération de grille - effectué".
- L'état de la connexion est **connecté**.
- Vous disposez de l'autorisation d'accès racine.

Assistant d'installation de S3 et opérations à effectuer

L'assistant d'installation de S3 vous permet de configurer StorageGRID pour une utilisation avec une application S3. L'assistant d'installation fournit les valeurs dont l'application a besoin pour accéder à un compartiment StorageGRID et pour enregistrer des objets.

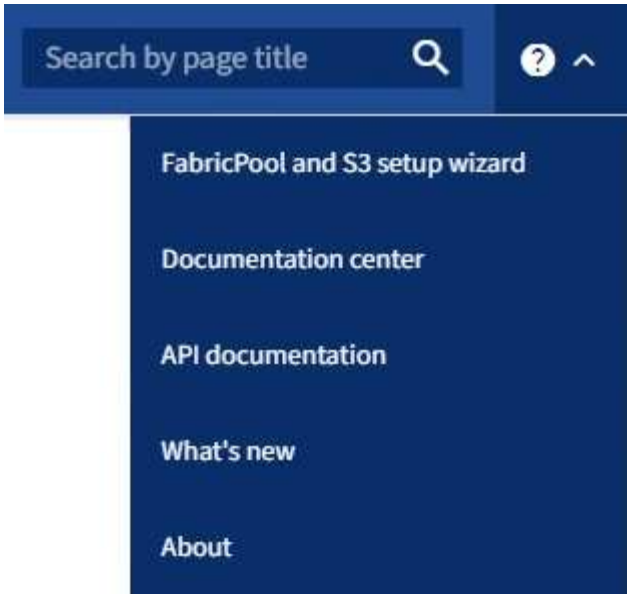
Avant de commencer

- Vous avez le "Autorisation d'accès racine".
- Vous avez passé en revue le "considérations et exigences" pour utiliser l'assistant.

Accéder à l'assistant

Étapes

1. Connectez-vous au Grid Manager à l'aide d'un "navigateur web pris en charge".
2. Si la bannière **FabricPool and S3 setup Wizard** apparaît sur le tableau de bord, sélectionnez le lien dans la bannière. Si la bannière ne s'affiche plus, sélectionnez l'icône d'aide dans la barre d'en-tête du Gestionnaire de grille et sélectionnez **Assistant d'installation FabricPool et S3**.



3. Dans la section application S3 de la page de l'assistant d'installation FabricPool et S3, sélectionnez **configurer maintenant**.

Étape 1 sur 6 : configuration du groupe haute disponibilité

Un groupe haute disponibilité est un ensemble de nœuds qui contiennent chacun le service StorageGRID Load Balancer. Un groupe haute disponibilité peut contenir des nœuds de passerelle, des nœuds d'administration, ou les deux.

Vous pouvez utiliser un groupe haute disponibilité pour maintenir les connexions de données S3 disponibles. En cas de défaillance de l'interface active du groupe haute disponibilité, une interface de sauvegarde peut gérer la charge de travail avec peu d'impact sur les opérations S3.

Pour plus d'informations sur cette tâche, reportez-vous à la section "Gérez les groupes haute disponibilité".

Étapes

1. Si vous prévoyez d'utiliser un équilibreur de charge externe, il n'est pas nécessaire de créer un groupe haute disponibilité. Sélectionnez **Ignorer cette étape** et passez à l' Étape 2 sur 6 : configuration du terminal de l'équilibreur de charge.
2. Pour utiliser l'équilibreur de charge StorageGRID, vous pouvez créer un nouveau groupe haute disponibilité ou utiliser un groupe haute disponibilité existant.

Création du groupe haute disponibilité

a. Pour créer un nouveau groupe HA, sélectionnez **Create HA group**.

b. Pour l'étape **entrer les détails**, remplissez les champs suivants.

Champ	Description
Nom du groupe HAUTE DISPONIBILITÉ	Un nom d'affichage unique pour ce groupe haute disponibilité.
Description (facultatif)	La description de ce groupe HA.

c. Pour l'étape **Ajouter des interfaces**, sélectionnez les interfaces de nœud que vous souhaitez utiliser dans ce groupe haute disponibilité.

Utilisez les en-têtes de colonne pour trier les lignes ou entrez un terme de recherche pour localiser les interfaces plus rapidement.

Vous pouvez sélectionner un ou plusieurs nœuds, mais vous ne pouvez sélectionner qu'une seule interface pour chaque nœud.

d. Pour l'étape **hiérarchiser les interfaces**, déterminez l'interface principale et les interfaces de sauvegarde pour ce groupe haute disponibilité.

Faites glisser des lignes pour modifier les valeurs de la colonne **ordre de priorité**.

La première interface de la liste est l'interface principale. L'interface principale est l'interface active, sauf en cas de défaillance.

Si le groupe haute disponibilité comprend plusieurs interfaces et que l'interface active est défaillante, les adresses IP virtuelles (VIP) sont déplacées vers la première interface de sauvegarde, dans l'ordre de priorité. Si cette interface échoue, les adresses VIP passent à l'interface de sauvegarde suivante, etc. Lorsque les pannes sont résolues, les adresses VIP reviennent à l'interface de priorité la plus élevée disponible.

e. Pour l'étape **entrer les adresses IP**, renseignez les champs suivants.

Champ	Description
Sous-réseau CIDR	Adresse du sous-réseau VIP en notation CIDR &#8212 ; adresse IPv4 suivie d'une barre oblique et de la longueur de sous-réseau (0-32). Aucun bit d'hôte ne doit être défini pour l'adresse réseau. Par exemple : `192.16.0.0/22`.
Adresse IP de la passerelle (facultative)	Si les adresses IP S3 utilisées pour accéder à StorageGRID ne se trouvent pas sur le même sous-réseau que les adresses VIP StorageGRID, entrez l'adresse IP de la passerelle locale VIP StorageGRID. L'adresse IP de la passerelle locale doit se trouver dans le sous-réseau VIP.

Champ	Description
Adresse IP virtuelle	Entrez au moins une et dix adresses VIP pour l'interface active du groupe HA. Toutes les adresses VIP doivent se trouver dans le sous-réseau VIP. Au moins une adresse doit être IPv4. Vous pouvez éventuellement spécifier des adresses IPv4 et IPv6 supplémentaires.

f. Sélectionnez **Create HA group**, puis **Finish** pour revenir à l'assistant d'installation S3.

g. Sélectionnez **Continuer** pour passer à l'étape d'équilibrage de charge.

Utilisez un groupe haute disponibilité existant

a. Pour utiliser un groupe HA existant, sélectionnez le nom du groupe HA dans le **Sélectionner un groupe HA**.

b. Sélectionnez **Continuer** pour passer à l'étape d'équilibrage de charge.

Étape 2 sur 6 : configuration du terminal de l'équilibreur de charge

StorageGRID utilise un équilibreur de charge pour gérer la charge de travail à partir des applications client. L'équilibrage de la charge optimise la vitesse et la capacité de connexion sur plusieurs nœuds de stockage.

Vous pouvez utiliser le service StorageGRID Load Balancer, qui existe sur tous les nœuds de passerelle et d'administration, ou vous pouvez vous connecter à un équilibreur de charge externe (tiers). L'utilisation de l'équilibreur de charge StorageGRID est recommandée.

Pour plus d'informations sur cette tâche, reportez-vous à la section "Considérations relatives à l'équilibrage de charge".

Pour utiliser le service StorageGRID Load Balancer, sélectionnez l'onglet **StorageGRID load balancer**, puis créez ou sélectionnez le noeud final de l'équilibreur de charge que vous souhaitez utiliser. Pour utiliser un équilibreur de charge externe, sélectionnez l'onglet **équilibreur de charge externe** et fournissez des détails sur le système que vous avez déjà configuré.

Créer un point final

Étapes

1. Pour créer un noeud final d'équilibrage de charge, sélectionnez **Créer un noeud final**.
2. Pour l'étape **entrer les détails du noeud final**, renseignez les champs suivants.

Champ	Description
Nom	Nom descriptif du noeud final.
Port	Port StorageGRID que vous souhaitez utiliser pour l'équilibrage de charge. Ce champ est défini par défaut sur 10433 pour le premier noeud final que vous créez, mais vous pouvez entrer n'importe quel port externe inutilisé. Si vous entrez 80 ou 443, le noeud final est configuré uniquement sur les noeuds de passerelle, car ces ports sont réservés sur les noeuds d'administration. **Remarque :** les ports utilisés par d'autres services de grille ne sont pas autorisés. Voir la"Référence du port réseau".
Type de client	Doit être **S3**.
Protocole réseau	Sélectionnez **HTTPS**. **Remarque** : la communication avec StorageGRID sans chiffrement TLS est prise en charge, mais elle n'est pas recommandée.

3. Pour l'étape **Sélectionner le mode de liaison**, spécifiez le mode de liaison. Le mode de liaison contrôle la façon dont le noeud final est accédé—en utilisant une adresse IP ou des adresses IP et des interfaces réseau spécifiques.

Option	Description
Global (par défaut)	Les clients peuvent accéder au point final en utilisant l'adresse IP de n'importe quel nœud de passerelle ou nœud d'administration, l'adresse IP virtuelle (VIP) de n'importe quel groupe haute disponibilité sur n'importe quel réseau, ou un FQDN correspondant. Utilisez le paramètre **Global** (valeur par défaut) sauf si vous devez restreindre l'accessibilité de ce point final.
Adresses IP virtuelles de groupes haute disponibilité	Les clients doivent utiliser une adresse IP virtuelle (ou le nom de domaine complet correspondant) d'un groupe haute disponibilité pour accéder à ce point final. Les terminaux associés à ce mode de liaison peuvent tous utiliser le même numéro de port, tant que les groupes haute disponibilité que vous sélectionnez pour les terminaux ne se chevauchent pas.

Option	Description
Interfaces de nœuds	Les clients doivent utiliser les adresses IP (ou les FQDN correspondants) des interfaces de nœud sélectionnées pour accéder à ce noeud final.
Type de nœud	En fonction du type de nœud que vous sélectionnez, les clients doivent utiliser l'adresse IP (ou le nom de domaine complet correspondant) de tout nœud d'administration ou l'adresse IP (ou le nom de domaine complet correspondant) de tout nœud de passerelle pour accéder à ce point final.

4. Pour l'étape d'accès locataire, sélectionnez l'une des options suivantes :

Champ	Description
Autoriser tous les locataires (par défaut)	Tous les comptes de locataires peuvent utiliser ce terminal pour accéder à leurs compartiments.
Autoriser les locataires sélectionnés	Seuls les comptes de locataire sélectionnés peuvent utiliser ce terminal pour accéder à leurs compartiments.
Bloquez les locataires sélectionnés	Les comptes de locataire sélectionnés ne peuvent pas utiliser ce terminal pour accéder à leurs compartiments. Tous les autres locataires peuvent utiliser ce noeud final.

5. Pour l'étape **joindre un certificat**, sélectionnez l'une des options suivantes :

Champ	Description
Télécharger le certificat (recommandé)	Utilisez cette option pour télécharger un certificat de serveur signé par une autorité de certification, une clé privée de certificat et un ensemble d'autorité de certification facultatif.
Générez un certificat	Utilisez cette option pour générer un certificat auto-signé. Voir "Configurer les terminaux de l'équilibreur de charge" pour plus de détails sur ce que vous devez saisir.
Utilisez les certificats StorageGRID S3 et Swift	Utilisez cette option uniquement si vous avez déjà téléchargé ou généré une version personnalisée du certificat global StorageGRID. Voir "Configurez les certificats API S3 et Swift" pour plus d'informations.

6. Sélectionnez **Terminer** pour revenir à l'assistant d'installation S3.
7. Sélectionnez **Continuer** pour accéder à l'étape tenant et bucket.

Les modifications apportées à un certificat de point final peuvent prendre jusqu'à 15 minutes pour être appliquées à tous les nœuds.

Utilisez le terminal d'équilibrage de charge existant

Étapes

1. Pour utiliser un noeud final existant, sélectionnez son nom dans le **sélectionnez un noeud final d'équilibrage de charge**.
2. Sélectionnez **Continuer** pour accéder à l'étape tenant et bucket.

Utiliser un équilibreur de charge externe

Étapes

1. Pour utiliser un équilibreur de charge externe, renseignez les champs suivants.

Champ	Description
FQDN	Nom de domaine complet (FQDN) de l'équilibreur de charge externe.
Port	Numéro de port que l'application S3 utilisera pour se connecter à l'équilibreur de charge externe.
Certificat	Copiez le certificat du serveur pour l'équilibreur de charge externe et collez-le dans ce champ.

2. Sélectionnez **Continuer** pour accéder à l'étape tenant et bucket.

Étape 3 sur 6 : création d'un locataire et d'un compartiment

Un locataire est une entité qui peut utiliser les applications S3 pour stocker et récupérer des objets dans StorageGRID. Chaque locataire dispose de ses propres utilisateurs, clés d'accès, compartiments, objets et un ensemble spécifique de fonctionnalités. Vous devez créer le tenant avant de pouvoir créer le compartiment que l'application S3 utilisera pour stocker ses objets.

Un compartiment est un conteneur utilisé pour stocker les objets d'un locataire et ses métadonnées d'objet. Même si certains locataires peuvent disposer de plusieurs compartiments, l'assistant vous aide à créer un locataire et un compartiment de la manière la plus rapide et la plus simple. Vous pouvez utiliser le gestionnaire de locataires ultérieurement pour ajouter des compartiments supplémentaires dont vous avez besoin.

Vous pouvez créer un locataire que cette application S3 pourra utiliser. Si vous le souhaitez, vous pouvez également créer un compartiment pour le nouveau locataire. Enfin, vous pouvez autoriser l'assistant à créer les clés d'accès S3 pour l'utilisateur root du locataire.

Pour plus d'informations sur cette tâche, reportez-vous à la section "Créer un compte de locataire" et"Créer un compartiment S3".

Étapes

1. Sélectionnez **Créer locataire**.
2. Pour les étapes entrer les détails, entrez les informations suivantes.

Champ	Description
Nom	Nom du compte de locataire. Les noms de locataires n'ont pas besoin d'être uniques. Lors de la création du compte locataire, il reçoit un ID de compte numérique unique.

Champ	Description
Description (facultatif)	Une description pour aider à identifier le locataire.
Type de client	Type de protocole client utilisé par ce locataire. Pour l'assistant d'installation S3, **S3** est sélectionné et le champ est désactivé.
Quota de stockage (facultatif)	Si vous souhaitez que ce locataire ait un quota de stockage, une valeur numérique pour le quota et les unités.

3. Sélectionnez **Continuer**.
4. Si vous le souhaitez, sélectionnez les autorisations dont ce locataire doit disposer.

> Certaines de ces autorisations ont des exigences supplémentaires. Pour plus de détails, sélectionnez l'icône d'aide pour chaque autorisation.

Autorisations	Si cette option est sélectionnée…
Autoriser les services de plate-forme	Le locataire peut utiliser des services de plateforme S3 tels que CloudMirror. Voir "Gestion des services de plateforme pour les comptes de locataires S3".
Utiliser son propre référentiel d'identité	Le locataire peut configurer et gérer son propre référentiel d'identité pour les groupes et utilisateurs fédérés. Cette option est désactivée si vous l'avez "SSO configuré" De votre système StorageGRID.
Autoriser la sélection S3	Le locataire peut émettre des requêtes d'API S3 SelectObjectContent pour filtrer et récupérer des données d'objet. Voir "Gérez S3 Select pour les comptes de locataires". **Important** : les requêtes SelectObjectContent peuvent réduire les performances de l'équilibreur de charge pour tous les clients S3 et tous les locataires. Activez cette fonctionnalité uniquement lorsque cela est nécessaire et uniquement pour les locataires de confiance.
Utiliser la connexion de fédération de grille	Le locataire peut utiliser une connexion de fédération de grille. Sélection de cette option : • Provoque le clonage de ce locataire et de tous les groupes de locataires et utilisateurs ajoutés au compte à partir de cette grille (la *grille source*) vers l'autre grille de la connexion sélectionnée (la *grille de destination*). • Permet à ce locataire de configurer la réplication entre les compartiments correspondants sur chaque grille. Voir "Gérer les locataires autorisés pour la fédération dans le grid". **Remarque** : vous ne pouvez sélectionner **utiliser la connexion de fédération de grille** que lorsque vous créez un nouveau locataire S3 ; vous ne pouvez pas sélectionner cette autorisation pour un locataire existant.

5. Si vous avez sélectionné **utiliser la connexion de fédération de grille**, sélectionnez l'une des connexions de fédération de grille disponibles.
6. Définissez l'accès racine pour le compte de locataire, selon que votre système StorageGRID utilise ou non "fédération des identités", "Authentification unique (SSO)", ou les deux.

Option	Faites ça
Si la fédération des identités n'est pas activée	Spécifiez le mot de passe à utiliser lors de la connexion au tenant en tant qu'utilisateur root local.
Si la fédération des identités est activée	a. Sélectionnez un groupe fédéré existant pour obtenir l'autorisation d'accès racine pour le tenant. b. Vous pouvez également spécifier le mot de passe à utiliser lors de la connexion au tenant en tant qu'utilisateur root local.
Si la fédération des identités et l'authentification unique (SSO) sont toutes deux activées	Sélectionnez un groupe fédéré existant pour obtenir l'autorisation d'accès racine pour le tenant. Aucun utilisateur local ne peut se connecter.

7. Si vous souhaitez que l'assistant crée l'ID de clé d'accès et la clé d'accès secrète pour l'utilisateur root, sélectionnez **Créer automatiquement la clé d'accès S3 de l'utilisateur root**.

> Sélectionnez cette option si le seul utilisateur du tenant sera l'utilisateur root. Si d'autres utilisateurs utilisent ce locataire, utilisez le Gestionnaire de locataires pour configurer les clés et les autorisations.

8. Sélectionnez **Continuer**.
9. Pour l'étape Créer un compartiment, vous pouvez éventuellement créer un compartiment pour les objets du locataire. Sinon, sélectionnez **Créer un locataire sans compartiment** pour accéder à l' étape de téléchargement des données.

> Si le verrouillage d'objet S3 est activé pour la grille, le verrouillage d'objet S3 n'est pas activé pour le compartiment créé à cette étape. Si vous devez utiliser un compartiment S3 Object Lock pour cette application S3, sélectionnez **Créer un locataire sans compartiment**. Ensuite, utilisez le Gestionnaire de locataires pour "créer le godet" à la place.

a. Entrez le nom du compartiment que l'application S3 utilisera. Par exemple : `S3-bucket`.

> Vous ne pouvez pas modifier le nom du compartiment après la création du compartiment.

b. Sélectionnez la **région** pour ce compartiment.

Utilisez la région par défaut (US-East-1), sauf si vous prévoyez d'utiliser ILM pour filtrer des objets en fonction de la région du compartiment.

c. Sélectionnez **Activer la gestion des versions d'objet** si vous souhaitez stocker chaque version de chaque objet dans ce compartiment.

d. Sélectionnez **Créer un locataire et un compartiment** et passez à l'étape de téléchargement des données.

étape 4 sur 6 : télécharger les données

Dans l'étape de téléchargement des données, vous pouvez télécharger un ou deux fichiers pour enregistrer les détails de ce que vous venez de configurer.

Étapes

1. Si vous avez sélectionné **Créer la clé d'accès S3 de l'utilisateur root automatiquement**, effectuez l'une des opérations suivantes ou les deux :
   - Sélectionnez **Télécharger les clés d'accès** pour télécharger un `.csv` Fichier contenant le nom du compte du locataire, l'ID de la clé d'accès et la clé d'accès secrète.
   - Sélectionnez l'icône de copie ( ) Pour copier l'ID de la clé d'accès et la clé d'accès secrète dans le presse-papiers.
2. Sélectionnez **Télécharger les valeurs de configuration** pour télécharger un `.txt` fichier contenant les paramètres du terminal de l'équilibreur de charge, le locataire, le compartiment et l'utilisateur root.
3. Enregistrez ces informations dans un emplacement sécurisé.

> Ne fermez pas cette page tant que vous n'avez pas copié les deux clés d'accès. Les touches ne seront pas disponibles après la fermeture de cette page. Veillez à enregistrer ces informations dans un emplacement sécurisé car elles peuvent être utilisées pour obtenir des données de votre système StorageGRID.

4. Si vous y êtes invité, cochez la case pour confirmer que vous avez téléchargé ou copié les clés.
5. Sélectionnez **Continuer** pour accéder à la règle ILM et à l'étape de stratégie.

Étape 5 sur 6 : examen de la règle ILM et de la règle ILM pour S3

Les règles de gestion du cycle de vie des informations (ILM) contrôlent le placement, la durée et le comportement d'ingestion de tous les objets de votre système StorageGRID. La règle ILM incluse à StorageGRID effectue deux copies répliquées de tous les objets. Cette stratégie est en vigueur jusqu'à ce que vous créiez une nouvelle stratégie proposée et l'activiez.

Étapes

1. Passez en revue les informations fournies sur la page.
2. Si vous souhaitez ajouter des instructions spécifiques pour les objets appartenant au nouveau locataire ou compartiment, créez une règle et une nouvelle règle. Voir "Création d'une règle ILM" et "Création de la règle ILM : présentation".
3. Sélectionnez **J'ai passé en revue ces étapes et je comprends ce que je dois faire**.
4. Cochez la case pour indiquer que vous comprenez ce qu'il faut faire ensuite.
5. Sélectionnez **Continuer** pour accéder à **Résumé**.

Étape 6 sur 6 : passez en revue le résumé

Étapes

1. Passez en revue le résumé.
2. Notez les détails des étapes suivantes, qui décrivent la configuration supplémentaire qui peut être

nécessaire avant de vous connecter au client S3. Par exemple, la sélection de **se connecter en tant que root** vous amène au gestionnaire de locataires, où vous pouvez ajouter des utilisateurs de tenant, créer des compartiments supplémentaires et mettre à jour les paramètres de compartiment.

3. Sélectionnez **Terminer**.
4. Configurez l'application à l'aide du fichier téléchargé à partir de StorageGRID ou des valeurs obtenues manuellement.

Gérer les groupes de haute disponibilité

Gestion des groupes haute disponibilité (HA) : présentation

Vous pouvez regrouper les interfaces réseau de plusieurs nœuds d'administration et de passerelle dans un groupe haute disponibilité. En cas de défaillance de l'interface active dans le groupe haute disponibilité, une interface de sauvegarde peut gérer la charge de travail.

Qu'est-ce qu'un groupe haute disponibilité ?

Vous pouvez utiliser des groupes HA (haute disponibilité) pour assurer des connexions de données hautement disponibles pour les clients S3 et Swift, ou fournir des connexions extrêmement disponibles à Grid Manager et au tenant Manager.

Chaque groupe HA permet d'accéder aux services partagés sur les nœuds sélectionnés.

- Les groupes HAUTE DISPONIBILITÉ, incluant les nœuds de passerelle et les nœuds d'administration, ou les deux, fournissent des connexions de données hautement disponibles pour les clients S3 et Swift.
- Les groupes HAUTE DISPONIBILITÉ comprenant uniquement des nœuds d'administration fournissent des connexions hautement disponibles au Grid Manager et au tenant Manager.
- Un groupe haute disponibilité comprenant uniquement des appliances SG100 ou SG1000 et des nœuds logiciels VMware peut offrir des connexions hautement disponibles pour "Locataires S3 avec S3 Select". Les groupes HAUTE DISPONIBILITÉ sont recommandés lors de l'utilisation de S3 Select, mais pas requis.

Comment créer un groupe haute disponibilité ?

1. Vous sélectionnez une interface réseau pour un ou plusieurs nœuds d'administration ou de passerelle. Vous pouvez utiliser une interface Grid Network (eth0), une interface réseau client (eth2), une interface VLAN ou une interface d'accès que vous avez ajoutée au nœud.

   > Vous ne pouvez pas ajouter d'interface à un groupe haute disponibilité si son adresse IP est attribuée par DHCP.

2. Vous spécifiez une interface à utiliser comme interface principale. L'interface principale est l'interface active, sauf en cas de défaillance.
3. Vous déterminez l'ordre de priorité des interfaces de sauvegarde.
4. Vous affectez une à 10 adresses IP virtuelles (VIP) au groupe. Les applications clients peuvent utiliser l'une de ces adresses VIP pour se connecter à StorageGRID.

Pour obtenir des instructions, reportez-vous à la section "Configurez les groupes haute disponibilité".

Qu’est-ce que l’interface active ?

En fonctionnement normal, toutes les adresses VIP du groupe haute disponibilité sont ajoutées à l’interface principale, qui est la première interface dans l’ordre prioritaire. Tant que l’interface principale reste disponible, elle est utilisée lorsque les clients se connectent à n’importe quelle adresse VIP pour le groupe. C’est-à-dire, en fonctionnement normal, l’interface principale est l’interface « active » du groupe.

De même, en fonctionnement normal, toute interface de priorité inférieure du groupe HA agit comme des interfaces de « sauvegarde ». Ces interfaces de sauvegarde ne sont utilisées que si l’interface principale (actuellement active) est indisponible.

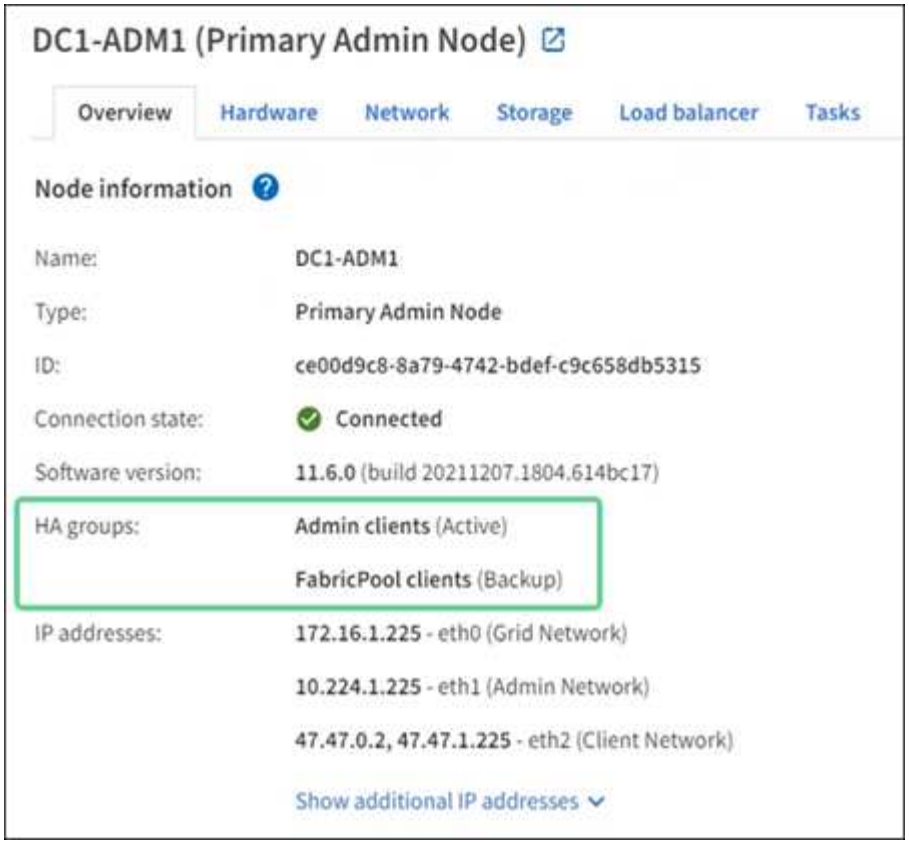
Afficher l’état actuel du groupe haute disponibilité d’un nœud

Pour vérifier si un nœud est affecté à un groupe HA et déterminer son état actuel, sélectionnez **NOEUDS** > ***node***.

Si l’onglet **Présentation** inclut une entrée pour **groupes HA**, le nœud est affecté aux groupes HA répertoriés. La valeur après le nom du groupe est l’état actuel du nœud du groupe HA :

- **Actif** : le groupe HA est actuellement hébergé sur ce nœud.
- **Backup** : le groupe HA n’utilise pas ce noeud, c’est une interface de sauvegarde.
- **Arrêté** : le groupe HA ne peut pas être hébergé sur ce nœud car le service haute disponibilité (keepalived) a été arrêté manuellement.
- **Fault** : le groupe HA ne peut pas être hébergé sur ce nœud en raison d’un ou plusieurs des éléments suivants :
  - Le service Load Balancer (ninx-gw) n’est pas exécuté sur le nœud.
  - L’interface eth0 ou VIP du nœud est en panne.
  - Le nœud ne fonctionne pas.

Dans cet exemple, le nœud d’administration principal a été ajouté à deux groupes HA. Ce nœud est actuellement l’interface active du groupe clients Admin et une interface de sauvegarde pour le groupe clients FabricPool.



Que se passe-t-il lorsque l'interface active tombe en panne ?

L'interface qui héberge actuellement les adresses VIP est l'interface active. Si le groupe haute disponibilité inclut plusieurs interfaces et que l'interface active tombe en panne, les adresses VIP sont transférées vers la première interface de sauvegarde disponible dans l'ordre de priorité. Si cette interface échoue, les adresses VIP passent à la prochaine interface de sauvegarde disponible, etc.

Le basculement peut être déclenché pour l'une des raisons suivantes :

- Le nœud sur lequel l'interface est configurée s'éteint.
- Le nœud sur lequel l'interface est configurée perd la connectivité sur tous les autres nœuds pendant au moins 2 minutes.
- L'interface active tombe en panne.
- Le service Load Balancer s'arrête.
- Le service haute disponibilité s'arrête.

> Le basculement peut ne pas être déclenché par des pannes réseau externes au nœud qui héberge l'interface active. De même, le basculement n'est pas déclenché par les services pour le Grid Manager ou le tenant Manager.

Le processus de basculement ne prend généralement que quelques secondes et est suffisamment rapide pour que les applications clientes aient peu d'impact et peuvent compter sur des comportements de tentatives normales pour poursuivre le fonctionnement.

Lorsqu'une panne est résolue et qu'une interface de priorité supérieure est à nouveau disponible, les adresses VIP sont automatiquement transférées vers l'interface de priorité la plus élevée disponible.

Comment sont utilisés les groupes haute disponibilité ?

Vous pouvez utiliser des groupes haute disponibilité pour fournir des connexions extrêmement disponibles à StorageGRID pour les données d'objet et pour les tâches d'administration.

- Un groupe haute disponibilité peut fournir des connexions administratives hautement disponibles vers le Grid Manager ou le tenant Manager.
- Un groupe haute disponibilité peut fournir des connexions de données extrêmement disponibles pour les clients S3 et Swift.
- Un groupe haute disponibilité ne contenant qu'une interface vous permet de fournir de nombreuses adresses VIP et de définir explicitement des adresses IPv6.

Un groupe haute disponibilité peut assurer la haute disponibilité uniquement si tous les nœuds du groupe fournissent les mêmes services. Lorsque vous créez un groupe haute disponibilité, ajoutez des interfaces à partir des types de nœuds qui fournissent les services requis.

- **Nœuds d'administration** : incluez le service Load Balancer et activez l'accès au Grid Manager ou au Gestionnaire de locataires.
- **Nœuds de passerelle** : inclure le service Load Balancer.

Objectif du groupe haute disponibilité	Ajout de nœuds de ce type au groupe haute disponibilité
Accès à Grid Manager	• Nœud d'administration principal (**primaire**) • Nœuds d'administration non primaires **Remarque :** le noeud d'administration principal doit être l'interface principale. Certaines procédures de maintenance peuvent uniquement être effectuées depuis le nœud d'administration principal.
Accès au Gestionnaire de locataires uniquement	• Nœuds d'administration primaires ou non primaires
Accès client S3 ou Swift — Service Load Balancer	• Nœuds d'administration • Nœuds de passerelle
Accès client S3 pour "S3 Select"	• Appareils SG100 ou SG1000 • Nœuds logiciels VMware **Remarque** : les groupes HA sont recommandés lors de l'utilisation de S3 Select, mais pas requis.

Restrictions liées à l'utilisation de groupes haute disponibilité avec Grid Manager ou tenant Manager

En cas de défaillance d'un service Grid Manager ou tenant Manager, le basculement du groupe haute disponibilité n'est pas déclenché.

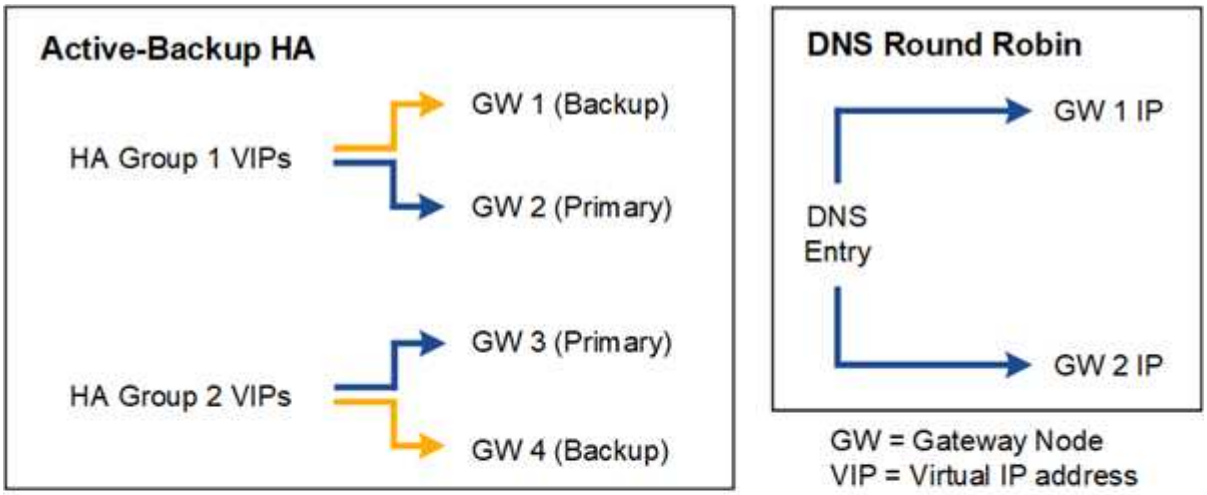
Si vous êtes connecté au Grid Manager ou au tenant Manager lors du basculement, vous êtes déconnecté et vous devez vous reconnecter pour reprendre votre tâche.

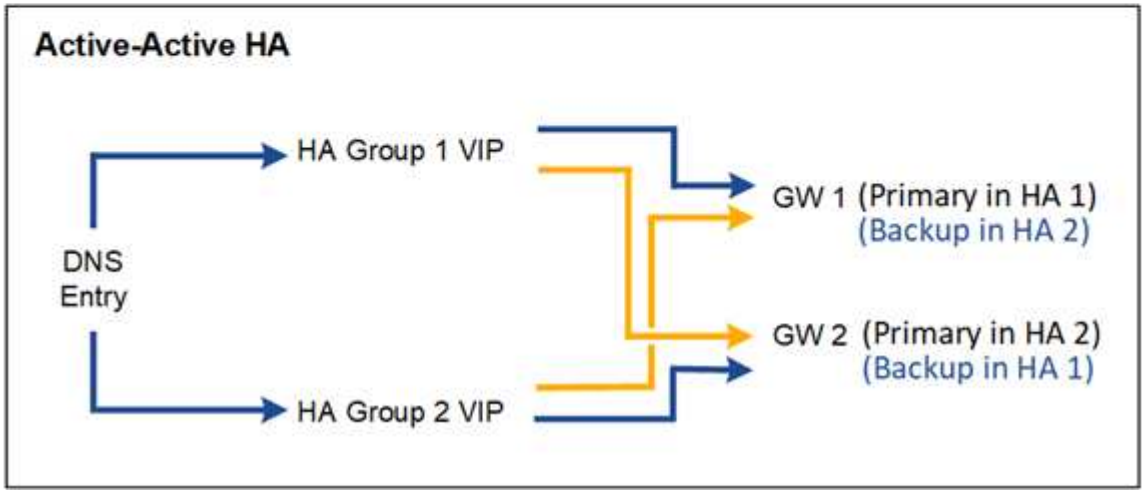
Certaines procédures de maintenance ne peuvent pas être effectuées lorsque le nœud d'administration principal n'est pas disponible. Pendant le basculement, vous pouvez utiliser le Gestionnaire de grille pour surveiller votre système StorageGRID.

Options de configuration pour les groupes haute disponibilité

Les schémas ci-dessous fournissent des exemples de différentes façons de configurer les groupes haute disponibilité. Chaque option présente des avantages et des inconvénients.

Dans les schémas, le bleu indique l'interface principale du groupe haute disponibilité et la jaune indique l'interface de sauvegarde du groupe haute disponibilité.





Le tableau récapitule les avantages de chaque configuration de haute disponibilité illustrée sur le schéma.

Configuration	Avantages	Inconvénients
Active-Backup HA	• Gérées par StorageGRID sans dépendances externes • Basculement rapide	• Un seul nœud d'un groupe haute disponibilité est actif. Au moins un nœud par groupe haute disponibilité sera inactif.

Configuration	Avantages	Inconvénients
DNS Round Robin	• Un débit global supérieur. • Aucun hôte inactif.	• Basculement lent, qui peut dépendre du comportement des clients. • Nécessite une configuration matérielle en dehors du StorageGRID. • Nécessite une vérification de l'état implémentée par le client.
Haute disponibilité actif-actif	• Le trafic est réparti entre plusieurs groupes haute disponibilité. • Débit global élevé qui évolue en même temps que le nombre de groupes HA. • Basculement rapide	• Configuration plus complexe. • Nécessite une configuration matérielle en dehors du StorageGRID. • Nécessite une vérification de l'état implémentée par le client.

Configurez les groupes haute disponibilité

Vous pouvez configurer des groupes haute disponibilité pour fournir un accès haute disponibilité aux services sur des nœuds d'administration ou de passerelle.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous disposez de l'autorisation d'accès racine.
- Si vous prévoyez d'utiliser une interface VLAN dans un groupe haute disponibilité, vous avez créé cette interface. Voir "Configurez les interfaces VLAN".
- Si vous prévoyez d'utiliser une interface d'accès pour un nœud d'un groupe haute disponibilité, vous avez créé l'interface :
  - **Red Hat Enterprise Linux ou CentOS (avant d'installer le nœud)** : "Créez des fichiers de configuration de nœud"
  - **Ubuntu ou Debian (avant d'installer le nœud)** : "Créez des fichiers de configuration de nœud"
  - **Linux (après l'installation du nœud)** : "Linux : ajoutez une jonction ou des interfaces d'accès à un nœud"
  - **VMware (après l'installation du noeud)** : "VMware : ajoutez du jonction ou des interfaces d'accès à un nœud"

Créez un groupe haute disponibilité

Lorsque vous créez un groupe haute disponibilité, vous sélectionnez une ou plusieurs interfaces et organisez-les par ordre de priorité. Vous affectez ensuite une ou plusieurs adresses VIP au groupe.

Pour qu'un nœud de passerelle ou un nœud d'administration soit inclus dans un groupe haute disponibilité, une interface doit être configurée pour inclure un nœud de passerelle. Un groupe haute disponibilité ne peut utiliser qu'une interface pour un nœud donné. Toutefois, les autres interfaces du même nœud peuvent être utilisées dans d'autres groupes haute disponibilité.

Accéder à l'assistant

Étapes

1. Sélectionnez **CONFIGURATION** > **réseau** > **groupes haute disponibilité**.
2. Sélectionnez **Créer**.

Entrez les détails du groupe haute disponibilité

Étapes

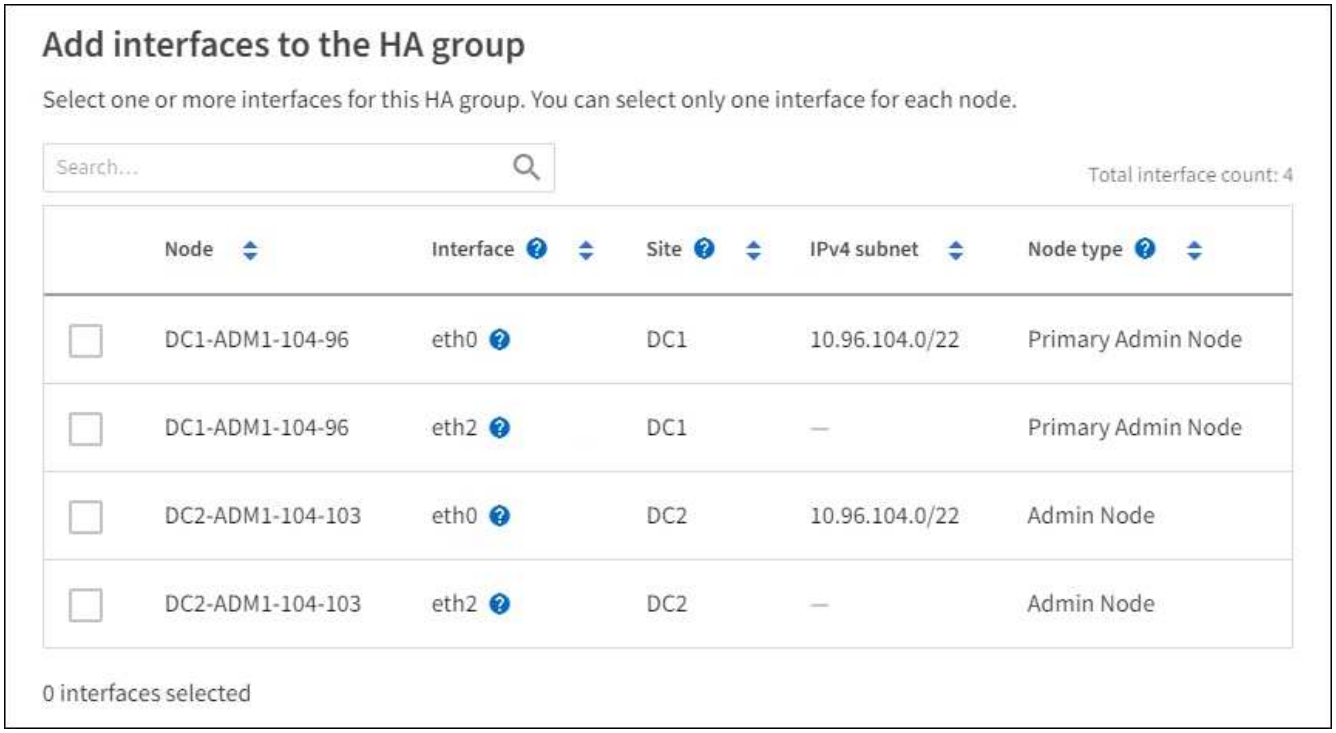
1. Indiquez un nom unique pour le groupe HA.
2. Si vous le souhaitez, entrez une description pour le groupe HA.
3. Sélectionnez **Continuer**.

Ajouter des interfaces au groupe haute disponibilité

Étapes

1. Sélectionnez une ou plusieurs interfaces à ajouter à ce groupe haute disponibilité.

   Utilisez les en-têtes de colonne pour trier les lignes ou entrez un terme de recherche pour localiser les interfaces plus rapidement.



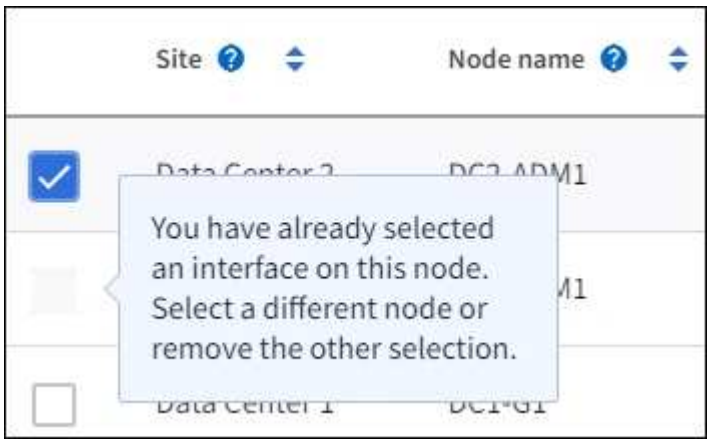
> Après avoir créé une interface VLAN, attendez jusqu'à 5 minutes que la nouvelle interface apparaisse dans le tableau.

Consignes de sélection des interfaces

- Vous devez sélectionner au moins une interface.
- Vous ne pouvez sélectionner qu'une interface pour un nœud.
- Si le groupe HA est destiné à la protection haute disponibilité des services des nœuds d'administration, qui incluent le Grid Manager et le tenant Manager, sélectionnez les interfaces sur les nœuds

d’administration uniquement.

- Si le groupe HA est destiné à la protection HA du trafic client S3 ou Swift, sélectionnez les interfaces dans les nœuds d’administration, les nœuds de passerelle ou les deux.
- Si vous sélectionnez des interfaces sur différents types de nœuds, une note d’information s’affiche. Il est rappelé que en cas de basculement, les services fournis par le nœud actif précédemment risquent de ne pas être disponibles sur le nouveau nœud actif. Par exemple, un nœud de passerelle de sauvegarde ne peut pas assurer la protection haute disponibilité des services du nœud d’administration. De même, un nœud d’administration des sauvegardes ne peut pas effectuer toutes les procédures de maintenance que le nœud d’administration principal peut fournir.
- Si vous ne pouvez pas sélectionner une interface, sa case à cocher est désactivée. L’info-bulle fournit plus d’informations.



- Vous ne pouvez pas sélectionner d’interface si sa valeur de sous-réseau ou sa passerelle entre en conflit avec une autre interface sélectionnée.
- Vous ne pouvez pas sélectionner une interface configurée si elle ne possède pas d’adresse IP statique.

2. Sélectionnez **Continuer**.

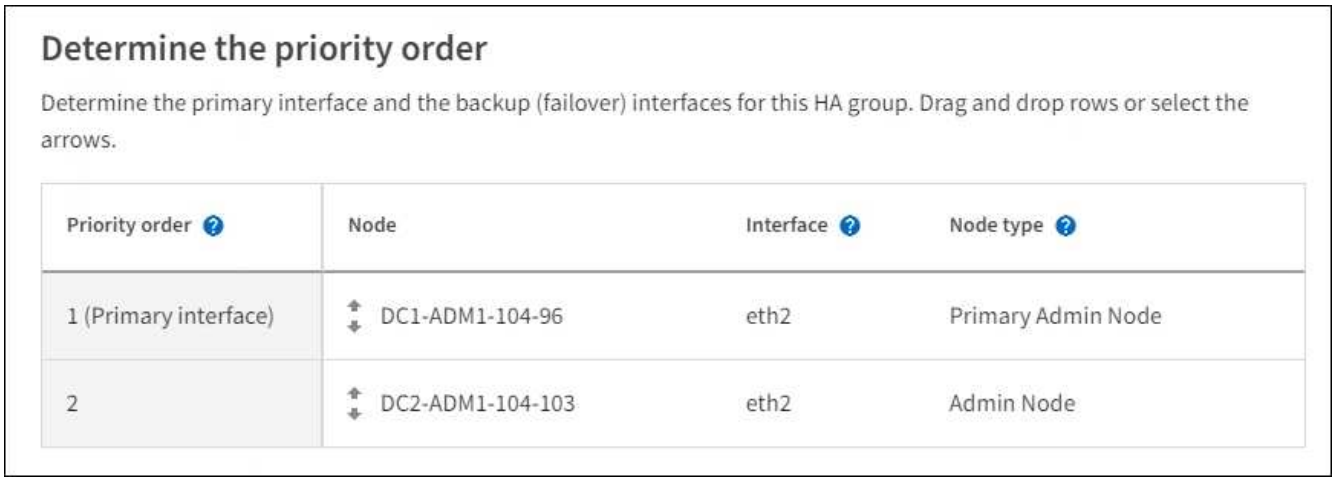
Déterminez l’ordre de priorité

Si le groupe haute disponibilité comprend plusieurs interfaces, vous pouvez déterminer qui est l’interface principale et quelles sont les interfaces de sauvegarde (basculement). Si l’interface principale échoue, les adresses VIP passent à l’interface de priorité la plus élevée disponible. En cas d’échec de cette interface, les adresses VIP passent à l’interface de priorité supérieure suivante disponible, etc.

Étapes

1. Faites glisser des lignes dans la colonne **ordre de priorité** pour déterminer l’interface principale et les interfaces de sauvegarde.

   La première interface de la liste est l’interface principale. L’interface principale est l’interface active, sauf en cas de défaillance.



Si le groupe HA donne accès à Grid Manager, vous devez sélectionner une interface sur le nœud d'administration principal pour qu'il soit l'interface principale. Certaines procédures de maintenance peuvent uniquement être effectuées depuis le nœud d'administration principal.

2. Sélectionnez **Continuer**.

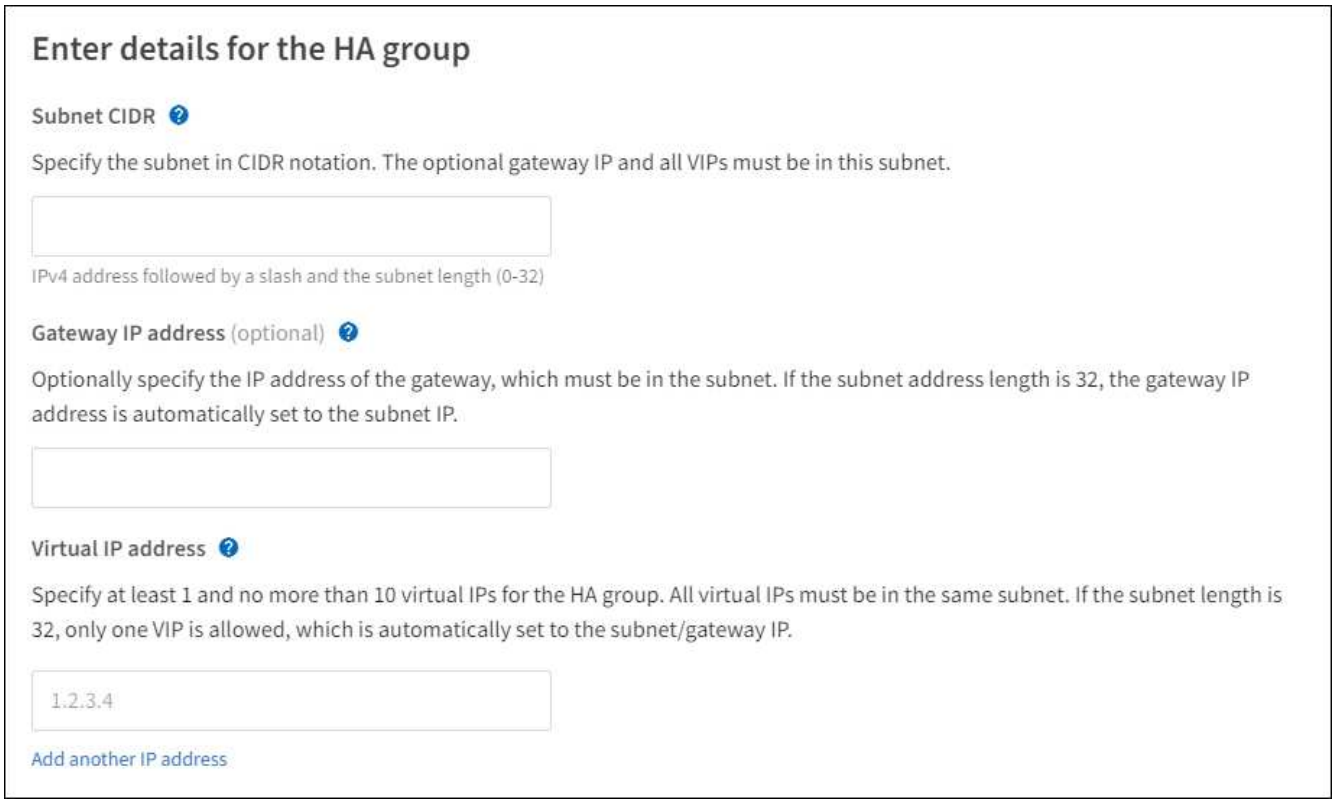
Saisissez les adresses IP

Étapes

1. Dans le champ **Subnet CIDR**, spécifiez le sous-réseau VIP en notation CIDR—une adresse IPv4 suivie d'une barre oblique et de la longueur du sous-réseau (0-32).

   Aucun bit d'hôte ne doit être défini pour l'adresse réseau. Par exemple : `192.16.0.0/22`.

   Si vous utilisez un préfixe 32 bits, l'adresse réseau VIP sert également d'adresse de passerelle et d'adresse VIP.



2. Si des clients S3, Swift, d'administration ou de locataires accèdent à ces adresses VIP à partir d'un sous-réseau différent, saisissez l'adresse IP **Gateway**. L'adresse de la passerelle doit se trouver dans le sous-réseau VIP.

   Les utilisateurs client et admin utiliseront cette passerelle pour accéder aux adresses IP virtuelles.

3. Entrez au moins une et dix adresses VIP pour l'interface active du groupe HA. Toutes les adresses VIP doivent se trouver dans le sous-réseau VIP et toutes seront actives en même temps sur l'interface active.

   Vous devez fournir au moins une adresse IPv4. Vous pouvez éventuellement spécifier des adresses IPv4 et IPv6 supplémentaires.

4. Sélectionnez **Créer groupe HA** et **Terminer**.

   Le groupe haute disponibilité est créé et vous pouvez maintenant utiliser les adresses IP virtuelles configurées.

> Attendez 15 minutes que les modifications d'un groupe haute disponibilité soient appliquées à tous les nœuds.

Étapes suivantes

Si vous utilisez ce groupe haute disponibilité pour équilibrer la charge, créez un terminal d'équilibreur de charge afin de déterminer le port et le protocole réseau, et de connecter tous les certificats requis. Voir "Configurer les terminaux de l'équilibreur de charge".

Modifiez un groupe haute disponibilité

Vous pouvez modifier un groupe haute disponibilité (HA) pour modifier son nom et sa description, ajouter ou supprimer des interfaces, modifier l'ordre de priorité ou ajouter ou mettre à jour des adresses IP virtuelles.

Par exemple, vous devrez peut-être modifier un groupe haute disponibilité si vous souhaitez supprimer le nœud associé à une interface sélectionnée dans la procédure de mise hors service d'un site ou d'un nœud.

Étapes

1. Sélectionnez **CONFIGURATION** > **réseau** > **groupes haute disponibilité**.

   La page groupes haute disponibilité affiche tous les groupes haute disponibilité existants.

2. Cochez la case du groupe haute disponibilité à modifier.
3. Effectuez l'une des opérations suivantes, en fonction de ce que vous souhaitez mettre à jour :
   - Sélectionnez **actions** > **Modifier l'adresse IP virtuelle** pour ajouter ou supprimer des adresses VIP.
   - Sélectionnez **actions** > **Modifier le groupe HA** pour mettre à jour le nom ou la description du groupe, ajouter ou supprimer des interfaces, modifier l'ordre de priorité ou ajouter ou supprimer des adresses VIP.
4. Si vous avez sélectionné **Modifier l'adresse IP virtuelle** :
   a. Mettre à jour les adresses IP virtuelles du groupe haute disponibilité.
   b. Sélectionnez **Enregistrer**.
   c. Sélectionnez **Terminer**.
5. Si vous avez sélectionné **Modifier le groupe HA** :
   a. Vous pouvez également mettre à jour le nom ou la description du groupe.
   b. Vous pouvez également cocher ou décocher les cases pour ajouter ou supprimer des interfaces.

      Si le groupe HA donne accès à Grid Manager, vous devez sélectionner une interface sur le nœud d'administration principal pour qu'il soit l'interface principale. Certaines procédures de maintenance peuvent uniquement être effectuées depuis le nœud d'administration principal

   c. Vous pouvez également faire glisser des lignes pour modifier l'ordre de priorité de l'interface principale et des interfaces de sauvegarde de ce groupe haute disponibilité.
   d. Si vous le souhaitez, mettez à jour les adresses IP virtuelles.
   e. Sélectionnez **Enregistrer**, puis **Terminer**.

Attendez 15 minutes que les modifications d'un groupe haute disponibilité soient appliquées à tous les nœuds.

Supprimer un groupe haute disponibilité

Vous pouvez supprimer un ou plusieurs groupes haute disponibilité (HA) à la fois.

Vous ne pouvez pas supprimer un groupe haute disponibilité s'il est lié à un terminal d'équilibrage de charge. Pour supprimer un groupe haute disponibilité, vous devez le supprimer de tous les terminaux d'équilibrage de charge qui l'utilisent.

Pour éviter les interruptions de vos clients, mettez à jour les applications clients S3 ou Swift affectées avant de supprimer un groupe haute disponibilité. Mettre à jour chaque client pour se connecter à l'aide d'une autre adresse IP, par exemple l'adresse IP virtuelle d'un autre groupe haute disponibilité ou l'adresse IP configurée pour une interface lors de l'installation.

Étapes

1. Sélectionnez **CONFIGURATION** > **réseau** > **groupes haute disponibilité**.
2. Consultez la colonne **Load Balancer Endpoints** pour chaque groupe HA que vous souhaitez supprimer. Si des terminaux d'équilibrage de charge sont répertoriés :
   a. Accédez à **CONFIGURATION** > **réseau** > **noeuds finaux de l'équilibreur de charge**.
   b. Cochez la case du point final.
   c. Sélectionnez **actions** > **Modifier le mode de liaison du point final**.
   d. Mettez à jour le mode de liaison pour supprimer le groupe HA.
   e. Sélectionnez **Enregistrer les modifications**.
3. Si aucun point final de l'équilibreur de charge n'est répertorié, cochez la case de chaque groupe haute disponibilité à supprimer.
4. Sélectionnez **actions** > **Supprimer groupe HA**.
5. Vérifiez le message et sélectionnez **Supprimer le groupe HA** pour confirmer votre sélection.

   Tous les groupes HA sélectionnés sont supprimés. Une bannière de réussite verte apparaît sur la page groupes de haute disponibilité.

Gérer l'équilibrage des charges

Considérations relatives à l'équilibrage de charge

Vous pouvez utiliser l'équilibrage des charges pour gérer les workloads d'ingestion et de récupération des clients S3 et Swift.

Qu'est-ce que l'équilibrage de la charge ?

Lorsqu'une application client enregistre ou récupère les données d'un système StorageGRID, StorageGRID utilise un équilibreur de charge pour gérer la charge de travail d'ingestion et de récupération. L'équilibrage de la charge optimise la vitesse et la capacité de connexion en répartissant la charge de travail sur plusieurs nœuds de stockage.

Le service StorageGRID Load Balancer est installé sur tous les nœuds d'administration et sur tous les nœuds de passerelle. Il assure l'équilibrage de la charge de couche 7. Il effectue la résiliation du protocole TLS (transport Layer Security) des requêtes du client, inspecte les requêtes et établit de nouvelles connexions sécurisées vers les nœuds de stockage.

Le service Load Balancer de chaque nœud fonctionne indépendamment lors du transfert du trafic client vers les nœuds de stockage. Par le biais d'un processus de pondération, le service Load Balancer achemine davantage de requêtes vers des nœuds de stockage avec une disponibilité de processeur supérieure.

> Bien que le service StorageGRID Load Balancer soit le mécanisme d'équilibrage de la charge recommandé, vous pouvez à la place intégrer un équilibreur de charge tiers. Pour plus d'informations, contactez votre ingénieur commercial NetApp ou consultez "Tr-4626 : équilibreurs de charge mondiaux et tiers StorageGRID".

De combien de nœuds d'équilibrage de charge ai-je besoin ?

Dans le cadre des meilleures pratiques générales, chaque site de votre système StorageGRID doit inclure au moins deux nœuds avec le service Load Balancer. Par exemple, un site peut inclure deux nœuds de

passerelle ou un nœud d'administration et un nœud de passerelle. S'assurer que l'infrastructure de mise en réseau, matérielle ou de virtualisation est adéquate pour chaque nœud d'équilibrage de charge, que vous utilisiez des appliances de services SG100 ou SG1000, des nœuds bare Metal ou des nœuds basés sur des machines virtuelles.

Qu'est-ce qu'un terminal d'équilibrage de charge ?

Un noeud final d'équilibrage de charge définit le port et le protocole réseau (HTTPS ou HTTP) utilisés par les demandes d'applications clientes entrantes et sortantes pour accéder aux noeuds qui contiennent le service d'équilibrage de charge. Le terminal définit également le type de client (S3 ou Swift), le mode de liaison et, éventuellement, la liste des locataires autorisés ou bloqués.

Pour créer un noeud final d'équilibrage de charge, sélectionnez **CONFIGURATION** > **réseau** > **noeuds finaux d'équilibrage de charge** ou exécutez l'assistant d'installation FabricPool et S3. Pour obtenir des instructions :

- "Configurer les terminaux de l'équilibreur de charge"
- "Utilisez l'assistant d'installation S3"
- "Utilisez l'assistant de configuration FabricPool"

Considérations relatives au port

Par défaut, le port d'un noeud final d'équilibrage de charge est 10433 pour le premier noeud final que vous créez, mais vous pouvez spécifier tout port externe inutilisé compris entre 1 et 65535. Si vous utilisez le port 80 ou 443, le noeud final utilisera le service Load Balancer sur les noeuds passerelle uniquement. Ces ports sont réservés sur des nœuds d'administration. Si vous utilisez le même port pour plusieurs noeuds finaux, vous devez spécifier un mode de liaison différent pour chaque noeud final.

Les ports utilisés par d'autres services de grille ne sont pas autorisés. Voir la "Référence du port réseau".

Considérations relatives au protocole réseau

Dans la plupart des cas, les connexions entre les applications clientes et StorageGRID doivent utiliser le chiffrement TLS (transport Layer Security). La connexion à StorageGRID sans chiffrement TLS est prise en charge, mais elle n'est pas recommandée, en particulier dans les environnements de production. Lorsque vous sélectionnez le protocole réseau pour le noeud final de l'équilibreur de charge StorageGRID, vous devez sélectionner **HTTPS**.

Considérations relatives aux certificats de terminaux d'équilibrage de charge

Si vous sélectionnez **HTTPS** comme protocole réseau pour le noeud final de l'équilibreur de charge, vous devez fournir un certificat de sécurité. Lorsque vous créez le terminal de l'équilibreur de charge, vous pouvez utiliser l'une de ces trois options :

- **Télécharger un certificat signé (recommandé)**. Ce certificat peut être signé par une autorité de certification publique ou privée. Il est recommandé d'utiliser un certificat de serveur d'autorité de certification de confiance publique pour sécuriser la connexion. Contrairement aux certificats générés, les certificats signés par une autorité de certification peuvent être permutés sans interruption, ce qui permet d'éviter les problèmes d'expiration.

  Vous devez obtenir les fichiers suivants avant de créer le noeud final de l'équilibreur de charge :

  - Le fichier de certificat de serveur personnalisé.
  - Le fichier de clé privée du certificat de serveur personnalisé.

    - Éventuellement, un paquet CA des certificats de chaque autorité de certification intermédiaire émettrice.
- **Générer un certificat auto-signé**.
- **Utilisez le certificat global StorageGRID S3 et Swift**. Vous devez télécharger ou générer une version personnalisée de ce certificat avant de pouvoir le sélectionner pour le noeud final de l'équilibreur de charge. Voir "Configurez les certificats API S3 et Swift".

Quelles valeurs ai-je besoin ?

Pour créer le certificat, vous devez connaître tous les noms de domaine et adresses IP que les applications client S3 ou Swift utiliseront pour accéder au terminal.

L'entrée **Subject DN** (Distinguished Name) du certificat doit inclure le nom de domaine complet que l'application client utilisera pour StorageGRID. Par exemple :

```
Subject DN:
/C=Country/ST=State/O=Company,Inc./CN=s3.storagegrid.example.com
```

Si nécessaire, le certificat peut utiliser des caractères génériques pour représenter les noms de domaine complets de tous les nœuds d'administration et nœuds de passerelle exécutant le service Load Balancer. Par exemple : `*.storagegrid.example.com` utilise le caractère générique * pour représenter `adm1.storagegrid.example.com` et `gn1.storagegrid.example.com`.

Si vous prévoyez d'utiliser des demandes de type hébergement virtuel S3, le certificat doit également inclure une entrée **alternative Name** pour chacune d'entre elles "Nom du domaine du terminal S3" vous avez configuré, y compris les noms génériques. Par exemple :

```
Alternative Name: DNS:*.s3.storagegrid.example.com
```

> Si vous utilisez des caractères génériques pour les noms de domaine, consultez le "Consignes de renforcement des certificats de serveur".

Vous devez également définir une entrée DNS pour chaque nom du certificat de sécurité.

Comment gérer les certificats arrivant à expiration ?

> Si le certificat utilisé pour sécuriser la connexion entre l'application S3 et StorageGRID expire, l'application risque de perdre temporairement l'accès à StorageGRID.

Pour éviter les problèmes d'expiration des certificats, suivez les bonnes pratiques suivantes :

- Surveillez attentivement toutes les alertes qui vous avertissent d'une date d'expiration de certificat proche, telles que les alertes **expiration du certificat de noeud final de l'équilibreur de charge** et **expiration du certificat de serveur global pour les alertes S3 et Swift API**.
- Synchronisez toujours les versions du certificat des applications StorageGRID et S3. Si vous remplacez ou renouvelez le certificat utilisé pour un terminal d'équilibrage de charge, vous devez remplacer ou renouveler le certificat équivalent utilisé par l'application S3.

- Utiliser un certificat d'autorité de certification signé publiquement. Si vous utilisez un certificat signé par une autorité de certification, vous pouvez remplacer les certificats bientôt expirés sans interruption.
- Si vous avez généré un certificat StorageGRID auto-signé et que ce certificat est sur le point d'expirer, vous devez le remplacer manuellement dans StorageGRID et dans l'application S3 avant que le certificat existant n'expire.

Considérations relatives au mode de liaison

Le mode de liaison vous permet de contrôler les adresses IP qui peuvent être utilisées pour accéder à un noeud final de l'équilibreur de charge. Si un noeud final utilise un mode de liaison, les applications clientes peuvent uniquement accéder au noeud final si elles utilisent une adresse IP autorisée ou son nom de domaine complet (FQDN) correspondant. Les applications clientes utilisant une autre adresse IP ou un autre nom de domaine complet ne peuvent pas accéder au point final.

Vous pouvez spécifier l'un des modes de reliure suivants :

- **Global** (par défaut) : les applications clientes peuvent accéder au noeud final en utilisant l'adresse IP de n'importe quel noeud de passerelle ou noeud d'administration, l'adresse IP virtuelle (VIP) de n'importe quel groupe HA sur n'importe quel réseau, ou un FQDN correspondant. Utilisez ce paramètre, sauf si vous avez besoin de restreindre l'accessibilité d'un noeud final.
- **Adresses IP virtuelles des groupes HA**. Les applications client doivent utiliser une adresse IP virtuelle (ou le nom de domaine complet correspondant) d'un groupe haute disponibilité.
- **Interfaces de nœud**. Les clients doivent utiliser les adresses IP (ou les FQDN correspondants) des interfaces de nœud sélectionnées.
- **Type de noeud**. En fonction du type de nœud que vous sélectionnez, les clients doivent utiliser l'adresse IP (ou le nom de domaine complet correspondant) de tout nœud d'administration ou l'adresse IP (ou le nom de domaine complet correspondant) de tout nœud de passerelle.

Considérations relatives à l'accès des locataires

L'accès aux locataires est une fonction de sécurité facultative qui vous permet de contrôler quels comptes de locataires StorageGRID peuvent utiliser un terminal d'équilibrage des charges pour accéder à leurs compartiments. Vous pouvez autoriser tous les locataires à accéder à un noeud final (par défaut), ou vous pouvez spécifier une liste des locataires autorisés ou bloqués pour chaque noeud final.

Vous pouvez utiliser cette fonction pour améliorer l'isolation de sécurité entre les locataires et leurs terminaux. Par exemple, vous pouvez utiliser cette fonction pour vous assurer que les matériaux les plus secrets ou les matériaux hautement classés appartenant à un locataire restent complètement inaccessibles aux autres locataires.

> Aux fins du contrôle d'accès, le locataire est déterminé à partir des clés d'accès utilisées dans la demande du client, si aucune clé d'accès n'est fournie dans le cadre de la demande (par exemple avec un accès anonyme), le propriétaire du compartiment est utilisé pour déterminer le locataire.

Exemple d'accès aux locataires

Pour comprendre le fonctionnement de cette fonction de sécurité, prenez l'exemple suivant :

1. Vous avez créé deux terminaux d'équilibrage de charge, comme suit :
    - **Noeud final public** : utilise le port 10443 et permet l'accès à tous les locataires.

- **Point final Top secret** : utilise le port 10444 et permet l'accès au locataire **Top secret** uniquement. Tous les autres locataires ne peuvent pas accéder à ce noeud final.

2. Le `top-secret.pdf` Est dans un seau appartenant au locataire **Top secret**.

Pour accéder au `top-secret.pdf`, Un utilisateur du locataire **Top secret** peut émettre une demande GET à `https://w.x.y.z:10444/top-secret.pdf`. Comme ce locataire est autorisé à utiliser le noeud final 10444, l'utilisateur peut accéder à l'objet. Cependant, si un utilisateur appartenant à un autre locataire envoie la même requête à la même URL, il reçoit un message accès refusé immédiat. L'accès est refusé même si les informations d'identification et la signature sont valides.

Disponibilité du processeur

Le service Load Balancer sur chaque nœud d'administration et chaque nœud de passerelle fonctionne de manière indépendante lors du transfert du trafic S3 ou Swift vers les nœuds de stockage. Par le biais d'un processus de pondération, le service Load Balancer achemine davantage de requêtes vers des nœuds de stockage avec une disponibilité de processeur supérieure. Les informations de charge de l'UC du nœud sont mises à jour toutes les quelques minutes, mais la pondération peut être mise à jour plus fréquemment. Tous les nœuds de stockage se voient attribuer une valeur de poids de base minimale, même si un nœud indique une utilisation de 100 % ou ne parvient pas à signaler son utilisation.

Dans certains cas, les informations relatives à la disponibilité du processeur sont limitées au site où se trouve le service Load Balancer.

Configurer les terminaux de l'équilibreur de charge

Les terminaux d'équilibrage de la charge déterminent les ports et les protocoles réseau que les clients S3 et Swift peuvent utiliser pour la connexion à l'équilibreur de charge StorageGRID sur les nœuds de passerelle et d'administration.

> La prise en charge des applications du client Swift a été obsolète et sera supprimée dans une prochaine version.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous disposez de l'autorisation d'accès racine.
- Vous avez passé en revue le "considérations relatives à l'équilibrage de charge".
- Si vous avez précédemment mappé à nouveau un port que vous souhaitez utiliser pour le noeud final de l'équilibreur de charge, vous avez "retirez le schéma de câblage des ports - effectué".
- Vous avez créé tous les groupes à haute disponibilité (HA) que vous prévoyez d'utiliser. Les groupes HAUTE DISPONIBILITÉ sont recommandés, mais pas obligatoires. Voir "Gérez les groupes haute disponibilité".
- Si le point final de l'équilibreur de charge est utilisé par "Locataires S3 pour S3 Select", Il ne doit pas utiliser les adresses IP ou FQDN de tout noeud bare-Metal. Seuls les appliances SG100 ou SG1000 et les nœuds logiciels VMware sont autorisés pour les terminaux d'équilibrage de charge utilisés pour S3 Select.
- Vous avez configuré toutes les interfaces VLAN que vous prévoyez d'utiliser. Voir "Configurez les interfaces VLAN".
- Si vous créez un noeud final HTTPS (recommandé), vous disposez des informations relatives au certificat de serveur.

Les modifications apportées à un certificat de point final peuvent prendre jusqu'à 15 minutes pour être appliquées à tous les nœuds.

- Pour télécharger un certificat, vous avez besoin du certificat de serveur, de la clé privée de certificat et, éventuellement, d'un bundle CA.
- Pour générer un certificat, vous devez disposer de tous les noms de domaine et adresses IP que les clients S3 ou Swift utiliseront pour accéder au terminal. Vous devez également connaître le sujet (Nom unique).
- Si vous souhaitez utiliser le certificat API StorageGRID S3 et Swift (qui peut également être utilisé pour les connexions directement aux nœuds de stockage), vous avez déjà remplacé le certificat par défaut par un certificat personnalisé signé par une autorité de certification externe. Voir"Configurez les certificats API S3 et Swift".

Créer un noeud final d'équilibreur de charge

Chaque point final de l'équilibreur de charge spécifie un port, un type de client (S3 ou Swift) et un protocole réseau (HTTP ou HTTPS).

Accéder à l'assistant

Étapes

1. Sélectionnez **CONFIGURATION** > **réseau** > **noeuds finaux de l'équilibreur de charge**.
2. Sélectionnez **Créer**.

Saisissez les détails du point final

Étapes

1. Saisissez les détails du noeud final.

Champ	Description
Nom	Nom descriptif du noeud final, qui apparaîtra dans le tableau sur la page noeuds finaux de l'équilibreur de charge.
Port	Port StorageGRID que vous souhaitez utiliser pour l'équilibrage de charge. Ce champ est défini par défaut sur 10433 pour le premier noeud final que vous créez, mais vous pouvez entrer n'importe quel port externe inutilisé entre 1 et 65535. Si vous saisissez **80** ou **443**, le noeud final est configuré uniquement sur les noeuds de passerelle. Ces ports sont réservés sur des nœuds d'administration.
Type de client	Type d'application client qui utilisera ce noeud final, **S3** ou **Swift**.

Champ	Description
Protocole réseau	Protocole réseau utilisé par les clients lors de la connexion à ce noeud final. • Sélectionnez **HTTPS** pour la communication sécurisée et cryptée TLS (recommandé). Vous devez joindre un certificat de sécurité avant de pouvoir enregistrer le noeud final. • Sélectionnez **HTTP** pour une communication moins sécurisée et non chiffrée. Utilisez HTTP uniquement pour une grille autre que la production.

2. Sélectionnez **Continuer**.

Sélectionnez un mode de reliure

Étapes

1. Sélectionnez un mode de liaison pour le noeud final afin de contrôler l'accès au noeud final—à l'aide d'une adresse IP ou d'une adresse IP et d'interfaces réseau spécifiques.

Option	Description
Global (par défaut)	Les clients peuvent accéder au point final en utilisant l'adresse IP de n'importe quel nœud de passerelle ou nœud d'administration, l'adresse IP virtuelle (VIP) de n'importe quel groupe haute disponibilité sur n'importe quel réseau, ou un FQDN correspondant. Utilisez le paramètre **Global** (valeur par défaut) sauf si vous devez restreindre l'accessibilité de ce point final.
Adresses IP virtuelles de groupes haute disponibilité	Les clients doivent utiliser une adresse IP virtuelle (ou le nom de domaine complet correspondant) d'un groupe haute disponibilité pour accéder à ce point final. Les terminaux associés à ce mode de liaison peuvent tous utiliser le même numéro de port, tant que les groupes haute disponibilité que vous sélectionnez pour les terminaux ne se chevauchent pas.
Interfaces de nœuds	Les clients doivent utiliser les adresses IP (ou les FQDN correspondants) des interfaces de nœud sélectionnées pour accéder à ce noeud final.
Type de nœud	En fonction du type de nœud que vous sélectionnez, les clients doivent utiliser l'adresse IP (ou le nom de domaine complet correspondant) de tout nœud d'administration ou l'adresse IP (ou le nom de domaine complet correspondant) de tout nœud de passerelle pour accéder à ce point final.

Si plusieurs noeuds finaux utilisent le même port, StorageGRID utilise cet ordre de priorité pour décider quel noeud final utiliser : **adresses IP virtuelles des groupes HA** > **interfaces de noeud** > **Type de noeud** > **Global**.

2. Si vous avez sélectionné **IP virtuelles de groupes HA**, sélectionnez un ou plusieurs groupes HA.
3. Si vous avez sélectionné **Node interfaces**, sélectionnez une ou plusieurs interfaces de nœud pour chaque

noeud d'administration ou nœud de passerelle que vous souhaitez associer à ce noeud final.

4. Si vous avez sélectionné **Type de noeud**, sélectionnez soit noeuds Admin, qui comprend à la fois le noeud Admin principal et tous les noeuds Admin non primaires, soit noeuds Gateway.

Contrôle de l'accès des locataires

Étapes

1. Pour l'étape **tenant Access**, sélectionnez l'une des options suivantes :

Champ	Description
Autoriser tous les locataires (par défaut)	Tous les comptes de locataires peuvent utiliser ce terminal pour accéder à leurs compartiments. Vous devez sélectionner cette option si vous n'avez pas encore créé de compte de locataire. Après avoir ajouté des comptes de locataire, vous pouvez modifier le terminal de l'équilibreur de charge pour autoriser ou bloquer des comptes spécifiques.
Autoriser les locataires sélectionnés	Seuls les comptes de locataire sélectionnés peuvent utiliser ce terminal pour accéder à leurs compartiments.
Bloquez les locataires sélectionnés	Les comptes de locataire sélectionnés ne peuvent pas utiliser ce terminal pour accéder à leurs compartiments. Tous les autres locataires peuvent utiliser ce noeud final.

2. Si vous créez un noeud final **HTTP**, vous n'avez pas besoin de joindre un certificat. Sélectionnez **Créer** pour ajouter le nouveau noeud final de l'équilibreur de charge. Ensuite, passez à Une fois que vous avez terminé. Sinon, sélectionnez **Continuer** pour joindre le certificat.

Joindre un certificat

Étapes

1. Si vous créez un noeud final **HTTPS**, sélectionnez le type de certificat de sécurité que vous souhaitez associer au noeud final.

   Le certificat sécurise les connexions entre les clients S3 et Swift et le service Load Balancer sur les nœuds d'administration ou de passerelle.

   - **Télécharger le certificat**. Sélectionnez cette option si vous avez des certificats personnalisés à télécharger.
   - **Générer un certificat**. Sélectionnez cette option si vous avez les valeurs nécessaires pour générer un certificat personnalisé.
   - **Utilisez le certificat StorageGRID S3 et Swift**. Sélectionnez cette option pour utiliser le certificat d'API S3 et Swift global, qui peut également être utilisé pour les connexions directement aux nœuds de stockage.

     Vous ne pouvez sélectionner cette option que si vous avez remplacé le certificat d'API S3 et Swift par défaut, signé par l'autorité de certification de la grille, par un certificat personnalisé signé par une autorité de certification externe. Voir"Configurez les certificats API S3 et Swift".

2. Si vous n’utilisez pas les certificats StorageGRID S3 et Swift, téléchargez ou générez le certificat.

Télécharger le certificat

a. Sélectionnez **Télécharger le certificat**.

b. Téléchargez les fichiers de certificat de serveur requis :

- **Certificat de serveur** : fichier de certificat de serveur personnalisé dans le codage PEM.
- **Clé privée de certificat** : fichier de clé privée de certificat de serveur personnalisé (`.key`).

> Les clés privées EC doivent être de 224 bits ou plus. Les clés privées RSA doivent être de 2048 bits ou plus.

- **Paquet CA** : un fichier facultatif unique contenant les certificats de chaque autorité de certification intermédiaire (AC). Le fichier doit contenir chacun des fichiers de certificat d'autorité de certification codés au PEM, concaténés dans l'ordre de la chaîne de certificats.

c. Développez **Détails du certificat** pour afficher les métadonnées de chaque certificat que vous avez téléchargé. Si vous avez téléchargé un bundle CA facultatif, chaque certificat s'affiche sur son propre onglet.

- Sélectionnez **Télécharger le certificat** pour enregistrer le fichier de certificat ou sélectionnez **Télécharger le paquet CA** pour enregistrer le lot de certificats.

  Spécifiez le nom du fichier de certificat et l'emplacement de téléchargement. Enregistrez le fichier avec l'extension `.pem`.

  Par exemple : `storagegrid_certificate.pem`

- Sélectionnez **Copy certificate PEM** ou **Copy CA bundle PEM** pour copier le contenu du certificat pour le coller ailleurs.

d. Sélectionnez **Créer**. + le noeud final de l'équilibreur de charge est créé. Le certificat personnalisé est utilisé pour toutes les nouvelles connexions ultérieures entre les clients S3 et Swift et le terminal.

Générez un certificat

a. Sélectionnez **générer certificat**.

b. Spécifiez les informations de certificat :

Champ	Description
Nom de domaine	Un ou plusieurs noms de domaine complets à inclure dans le certificat. Utilisez un * comme caractère générique pour représenter plusieurs noms de domaine.
IP	Une ou plusieurs adresses IP à inclure dans le certificat.
Objet (facultatif)	Objet X.509 ou nom distinctif (DN) du propriétaire du certificat. Si aucune valeur n'est saisie dans ce champ, le certificat généré utilise le premier nom de domaine ou l'adresse IP comme nom commun de l'objet (CN).

Champ	Description
Jours valides	Nombre de jours après la création, pendant lesquels le certificat expire.
Ajouter des extensions d'utilisation de clé	Si cette option est sélectionnée (par défaut et recommandée), l'utilisation des clés et les extensions d'utilisation des clés étendues sont ajoutées au certificat généré. Ces extensions définissent l'objectif de la clé contenue dans le certificat. **Remarque** : ne cochez pas cette case si vous rencontrez des problèmes de connexion avec des clients plus anciens lorsque les certificats incluent ces extensions.

c. Sélectionnez **generate**.

d. Sélectionnez **Détails du certificat** pour afficher les métadonnées du certificat généré.

- Sélectionnez **Télécharger le certificat** pour enregistrer le fichier de certificat.

  Spécifiez le nom du fichier de certificat et l'emplacement de téléchargement. Enregistrez le fichier avec l'extension `.pem`.

  Par exemple : `storagegrid_certificate.pem`

- Sélectionnez **Copier le certificat PEM** pour copier le contenu du certificat pour le coller ailleurs.

e. Sélectionnez **Créer**.

Le noeud final de l'équilibreur de charge est créé. Le certificat personnalisé est utilisé pour toutes les nouvelles connexions ultérieures entre les clients S3 et Swift et ce terminal.

Une fois que vous avez terminé

Étapes

1. Si vous utilisez un DNS, assurez-vous que le DNS inclut un enregistrement pour associer le nom de domaine complet (FQDN) StorageGRID à chaque adresse IP que les clients utiliseront pour établir des connexions.

   L'adresse IP que vous entrez dans l'enregistrement DNS dépend de l'utilisation ou non d'un groupe HA de nœuds d'équilibrage de la charge :

   - Si vous avez configuré un groupe haute disponibilité, les clients se connectent aux adresses IP virtuelles de ce groupe haute disponibilité.
   - Si vous n'utilisez pas de groupe haute disponibilité, les clients se connectent au service StorageGRID Load Balancer à l'aide de l'adresse IP d'un nœud de passerelle ou d'un nœud d'administration.

     Vous devez également vous assurer que l'enregistrement DNS référence tous les noms de domaine de point final requis, y compris les noms de caractères génériques.

2. Fournissez aux clients S3 et Swift les informations nécessaires pour se connecter au terminal :

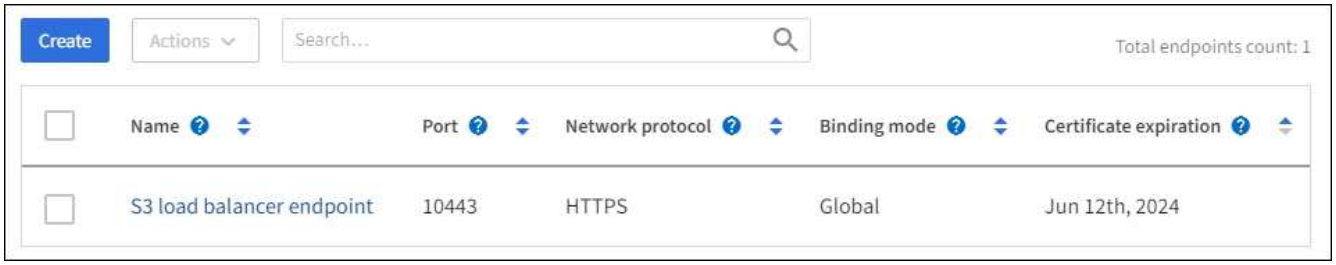
- Numéro de port
- Nom de domaine ou adresse IP complet
- Tous les détails de certificat requis

Afficher et modifier les points finaux de l'équilibreur de charge

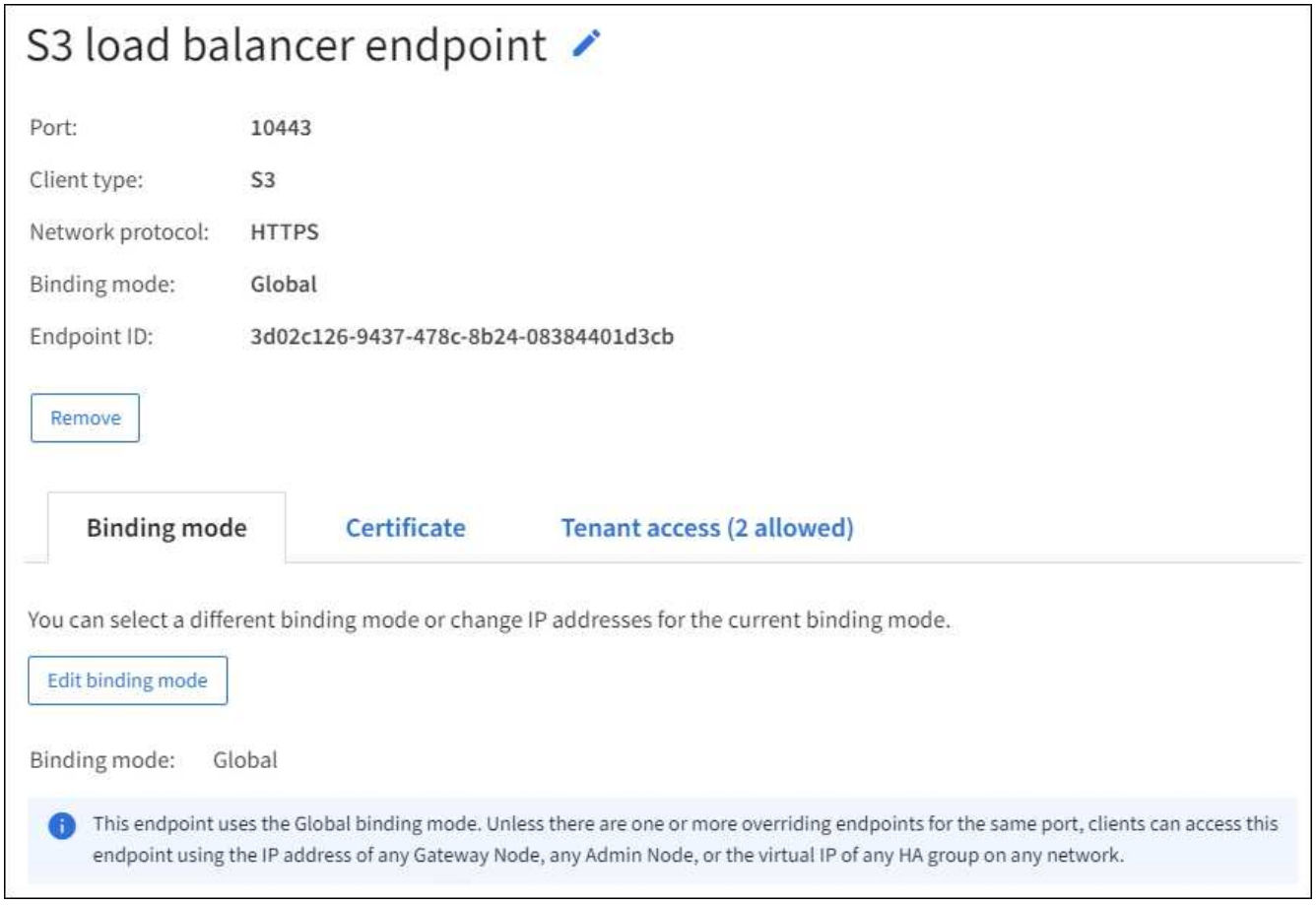
Vous pouvez afficher les détails des noeuds finaux existants de l'équilibreur de charge, y compris les métadonnées de certificat d'un noeud final sécurisé. Vous pouvez également modifier le nom d'un noeud final ou le mode de liaison et mettre à jour tous les certificats associés.

Vous ne pouvez pas modifier le type de service (S3 ou Swift), le port ou le protocole (HTTP ou HTTPS).

- Pour afficher les informations de base de tous les noeuds finaux de l'équilibreur de charge, consultez le tableau de la page noeuds finaux de l'équilibreur de charge.



- Pour afficher tous les détails sur un noeud final spécifique, y compris les métadonnées du certificat, sélectionnez le nom du noeud final dans le tableau.



- Pour modifier un noeud final, utilisez le menu **actions** de la page noeuds finaux de l'équilibreur de charge ou la page de détails d'un noeud final spécifique.

> Après avoir modifié un noeud final, vous devrez peut-être attendre jusqu'à 15 minutes que vos modifications soient appliquées à tous les noeuds.

Tâche	Menu actions	Page de détails
Modifier le nom du point final	a. Cochez la case du point final. b. Sélectionnez **actions** > **Modifier le nom du point final**. c. Saisissez le nouveau nom. d. Sélectionnez **Enregistrer**.	a. Sélectionnez le nom du noeud final pour afficher les détails. b. Sélectionnez l'icône de modification . c. Saisissez le nouveau nom. d. Sélectionnez **Enregistrer**.
Modifier le mode de liaison du point final	a. Cochez la case du point final. b. Sélectionnez **actions** > **Modifier le mode de liaison du point final**. c. Mettez à jour le mode de liaison si nécessaire. d. Sélectionnez **Enregistrer les modifications**.	a. Sélectionnez le nom du noeud final pour afficher les détails. b. Sélectionnez **Modifier le mode de liaison**. c. Mettez à jour le mode de liaison si nécessaire. d. Sélectionnez **Enregistrer les modifications**.
Modifier le certificat de point final	a. Cochez la case du point final. b. Sélectionnez **actions** > **Modifier le certificat de point final**. c. Chargez ou générez un nouveau certificat personnalisé ou commencez à utiliser le certificat Global S3 et Swift, si nécessaire. d. Sélectionnez **Enregistrer les modifications**.	a. Sélectionnez le nom du noeud final pour afficher les détails. b. Sélectionnez l'onglet **certificat**. c. Sélectionnez **Modifier le certificat**. d. Chargez ou générez un nouveau certificat personnalisé ou commencez à utiliser le certificat Global S3 et Swift, si nécessaire. e. Sélectionnez **Enregistrer les modifications**.

Tâche	Menu actions	Page de détails
Modifier l'accès du locataire	a. Cochez la case du point final. b. Sélectionnez **actions** > **Modifier l'accès locataire**. c. Choisissez une autre option d'accès, sélectionnez ou supprimez des locataires de la liste, ou effectuez les deux. d. Sélectionnez **Enregistrer les modifications**.	a. Sélectionnez le nom du noeud final pour afficher les détails. b. Sélectionnez l'onglet **tenant Access**. c. Sélectionnez **Modifier l'accès locataire**. d. Choisissez une autre option d'accès, sélectionnez ou supprimez des locataires de la liste, ou effectuez les deux. e. Sélectionnez **Enregistrer les modifications**.

Supprimez les points finaux de l'équilibreur de charge

Vous pouvez supprimer un ou plusieurs noeuds finaux à l'aide du menu **actions**, ou vous pouvez supprimer un seul noeud final de la page de détails.

> Pour éviter toute interruption de vos clients, mettez à jour les applications client S3 ou Swift affectées avant de supprimer un terminal d'équilibrage de charge. Mettez à jour chaque client pour vous connecter à l'aide d'un port attribué à un autre noeud final de l'équilibreur de charge. Assurez-vous également de mettre à jour les informations de certificat requises.

- Pour supprimer un ou plusieurs noeuds finaux :
  a. Sur la page équilibreur de charge, cochez la case correspondant à chaque noeud final à supprimer.
  b. Sélectionnez **actions** > **Supprimer**.
  c. Sélectionnez **OK**.
- Pour supprimer un noeud final de la page de détails :
  a. À partir de la page équilibreur de charge. sélectionnez le nom du noeud final.
  b. Sélectionnez **Supprimer** sur la page de détails.
  c. Sélectionnez **OK**.

Configuration des noms de domaine de terminaux S3

Pour prendre en charge les requêtes de type hébergement virtuel S3, vous devez utiliser le gestionnaire Grid pour configurer la liste des noms de domaine de terminaux S3 auxquels les clients S3 se connectent.

> L'utilisation d'une adresse IP pour un nom de domaine de noeud final n'est pas prise en charge. Les versions ultérieures empêcheront cette configuration.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous avez "autorisations d'accès spécifiques".

- Vous avez confirmé qu'une mise à niveau de la grille n'est pas en cours.

> N'apportez aucune modification à la configuration du nom de domaine lorsqu'une mise à niveau de grille est en cours.

Description de la tâche

Pour permettre aux clients d'utiliser les noms de domaine de terminaux S3, vous devez effectuer toutes les opérations suivantes :

- Utilisez le Gestionnaire de grille pour ajouter les noms de domaine de points de terminaison S3 au système StorageGRID.
- S'assurer que le "Certificat utilisé par le client pour les connexions HTTPS à StorageGRID" est signé pour tous les noms de domaine requis par le client.

  Par exemple, si le noeud final est `s3.company.com`, Vous devez vous assurer que le certificat utilisé pour les connexions HTTPS inclut le `s3.company.com` Nom de l'alternative (SAN) de l'objet générique du noeud final et du noeud final : `*.s3.company.com`.

- Configurez le serveur DNS utilisé par le client. Incluez les enregistrements DNS pour les adresses IP utilisées par les clients pour établir des connexions et assurez-vous que les enregistrements référencent tous les noms de domaine de point final S3 requis, y compris les noms génériques.

> Les clients peuvent se connecter à StorageGRID à l'aide de l'adresse IP d'un nœud de passerelle, d'un nœud d'administration ou d'un nœud de stockage, ou en se connectant à l'adresse IP virtuelle d'un groupe haute disponibilité. Vous devez comprendre comment les applications client se connectent à la grille pour inclure les adresses IP correctes dans les enregistrements DNS.

Les clients qui utilisent des connexions HTTPS (recommandées) au grid peuvent utiliser l'un des certificats suivants :

- Les clients qui se connectent à un noeud final d'équilibreur de charge peuvent utiliser un certificat personnalisé pour ce noeud final. Chaque terminal d'équilibrage de la charge peut être configuré de manière à reconnaître différents noms de domaine de terminaux S3.
- Les clients qui se connectent à un terminal d'équilibrage de charge ou directement à un nœud de stockage peuvent personnaliser le certificat d'API S3 et Swift global pour inclure tous les noms de domaine de terminaux S3 requis.

> Si vous n'ajoutez pas de noms de domaine de terminaux S3 et que la liste est vide, la prise en charge des demandes de type hébergement virtuel S3 est désactivée.

Ajoutez un nom de domaine de terminal S3

Étapes

1. Sélectionnez **CONFIGURATION** > **réseau** > **noms de domaine de noeud final S3**.
2. Entrez le nom de domaine dans le champ **Nom de domaine 1**. Sélectionnez **Ajouter un autre nom de domaine** pour ajouter d'autres noms de domaine.
3. Sélectionnez **Enregistrer**.
4. Assurez-vous que les certificats de serveur utilisés par les clients correspondent aux noms de domaine de

noeud final S3 requis.

- Si les clients se connectent à un terminal d'équilibrage de charge qui utilise son propre certificat, "mettez à jour le certificat associé au noeud final".
- Si les clients se connectent à un terminal d'équilibreur de charge qui utilise le certificat API S3 et Swift global ou directement aux nœuds de stockage, "Mise à jour du certificat d'API S3 et Swift global".

5. Ajoutez les enregistrements DNS requis pour vous assurer que les demandes de nom de domaine de point final peuvent être résolues.

Résultat

Maintenant, lorsque les clients utilisent le noeud final `bucket.s3.company.com`, Le serveur DNS résout le noeud final correct et le certificat authentifie le noeud final comme prévu.

Renommer un nom de domaine de terminal S3

Si vous modifiez un nom utilisé par les applications S3, les demandes de type hébergement virtuel échouent.

Étapes

1. Sélectionnez **CONFIGURATION** > **réseau** > **noms de domaine de noeud final S3**.
2. Sélectionnez le champ de nom de domaine que vous souhaitez modifier et apportez les modifications nécessaires.
3. Sélectionnez **Enregistrer**.
4. Sélectionnez **Oui** pour confirmer votre modification.

Supprimez un nom de domaine de terminal S3

Si vous supprimez un nom utilisé par les applications S3, les demandes de type hébergement virtuel échoueront.

Étapes

1. Sélectionnez **CONFIGURATION** > **réseau** > **noms de domaine de noeud final S3**.
2. Sélectionnez l'icône de suppression ✕ en regard du nom de domaine.
3. Sélectionnez **Oui** pour confirmer la suppression.

Informations associées

- "UTILISEZ L'API REST S3"
- "Afficher les adresses IP"
- "Configurez les groupes haute disponibilité"

Résumé : adresses IP et ports pour les connexions client

Pour stocker ou récupérer des objets, les applications clientes S3 et Swift se connectent au service Load Balancer, qui est inclus sur tous les nœuds d'administration et les nœuds de passerelle, ou au service LDR (local distribution Router), qui est inclus sur tous les nœuds de stockage.

Les applications client peuvent se connecter à StorageGRID en utilisant l'adresse IP d'un nœud grid et le numéro de port du service sur ce nœud. Vous pouvez également créer des groupes haute disponibilité de nœuds d'équilibrage de la charge pour fournir des connexions haute disponibilité utilisant des adresses IP

virtuelles (VIP). Si vous souhaitez vous connecter à StorageGRID à l'aide d'un nom de domaine complet (FQDN) au lieu d'une adresse IP ou VIP, vous pouvez configurer des entrées DNS.

Ce tableau récapitule les différentes façons dont les clients peuvent se connecter à StorageGRID ainsi que les adresses IP et les ports utilisés pour chaque type de connexion. Si vous avez déjà créé des terminaux d'équilibrage de charge et des groupes haute disponibilité (HA), reportez-vous à la section Où trouver les adresses IP Pour localiser ces valeurs dans le Gestionnaire de grille.

Là où la connexion est établie	Service auquel le client se connecte	Adresse IP	Port
Groupe HAUTE DISPONIBILITÉ	Équilibreur de charge	Adresse IP virtuelle d'un groupe haute disponibilité	Port attribué au noeud final de l'équilibreur de charge
Nœud d'administration	Équilibreur de charge	Adresse IP du nœud d'administration	Port attribué au noeud final de l'équilibreur de charge
Nœud de passerelle	Équilibreur de charge	Adresse IP du nœud de passerelle	Port attribué au noeud final de l'équilibreur de charge
Nœud de stockage	LDR	Adresse IP du nœud de stockage	Ports S3 par défaut : • HTTPS: 18082 • HTTP : 18084 Ports Swift par défaut : • HTTPS: 18083 • HTTP : 18085

Exemples d'URL

Pour connecter une application client au point de terminaison Load Balancer d'un groupe haute disponibilité de nœuds de passerelle, utilisez une URL structurée comme indiqué ci-dessous :

`https://VIP-of-HA-group:LB-endpoint-port`

Par exemple, si l'adresse IP virtuelle du groupe haute disponibilité est 192.0.2.5 et que le numéro de port du terminal de l'équilibreur de charge est 10443, une application peut utiliser l'URL suivante pour se connecter à StorageGRID :

`https://192.0.2.5:10443`

Où trouver les adresses IP

1. Connectez-vous au Grid Manager à l'aide d'un "navigateur web pris en charge".
2. Pour trouver l'adresse IP d'un nœud de grille :
   a. Sélectionnez **NOEUDS**.

b. Sélectionnez le nœud d'administration, le nœud de passerelle ou le nœud de stockage auquel vous souhaitez vous connecter.

c. Sélectionnez l'onglet **Aperçu**.

d. Dans la section informations sur le nœud, notez les adresses IP du nœud.

e. Sélectionnez **Afficher plus** pour afficher les adresses IPv6 et les mappages d'interface.

Vous pouvez établir des connexions entre les applications client et n'importe quelle adresse IP de la liste :

- **Eth0:** réseau de grille
- **Eth1:** réseau d'administration (facultatif)
- **Eth2:** réseau client (facultatif)

> ⓘ Si vous affichez un nœud d'administration ou un nœud de passerelle et qu'il s'agit du nœud actif dans un groupe haute disponibilité, l'adresse IP virtuelle du groupe haute disponibilité est affichée sur eth2.

3. Pour trouver l'adresse IP virtuelle d'un groupe haute disponibilité :
   a. Sélectionnez **CONFIGURATION** > **réseau** > **groupes haute disponibilité**.
   b. Dans le tableau, noter l'adresse IP virtuelle du groupe haute disponibilité.
4. Pour trouver le numéro de port d'un noeud final Load Balancer :
   a. Sélectionnez **CONFIGURATION** > **réseau** > **noeuds finaux de l'équilibreur de charge**.
   b. Notez le numéro de port du noeud final que vous souhaitez utiliser.

> ⓘ Si le numéro de port est 80 ou 443, le noeud final est configuré uniquement sur les noeuds de passerelle, car ces ports sont réservés sur les noeuds d'administration. Tous les autres ports sont configurés sur les nœuds de passerelle et sur les nœuds d'administration.

   c. Sélectionnez le nom du noeud final dans la table.
   d. Vérifiez que le **Type de client** (S3 ou Swift) correspond à l'application cliente qui utilisera le noeud final.

Gestion des réseaux et des connexions

Configuration des paramètres réseau : présentation

Vous pouvez configurer différents paramètres réseau à partir du Gestionnaire de grille pour affiner le fonctionnement de votre système StorageGRID.

Configurez les interfaces VLAN

C'est possible "Créez des interfaces VLAN (Virtual LAN)" pour isoler et partitionner le trafic pour assurer la sécurité, la flexibilité et les performances. Chaque interface VLAN est associée à une ou plusieurs interfaces parents sur les nœuds d'administration et les nœuds de passerelle. Vous pouvez utiliser des interfaces VLAN dans des groupes haute disponibilité et dans des terminaux d'équilibrage de charge pour isoler le trafic client ou administratif par application ou locataire.

Politiques de classification du trafic

Vous pouvez utiliser "politiques de classification du trafic" identifier et gérer différents types de trafic réseau, notamment le trafic lié à des compartiments, des locataires, des sous-réseaux clients ou des terminaux d'équilibrage de la charge spécifiques. Ces règles peuvent vous aider à limiter le trafic et à surveiller le trafic.

Instructions pour les réseaux StorageGRID

Vous pouvez utiliser le Gestionnaire de grille pour configurer et gérer les réseaux et les connexions StorageGRID.

Voir "Configurez les connexions des clients S3 et Swift" Pour apprendre à connecter des clients S3 ou Swift.

Réseaux StorageGRID par défaut

Par défaut, StorageGRID prend en charge trois interfaces réseau par nœud grid, ce qui vous permet de configurer le réseau pour chaque nœud grid en fonction de vos besoins de sécurité et d'accès.

Pour plus d'informations sur la topologie du réseau, reportez-vous à la section "Instructions de mise en réseau".

Réseau Grid

Obligatoire. Le réseau Grid est utilisé pour l'ensemble du trafic StorageGRID interne. Il assure la connectivité entre tous les nœuds de la grille, sur tous les sites et sous-réseaux.

Réseau d'administration

Facultatif. Le réseau d'administration est généralement utilisé pour l'administration et la maintenance du système. Il peut également être utilisé pour l'accès au protocole client. Le réseau Admin est généralement un réseau privé et n'a pas besoin d'être routable entre les sites.

Réseau client

Facultatif. Le réseau client est un réseau ouvert généralement utilisé pour fournir l'accès aux applications client S3 et Swift, de sorte que le réseau Grid puisse être isolé et sécurisé. Le réseau client peut communiquer avec tout sous-réseau accessible via la passerelle locale.

Directives

- Chaque nœud de grid StorageGRID nécessite une interface réseau dédiée, une adresse IP, un masque de sous-réseau et une passerelle pour chaque réseau auquel il est attribué.
- Un nœud de grille ne peut pas avoir plus d'une interface sur un réseau.
- Une passerelle unique, par réseau et par nœud grid est prise en charge et doit être sur le même sous-réseau que le nœud. Vous pouvez implémenter un routage plus complexe dans la passerelle, si nécessaire.
- Sur chaque nœud, chaque réseau est mappé à une interface réseau spécifique.

Le réseau	Nom de l'interface
Grille	eth0

Le réseau	Nom de l'interface
Administrateur (en option)	eth1
Client (facultatif)	eth2

- Si le nœud est connecté à une appliance StorageGRID, des ports spécifiques sont utilisés pour chaque réseau. Pour plus de détails, reportez-vous aux instructions d'installation de votre appareil.
- La route par défaut est générée automatiquement, par nœud. Si eth2 est activé, 0.0.0.0/0 utilise le réseau client sur eth2. Si eth2 n'est pas activé, alors 0.0.0.0/0 utilise le réseau Grid sur eth0.
- Le réseau client n'est opérationnel qu'après que le nœud de la grille ait rejoint la grille
- Le réseau Admin peut être configuré pendant le déploiement du nœud grid pour permettre l'accès à l'interface utilisateur d'installation avant que la grille soit entièrement installée.

Interfaces en option

Vous pouvez également ajouter des interfaces supplémentaires à un nœud. Par exemple, vous pouvez ajouter une interface de ligne réseau à un nœud d'administration ou de passerelle pour que vous puissiez utiliser "Interfaces VLAN" pour isoler le trafic appartenant à différentes applications ou locataires. Vous pouvez également ajouter une interface d'accès à utiliser dans un "Groupe haute disponibilité (HA)".

Pour ajouter une jonction ou des interfaces d'accès, consultez les éléments suivants :

- **VMware (après l'installation du noeud)** : "VMware : ajoutez du jonction ou des interfaces d'accès à un nœud"
  - **RHEL ou CentOS (avant d'installer le nœud)** : "Créez des fichiers de configuration de nœud"
  - **Ubuntu ou Debian (avant d'installer le nœud)** : "Créez des fichiers de configuration de nœud"
  - **RHEL, CentOS, Ubuntu ou Debian (après l'installation du nœud)** : "Linux : ajoutez une jonction ou des interfaces d'accès à un nœud"

Afficher les adresses IP

Vous pouvez afficher l'adresse IP de chaque nœud grid dans votre système StorageGRID. Vous pouvez ensuite utiliser cette adresse IP pour vous connecter au nœud de grille sur la ligne de commande et effectuer diverses procédures de maintenance.

Avant de commencer

Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".

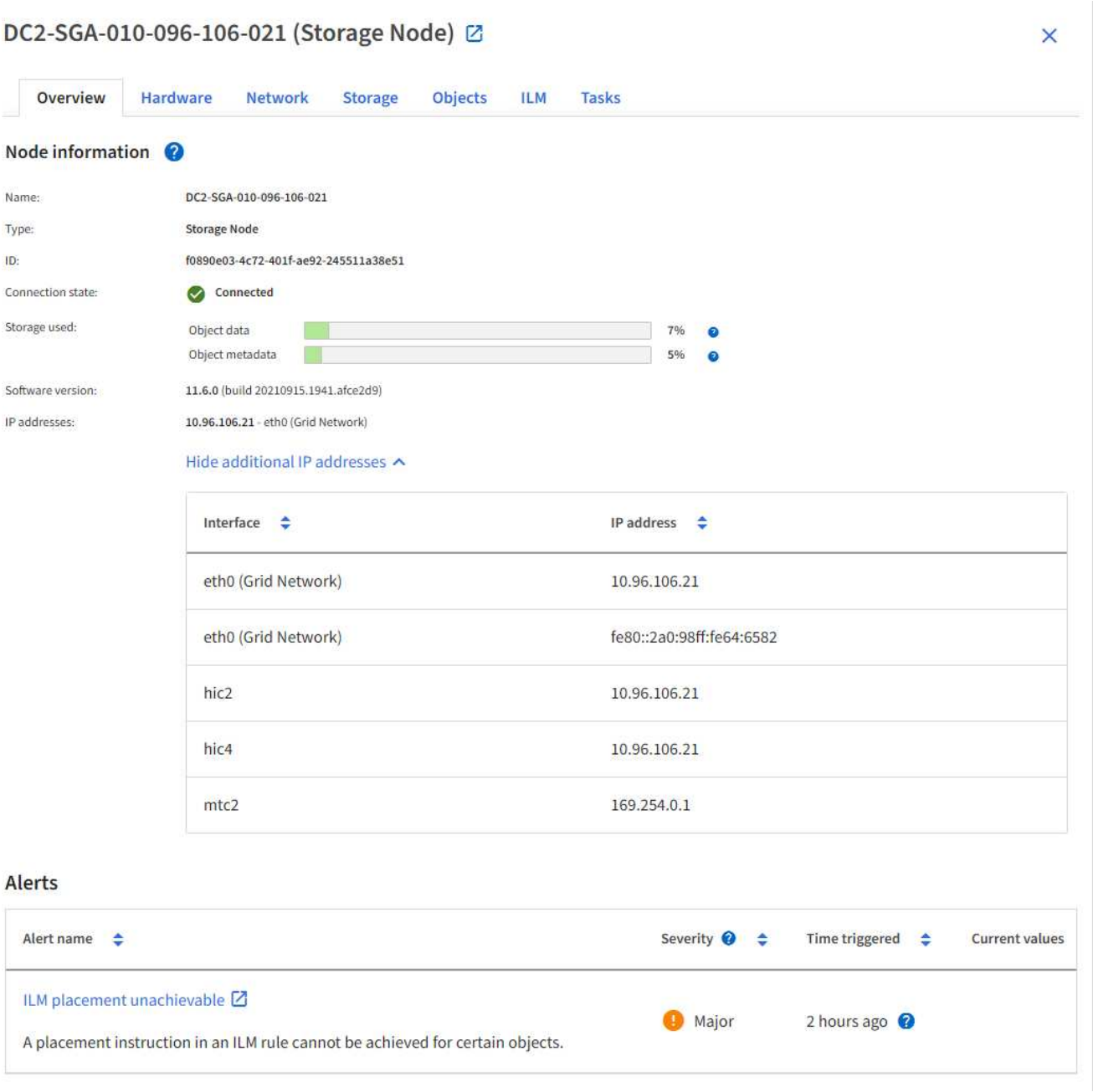
Description de la tâche

Pour plus d'informations sur la modification des adresses IP, reportez-vous à la section "Configurez les adresses IP".

Étapes

1. Sélectionnez **NODES** > ***grid node*** > **Overview**.
2. Sélectionnez **Afficher plus** à droite du titre des adresses IP.

   Les adresses IP de ce nœud de grille sont répertoriées dans un tableau.



Chiffrement pris en charge pour les connexions TLS sortantes

Le système StorageGRID prend en charge un ensemble limité de suites de chiffrement pour les connexions TLS (transport Layer Security) avec les systèmes externes utilisés pour la fédération des identités et les pools de stockage cloud.

Versions supportées de TLS

StorageGRID prend en charge TLS 1.2 et TLS 1.3 pour les connexions aux systèmes externes utilisés pour la fédération des identités et les pools de stockage cloud.

Les chiffrements TLS qui sont pris en charge pour une utilisation avec des systèmes externes ont été sélectionnés pour assurer la compatibilité avec une gamme de systèmes externes. La liste est plus grande que la liste des chiffrements pris en charge pour une utilisation avec les applications client S3 ou Swift. Pour configurer les chiffrements, accédez à **CONFIGURATION** > **sécurité** > **Paramètres de sécurité** et

sélectionnez **règles TLS et SSH**.

> Les options de configuration TLS telles que les versions de protocole, les chiffrements, les algorithmes d'échange de clés et les algorithmes MAC ne sont pas configurables dans StorageGRID. Contactez votre ingénieur commercial NetApp pour toute demande spécifique concernant ces paramètres.

Configurez les interfaces VLAN

Vous pouvez créer des interfaces VLAN sur des nœuds d'administration et de passerelle et les utiliser dans des groupes haute disponibilité et des terminaux d'équilibrage de la charge pour isoler et partitionner le trafic afin d'assurer la sécurité, la flexibilité et les performances.

Considérations relatives aux interfaces VLAN

- Vous créez une interface VLAN en entrant un ID VLAN et en choisissant une interface parent sur un ou plusieurs nœuds.
- Une interface parent doit être configurée comme une interface de ligne réseau au niveau du commutateur.
- Une interface parent peut être la Grid Network (eth0), le réseau client (eth2) ou une interface de ligne de jonction supplémentaire pour la VM ou l'hôte bare-Metal (par exemple, en256).
- Pour chaque interface VLAN, vous ne pouvez sélectionner qu'une seule interface parent pour un nœud donné. Par exemple, vous ne pouvez pas utiliser à la fois l'interface réseau Grid et l'interface réseau client sur le même nœud passerelle que l'interface parent pour le même VLAN.
- Si l'interface VLAN est destinée au trafic du nœud d'administration, qui inclut le trafic lié au Grid Manager et au Gestionnaire de locataires, sélectionnez uniquement les interfaces sur les nœuds d'administration.
- Si l'interface VLAN est destinée au trafic client S3 ou Swift, sélectionnez les interfaces dans les nœuds d'administration ou les nœuds de passerelle.
- Si vous avez besoin d'ajouter des interfaces de jonction, consultez les informations suivantes :
  - **VMware (après l'installation du noeud)** : "VMware : ajoutez du jonction ou des interfaces d'accès à un nœud"
  - **RHEL ou CentOS (avant d'installer le nœud)** : "Créez des fichiers de configuration de nœud"
  - **Ubuntu ou Debian (avant d'installer le nœud)** : "Créez des fichiers de configuration de nœud"
  - **RHEL, CentOS, Ubuntu ou Debian (après l'installation du nœud)** : "Linux : ajoutez une jonction ou des interfaces d'accès à un nœud"

Créez une interface VLAN

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous disposez de l'autorisation d'accès racine.
- Une interface de ligne réseau a été configurée sur le réseau et connectée au VM ou au nœud Linux. Vous connaissez le nom de l'interface de ligne réseau.
- Vous connaissez l'ID du VLAN que vous configurez.

Description de la tâche

Votre administrateur réseau a peut-être configuré une ou plusieurs interfaces de jonction et un ou plusieurs

VLAN pour isoler le trafic client ou administrateur appartenant à différentes applications ou locataires. Chaque VLAN est identifié par un ID numérique ou une balise. Par exemple, votre réseau peut utiliser le VLAN 100 pour le trafic FabricPool et le VLAN 200 pour une application d'archivage.

Vous pouvez utiliser Grid Manager pour créer des interfaces VLAN qui permettent aux clients d'accéder à StorageGRID sur un VLAN spécifique. Lorsque vous créez des interfaces VLAN, vous spécifiez l'ID VLAN et sélectionnez des interfaces parent (trunk) sur un ou plusieurs nœuds.

Accéder à l'assistant

Étapes

1. Sélectionnez **CONFIGURATION** > **réseau** > **interfaces VLAN**.
2. Sélectionnez **Créer**.

Entrez les détails des interfaces VLAN

Étapes

1. Spécifiez l'ID du VLAN de votre réseau. Vous pouvez entrer n'importe quelle valeur comprise entre 1 et 4094.

   Les ID VLAN n'ont pas besoin d'être uniques. Par exemple, vous pouvez utiliser l'ID VLAN 200 pour le trafic administratif sur un site et le même ID VLAN pour le trafic client sur un autre site. Vous pouvez créer des interfaces VLAN distinctes avec différents ensembles d'interfaces parent sur chaque site. Cependant, deux interfaces VLAN avec le même ID ne peuvent pas partager la même interface sur un nœud. Si vous spécifiez un ID déjà utilisé, un message s'affiche.

2. Vous pouvez également saisir une brève description de l'interface VLAN.
3. Sélectionnez **Continuer**.

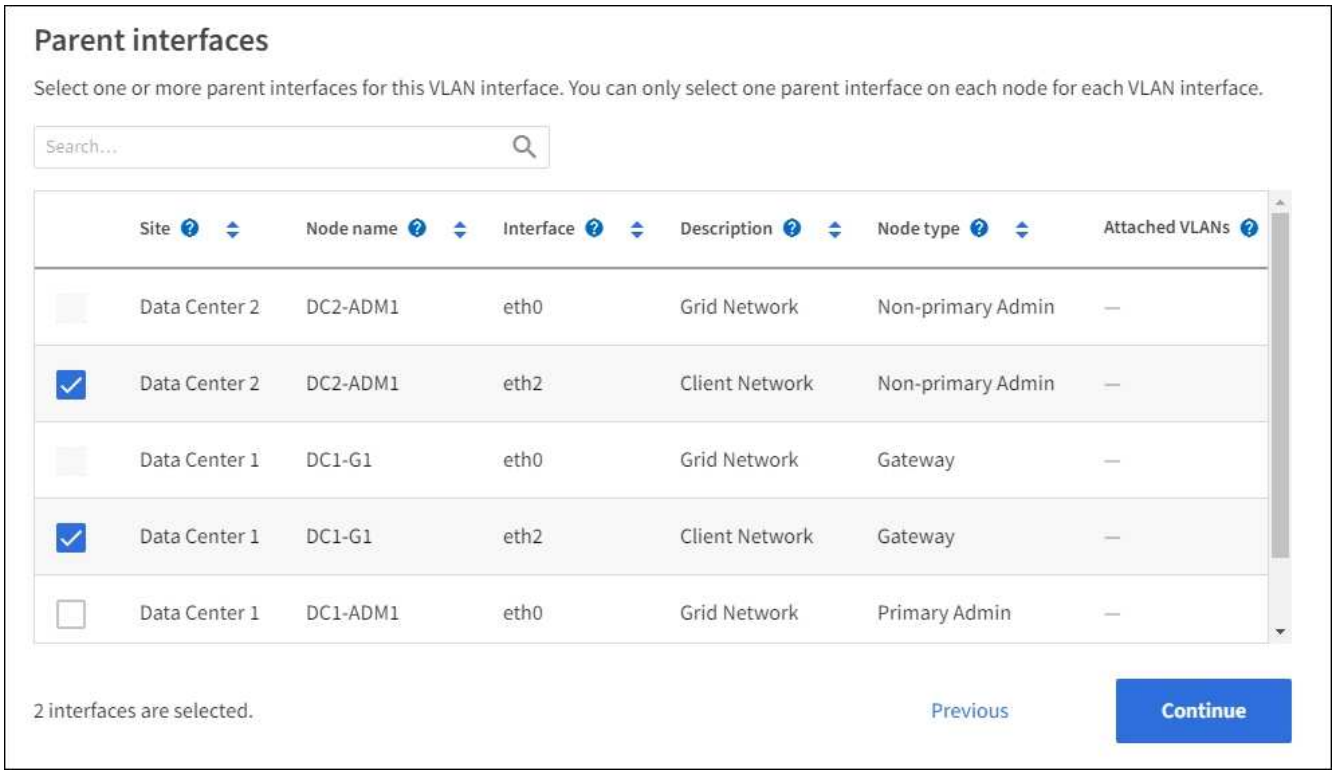
Choisissez les interfaces parents

Le tableau répertorie les interfaces disponibles pour tous les nœuds d'administration et de passerelle de chaque site de votre grille. Les interfaces Admin Network (eth1) ne peuvent pas être utilisées comme interfaces parents et ne sont pas affichées.

Étapes

1. Sélectionnez une ou plusieurs interfaces parent à laquelle relier ce VLAN.

   Par exemple, il peut être nécessaire de connecter un VLAN à l'interface eth2 (client Network) pour un nœud de passerelle et un nœud d'administration.



2. Sélectionnez **Continuer**.

Confirmez les paramètres

Étapes

1. Passez en revue la configuration et apportez les modifications nécessaires.
   - Si vous devez modifier l'ID ou la description du VLAN, sélectionnez **entrer les détails du VLAN** en haut de la page.
   - Si vous devez modifier une interface parent, sélectionnez **Choisissez les interfaces parent** en haut de la page ou sélectionnez **Précédent**.
   - Si vous devez supprimer une interface parent, sélectionnez la corbeille .
2. Sélectionnez **Enregistrer**.
3. Attendez jusqu'à 5 minutes que la nouvelle interface apparaisse comme une sélection sur la page groupes haute disponibilité et qu'elle soit répertoriée dans la table **interfaces réseau** pour le nœud (**NOEUDS** > ***parent interface node*** > **Network**).

Modifiez une interface VLAN

Lorsque vous modifiez une interface VLAN, vous pouvez effectuer les types de modifications suivants :

- Modifiez l'ID ou la description du VLAN.
- Ajouter ou supprimer des interfaces parent.

Par exemple, vous pouvez vouloir supprimer une interface parent d'une interface VLAN si vous envisagez de désaffecter le nœud associé.

Notez ce qui suit :

- Vous ne pouvez pas modifier un ID de VLAN si l'interface VLAN est utilisée dans un groupe haute disponibilité.
- Vous ne pouvez pas supprimer une interface parent si cette interface parent est utilisée dans un groupe haute disponibilité.

  Par exemple, supposons que le VLAN 200 soit connecté aux interfaces parents des nœuds A et B. Si un groupe HA utilise l'interface VLAN 200 pour le nœud A et l'interface eth2 pour le nœud B, vous pouvez supprimer l'interface parent non utilisée pour le nœud B, mais vous ne pouvez pas supprimer l'interface parent utilisée pour le nœud A.

Étapes

1. Sélectionnez **CONFIGURATION** > **réseau** > **interfaces VLAN**.
2. Cochez la case correspondant à l'interface VLAN à modifier. Sélectionnez ensuite **actions** > **Modifier**.
3. Vous pouvez également mettre à jour l'ID VLAN ou la description. Sélectionnez ensuite **Continuer**.

   Vous ne pouvez pas mettre à jour un ID VLAN si ce dernier est utilisé dans un groupe haute disponibilité.

4. Si vous le souhaitez, cochez ou décochez les cases pour ajouter des interfaces parent ou supprimer des interfaces inutilisées. Sélectionnez ensuite **Continuer**.
5. Passez en revue la configuration et apportez les modifications nécessaires.
6. Sélectionnez **Enregistrer**.

Supprime une interface VLAN

Vous pouvez supprimer une ou plusieurs interfaces VLAN.

Vous ne pouvez pas supprimer une interface VLAN si elle est actuellement utilisée dans un groupe haute disponibilité. Vous devez supprimer l'interface VLAN du groupe haute disponibilité avant de pouvoir le supprimer.

Pour éviter toute perturbation du trafic client, envisagez d'effectuer l'une des opérations suivantes :

- Ajoutez une nouvelle interface VLAN au groupe haute disponibilité avant de supprimer cette interface VLAN.
- Créez un nouveau groupe haute disponibilité qui n'utilise pas cette interface VLAN.
- Si l'interface VLAN que vous souhaitez supprimer est actuellement l'interface active, modifiez le groupe HA. Déplacez l'interface VLAN que vous souhaitez supprimer au bas de la liste des priorités. Attendez que la communication soit établie sur la nouvelle interface principale, puis retirez l'ancienne interface du groupe haute disponibilité. Enfin, supprimez l'interface VLAN de ce nœud.

Étapes

1. Sélectionnez **CONFIGURATION** > **réseau** > **interfaces VLAN**.
2. Cochez la case correspondant à chaque interface VLAN à supprimer. Sélectionnez ensuite **actions** > **Supprimer**.
3. Sélectionnez **Oui** pour confirmer votre sélection.

   Toutes les interfaces VLAN sélectionnées sont supprimées. Une bannière de réussite verte apparaît sur la page interfaces VLAN.

Gérer les stratégies de classification du trafic

Gestion des stratégies de classification du trafic : présentation

Pour améliorer vos offres de qualité de service (QoS), vous pouvez créer des stratégies de classification du trafic afin d'identifier et de surveiller différents types de trafic réseau. Ces règles peuvent vous aider à limiter le trafic et à surveiller le trafic.

Les règles de classification du trafic sont appliquées aux terminaux du service StorageGRID Load Balancer pour les nœuds de passerelle et les nœuds d'administration. Pour créer des stratégies de classification de trafic, vous devez avoir déjà créé des points d'extrémité d'équilibreur de charge.

Règles de correspondance

Chaque règle de classification de trafic contient une ou plusieurs règles de correspondance permettant d'identifier le trafic réseau lié à une ou plusieurs des entités suivantes :

- Seaux
- Sous-réseau
- Locataire
- Terminaux d'équilibrage de charge

StorageGRID surveille le trafic qui correspond à n'importe quelle règle de la stratégie conformément aux objectifs de la règle. Tout trafic qui correspond à une règle d'une stratégie est géré par cette règle. Inversement, vous pouvez définir des règles qui correspondent à tout le trafic, à l'exception d'une entité spécifiée.

Limitation du trafic

Vous pouvez également ajouter les types de limite suivants à une règle :

- Bande passante de l'agrégat
- Bande passante par demande
- Requêtes simultanées
- Taux de demande

Les valeurs limites sont appliquées par équilibreur de charge. Si le trafic est réparti simultanément sur plusieurs équilibreurs de charge, les débits maximaux totaux sont un multiple des limites de débit que vous spécifiez.

> Vous pouvez créer des règles pour limiter la bande passante agrégée ou limiter la bande passante par requête. Cependant, StorageGRID ne peut pas limiter les deux types de bande passante en même temps. Les limites de bande passante globales peuvent imposer un impact mineur supplémentaire sur les performances du trafic non limité.

Pour les limites de bande passante globale ou par requête, les demandes sont envoyées vers l'intérieur ou vers l'extérieur au débit défini. StorageGRID ne peut appliquer qu'une seule vitesse. La correspondance des règles la plus spécifique, par type de contrôleur, est donc la plus appliquée. La bande passante consommée par la requête n'est pas prise en compte par rapport à d'autres stratégies de correspondance moins spécifiques contenant des règles de limite de bande passante de l'agrégat. Pour tous les autres types de limite, les demandes des clients sont retardées de 250 millisecondes et reçoivent une réponse lente de 503

pour les demandes dépassant toute limite de stratégie correspondante.

Dans Grid Manager, vous pouvez afficher les diagrammes de trafic et vérifier que les stratégies appliquent les limites de trafic que vous attendez.

Utilisez les stratégies de classification du trafic avec les contrats de niveau de service

Vous pouvez utiliser des règles de classification du trafic en association avec les limites de capacité et la protection des données pour appliquer des accords de niveau de service (SLA) qui fournissent des spécificités en matière de capacité, de protection des données et de performances.

L'exemple suivant montre trois niveaux d'un SLA. Vous pouvez créer des règles de classification du trafic pour atteindre les objectifs de performances de chaque niveau de contrat de niveau de service.

Niveau de service	Puissance	La protection des données	Performances maximales autorisées	Le coût
Or	1 po de stockage autorisé	Règle ILM de 3 copies	25 000 demandes/s Bande passante de 5 Go/s (40 Gbit/s)	par mois
Argent	Stockage de 250 To autorisé	Règle ILM 2 copies	10 000 demandes/s Bande passante de 1.25 Go/s (10 Gbit/s)	$$ par mois
Bronze	Stockage de 100 To autorisé	Règle ILM 2 copies	5 000 demandes/s Bande passante de 1 Go/s (8 Gbit/s)	$ par mois

Créer des stratégies de classification du trafic

Vous pouvez créer des règles de classification du trafic si vous souhaitez contrôler et éventuellement limiter le trafic réseau par compartiment, Regex de compartiment, CIDR, terminal d'équilibrage de charge ou locataire. Vous pouvez également définir des limites pour une stratégie en fonction de la bande passante, du nombre de demandes simultanées ou du taux de demande.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous disposez de l'autorisation d'accès racine.
- Vous avez créé tous les noeuds finaux de l'équilibreur de charge que vous souhaitez associer.
- Vous avez créé les locataires que vous souhaitez associer.

Étapes

1. Sélectionnez **CONFIGURATION** > **réseau** > **classification du trafic**.

2. Sélectionnez **Créer**.
3. Entrez un nom et une description (facultatif) pour la stratégie et sélectionnez **Continuer**.

   Par exemple, décrivez à quoi s'applique cette politique de classification de trafic et à quoi elle limite.

4. Sélectionnez **Ajouter une règle** et spécifiez les détails suivants pour créer une ou plusieurs règles de correspondance pour la stratégie. Toute stratégie que vous créez doit comporter au moins une règle correspondante. Sélectionnez **Continuer**.

Champ	Description
Type	Sélectionnez les types de trafic auxquels s'applique la règle correspondante. Les types de trafic sont le compartiment, le Regex de compartiment, le CIDR, le terminal d'équilibrage de la charge et le locataire.
Valeur de correspondance	Entrez la valeur correspondant au type sélectionné. • Compartiment : entrez un ou plusieurs noms de compartiment. • Regex de compartiment : saisissez une ou plusieurs expressions régulières utilisées pour correspondre à un ensemble de noms de compartiment. L'expression régulière n'est pas ancrée. Utilisez l'ancrage ^ pour faire correspondre au début du nom du compartiment et utilisez l'ancrage $ pour faire correspondre à la fin du nom. La correspondance d'expression régulière prend en charge un sous-ensemble de la syntaxe PCRE (expression régulière compatible Perl). • CIDR : saisissez un ou plusieurs sous-réseaux IPv4, en notation CIDR, qui correspondent au sous-réseau souhaité. • Noeud final de l'équilibreur de charge : sélectionnez un nom de noeud final. Il s'agit des terminaux d'équilibrage de charge que vous avez définis sur le système "Configurer les terminaux de l'équilibreur de charge". • Tenant : le tenant Matching utilise l'ID de clé d'accès. Si la demande ne contient pas d'ID de clé d'accès (par exemple, un accès anonyme), la propriété du compartiment auquel vous accédez est utilisée pour déterminer le locataire.
Comparaison inverse	Si vous voulez faire correspondre tout le trafic réseau *except* avec la valeur Type et correspondance que vous venez de définir, cochez la case **comparaison inverse**. Sinon, laissez la case à cocher désactivée. Par exemple, si vous souhaitez que cette stratégie s'applique à tous les noeuds finaux de l'équilibreur de charge sauf un, spécifiez le noeud final de l'équilibreur de charge à exclure et sélectionnez **comparaison inverse**. Dans le cas d'une règle contenant plusieurs matcheurs où au moins un est un matcher inverse, veillez à ne pas créer une règle qui correspond à toutes les demandes.

5. Si vous le souhaitez, sélectionnez **Ajouter une limite** et sélectionnez les détails suivants pour ajouter une

ou plusieurs limites afin de contrôler le trafic réseau correspondant à une règle.

StorageGRID collecte des mesures, même si vous n'ajoutez aucune limite, pour vous permettre de comprendre les tendances du trafic.

Champ	Description
Type	Type de limite que vous souhaitez appliquer au trafic réseau correspondant à la règle. Par exemple, vous pouvez limiter la bande passante ou le taux de demande. **Remarque** : vous pouvez créer des stratégies pour limiter la bande passante agrégée ou pour limiter la bande passante par demande. Cependant, StorageGRID ne peut pas limiter les deux types de bande passante en même temps. Lorsque la bande passante de l'agrégat est utilisée, la bande passante par demande n'est pas disponible. Inversement, lorsque la bande passante par demande est utilisée, la bande passante de l'agrégat n'est pas disponible. Les limites de bande passante globales peuvent imposer un impact mineur supplémentaire sur les performances du trafic non limité. Pour les limites de bande passante, StorageGRID applique la règle qui correspond le mieux au type de limite défini. Par exemple, si vous avez une stratégie qui limite le trafic dans une seule direction, alors le trafic dans la direction opposée sera illimité, même s'il y a un trafic qui correspond à des stratégies supplémentaires qui ont des limites de bande passante. StorageGRID met en œuvre les « meilleures » correspondances pour les limites de bande passante dans l'ordre suivant : • Adresse IP exacte (/32 masque) • Nom exact du compartiment • Seau regex • Locataire • Point final • Correspondances CIDR non exactes (pas /32) • Correspondances inverses
S'applique à	Indique si cette limite s'applique aux demandes de lecture client (GET ou HEAD) ou aux demandes d'écriture (PUT, POST ou DELETE).
Valeur	Valeur à laquelle le trafic réseau sera limité, en fonction de l'unité sélectionnée. Par exemple, entrez 10 et sélectionnez MIB/s pour empêcher le trafic réseau correspondant à cette règle de dépasser 10 Mio/s. **Remarque** : selon le réglage des unités, les unités disponibles seront soit binaires (par exemple, Gio), soit décimales (par exemple, GB). Pour modifier le paramètre unités, sélectionnez la liste déroulante utilisateur dans le coin supérieur droit du Gestionnaire de grille, puis sélectionnez **Préférences utilisateur**.

Champ	Description
Unité	Unité qui décrit la valeur que vous avez saisie.

Par exemple, si vous souhaitez créer une limite de bande passante de 40 Gbit/s pour un niveau SLA, créez deux limites de bande passante agrégée : GET/HEAD à 40 Gbit/s et PUT/POST/DELETE à 40 Gbit/s.

6. Sélectionnez **Continuer**.
7. Lisez et passez en revue la politique de classification du trafic. Utilisez le bouton **Précédent** pour revenir en arrière et apporter les modifications nécessaires. Lorsque vous êtes satisfait de la stratégie, sélectionnez **Enregistrer et continuer**.

   Le trafic des clients S3 et Swift est désormais géré conformément à la règle de classification du trafic.

Une fois que vous avez terminé

"Afficher les données de trafic réseau" pour vérifier que les stratégies appliquent les limites de trafic que vous attendez.

Modifier la stratégie de classification du trafic

Vous pouvez modifier une stratégie de classification de trafic pour modifier son nom ou sa description, ou pour créer, modifier ou supprimer des règles ou des limites de la stratégie.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous disposez de l'autorisation d'accès racine.

Étapes

1. Sélectionnez **CONFIGURATION** > **réseau** > **classification du trafic**.

   La page règles de classification du trafic s'affiche et les stratégies existantes sont répertoriées dans un tableau.

2. Modifiez la stratégie à l'aide du menu actions ou de la page de détails. Voir "créez des stratégies de classification du trafic" pour quoi participer.

   Menu actions

   a. Cochez la case correspondant à la règle.

   b. Sélectionnez **actions** > **Modifier**.

   Page de détails

   a. Sélectionnez le nom de la stratégie.

   b. Sélectionnez le bouton **Modifier** en regard du nom de la stratégie.

3. Pour l'étape entrer le nom de la stratégie, modifiez éventuellement le nom ou la description de la stratégie et sélectionnez **Continuer**.

4. Pour l'étape Ajouter des règles de correspondance, ajoutez éventuellement une règle ou modifiez **Type** et **valeur de correspondance** de la règle existante, puis sélectionnez **Continuer**.
5. Pour l'étape définir les limites, ajoutez, modifiez ou supprimez une limite, et sélectionnez **Continuer**.
6. Consultez la stratégie mise à jour et sélectionnez **Enregistrer et continuer**.

   Les modifications apportées à la stratégie sont enregistrées et le trafic réseau est désormais géré conformément aux règles de classification du trafic. Vous pouvez afficher les diagrammes de trafic et vérifier que les stratégies appliquent les limites de trafic auxquelles vous vous attendez.

Supprimer une règle de classification du trafic

Vous pouvez supprimer une stratégie de classification du trafic si vous n'en avez plus besoin. Assurez-vous de supprimer la stratégie appropriée car une stratégie ne peut pas être récupérée lorsqu'elle est supprimée.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous disposez de l'autorisation d'accès racine.

Étapes

1. Sélectionnez **CONFIGURATION** > **réseau** > **classification du trafic**.

   La page stratégies de classification du trafic s'affiche avec les stratégies existantes répertoriées dans un tableau.

2. Supprimez la stratégie à l'aide du menu actions ou de la page de détails.

   Menu actions

   a. Cochez la case correspondant à la règle.
   b. Sélectionnez **actions** > **Supprimer**.

   Page de détails de la police

   a. Sélectionnez le nom de la stratégie.
   b. Sélectionnez le bouton **Supprimer** en regard du nom de la stratégie.

3. Sélectionnez **Oui** pour confirmer que vous souhaitez supprimer la stratégie.

   La stratégie est supprimée.

Afficher les données de trafic réseau

Vous pouvez surveiller le trafic réseau en affichant les graphiques disponibles à partir de la page stratégies de classification du trafic.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous disposez de l'autorisation d'accès racine ou des droits d'accès aux comptes de tenant.

Description de la tâche

Pour toute règle de classification de trafic existante, vous pouvez afficher les mesures du service d'équilibrage de charge pour déterminer si la règle limite avec succès le trafic sur le réseau. Les données des graphiques peuvent vous aider à déterminer si vous devez ajuster la règle.

Même si aucune limite n'est définie pour une stratégie de classification du trafic, des mesures sont recueillies et les graphiques fournissent des informations utiles pour comprendre les tendances du trafic.

Étapes

1. Sélectionnez **CONFIGURATION** > **réseau** > **classification du trafic**.

   La page règles de classification du trafic s'affiche et les stratégies existantes sont répertoriées dans le tableau.

2. Sélectionnez le nom de la stratégie de classification de trafic pour laquelle vous souhaitez afficher les mesures.
3. Sélectionnez l'onglet **Metrics**.

   Les graphiques de stratégie de classification du trafic s'affichent. Les graphiques affichent des mesures uniquement pour le trafic correspondant à la stratégie sélectionnée.

   Les graphiques suivants sont inclus sur la page.

   - Taux de demande : ce graphique indique la quantité de bande passante correspondant à cette règle gérée par tous les équilibreurs de charge. Les données reçues incluent les en-têtes de demande pour toutes les demandes et la taille des données de corps pour les réponses qui ont des données de corps. Envoyé inclut les en-têtes de réponse pour toutes les demandes et la taille des données du corps de réponse pour les demandes qui incluent des données du corps dans la réponse.

     > Lorsque les demandes sont terminées, ce graphique indique uniquement l'utilisation de la bande passante. Pour les demandes d'objets lents ou volumineux, la bande passante instantanée réelle peut différer des valeurs indiquées dans ce graphique.

   - Taux de réponse aux erreurs : ce graphique fournit une fréquence approximative à laquelle les demandes correspondant à cette stratégie renvoient des erreurs (code d'état HTTP >= 400) aux clients.
   - Durée moyenne des demandes (sans erreur) : ce graphique fournit une durée moyenne des demandes réussies correspondant à cette stratégie.
   - Utilisation de la bande passante de la règle : ce graphique indique la quantité de bande passante correspondant à cette règle gérée par tous les équilibreurs de charge. Les données reçues incluent les en-têtes de demande pour toutes les demandes et la taille des données de corps pour les réponses qui ont des données de corps. Envoyé inclut les en-têtes de réponse pour toutes les demandes et la taille des données du corps de réponse pour les demandes qui incluent des données du corps dans la réponse.
4. Placez le curseur sur un graphique linéaire pour afficher une fenêtre contextuelle de valeurs sur une partie spécifique du graphique.
5. Sélectionnez **Grasana Dashboard** juste en dessous du titre Metrics pour afficher tous les graphiques d'une police. En plus des quatre graphiques de l'onglet **Metrics**, vous pouvez afficher deux autres graphiques :

   - Taux de demande d'écriture par taille d'objet : taux pour les demandes PUT/POST/DELETE correspondant à cette règle. Le positionnement sur une cellule individuelle affiche des débits par

seconde. Les taux affichés dans la vue de survol sont tronqués aux nombres entiers et peuvent indiquer 0 lorsqu'il y a des demandes non nulles dans le compartiment.

- Taux de demande de lecture par taille d'objet : taux des demandes GET/HEAD correspondant à cette règle. Le positionnement sur une cellule individuelle affiche des débits par seconde. Les taux affichés dans la vue de survol sont tronqués aux nombres entiers et peuvent indiquer 0 lorsqu'il y a des demandes non nulles dans le compartiment.

6. Vous pouvez également accéder aux graphiques à partir du menu **SUPPORT**.
   a. Sélectionnez **SUPPORT** > **Outils** > **métriques**.
   b. Sélectionnez **politique de classification du trafic** dans la section **Grafana**.
   c. Sélectionnez la stratégie dans le menu en haut à gauche de la page.
   d. Placez le curseur sur un graphique pour afficher une fenêtre contextuelle indiquant la date et l'heure de l'échantillon, les tailles d'objet agrégées dans le nombre et le nombre de demandes par seconde pendant cette période.

      Les politiques de classification du trafic sont identifiées par leur ID. Les ID de stratégie sont répertoriés sur la page règles de classification de trafic.

7. Analysez les graphiques pour déterminer à quelle fréquence la stratégie limite le trafic et si vous devez ajuster la stratégie.

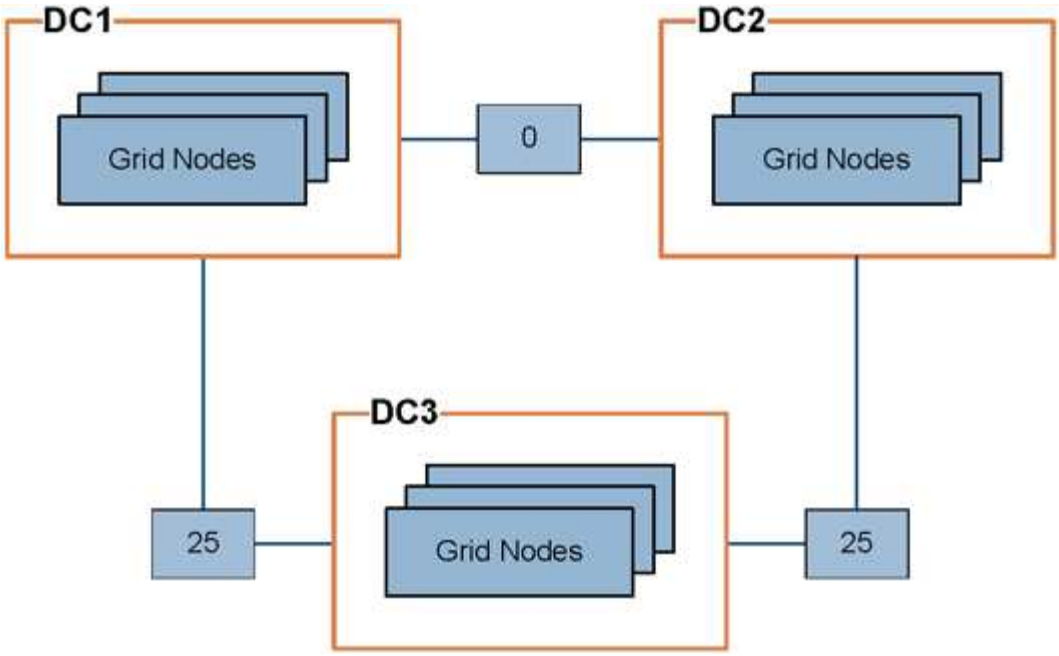
Gérer les coûts de liaison

Les coûts de liaison vous permettent de définir la priorité du site de data Center qui fournit un service demandé lorsqu'au moins deux sites de data Center existent. Vous pouvez ajuster les coûts de liaison pour refléter la latence entre les sites.

Quels sont les coûts de liaison ?

- Les coûts des liens permettent de classer par ordre de priorité la copie d'objet utilisée pour les récupérations d'objets.
- Les coûts des liaisons sont utilisés par l'API de gestion du grid et l'API de gestion des locataires pour déterminer quels services StorageGRID internes utiliser.
- Les coûts de liaison sont utilisés par le service Load Balancer sur les nœuds d'administration et les nœuds de passerelle pour diriger les connexions client. Voir "Considérations relatives à l'équilibrage de charge".

Le schéma présente une grille de trois sites avec des coûts de liaison configurés entre les sites :



- Le service Load Balancer sur les nœuds d'administration et les nœuds de passerelle répartit uniformément les connexions client vers tous les nœuds de stockage sur le même site de data Center et vers tous les sites de data Center, avec un coût de liaison de 0.

  Dans l'exemple, un nœud passerelle du site de data Center 1 (DC1) distribue également les connexions client aux nœuds de stockage du DC1 et aux nœuds de stockage du DC2. Un nœud de passerelle du DC3 envoie des connexions client uniquement aux nœuds de stockage du DC3.

- Lors de la récupération d'un objet existant sous forme de plusieurs copies répliquées, StorageGRID récupère la copie au niveau du data Center présentant le coût de liaison le plus faible.

  Dans cet exemple, si une application client sur DC2 récupère un objet stocké à la fois sur DC1 et DC3, l'objet est récupéré de DC1, car le coût de la liaison de DC1 à DC2 est 0, ce qui est inférieur au coût de la liaison de DC3 à DC2 (25).

Les coûts de liaison sont des nombres relatifs arbitraires sans unité de mesure spécifique. Par exemple, un coût de lien de 50 est utilisé de manière moins préférentielle qu'un coût de lien de 25. Le tableau indique les coûts de liaison couramment utilisés.

Lien	Coût des liens	Remarques
Entre les sites de data centers physiques	25 (par défaut)	Data centers connectés par une liaison WAN.
Entre des sites de data centers logiques au même emplacement physique	0	Data centers logiques dans le même bâtiment physique ou campus connecté par un réseau LAN.

Mettre à jour les coûts des liens

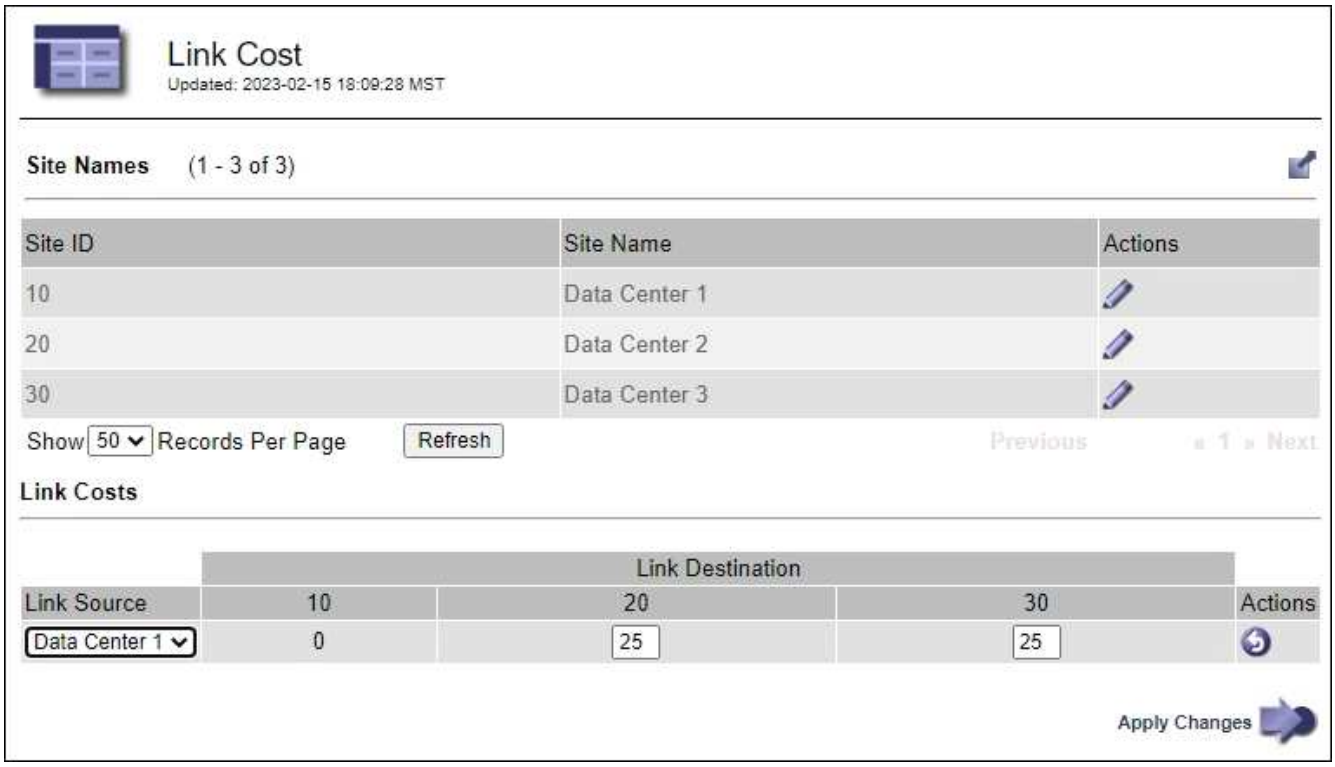
Vous pouvez mettre à jour les coûts de liaison entre les sites de data Center afin de refléter la latence entre les sites.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous avez le "Autorisation de configuration de la page de topologie de grille".

Étapes

1. Sélectionnez **SUPPORT** > **autre** > **coût du lien**.



2. Sélectionnez un site sous **Link Source** et entrez une valeur de coût comprise entre 0 et 100 sous **Link destination**.

   Vous ne pouvez pas modifier le coût du lien si la source est identique à la destination.

   Pour annuler les modifications, sélectionnez **Retour**.

3. Sélectionnez **appliquer les modifications**.

Utiliser AutoSupport

Utilisez AutoSupport : présentation

La fonctionnalité AutoSupport permet à votre système StorageGRID d'envoyer des messages d'état et d'état au support technique.

L'utilisation de AutoSupport peut considérablement accélérer l'identification et la résolution des problèmes. Le support technique peut également surveiller les besoins en stockage de votre système et vous aider à déterminer si vous devez ajouter de nouveaux nœuds ou sites. Vous pouvez également configurer l'envoi des messages AutoSupport à une destination supplémentaire.

Vous devez configurer StorageGRID AutoSupport uniquement sur le nœud d'administration principal. Toutefois, vous devez configurer AutoSupport matériel sur chaque appareil.

Informations incluses dans les messages AutoSupport

Les messages AutoSupport incluent des informations telles que :

- Version du logiciel StorageGRID
- Version du système d'exploitation
- Informations sur les attributs au niveau du système et de l'emplacement
- Alertes et alarmes récentes (système hérité)
- État actuel de toutes les tâches de la grille, y compris les données historiques
- Utilisation de la base de données du nœud d'administration
- Nombre d'objets perdus ou manquants
- Paramètres de configuration de la grille
- Entités NMS
- Règle ILM active
- Fichier de spécification de grille provisionné
- Les mesures de diagnostic

Vous pouvez activer la fonctionnalité AutoSupport et les options AutoSupport individuelles lors de la première installation de StorageGRID, ou vous pouvez les activer ultérieurement. Si AutoSupport n'est pas activé, un message s'affiche sur le tableau de bord du Gestionnaire de grille. Le message inclut un lien vers la page de configuration de AutoSupport.

Si vous fermez le message, il n'apparaîtra plus tant que le cache de votre navigateur n'aura pas été effacé, même si AutoSupport reste désactivé.

Qu'est-ce que Digital Advisor ?

Digital Advisor est une solution cloud qui exploite l'analytique prédictive et les connaissances de la communauté issues de la base installée de NetApp. Les évaluations continues des risques, les alertes prédictives, les conseils normatifs et les actions automatisées vous aident à anticiper les problèmes, ce qui permet d'améliorer l'état et la disponibilité du système.

Vous devez activer AutoSupport si vous souhaitez utiliser les tableaux de bord et les fonctionnalités de Digital Advisor sur le site de support NetApp.

"Documentation Digital Advisor"

Protocoles pour l'envoi des messages AutoSupport

Vous pouvez choisir l'un des trois protocoles pour l'envoi des messages AutoSupport :

- HTTPS
- HTTP

- SMTP

Si vous utilisez SMTP comme protocole pour les messages AutoSupport, vous devez configurer un serveur de messagerie SMTP.

Options AutoSupport

Toutes les combinaisons d'options suivantes vous permettent d'envoyer des messages AutoSupport au support technique :

- **Hebdomadaire**: Envoyer automatiquement des messages AutoSupport une fois par semaine. Paramètre par défaut : activé.
- **Event-déclenché** : envoie automatiquement des messages AutoSupport toutes les heures ou lorsque des événements système importants se produisent. Paramètre par défaut : activé.
- **On Demand**: Laissez le support technique demander à votre système StorageGRID d'envoyer automatiquement des messages AutoSupport, ce qui est utile lorsqu'ils travaillent activement en cas de problème (nécessite le protocole de transmission HTTPS AutoSupport). Paramètre par défaut : Désactivé.
- **Déclenché par l'utilisateur** : envoyez manuellement des messages AutoSupport à tout moment.

AutoSupport pour appliances

AutoSupport for Appliances signale les problèmes liés au matériel StorageGRID, tandis que StorageGRID AutoSupport signale les problèmes liés au logiciel StorageGRID (sauf pour SGF6112, où StorageGRID AutoSupport signale les problèmes matériels et logiciels). Vous devez configurer AutoSupport sur chaque appliance, à l'exception du SGF6112 qui ne nécessite pas de configuration supplémentaire. AutoSupport est implémenté différemment pour les services et les appliances de stockage.

Vous devez activer AutoSupport dans SANtricity pour chaque appliance de stockage. Vous pouvez configurer SANtricity AutoSupport lors de la configuration initiale de l'appliance ou après l'installation d'une appliance :

- Pour les appliances SG6000 et SG5700 "Configurez AutoSupport dans SANtricity System Manager"

Les messages AutoSupport des appliances E-Series peuvent être inclus dans StorageGRID AutoSupport si vous configurez la livraison AutoSupport par proxy dans "SANtricity System Manager".

StorageGRID AutoSupport ne signale pas de problèmes matériels, tels que des pannes de module DIMM ou de carte d'interface hôte (HIC). Cependant, certaines défaillances de composant peuvent se déclencher "alertes matérielles". Pour les appliances StorageGRID dotées d'un contrôleur BMC (Baseboard Management Controller), comme SG100, SG1000, SG6060 ou SGF6024, vous pouvez configurer des interruptions SNMP et e-mail pour signaler des défaillances matérielles :

- "Configurez les notifications par e-mail pour les alertes"
- "Configurer les paramètres SNMP" Pour le contrôleur SG6000-CN ou les appliances de services SG100 et SG1000

Informations associées

"Support NetApp"

Configurez AutoSupport

Vous pouvez activer la fonctionnalité AutoSupport et les options AutoSupport individuelles lors de la première installation de StorageGRID, ou vous pouvez les activer

ultérieurement.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous disposez de l'autorisation d'accès racine ou d'une autre autorisation de configuration de grille.
- Si vous utilisez HTTPS pour envoyer des messages AutoSupport, vous avez fourni un accès Internet sortant au nœud d'administration principal, directement ou "utilisation d'un serveur proxy" (connexions entrantes non requises).
- Si HTTP est sélectionné sur la page StorageGRID AutoSupport, vous avez configuré un serveur proxy pour transférer les messages AutoSupport en HTTPS. Les serveurs AutoSupport de NetApp rejetteront les messages envoyés via HTTP.

  "En savoir plus sur la configuration des paramètres du proxy d'administration".

- Si vous utilisez SMTP comme protocole pour les messages AutoSupport, vous avez configuré un serveur de messagerie SMTP. La même configuration de serveur de messagerie est utilisée pour les notifications par e-mail d'alarme (système hérité).

Spécifiez le protocole des messages AutoSupport

Vous pouvez utiliser les protocoles suivants pour l'envoi des messages AutoSupport :

- **HTTPS** : il s'agit du paramètre par défaut et recommandé pour les nouvelles installations. Ce protocole utilise le port 443. Si vous le souhaitez Activez la fonction AutoSupport On Demand, Vous devez utiliser HTTPS.
- **HTTP** : si vous sélectionnez HTTP, vous devez configurer un serveur proxy pour transférer les messages AutoSupport en HTTPS. Les serveurs AutoSupport de NetApp rejettent les messages envoyés via HTTP. Ce protocole utilise le port 80.
- **SMTP**: Utilisez cette option si vous souhaitez que les messages AutoSupport soient envoyés par e-mail. Si vous utilisez SMTP comme protocole pour les messages AutoSupport, vous devez configurer un serveur de messagerie SMTP sur la page Configuration de l'e-mail héritée (**SUPPORT** > **alarmes (hérité)** > **Configuration de l'e-mail héritée**).

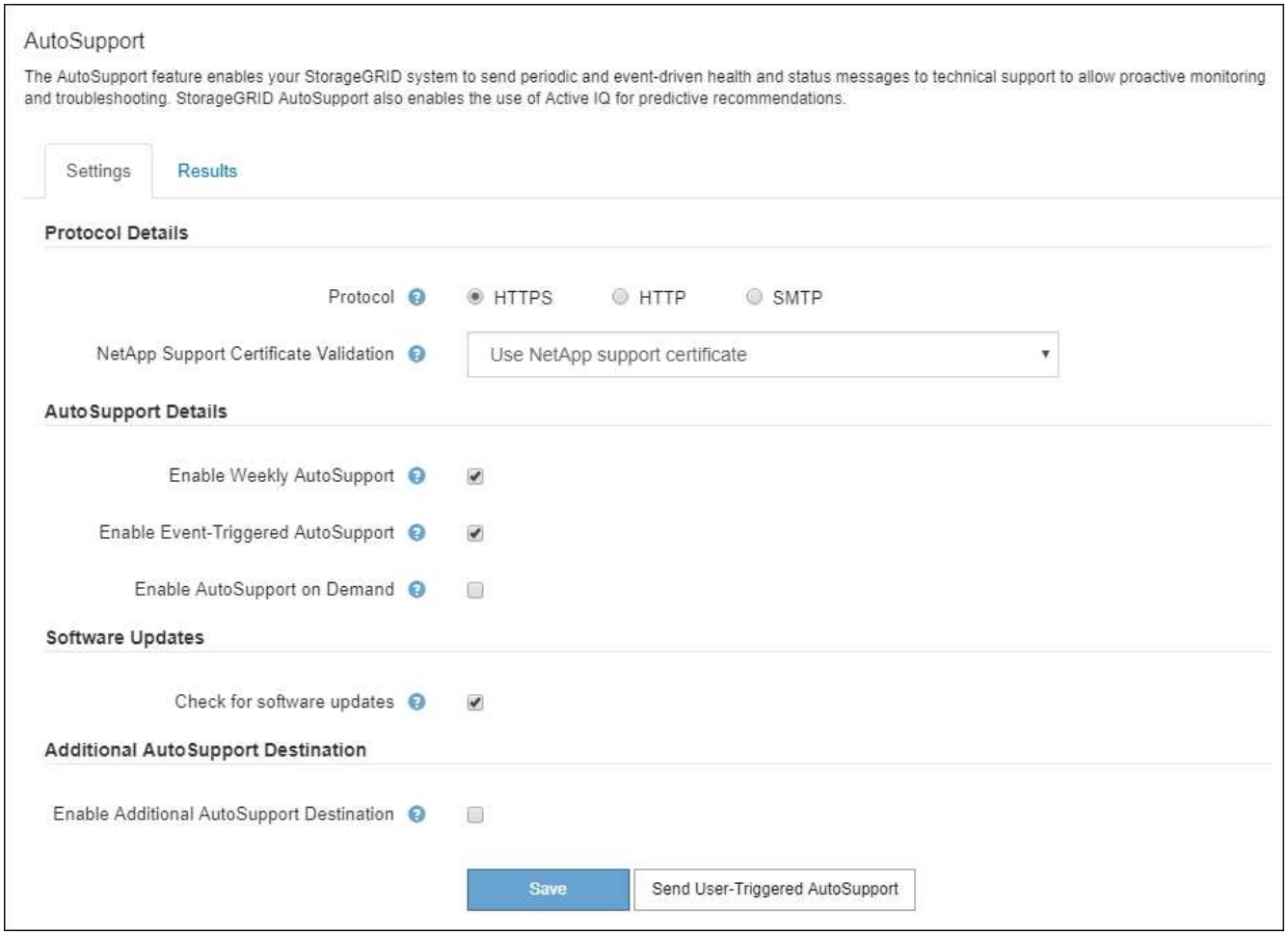
> SMTP était le seul protocole disponible pour les messages AutoSupport avant la version de StorageGRID 11.2. Si vous avez installé une version antérieure de StorageGRID au départ, SMTP est peut-être le protocole sélectionné.

Le protocole que vous définissez permet d'envoyer tous les types de messages AutoSupport.

Étapes

1. Sélectionnez **SUPPORT** > **Outils** > **AutoSupport**.

   La page AutoSupport s'affiche et l'onglet **Paramètres** est sélectionné.



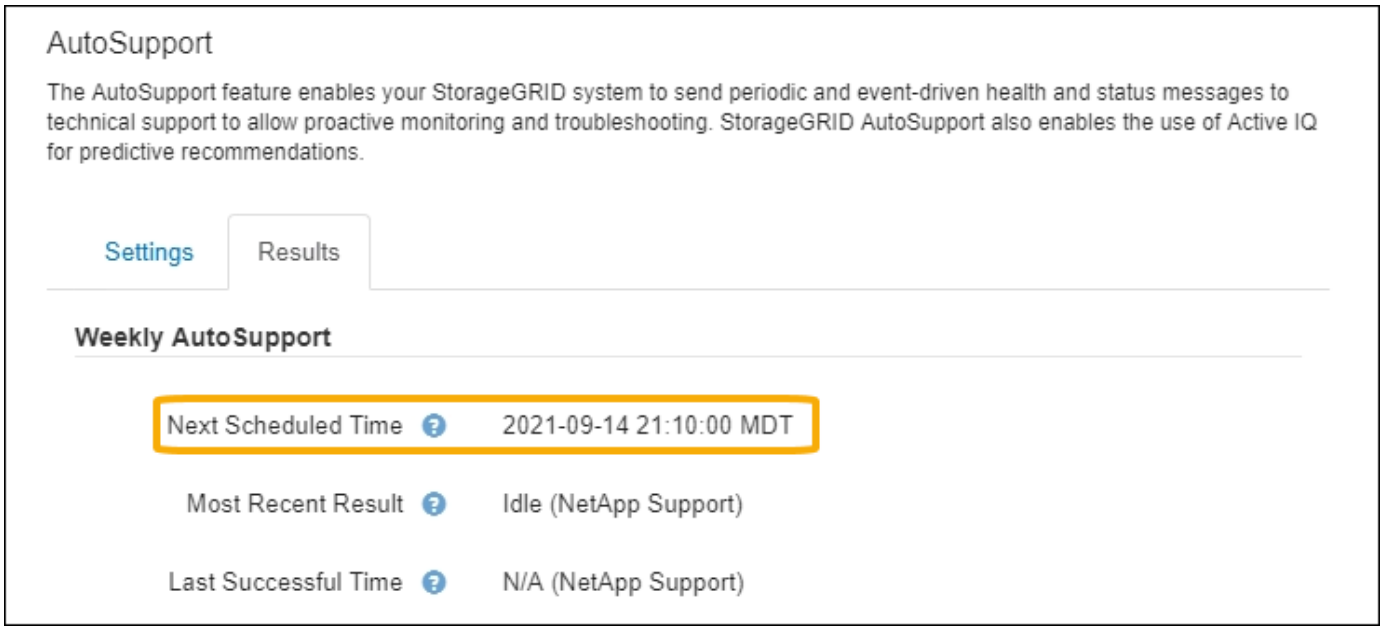
2. Sélectionnez le protocole à utiliser pour envoyer des messages AutoSupport.
3. Si vous avez sélectionné **HTTPS**, indiquez si vous souhaitez utiliser un certificat TLS pour sécuriser la connexion au serveur de support NetApp.
   - **Utiliser le certificat de support NetApp** (par défaut) : la validation du certificat permet de garantir la sécurité de la transmission des messages AutoSupport. Le certificat de support NetApp est déjà installé avec le logiciel StorageGRID.
   - **Ne pas vérifier le certificat** : sélectionnez cette option uniquement si vous avez une bonne raison de ne pas utiliser la validation de certificat, par exemple lorsqu'il y a un problème temporaire avec un certificat.
4. Sélectionnez **Enregistrer**.

   Tous les messages hebdomadaires, déclenchés par l'utilisateur et déclenchés par des événements sont envoyés à l'aide du protocole sélectionné.

Désactiver les messages AutoSupport hebdomadaires

Par défaut, le système StorageGRID est configuré pour envoyer un message AutoSupport au support NetApp une fois par semaine.

Pour déterminer quand le message AutoSupport hebdomadaire sera envoyé, accédez à l'onglet **AutoSupport** > **Résultats**. Dans la section **AutoSupport hebdomadaire**, examinez la valeur de **prochaine heure programmée**.



Vous pouvez désactiver l'envoi automatique de messages AutoSupport hebdomadaires à tout moment.

Étapes

1. Sélectionnez **SUPPORT** > **Outils** > **AutoSupport**.
2. Décochez la case **Activer AutoSupport hebdomadaire**.
3. Sélectionnez **Enregistrer**.

Désactivez les messages AutoSupport déclenchés par les événements

Par défaut, le système StorageGRID est configuré de manière à envoyer un message AutoSupport au support NetApp lorsqu'une alerte importante ou un autre événement système important se produit.

Vous pouvez désactiver à tout moment les messages AutoSupport déclenchés par les événements.

Étapes

1. Sélectionnez **SUPPORT** > **Outils** > **AutoSupport**.
2. Décochez la case **Activer AutoSupport** déclenché par un événement.
3. Sélectionnez **Enregistrer**.

Activez AutoSupport on Demand

AutoSupport On Demand peut vous aider à résoudre les problèmes sur lesquels le support technique travaille activement.

AutoSupport On Demand est désactivé par défaut. L'activation de cette fonction permet au support technique de demander à votre système StorageGRID d'envoyer automatiquement des messages AutoSupport. Le support technique peut également définir l'intervalle d'interrogation pour les requêtes AutoSupport On Demand.

Le support technique ne peut ni activer ni désactiver AutoSupport On Demand.

Étapes

1. Sélectionnez **SUPPORT** > **Outils** > **AutoSupport**.

2. Sélectionnez le **HTTPS** pour le protocole.
3. Cochez la case **Activer AutoSupport hebdomadaire**.
4. Cochez la case **Activer AutoSupport On Demand**.
5. Sélectionnez **Enregistrer**.

   AutoSupport On Demand est activé et le support technique peut envoyer des demandes AutoSupport On Demand à StorageGRID.

Désactive les vérifications des mises à jour logicielles

Par défaut, StorageGRID contacte NetApp pour déterminer si des mises à jour logicielles sont disponibles pour votre système. Si un correctif StorageGRID ou une nouvelle version est disponible, la nouvelle version s'affiche sur la page mise à niveau StorageGRID.

Si nécessaire, vous pouvez éventuellement désactiver la vérification des mises à jour logicielles. Par exemple, si votre système ne dispose pas d'un accès WAN, vous devez désactiver la vérification pour éviter les erreurs de téléchargement.

Étapes

1. Sélectionnez **SUPPORT** > **Outils** > **AutoSupport**.
2. Décochez la case **Rechercher les mises à jour logicielles**.
3. Sélectionnez **Enregistrer**.

Ajouter une destination AutoSupport supplémentaire

Lorsque vous activez AutoSupport, des messages d'état et d'état sont envoyés au support NetApp. Vous pouvez indiquer une destination supplémentaire pour tous les messages AutoSupport.

Pour vérifier ou modifier le protocole utilisé pour envoyer des messages AutoSupport, reportez-vous aux instructions à Spécifiez le protocole des messages AutoSupport.

> Vous ne pouvez pas utiliser le protocole SMTP pour envoyer des messages AutoSupport à une destination supplémentaire.

Étapes

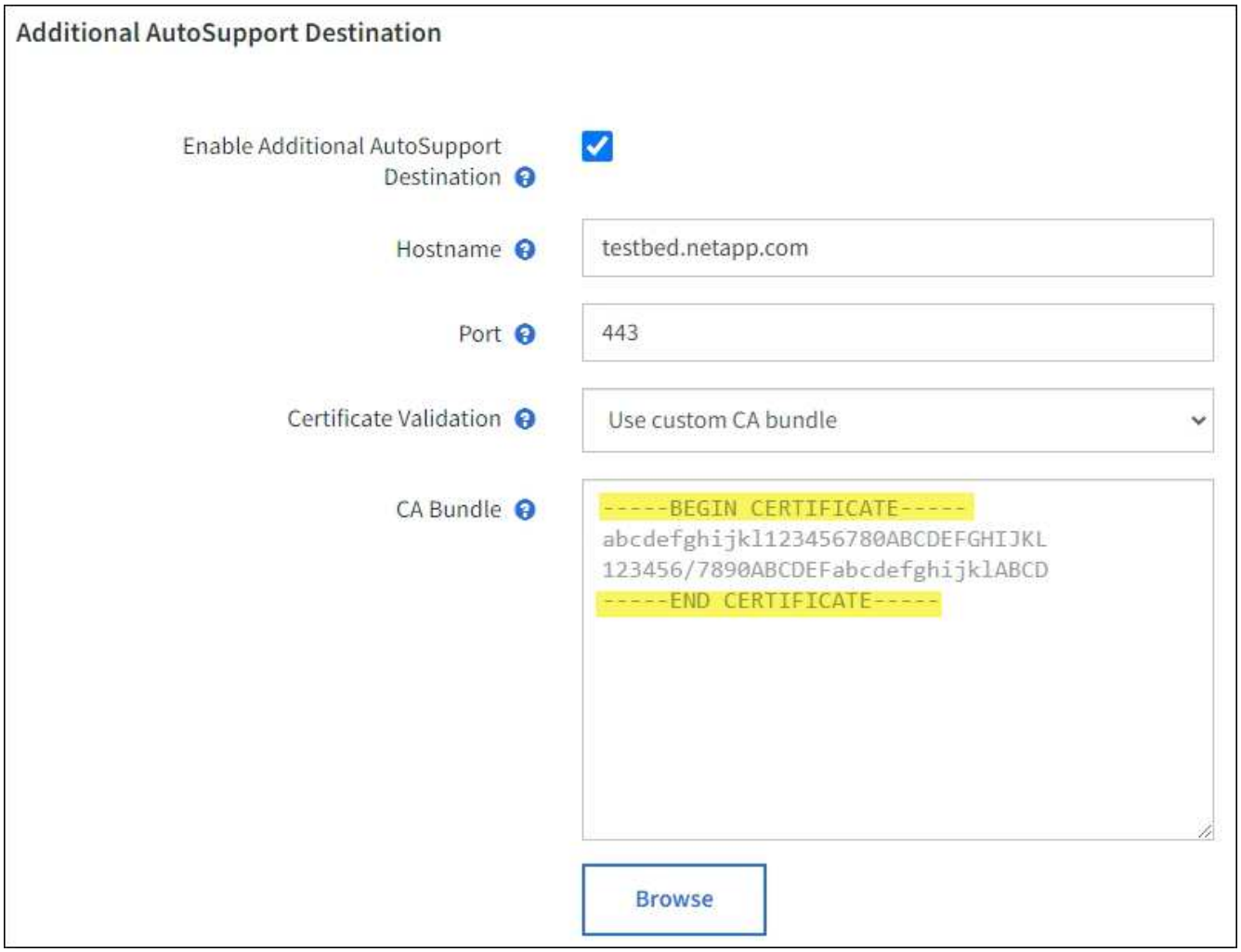
1. Sélectionnez **SUPPORT** > **Outils** > **AutoSupport**.
2. Sélectionnez **Activer la destination AutoSupport supplémentaire**.
3. Spécifiez les éléments suivants :

Champ	Description
Nom d'hôte	Nom d'hôte ou adresse IP du serveur d'un serveur de destination AutoSupport supplémentaire. **Remarque** : vous ne pouvez entrer qu'une seule destination supplémentaire.

Champ	Description
Port	Port utilisé pour se connecter à un serveur de destination AutoSupport supplémentaire. La valeur par défaut est le port 80 pour HTTP ou le port 443 pour HTTPS.
Validation de la certification	Indique si un certificat TLS est utilisé pour sécuriser la connexion à la destination supplémentaire. • Sélectionnez **ne pas vérifier le certificat** pour envoyer vos messages AutoSupport sans validation de certificat. Sélectionnez cette option uniquement si vous avez une bonne raison de ne pas utiliser la validation de certificat, par exemple en cas de problème temporaire avec un certificat. • Sélectionnez **utiliser un paquet CA personnalisé** pour utiliser la validation de certificat.

4. Si vous avez sélectionné **utiliser un paquet CA personnalisé**, effectuez l'une des opérations suivantes :
   - Sélectionnez **Parcourir**, naviguez jusqu'au fichier contenant les certificats, puis sélectionnez **Ouvrir** pour télécharger le fichier.
   - Utilisez un outil d'édition pour copier et coller tout le contenu de chacun des fichiers de certificat CA codés au PEM dans le champ **CA Bundle**, concaténé dans l'ordre de la chaîne de certificats.

     Vous devez inclure `----BEGIN CERTIFICATE----` et `----END CERTIFICATE----` dans votre sélection.



5. Sélectionnez **Enregistrer**.

   Tous les futurs messages AutoSupport hebdomadaires, déclenchés par les événements et déclenchés par l'utilisateur seront envoyés à la destination supplémentaire.

Déclencher manuellement un message AutoSupport

Pour aider le support technique à résoudre les problèmes liés à votre système StorageGRID, vous pouvez déclencher manuellement un message AutoSupport à envoyer.

Avant de commencer

- Vous devez être connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous devez disposer de l'accès racine ou d'une autre autorisation de configuration de grille.

Étapes

1. Sélectionnez **SUPPORT** > **Outils** > **AutoSupport**.
2. Dans l'onglet **Paramètres**, sélectionnez **Envoyer AutoSupport** déclenché par l'utilisateur.

   StorageGRID tente d'envoyer un message AutoSupport au support technique. Si la tentative réussit, les valeurs **résultat le plus récent** et **dernier temps** réussi dans l'onglet **Résultats** sont mises à jour. En cas de problème, la valeur **résultat** la plus récente est mise à jour sur "échec" et StorageGRID n'essaie pas

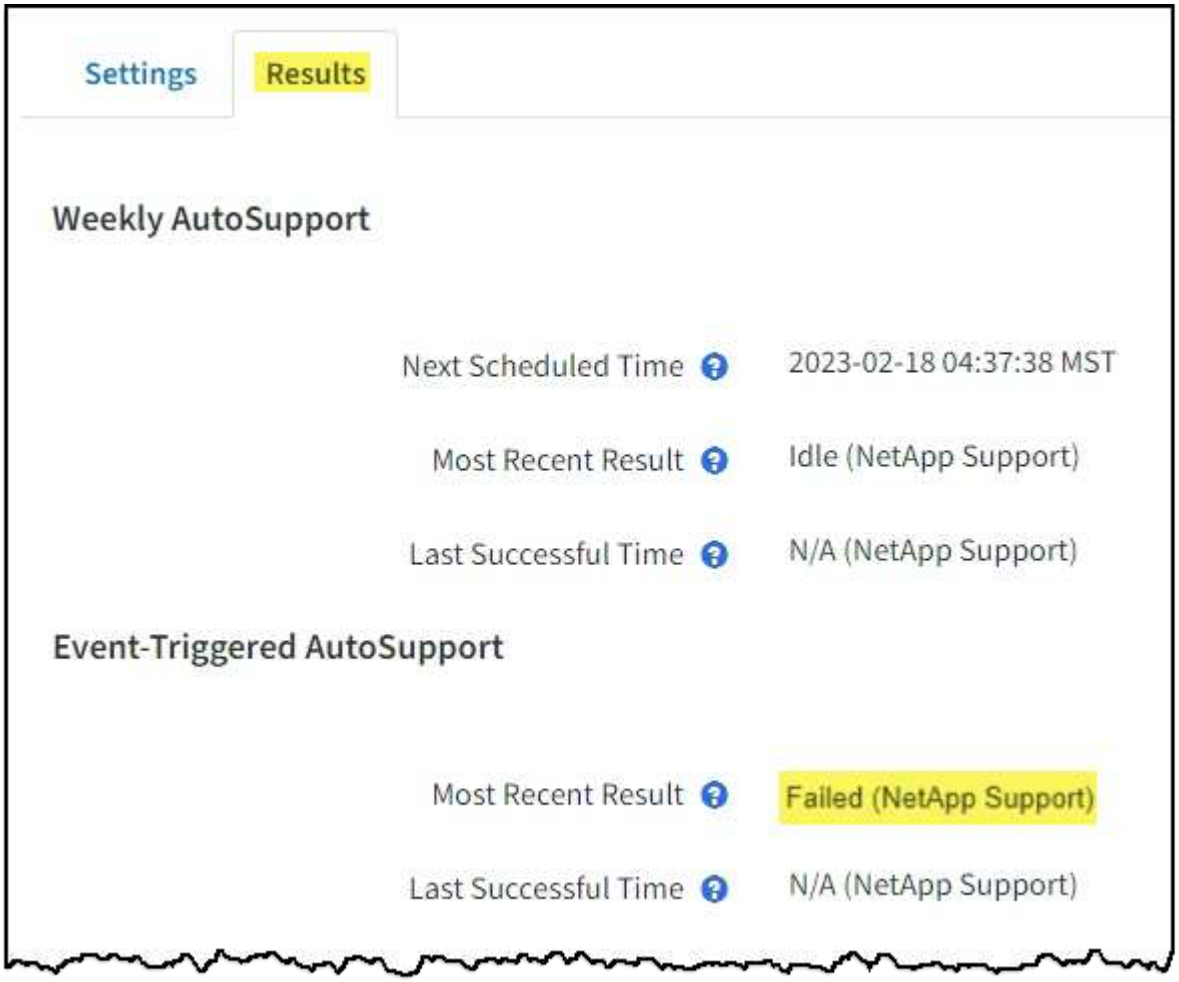
d’envoyer à nouveau le message AutoSupport.

> Après avoir envoyé un message AutoSupport déclenché par l’utilisateur, actualisez la page AutoSupport de votre navigateur après 1 minute pour accéder aux résultats les plus récents.

Dépanner les messages AutoSupport

Si la tentative d’envoi d’un message AutoSupport échoue, le système StorageGRID effectue différentes actions en fonction du type de message AutoSupport. Vous pouvez vérifier l’état des messages AutoSupport en sélectionnant **SUPPORT** > **Outils** > **AutoSupport** > **Résultats**.

Lorsque le message AutoSupport ne parvient pas à envoyer, ""FAILED"" s’affiche dans l’onglet **Résultats** de la page **AutoSupport**.



> Si vous avez configuré un serveur proxy pour transférer les messages AutoSupport à NetApp, vous devez le faire "vérifiez que les paramètres de configuration du serveur proxy sont corrects".

Échec hebdomadaire du message AutoSupport

Si un message AutoSupport hebdomadaire ne parvient pas à s’envoyer, le système StorageGRID prend les actions suivantes :

1. Met à jour l'attribut de résultat le plus récent pour réessayer.
2. Tente de renvoyer le message AutoSupport 15 fois toutes les quatre minutes pendant une heure.
3. Après une heure d'échec d'envoi, met à jour l'attribut de résultat le plus récent sur échec.
4. Tente à nouveau d'envoyer un message AutoSupport à l'heure programmée suivante.
5. Maintient le programme AutoSupport normal si le message échoue parce que le service NMS n'est pas disponible et si un message est envoyé avant sept jours.
6. Lorsque le service NMS est de nouveau disponible, envoie immédiatement un message AutoSupport si aucun message n'a été envoyé pendant sept jours ou plus.

Échec du message AutoSupport déclenché par l'utilisateur ou déclenché par un événement

Si l'envoi d'un message AutoSupport déclenché par l'utilisateur ou un événement ne parvient pas à s'effectuer, le système StorageGRID prend les actions suivantes :

1. Affiche un message d'erreur si l'erreur est connue. Par exemple, si un utilisateur sélectionne le protocole SMTP sans fournir les paramètres de configuration corrects de la messagerie, l'erreur suivante s'affiche : `AutoSupport messages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`
2. Ne tente pas d'envoyer le message à nouveau.
3. Consigne l'erreur dans `nms.log`.

En cas d'échec et si SMTP est le protocole sélectionné, vérifiez que le serveur de messagerie du système StorageGRID est correctement configuré et que votre serveur de messagerie est en cours d'exécution (**SUPPORT** > **alarmes (hérité)** > **> Configuration de l'e-mail héritée**). Le message d'erreur suivant peut apparaître sur la page AutoSupport : `AutoSupport messages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`

Découvrez comment "configurer les paramètres du serveur de messagerie".

Corrigez l'échec d'un message AutoSupport

En cas d'échec et si SMTP est le protocole sélectionné, vérifiez que le serveur de messagerie du système StorageGRID est correctement configuré et que votre serveur de messagerie est en cours d'exécution. Le message d'erreur suivant peut apparaître sur la page AutoSupport : `AutoSupport messages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`

Envoyez des messages AutoSupport E-Series via StorageGRID

Vous pouvez envoyer des messages AutoSupport E-Series SANtricity System Manager au support technique par l'intermédiaire d'un nœud d'administration StorageGRID plutôt que du port de gestion de l'appliance de stockage.

Voir "Matériel E-Series AutoSupport" Pour en savoir plus sur l'utilisation de AutoSupport avec les appliances E-Series.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous disposez de l'autorisation d'administrateur de l'appliance de stockage ou de l'autorisation d'accès racine.

- Vous avez configuré SANtricity AutoSupport :
  - Pour les appliances SG6000 et SG5700 "Configurez AutoSupport dans SANtricity System Manager"

> Vous devez disposer d'un firmware SANtricity 8.70 ou supérieur pour accéder à SANtricity System Manager à l'aide de Grid Manager.

Description de la tâche

Les messages AutoSupport E-Series contiennent des informations détaillées sur le matériel de stockage. Ils sont plus spécifiques que les autres messages AutoSupport envoyés par le système StorageGRID.

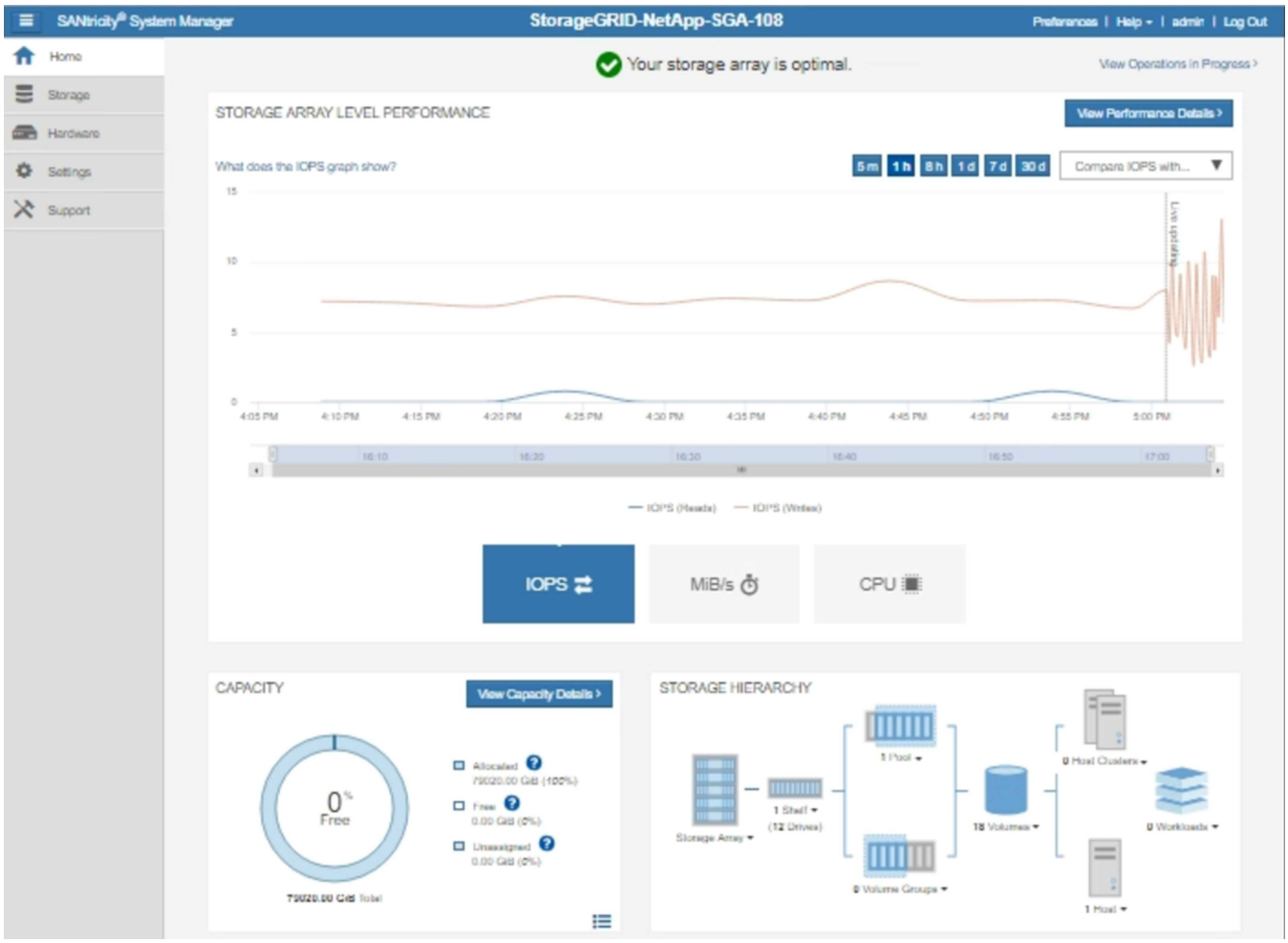
Vous pouvez configurer une adresse de serveur proxy spéciale dans le Gestionnaire système SANtricity pour transmettre des messages AutoSupport via un nœud d'administration StorageGRID sans utiliser le port de gestion de l'appliance. Les messages AutoSupport transmis de cette façon sont envoyés par le "Nœud d'administration de l'expéditeur préféré", et ils utilisent n'importe quel "Paramètres du proxy d'administration" Qui ont été configurés dans le Gestionnaire de grille.

> Cette procédure permet uniquement de configurer un serveur proxy StorageGRID pour les messages AutoSupport E-Series. Pour en savoir plus sur la configuration des baies E-Series AutoSupport, consultez le "Documentation NetApp E-Series et SANtricity".

Étapes

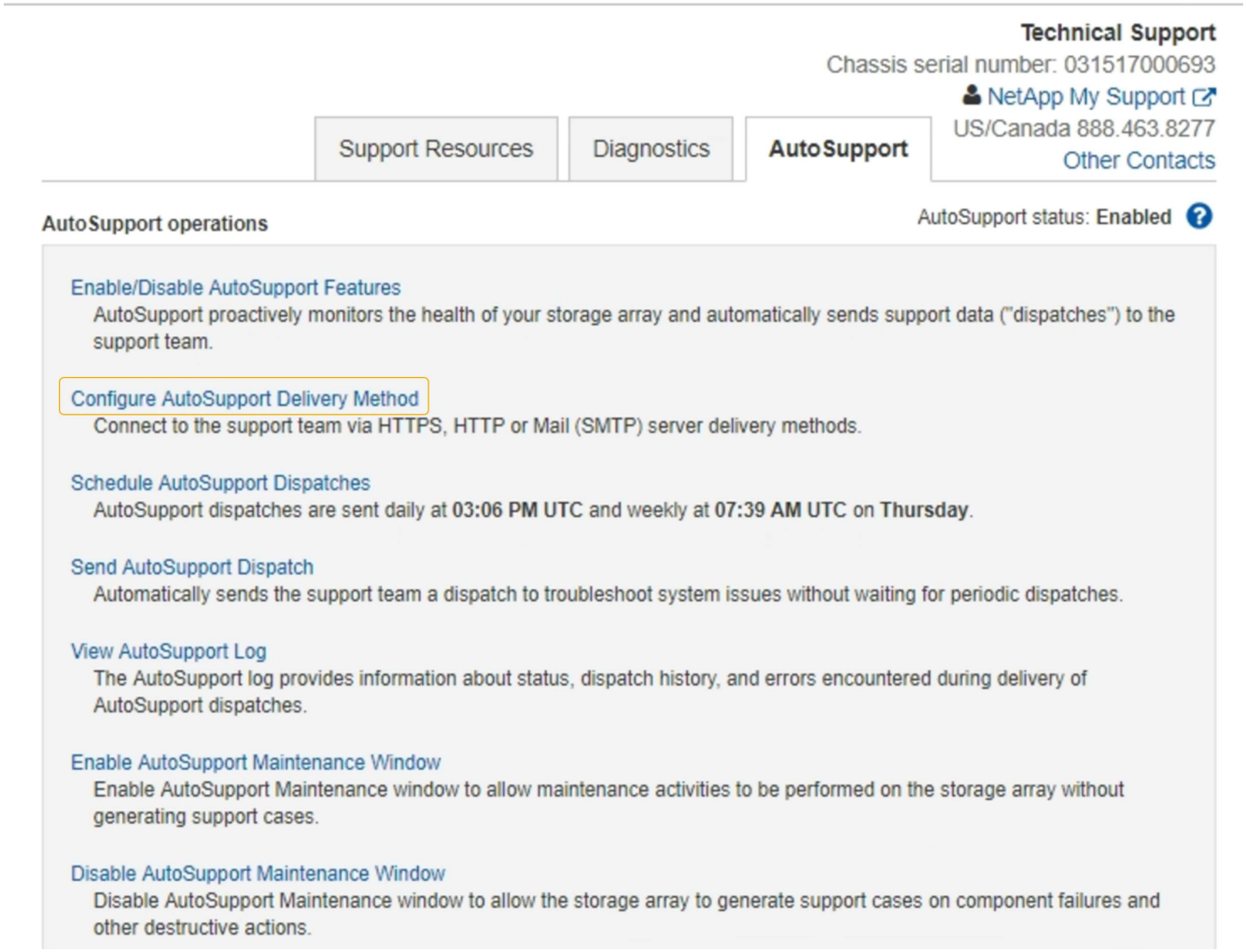
1. Dans le Gestionnaire de grille, sélectionnez **NOEUDS**.
2. Dans la liste des nœuds de gauche, sélectionnez le nœud d'appliance de stockage à configurer.
3. Sélectionnez **SANtricity System Manager**.

   La page d'accueil de SANtricity System Manager s'affiche.



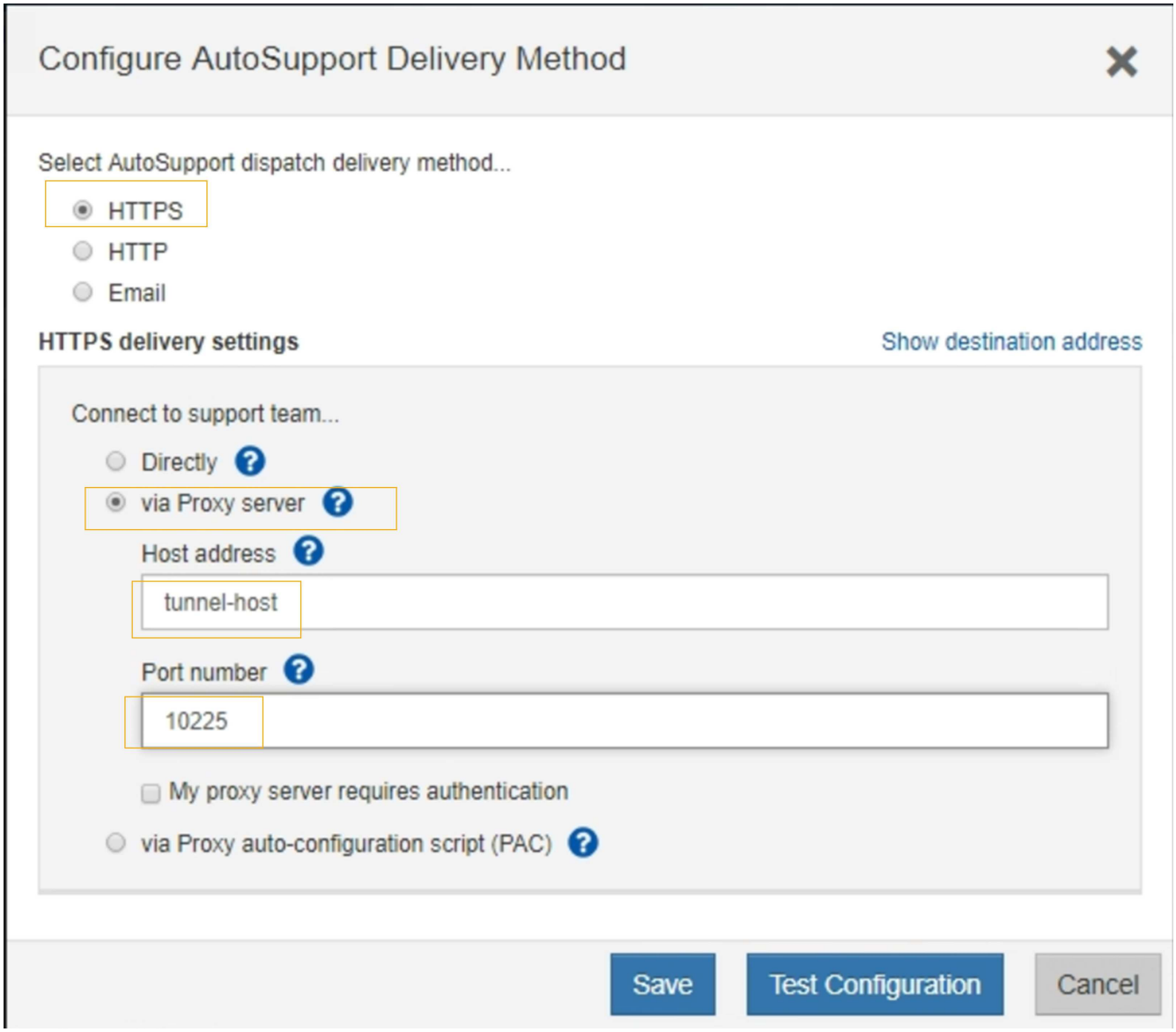
4. Sélectionnez **SUPPORT** > **support Center** > **AutoSupport**.

   La page opérations AutoSupport s'affiche.



5. Sélectionnez **configurer la méthode de livraison AutoSupport**.

   La page configurer la méthode de livraison AutoSupport s'affiche.



6. Sélectionnez **HTTPS** pour la méthode de livraison.

   Le certificat qui active HTTPS est préinstallé.

7. Sélectionnez **via le serveur proxy**.
8. Entrez `tunnel-host` Pour l'adresse **hôte**.

   `tunnel-host` Est l'adresse spéciale pour utiliser un nœud d'administration pour envoyer les messages AutoSupport E-Series.

9. Entrez `10225` Pour le **Numéro de port**.

   `10225` Numéro de port sur le serveur proxy StorageGRID qui reçoit des messages AutoSupport du contrôleur E-Series de l'appliance.

10. Sélectionnez **Tester la configuration** pour tester le routage et la configuration de votre serveur proxy AutoSupport.

    Si c'est le cas, un message apparaît dans une bannière verte : « votre configuration AutoSupport a été

vérifiée ».

Si le test échoue, un message d'erreur s'affiche dans une bannière rouge. Vérifiez vos paramètres DNS StorageGRID et la mise en réseau, assurez-vous que "Nœud d'administration de l'expéditeur préféré" Vous pouvez vous connecter au site du support NetApp et recommencer le test.

11. Sélectionnez **Enregistrer**.

    La configuration est enregistrée et un message de confirmation apparaît : « la méthode de livraison AutoSupport a été configurée ».

Gérer des nœuds de stockage

Gestion des nœuds de stockage : présentation

Des nœuds de stockage fournissent de la capacité de stockage sur disque et des services. La gestion des nœuds de stockage implique les tâches suivantes :

- Gestion des options de stockage
- Description des filigranes du volume de stockage et utilisation des filigranes pour contrôler le moment où les nœuds de stockage deviennent en lecture seule
- Contrôle et gestion de l'espace utilisé pour les métadonnées d'objet
- Configuration des paramètres globaux des objets stockés
- Application des paramètres de configuration du nœud de stockage
- Gestion des nœuds de stockage complets

Qu'est-ce qu'un nœud de stockage ?

Des nœuds de stockage gèrent et stockent les données et les métadonnées d'objets. Chaque système StorageGRID doit disposer d'au moins trois nœuds de stockage. Si vous avez plusieurs sites, chaque site de votre système StorageGRID doit également disposer de trois nœuds de stockage.

Un nœud de stockage inclut les services et les processus nécessaires pour stocker, déplacer, vérifier et récupérer les données d'objet et les métadonnées sur le disque. Vous pouvez afficher des informations détaillées sur les nœuds de stockage sur la page **NODES**.

Qu'est-ce que le service ADC ?

Le service contrôleur de domaine d'administration (ADC) authentifie les nœuds de la grille et leurs connexions entre eux. Le service ADC est hébergé sur chacun des trois premiers nœuds de stockage d'un site.

Le service ADC conserve les informations de topologie, notamment l'emplacement et la disponibilité des services. Lorsqu'un nœud de grille nécessite des informations provenant d'un autre nœud de grille ou qu'une action soit effectuée par un autre nœud de grille, il contacte un service ADC pour trouver le nœud de grille le plus adapté au traitement de sa demande. De plus, le service ADC conserve une copie des packs de configuration du déploiement StorageGRID, ce qui permet à n'importe quel nœud de la grille de récupérer les informations de configuration actuelles.vous pouvez afficher les informations ADC d'un nœud de stockage sur la page topologie de la grille (**PRISE EN CHARGE** > **topologie de la grille**).

Pour faciliter les opérations distribuées et en attente, chaque service ADC synchronise les certificats, les lots

de configuration et les informations sur les services et la topologie avec les autres services ADC du système StorageGRID.

En général, tous les nœuds de la grille maintiennent une connexion à au moins un service ADC. Les nœuds du grid accèdent ainsi aux informations les plus récentes. Lorsque les nœuds de la grille se connectent, ils mettent en cache les certificats d'autres nœuds de la grille, ce qui permet aux systèmes de continuer à fonctionner avec les nœuds de la grille connus même lorsqu'un service ADC n'est pas disponible. Les nouveaux nœuds de grille ne peuvent établir de connexions qu'à l'aide d'un service ADC.

La connexion de chaque nœud de grille permet au service ADC de collecter les informations de topologie. Ces informations sur le nœud de la grille incluent la charge CPU, l'espace disque disponible (si le système dispose de stockage), les services pris en charge et l'ID de site du nœud de la grille. D'autres services demandent au service ADC d'obtenir des informations sur la topologie par le biais de requêtes de topologie. Le service ADC répond à chaque requête avec les dernières informations reçues du système StorageGRID.

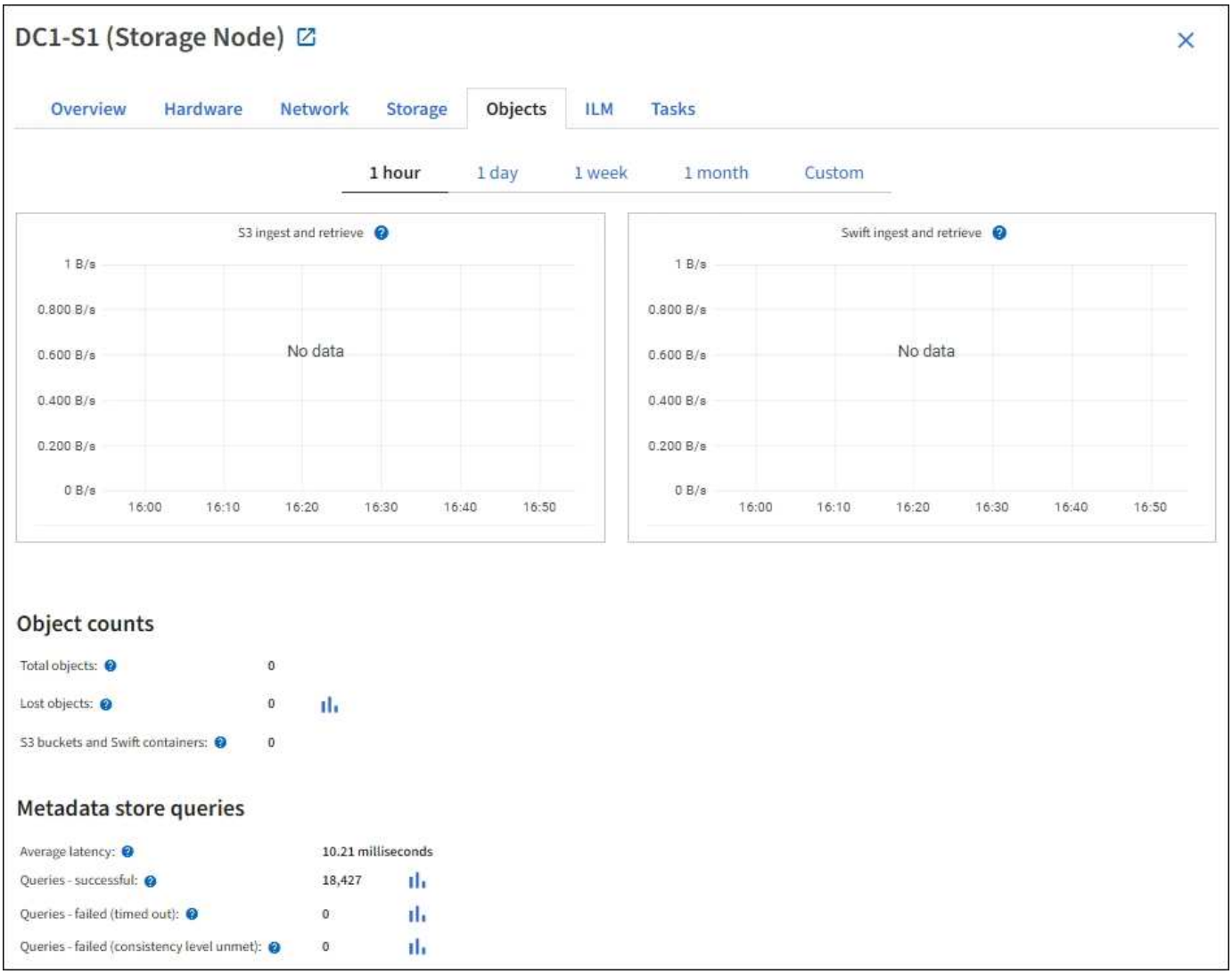
Qu'est-ce que le service DDS ?

Hébergé par un nœud de stockage, le service DDS (Distributed Data Store) s'interface avec la base de données Cassandra pour effectuer des tâches en arrière-plan sur les métadonnées d'objet stockées dans le système StorageGRID.

Nombre d'objets

Le service DDS suit le nombre total d'objets ingérés dans le système StorageGRID, ainsi que le nombre total d'objets ingérés par chacune des interfaces prises en charge par le système (S3 ou Swift).

Vous pouvez voir le nombre total d'objets sur la page nœuds > onglet objets pour n'importe quel nœud de stockage.



Requêtes

Vous pouvez identifier le temps moyen d'exécution d'une requête sur le magasin de métadonnées par le biais du service DDS spécifique, du nombre total de requêtes réussies et du nombre total de requêtes ayant échoué en raison d'un problème de délai d'attente.

Un examen des informations de requête peut être nécessaire afin de contrôler l'état du datastore Cassandra, ce qui a un impact sur les performances d'entrée et de récupération du système. Par exemple, si la latence d'une requête moyenne est lente et que le nombre de requêtes ayant échoué en raison de délais d'attente est élevé, le magasin de métadonnées peut rencontrer une charge plus élevée ou effectuer une autre opération.

Vous pouvez également afficher le nombre total de requêtes ayant échoué en raison d'échecs de cohérence. Les échecs de niveau de cohérence résultent d'un nombre insuffisant de magasins de métadonnées disponibles au moment où une requête est effectuée par le biais du service DDS spécifique.

Vous pouvez utiliser la page Diagnostics pour obtenir des informations supplémentaires sur l'état actuel de votre grille. Voir "Exécuter les diagnostics".

Garanties et contrôles de cohérence

StorageGRID garantit la cohérence de lecture après écriture pour les nouveaux objets. Toute opération GET après une opération PUT réussie sera capable de lire les données récemment écrites. Les écrasements

d’objets existants, les mises à jour de métadonnées et les suppressions restent cohérents.

Qu’est-ce que le service LDR ?

Hébergé par chaque nœud de stockage, le service LDR (local distribution Router) gère le transport de contenu pour le système StorageGRID. Le transport de contenu englobe de nombreuses tâches, dont le stockage des données, le routage et le traitement des demandes. Le service LDR effectue la plupart du travail acharné du système StorageGRID en gérant les charges de transfert de données et les fonctions de trafic de données.

Le service LDR gère les tâches suivantes :

- Requêtes
- Activité liée à la gestion du cycle de vie des informations (ILM)
- Suppression d’objet
- Stockage des données objet
- Transferts de données objet à partir d’un autre service LDR (nœud de stockage)
- Gestion du stockage des données
- Interfaces de protocole (S3 et Swift)

Le service LDR gère également le mappage d’objets S3 et Swift vers des UUID (« content handle ») uniques que le système StorageGRID attribue à chaque objet ingéré.

Requêtes

Les requêtes LDR incluent des requêtes pour l’emplacement des objets lors des opérations de récupération et d’archivage. Vous pouvez identifier le temps moyen d’exécution d’une requête, le nombre total de requêtes réussies et le nombre total de requêtes ayant échoué en raison d’un problème de délai d’attente.

Vous pouvez examiner les informations de requête afin de contrôler l’état du magasin de métadonnées, ce qui a un impact sur les performances d’entrée et de récupération du système. Par exemple, si la latence d’une requête moyenne est lente et que le nombre de requêtes ayant échoué en raison de délais d’attente est élevé, le magasin de métadonnées peut rencontrer une charge plus élevée ou effectuer une autre opération.

Vous pouvez également afficher le nombre total de requêtes ayant échoué en raison d’échecs de cohérence. Les défaillances de niveau de cohérence résultent d’un nombre insuffisant de magasins de métadonnées disponibles au moment où une requête est exécutée via le service LDR spécifique.

Vous pouvez utiliser la page Diagnostics pour obtenir des informations supplémentaires sur l’état actuel de votre grille. Voir "Exécuter les diagnostics".

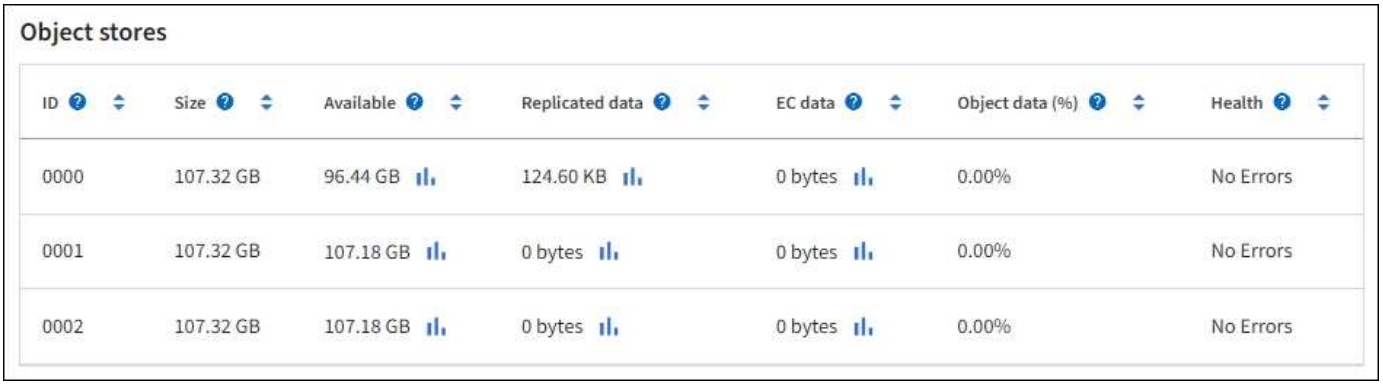
Activité des règles ILM

Les metrics de gestion du cycle de vie des informations vous permettent de surveiller la vitesse à laquelle les objets sont évalués pour la mise en œuvre de ILM. Vous pouvez afficher ces mesures sur le tableau de bord ou sur **NODES** > ***Storage Node*** > **ILM**.

Magasins d’objets

Le stockage sous-jacent d’un service LDR est divisé en un nombre fixe de magasins d’objets (aussi appelés volumes de stockage). Chaque magasin d’objets est un point de montage distinct.

Les magasins d’objets d’un nœud de stockage s’affichent sur la page nœuds > onglet stockage.



Les magasins d'objets d'un nœud de stockage sont identifiés par un nombre hexadécimal compris entre 0000 et 002F, appelé ID de volume. L'espace est réservé dans le premier magasin d'objets (volume 0) pour les métadonnées d'objet dans une base de données Cassandra. Tout espace restant sur ce volume est utilisé pour les données d'objet. Tous les autres magasins d'objets sont exclusivement utilisés pour les données d'objet, notamment les copies répliquées et les fragments avec code d'effacement.

Pour garantir même l'utilisation de l'espace pour les copies répliquées, les données d'objet d'un objet donné sont stockées dans un magasin d'objets basé sur l'espace de stockage disponible. Lorsqu'un ou plusieurs magasins d'objets sont remplis à la capacité, les magasins d'objets restants continuent de stocker des objets jusqu'à ce qu'il n'y ait plus d'espace sur le nœud de stockage.

Protection des métadonnées

Les métadonnées de l'objet sont des informations liées ou une description d'un objet. Par exemple, l'heure de modification de l'objet ou l'emplacement de stockage. StorageGRID stocke les métadonnées d'objet dans une base de données Cassandra, qui assure l'interface avec le service LDR.

Pour assurer la redondance et ainsi la protection contre la perte, trois copies des métadonnées d'objet sont conservées sur chaque site. Cette réplication n'est pas configurable et se fait automatiquement.

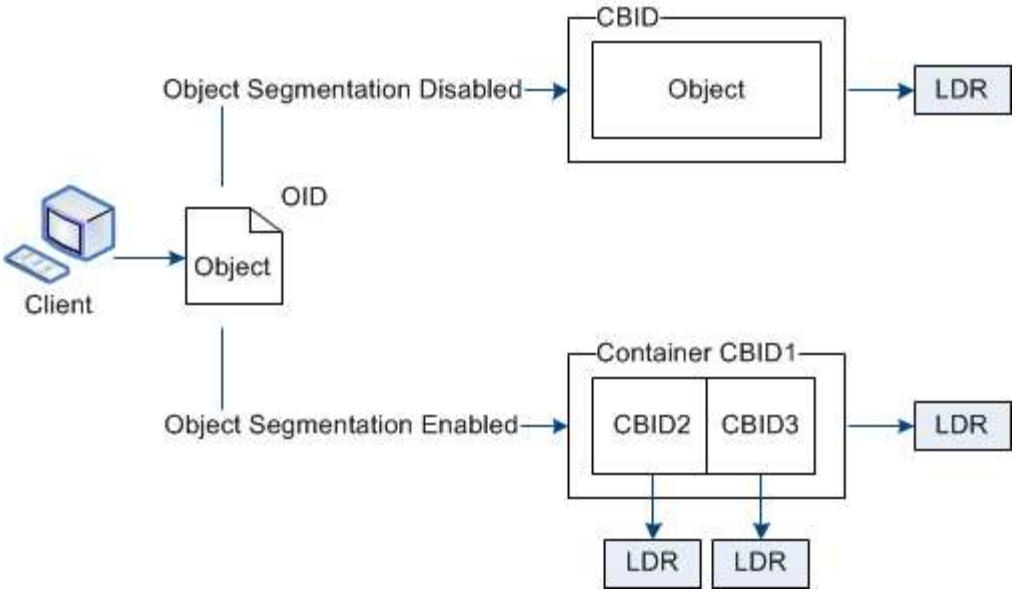
"Gérer le stockage des métadonnées d'objet"

Utilisez les options de stockage

Qu'est-ce que la segmentation d'objet ?

La segmentation d'objet consiste à diviser un objet en un ensemble d'objets de taille fixe plus petits afin d'optimiser l'utilisation du stockage et des ressources pour les objets de grande taille. Le téléchargement multi-pièces S3 crée également des objets segmentés, avec un objet représentant chaque pièce.

Lorsqu'un objet est ingéré dans le système StorageGRID, le service LDR divise l'objet en segments et crée un conteneur de segments qui répertorie les informations d'en-tête de tous les segments en tant que contenu.



Lors de la récupération d'un conteneur de segments, le service LDR assemble l'objet original à partir de ses segments et renvoie l'objet au client.

Le conteneur et les segments ne sont pas nécessairement stockés sur le même nœud de stockage. Les conteneurs et les segments peuvent être stockés sur n'importe quel nœud de stockage du pool de stockage spécifié dans la règle ILM.

Chaque segment est traité indépendamment par le système StorageGRID et contribue au nombre d'attributs tels que les objets gérés et les objets stockés. Par exemple, si un objet stocké dans le système StorageGRID est divisé en deux segments, la valeur des objets gérés augmente de trois après la fin de l'acquisition, comme suit :

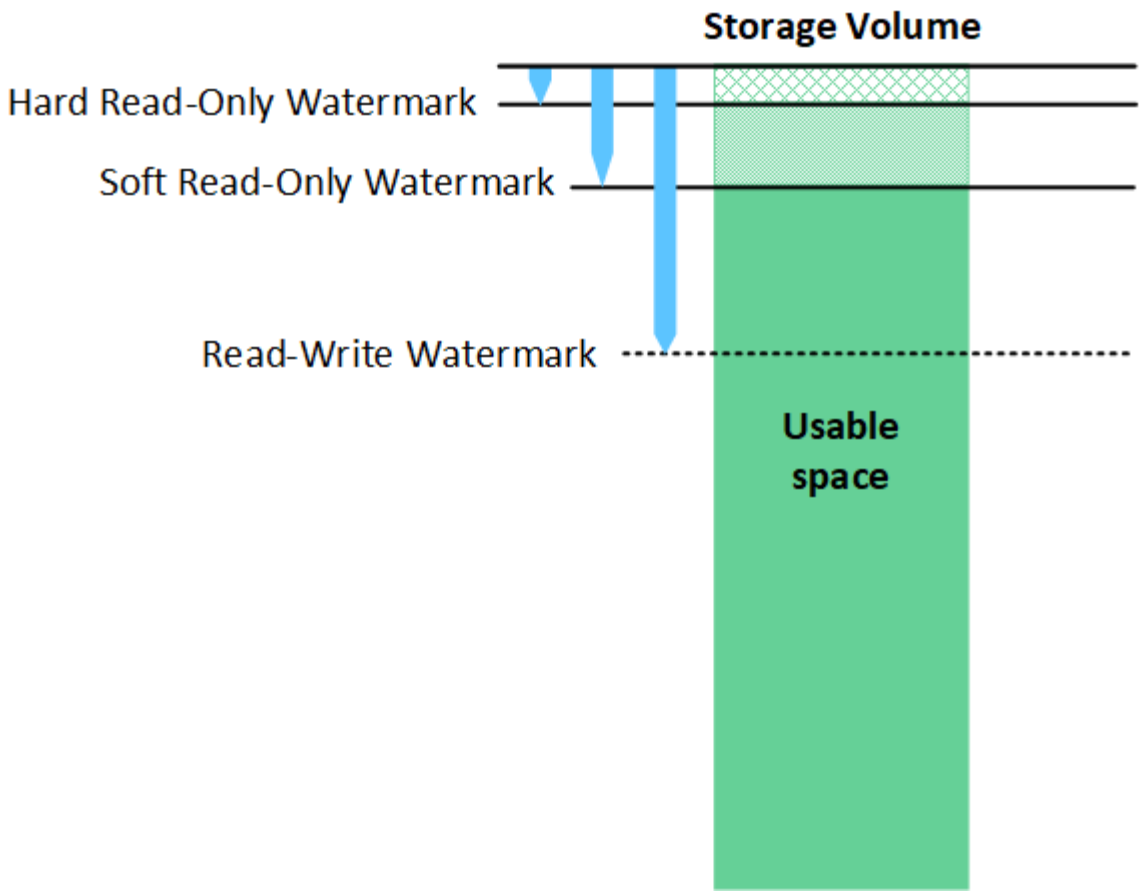
```
segment container + segment 1 + segment 2 = three stored objects
```

Vous pouvez améliorer les performances lors de la manipulation d'objets volumineux en vous assurant que :

- Chaque passerelle et nœud de stockage dispose d'une bande passante réseau suffisante pour le débit requis. Par exemple, configurez des réseaux Grid et client distincts sur des interfaces Ethernet 10 Gbits/s.
- Suffisamment de nœuds de passerelle et de stockage sont déployés pour le débit requis.
- Chaque nœud de stockage offre des performances d'E/S de disque suffisantes pour le débit requis.

Quelles sont les filigranes du volume de stockage ?

StorageGRID utilise trois filigranes de volume de stockage qui garantissent que les nœuds de stockage sont transférés en toute sécurité vers un état en lecture seule avant de s'exécuter avec un espace critique et que les nœuds de stockage ayant été transférés vers un état en lecture seule afin de devenir à nouveau en lecture/écriture.



Les filigranes du volume de stockage ne s'appliquent qu'à l'espace utilisé pour les données d'objets répliquées et codées par effacement. Pour en savoir plus sur l'espace réservé aux métadonnées d'objet sur le volume 0, accédez à"Gérer le stockage des métadonnées d'objet".

Qu'est-ce que le filigrane en lecture seule souple ?

Le filigrane **Volume de stockage en lecture seule** est le premier filigrane indiquant que l'espace utilisable d'un nœud de stockage pour les données d'objet est saturé.

Si chaque volume d'un nœud de stockage a moins d'espace libre que le filigrane en lecture seule programmable de ce volume, le nœud de stockage passe en mode *lecture seule*. Le mode lecture seule signifie que le nœud de stockage annonce des services en lecture seule au reste du système StorageGRID, mais remplit toutes les demandes d'écriture en attente.

Supposons par exemple que chaque volume d'un nœud de stockage dispose d'un filigrane en lecture seule de 10 Go. Dès que chaque volume dispose de moins de 10 Go d'espace libre, le nœud de stockage passe en mode veille souple en lecture seule.

Qu'est-ce que le filigrane en lecture seule difficile ?

Le filigrane **Volume de stockage en lecture seule matérielle** est le filigrane suivant pour indiquer que l'espace utilisable d'un nœud pour les données d'objet est en train de devenir plein.

Si l'espace libre d'un volume est inférieur au filigrane en lecture seule de ce volume, les écritures sur le volume échoueront. Cependant, les écritures sur d'autres volumes peuvent continuer jusqu'à ce que l'espace libre sur ces volumes soit inférieur à leurs filigranes en lecture seule.

Supposons par exemple que chaque volume d'un nœud de stockage dispose d'un filigrane en lecture seule de 5 Go. Dès que chaque volume dispose de moins de 5 Go d'espace libre, le nœud de stockage n'accepte plus de demandes d'écriture.

Le filigrane en lecture seule est toujours inférieur au filigrane en lecture seule.

Qu'est-ce que le filigrane Read-Write ?

Le filigrane **Storage Volume Read-Write** ne s'applique qu'aux nœuds de stockage ayant été passés en mode lecture seule. Il détermine quand le nœud peut redevenir lecture-écriture. Lorsque l'espace libre sur un volume de stockage d'un nœud de stockage est supérieur au filigrane de lecture-écriture de ce volume, le nœud revient automatiquement à l'état de lecture-écriture.

Supposons par exemple que le nœud de stockage est passé en mode lecture seule. Supposons également que chaque volume dispose d'un filigrane Read-Write de 30 Go. Dès que l'espace libre d'un volume augmente jusqu'à 30 Go, le nœud redevient read-write.

Le filigrane lu-Write est toujours plus grand que le filigrane en lecture seule et le filigrane en lecture seule.

Afficher les filigranes du volume de stockage

Vous pouvez afficher les paramètres actuels du filigrane ainsi que les valeurs optimisées par le système. Si les filigranes optimisés ne sont pas utilisés, vous pouvez déterminer si vous pouvez ou devez régler les paramètres.

Avant de commencer

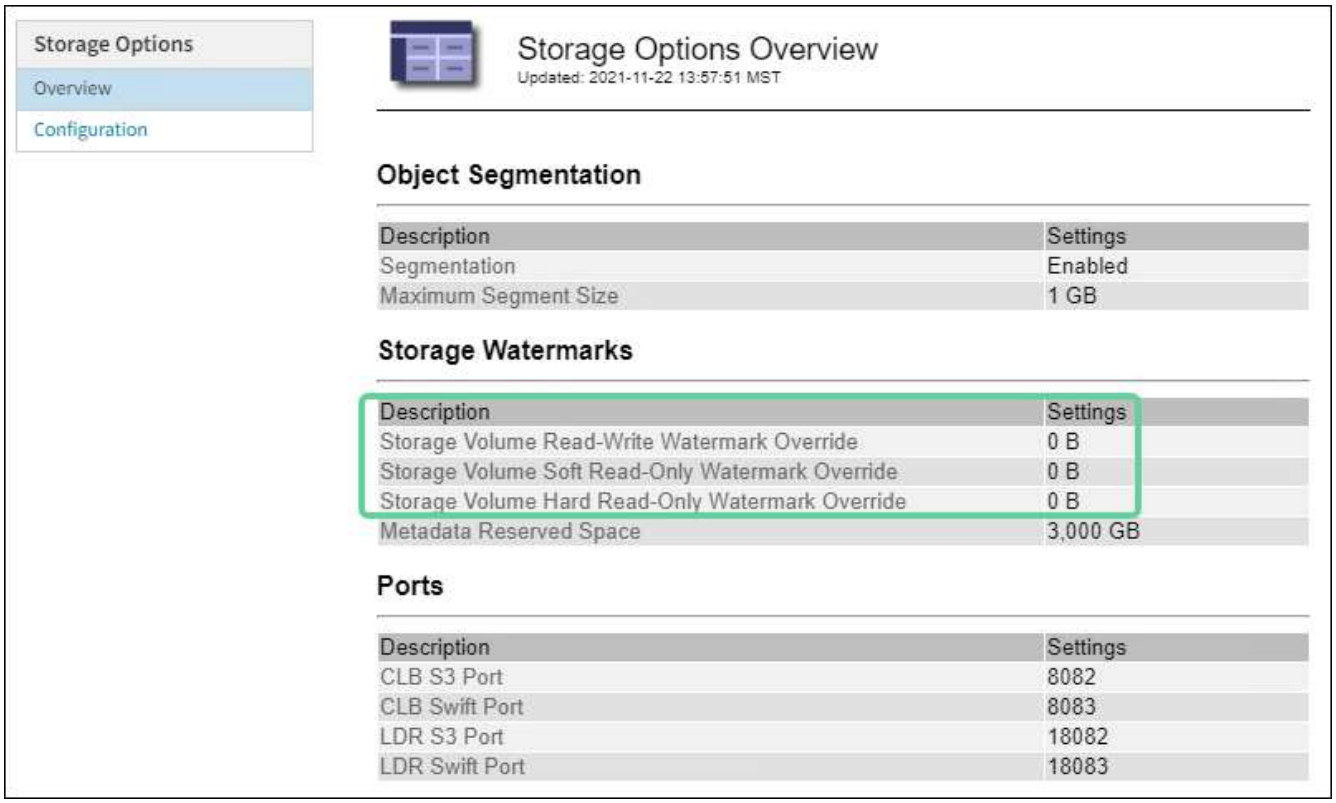
- Vous avez terminé la mise à niveau vers StorageGRID 11.6 ou une version ultérieure.
- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous disposez de l'autorisation d'accès racine.

Afficher les paramètres actuels du filigrane

Vous pouvez afficher les paramètres actuels du filigrane de stockage dans Grid Manager.

Étapes

1. Sélectionnez **CONFIGURATION** > **système** > **Options de stockage**.
2. Dans la section Storage Watermarks (filigranes de stockage), vérifiez les paramètres des trois remplacements de filigrane de volume de stockage.



- Si les remplacements de filigrane sont **0**, les trois filigranes sont optimisés pour chaque volume de stockage sur chaque nœud de stockage, en fonction de la taille du nœud de stockage et de la capacité relative du volume.

  Il s'agit du paramètre par défaut et recommandé. Vous ne devez pas mettre à jour ces valeurs. Si nécessaire, vous pouvez choisir Afficher des filigranes de stockage optimisés.

- Si les remplacements de filigrane ne sont pas des valeurs 0, des filigranes personnalisés (non optimisés) sont utilisés. L'utilisation de paramètres de filigrane personnalisés n'est pas recommandée. Suivez les instructions pour "Dépannage des alertes de remplacement du filigrane en lecture seule faible" pour déterminer si vous pouvez ou devez régler les paramètres.

Afficher des filigranes de stockage optimisés

StorageGRID utilise deux metrics Prometheus pour afficher les valeurs optimisées qu'il a calculées pour le filigrane **Volume de stockage en lecture seule**. Vous pouvez afficher les valeurs minimale et maximale optimisées pour chaque nœud de stockage de la grille.

1. Sélectionnez **SUPPORT** > **Outils** > **métriques**.
2. Dans la section Prometheus, sélectionnez le lien permettant d'accéder à l'interface utilisateur Prometheus.
3. Pour afficher le filigrane minimum en lecture seule programmable recommandé, entrez la mesure Prometheus suivante et sélectionnez **Execute** :

   ```
   storagegrid_storage_volume_minimum_optimized_soft_readonly_watermark
   ```

   La dernière colonne affiche la valeur minimale optimisée du filigrane en lecture seule pour tous les volumes de stockage de chaque nœud de stockage. Si cette valeur est supérieure au paramètre personnalisé pour le filigrane **Volume de stockage en lecture seule**, l'alerte **dépassement de filigrane en lecture seule faible** est déclenchée pour le nœud de stockage.

4. Pour afficher le filigrane maximal en lecture seule programmable recommandé, entrez la mesure Prometheus suivante et sélectionnez **Execute** :

   ```
   storagegrid_storage_volume_maximum_optimized_soft_readonly_watermark
   ```

   La dernière colonne affiche la valeur maximale optimisée du filigrane en lecture seule pour tous les volumes de stockage de chaque nœud de stockage.

Gérer le stockage des métadonnées d'objet

La capacité des métadonnées d'objet d'un système StorageGRID contrôle le nombre maximal d'objets qui peuvent être stockés sur le système en question. Pour s'assurer que votre système StorageGRID dispose d'un espace suffisant pour stocker les nouveaux objets, vous devez comprendre où et comment StorageGRID stocke les métadonnées d'objet.

Qu'est-ce que les métadonnées d'objet ?

Les métadonnées d'objet constituent toutes les informations qui décrivent un objet. StorageGRID utilise les métadonnées d'objet pour suivre l'emplacement de tous les objets de la grille, et pour gérer le cycle de vie de chaque objet au fil du temps.

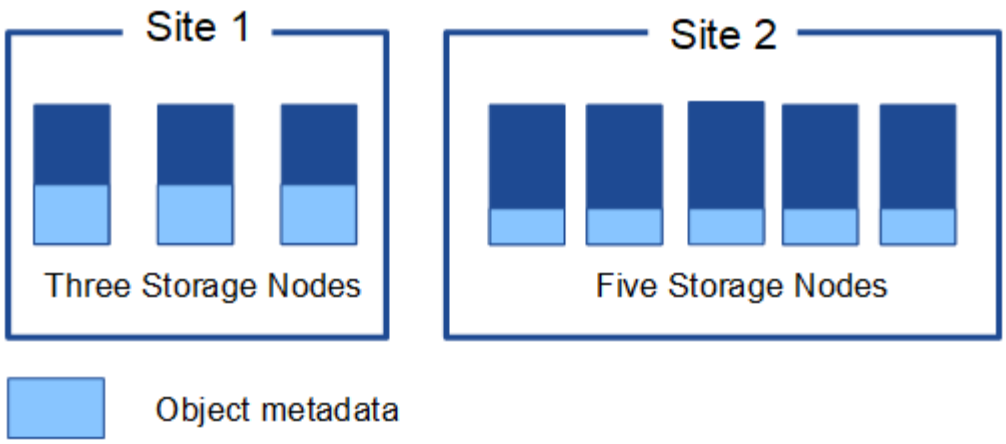
Pour un objet dans StorageGRID, les métadonnées d'objet incluent les types d'information suivants :

- Les métadonnées du système, y compris un ID unique pour chaque objet (UUID), le nom de l'objet, le nom du compartiment S3 ou du conteneur Swift, le nom ou l'ID du compte du locataire, la taille logique de l'objet, la date et l'heure de la première création de l'objet, et la date et l'heure de la dernière modification de l'objet.
- Toutes les paires de clé-valeur de métadonnées utilisateur personnalisées associées à l'objet.
- Pour les objets S3, toutes les paires de clé-valeur de balise d'objet associées à l'objet.
- Pour les copies d'objet répliquées, emplacement de stockage actuel de chaque copie.
- Pour les copies d'objets avec code d'effacement, l'emplacement de stockage actuel de chaque fragment.
- Pour les copies d'objet dans Cloud Storage Pool, l'emplacement de l'objet, notamment le nom du compartiment externe et l'identifiant unique de l'objet.
- Pour les objets segmentés et les objets à plusieurs parties, les identificateurs de segment et la taille des données.

Comment les métadonnées d'objet sont-elles stockées ?

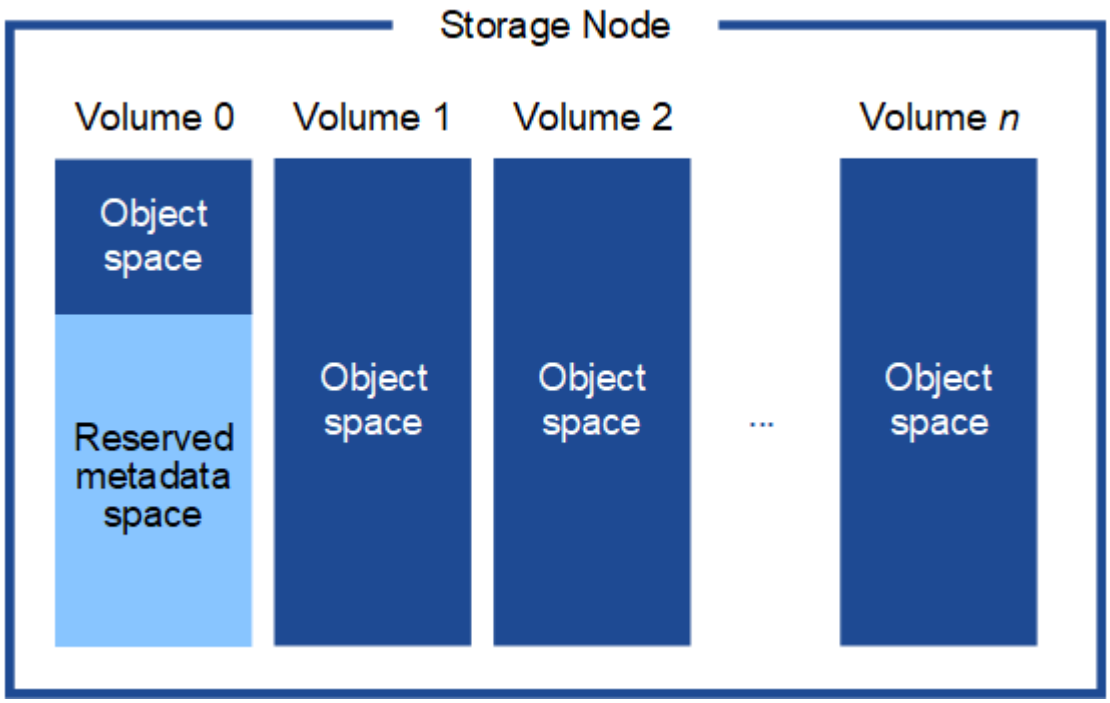
Les métadonnées d'objet sont conservées dans une base de données Cassandra, stockée indépendamment des données d'objet. StorageGRID Pour assurer la redondance et protéger les métadonnées d'objet contre la perte, StorageGRID stocke trois copies des métadonnées de tous les objets du système sur chaque site.

Cette figure représente les nœuds de stockage sur deux sites. Chaque site dispose du même volume de métadonnées objet, et les métadonnées de chaque site sont subdivisées en plusieurs nœuds de stockage sur ce site.



Où sont stockées les métadonnées d'objet ?

Cette figure représente les volumes de stockage d'un seul nœud de stockage.



Comme illustré dans la figure, StorageGRID réserve l'espace des métadonnées d'objet sur le volume de stockage 0 de chaque nœud de stockage. Il utilise l'espace réservé pour stocker les métadonnées d'objet et effectuer les opérations essentielles de la base de données. Tout espace restant sur le volume de stockage 0 et tous les autres volumes du nœud de stockage sont utilisés exclusivement pour les données d'objet (copies répliquées et fragments avec code d'effacement).

La quantité d'espace réservée aux métadonnées d'objet sur un nœud de stockage particulier dépend de plusieurs facteurs, décrits ci-dessous.

Paramètre Metadata Reserved Space

Le paramètre *Metadata Reserved Space* est un paramètre à l'échelle du système qui représente la quantité d'espace qui sera réservée aux métadonnées sur le volume 0 de chaque noeud de stockage. Comme indiqué dans le tableau, la valeur par défaut de ce paramètre est basée sur :

- La version du logiciel que vous utilisiez lors de l'installation initiale de StorageGRID.
- Quantité de RAM sur chaque nœud de stockage.

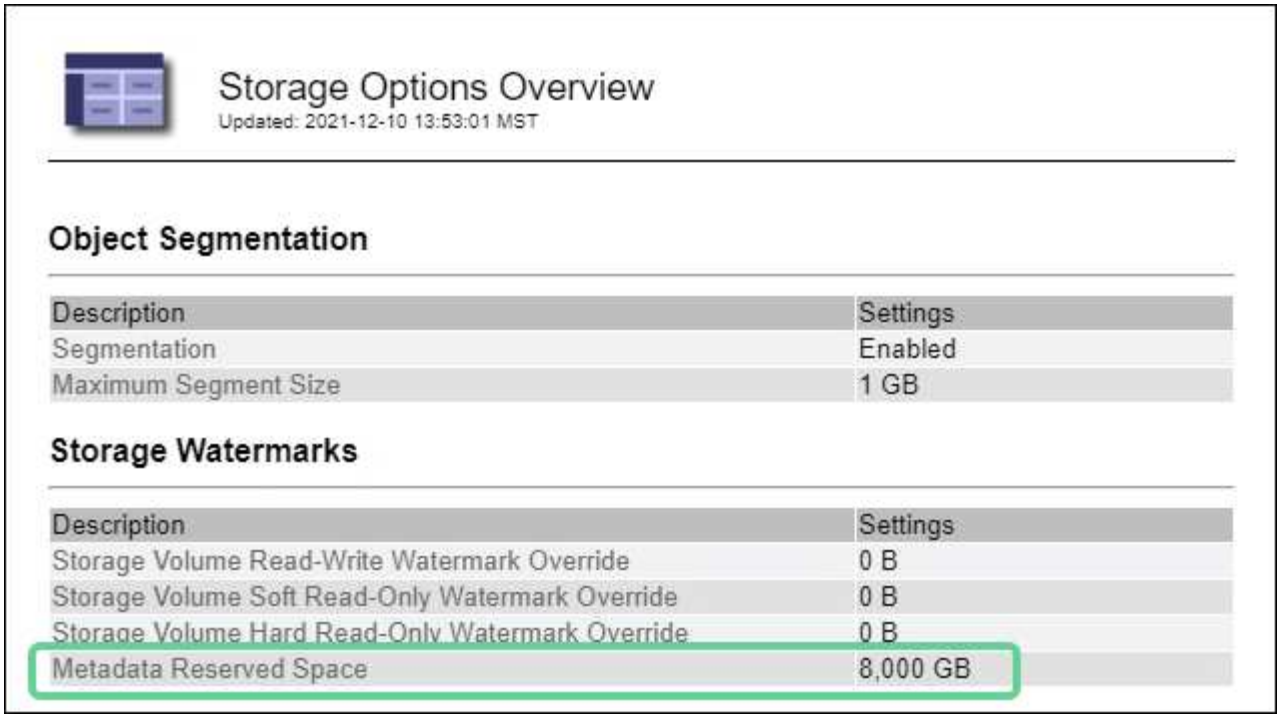
Version utilisée pour l'installation initiale de StorageGRID	Quantité de RAM sur les nœuds de stockage	Paramètre espace réservé aux métadonnées par défaut
11.5 à 11.7	Au moins 128 Go sur chaque nœud de stockage de la grille	8 TO (8,000 GO)
	Moins de 128 Go sur n'importe quel nœud de stockage de la grille	3 TO (3,000 GO)
11.1 à 11.4	128 Go ou plus sur chaque nœud de stockage sur un site	4 TO (4,000 GO)
	Moins de 128 Go sur n'importe quel nœud de stockage de chaque site	3 TO (3,000 GO)
11.0 ou antérieure	Tout montant	2 TO (2,000 GO)

Afficher le paramètre espace réservé aux métadonnées

Procédez comme suit pour afficher le paramètre espace réservé aux métadonnées de votre système StorageGRID.

Étapes

1. Sélectionnez **CONFIGURATION** > **système** > **Options de stockage**.
2. Dans le tableau des filigranes de stockage, localisez **espace réservé de métadonnées**.



Dans la capture d'écran, la valeur **Metadata Reserved Space** est de 8,000 Go (8 To). Il s'agit du paramètre par défaut d'une nouvelle installation StorageGRID 11.6 ou ultérieure dans laquelle chaque nœud de stockage dispose d'au moins 128 Go de RAM.

Espace réservé réel pour les métadonnées

Contrairement au paramètre espace réservé aux métadonnées pour l'ensemble du système, le paramètre *espace réservé réel* pour les métadonnées d'objet est déterminé pour chaque nœud de stockage. Pour un nœud de stockage donné, l'espace réservé réel pour les métadonnées dépend de la taille du volume 0 pour le nœud et du paramètre espace réservé * métadonnées * pour l'ensemble du système.

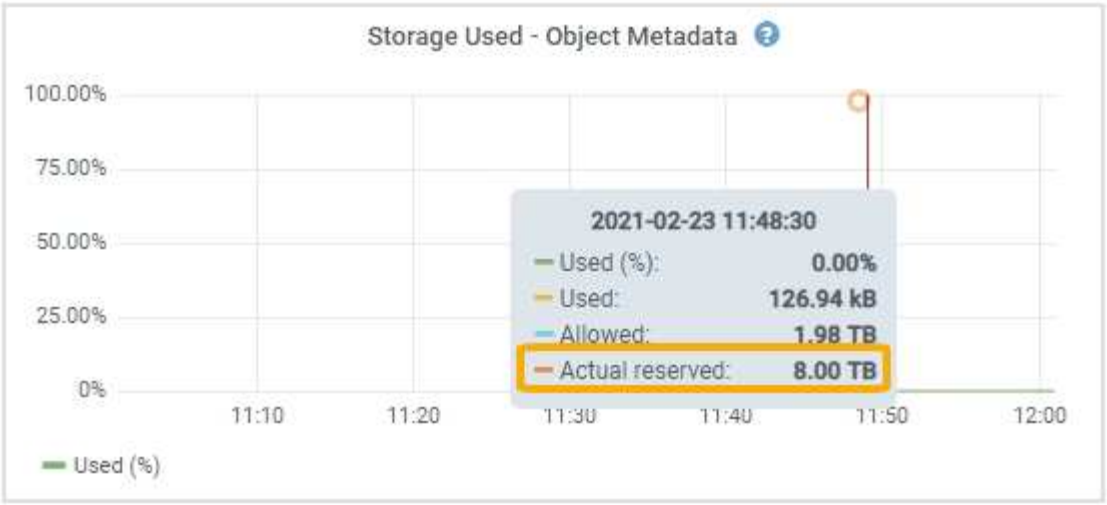
Taille du volume 0 pour le nœud	Espace réservé réel pour les métadonnées
Moins de 500 Go (non utilisé en production)	10 % du volume 0
500 Go ou plus	Plus ces valeurs sont faibles : • Volume 0 • Paramètre Metadata Reserved Space

Afficher l'espace réservé réel pour les métadonnées

La procédure suivante permet d'afficher l'espace réservé réel pour les métadonnées sur un nœud de stockage particulier.

Étapes

1. Dans Grid Manager, sélectionnez **NOEUDS** > ***Storage Node***.
2. Sélectionnez l'onglet **stockage**.
3. Placez votre curseur sur le graphique stockage utilisé - métadonnées de l'objet et localisez la valeur **réel réservé**.



Dans la capture d'écran, la valeur **réelle réservée** est de 8 To. Cette capture d'écran concerne un nœud de stockage grand format dans une nouvelle installation de StorageGRID 11.6. Étant donné que le paramètre espace réservé aux métadonnées pour l'ensemble du système est inférieur au volume 0 pour ce nœud de stockage, l'espace réservé réel pour ce nœud est égal au paramètre espace réservé aux métadonnées.

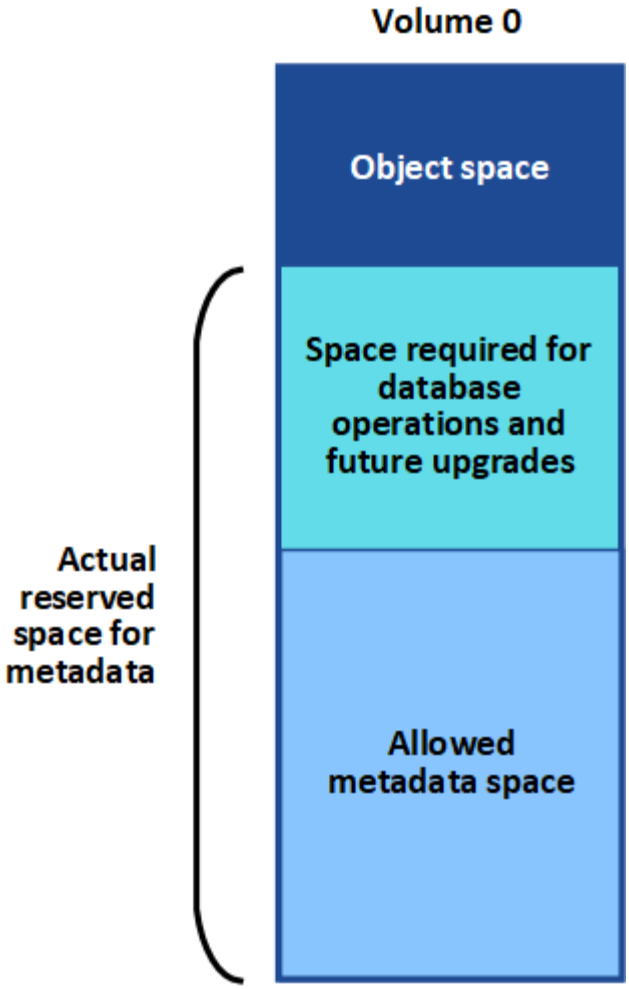
Exemple d'espace de métadonnées réservé réel

Supposons que vous installiez un nouveau système StorageGRID à l'aide de la version 11.7. Dans cet exemple, supposons que chaque nœud de stockage dispose de plus de 128 Go de RAM et que le volume 0 du nœud de stockage 1 (SN1) est de 6 To. Sur la base de ces valeurs :

- L'espace réservé * métadonnées* pour l'ensemble du système est défini sur 8 To. (Il s'agit de la valeur par défaut pour une nouvelle installation StorageGRID 11.6 ou supérieure si chaque nœud de stockage possède plus de 128 Go de RAM.)
- L'espace réservé réel pour les métadonnées pour SN1 est de 6 To. (Le volume entier est réservé car le volume 0 est inférieur au paramètre **Metadata Reserved Space**.)

Espace de métadonnées autorisé

L'espace réservé réel de chaque nœud de stockage pour les métadonnées est divisé en l'espace disponible pour les métadonnées d'objet (l'espace *autorisé metadata space*) et l'espace requis pour les opérations essentielles de bases de données (telles que la compaction et la réparation) et les mises à niveau matérielles et logicielles futures. L'espace de métadonnées autorisé régit la capacité globale des objets.



Le tableau suivant montre comment StorageGRID calcule l' **espace de métadonnées autorisé** pour différents nœuds de stockage, en fonction de la quantité de mémoire du nœud et de l'espace réservé réel pour les métadonnées.

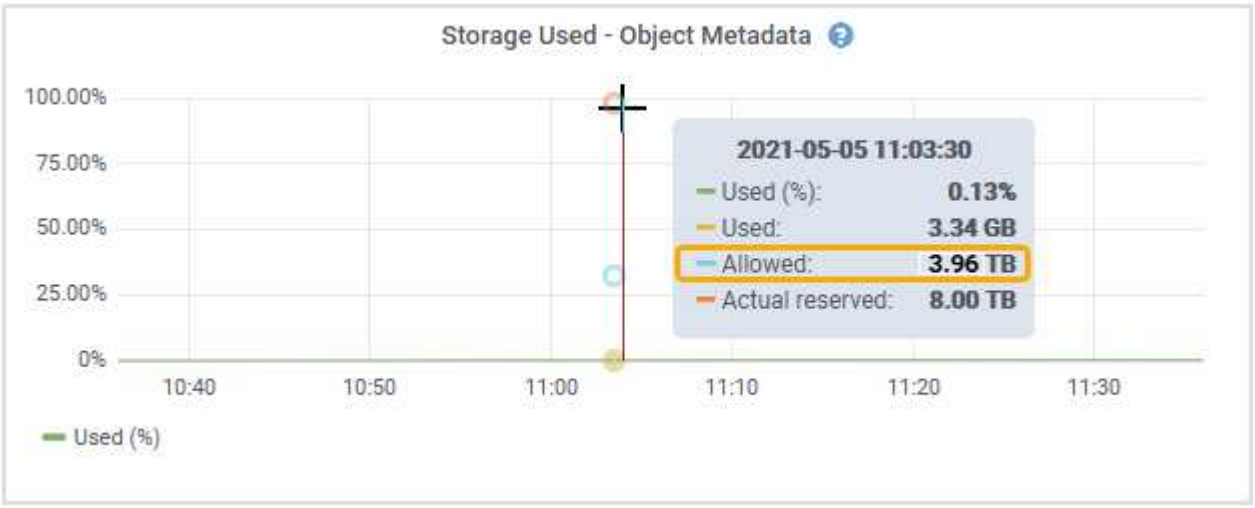
		Quantité de mémoire sur le noeud de stockage	
	&Lt ; 128 GB	&gt ;= 128 Go	**Espace réservé réel pour les métadonnées**
&Lt ;= 4 To	60 % de l'espace réservé réel pour les métadonnées, jusqu'à un maximum de 1.32 To	60 % de l'espace réservé réel pour les métadonnées, jusqu'à un maximum de 1.98 To	&gt ; 4 To

Afficher l'espace de métadonnées autorisé

La procédure suivante permet d'afficher l'espace de métadonnées autorisé pour un nœud de stockage.

Étapes

1. Dans Grid Manager, sélectionnez **NODES**.
2. Sélectionnez le nœud de stockage.
3. Sélectionnez l'onglet **stockage**.
4. Placez votre curseur sur le graphique de métadonnées de l'objet stockage utilisé - et localisez la valeur **autorisé**.



Dans la capture d'écran, la valeur **autorisé** est de 3.96 To, ce qui est la valeur maximale pour un noeud de stockage dont l'espace réservé réel pour les métadonnées est supérieur à 4 To.

La valeur **autorisé** correspond à cette métrique Prometheus :

```
storagegrid_storage_utilization_metadata_allowed_bytes
```

Exemple d'espace de métadonnées autorisé

Supposons que vous installez un système StorageGRID avec la version 11.6. Dans cet exemple, supposons que chaque nœud de stockage dispose de plus de 128 Go de RAM et que le volume 0 du nœud de stockage 1 (SN1) est de 6 To. Sur la base de ces valeurs :

- L'espace réservé * métadonnées* pour l'ensemble du système est défini sur 8 To. (Il s'agit de la valeur par défaut pour StorageGRID 11.6 ou supérieur lorsque chaque nœud de stockage dispose de plus de 128 Go de RAM.)
- L'espace réservé réel pour les métadonnées pour SN1 est de 6 To. (Le volume entier est réservé car le volume 0 est inférieur au paramètre **Metadata Reserved Space**.)
- L'espace autorisé pour les métadonnées sur SN1 est de 3 To, d'après le calcul présenté dans la tableau pour l'espace autorisé pour les métadonnées: (Espace réservé réel pour les métadonnées − 1 To) × 60 %, jusqu'à un maximum de 3.96 To.

La façon dont les nœuds de stockage de différentes tailles affectent la capacité des objets

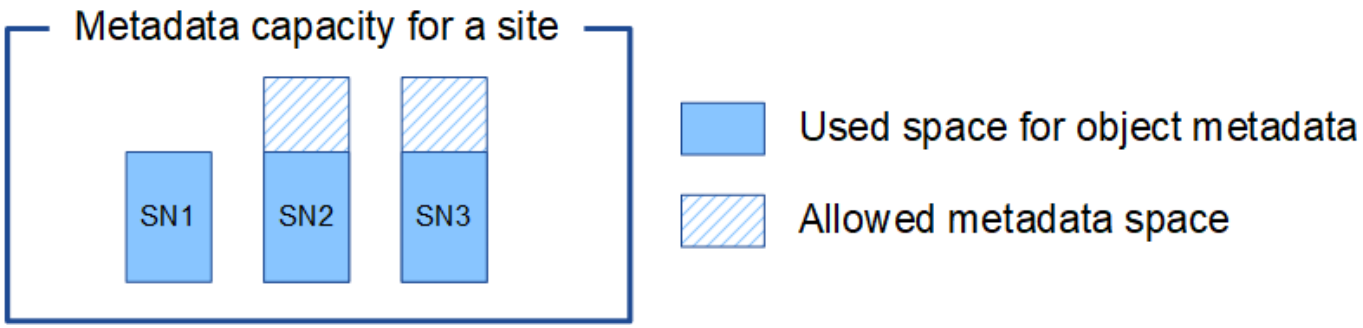
Comme décrit ci-dessus, StorageGRID distribue uniformément les métadonnées d'objet sur les nœuds de stockage sur chaque site. Par conséquent, si un site contient des nœuds de stockage de différentes tailles, le plus petit nœud du site détermine la capacité des métadonnées du site.

Prenons l'exemple suivant :

- Une grille sur un seul site contient trois nœuds de stockage de tailles différentes.
- Le paramètre **Metadata Reserved Space** est de 4 To.
- Les nœuds de stockage ont les valeurs suivantes pour l'espace réservé réel des métadonnées et l'espace autorisé pour les métadonnées.

Nœud de stockage	Taille du volume 0	Espace réservé réel des métadonnées	Espace de métadonnées autorisé
SN1	2.2 TO	2.2 TO	1.32 TO
SN2	5 TO	4 TO	1.98 TO
SN3	6 To	4 TO	1.98 TO

Les métadonnées de l'objet sont réparties de manière uniforme sur les nœuds de stockage d'un site. En effet, chaque nœud de cet exemple ne peut contenir que 1.32 To de métadonnées. Les 0.66 To supplémentaires d'espace de métadonnées autorisé pour SN2 et SN3 ne peuvent pas être utilisés.



De même, puisque StorageGRID conserve toutes les métadonnées d'objet d'un système StorageGRID sur chaque site, la capacité globale des métadonnées d'un système StorageGRID est déterminée par la capacité des métadonnées d'objet du plus petit site.

Étant donné que la capacité des métadonnées contrôle le nombre maximal d'objets, lorsqu'un nœud vient à manquer de capacité de métadonnées, la grille est véritablement pleine.

Informations associées

- Pour savoir comment surveiller la capacité des métadonnées d'objet pour chaque nœud de stockage, reportez-vous aux instructions de "Surveillance StorageGRID".
- Pour augmenter la capacité de métadonnées d'objet de votre système, "développez votre grille" En ajoutant de nouveaux nœuds de stockage.

Augmenter le paramètre d'espace réservé aux métadonnées

Vous pourrez peut-être augmenter le paramètre système Espace réservé aux métadonnées si vos nœuds de stockage répondent à des exigences spécifiques en matière de RAM et d'espace disponible.

Ce dont vous aurez besoin

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "navigateur web pris en charge".
- Vous avez le "Autorisation d'accès racine ou configuration de la page de topologie de la grille et autres autorisations de configuration de la grille".

Description de la tâche

Vous pourrez peut-être augmenter manuellement le paramètre d'espace réservé aux métadonnées à l'échelle du système jusqu'à 8 To.

Vous ne pouvez augmenter la valeur du paramètre Espace réservé aux métadonnées à l'échelle du système que si ces deux affirmations sont vraies :

- Les nœuds de stockage de n'importe quel site de votre système disposent chacun de 128 Go ou plus de RAM.
- Les nœuds de stockage de n'importe quel site de votre système disposent chacun d'un espace disponible suffisant sur le volume de stockage 0.

Sachez que si vous augmentez ce paramètre, vous réduirez simultanément l'espace disponible pour le stockage d'objets sur le volume de stockage 0 de tous les nœuds de stockage. Pour cette raison, vous préférerez peut-être définir l'espace réservé aux métadonnées sur une valeur inférieure à 8 To, en fonction de vos besoins en métadonnées d'objet attendus.

> En général, il est préférable d'utiliser une valeur supérieure plutôt qu'une valeur inférieure. Si le paramètre Espace réservé aux métadonnées est trop grand, vous pouvez le diminuer ultérieurement. En revanche, si vous augmentez la valeur ultérieurement, le système devra peut-être déplacer les données de l'objet pour libérer de l'espace.

Pour une explication détaillée de l'influence du paramètre Espace réservé aux métadonnées sur l'espace autorisé pour le stockage des métadonnées d'objet sur un nœud de stockage particulier, consultez "Gérer le stockage des métadonnées d'objet".

Étapes

1. Déterminez le paramètre actuel de l'espace réservé aux métadonnées.
   a. Sélectionnez **CONFIGURATION** > **système** > **Options de stockage**.
   b. Dans la section Filigranes de stockage, notez la valeur de **Espace réservé aux métadonnées**.
2. Assurez-vous de disposer de suffisamment d'espace disponible sur le volume de stockage 0 de chaque nœud de stockage pour augmenter cette valeur.
   a. Sélectionnez **NOEUDS**.
   b. Sélectionnez le premier nœud de stockage dans la grille.
   c. Sélectionnez l'onglet Stockage.
   d. Dans la section Volumes, recherchez l'entrée **/var/local/rangedb/0**.
   e. Confirmez que la valeur disponible est égale ou supérieure à la différence entre la nouvelle valeur que vous souhaitez utiliser et la valeur actuelle de l'espace réservé aux métadonnées.

      Par exemple, si le paramètre Espace réservé aux métadonnées est actuellement de 4 To et que vous souhaitez l'augmenter à 6 To, la valeur Disponible doit être de 2 To ou plus.

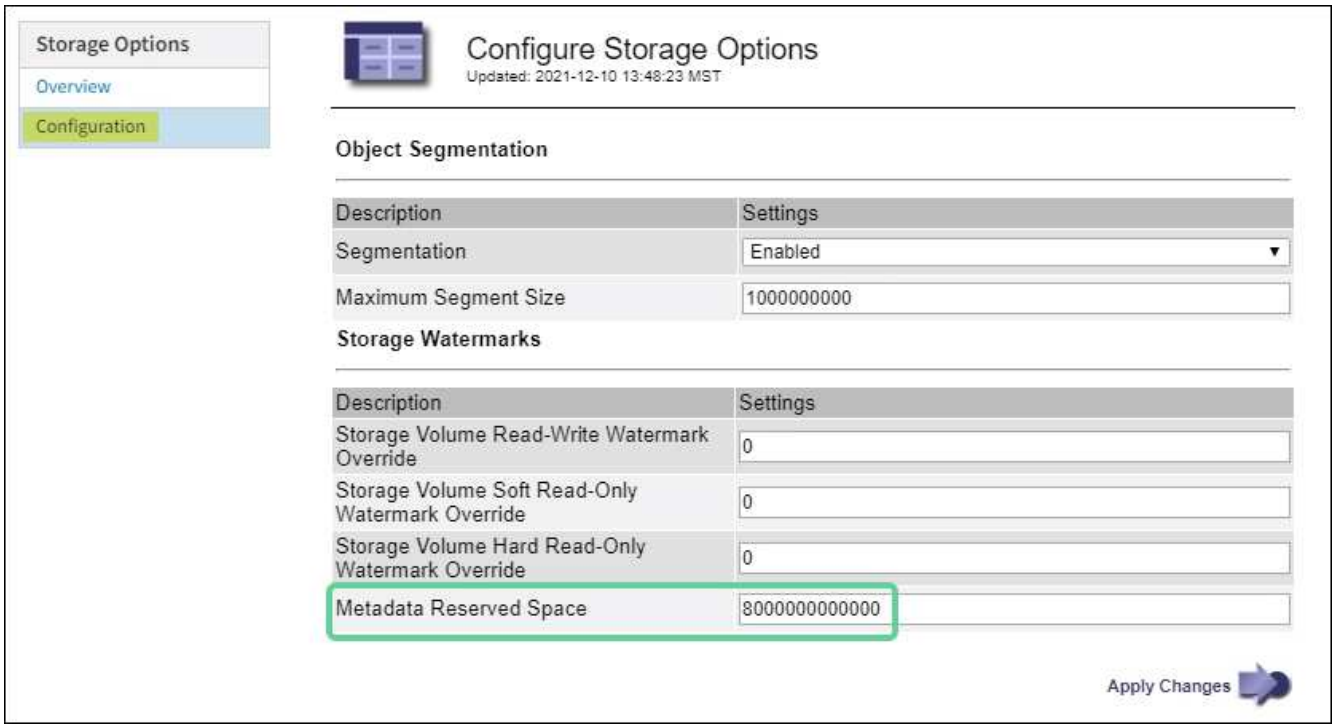
   f. Répétez ces étapes pour tous les nœuds de stockage.
      - Si un ou plusieurs nœuds de stockage ne disposent pas de suffisamment d'espace disponible, la valeur de l'espace réservé aux métadonnées ne peut pas être augmentée. Ne continuez pas cette

procédure.

- Si chaque nœud de stockage dispose de suffisamment d'espace disponible sur le volume 0, passez à l'étape suivante.

3. Assurez-vous d'avoir au moins 128 Go de RAM sur chaque nœud de stockage.
   a. Sélectionnez **NOEUDS**.
   b. Sélectionnez le premier nœud de stockage dans la grille.
   c. Sélectionnez l'onglet **matériel**.
   d. Passez votre curseur sur le graphique d'utilisation de la mémoire. Assurez-vous que la **mémoire totale** est d'au moins 128 Go.
   e. Répétez ces étapes pour tous les nœuds de stockage.
      - Si un ou plusieurs nœuds de stockage ne disposent pas de suffisamment de mémoire totale disponible, la valeur de l'espace réservé aux métadonnées ne peut pas être augmentée. Ne continuez pas cette procédure.
      - Si chaque nœud de stockage dispose d'au moins 128 Go de mémoire totale, passez à l'étape suivante.
4. Mettre à jour le paramètre Espace réservé aux métadonnées.
   a. Sélectionnez **CONFIGURATION** > **système** > **Options de stockage**.
   b. Sélectionnez l'onglet Configuration.
   c. Dans la section Filigranes de stockage, sélectionnez **Espace réservé aux métadonnées**.
   d. Entrez la nouvelle valeur.

      Par exemple, pour saisir 8 To, qui est la valeur maximale prise en charge, saisissez **8000000000000** (8, suivi de 12 zéros)



   a. Sélectionnez **appliquer les modifications**.

Compresser les objets stockés

Vous pouvez activer la compression des objets afin de réduire la taille des objets stockés dans StorageGRID, de sorte que les objets consomment moins d'espace de stockage.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous disposez d'autorisations d'accès spécifiques.

Description de la tâche

Par défaut, la compression des objets est désactivée. Si vous activez la compression, StorageGRID tente de compresser chaque objet lors de son enregistrement à l'aide de la compression sans perte.

> Si vous modifiez ce paramètre, il faudra environ une minute pour appliquer le nouveau paramètre. La valeur configurée est mise en cache pour les performances et l'évolutivité.

Avant d'activer la compression d'objets, tenez compte des points suivants :

- Vous ne devez pas sélectionner **Compresser les objets stockés**, sauf si vous savez que les données stockées sont compressibles.
- Les applications qui enregistrent des objets dans StorageGRID peuvent compresser les objets avant de les enregistrer. Si une application client a déjà compressé un objet avant de l'enregistrer dans StorageGRID, la sélection de cette option ne réduira pas davantage la taille d'un objet.
- Ne sélectionnez pas **Compresser les objets stockés** si vous utilisez NetApp FabricPool avec StorageGRID.
- Si **Compress Stored objects** est sélectionné, les applications clientes S3 et Swift doivent éviter d'effectuer des opérations GET Object qui spécifient une plage d'octets. Ces opérations de « lecture à plage » sont inefficaces, car StorageGRID doit décompresser efficacement les objets pour accéder aux octets demandés. LES opérations GET Object qui demandent une petite plage d'octets provenant d'un objet très volumineux sont particulièrement inefficaces. Par exemple, il est inefficace de lire une plage de 10 Mo sur un objet compressé de 50 Go.

  Si les plages sont lues à partir d'objets compressés, les demandes client peuvent être en attente.

  > Si vous devez compresser des objets et que votre application client doit utiliser des lectures de plage, augmentez le délai de lecture de l'application.

Étapes

1. Sélectionnez **CONFIGURATION** > **système** > **compression objet**.
2. Cochez la case **Compresser les objets stockés**.
3. Sélectionnez **Enregistrer**.

Paramètres de configuration du nœud de stockage

Chaque nœud de stockage utilise plusieurs paramètres de configuration et compteurs. Vous devrez peut-être afficher les paramètres actuels ou réinitialiser les compteurs pour effacer les alarmes (système hérité).

Sauf en cas d'instruction spécifique dans la documentation, consultez le support technique avant de modifier les paramètres de configuration des nœuds de stockage. Si nécessaire, vous pouvez réinitialiser les compteurs d'événements pour effacer les alarmes héritées.

Procédez comme suit pour accéder aux paramètres de configuration et aux compteurs d'un nœud de stockage.

Étapes

1. Sélectionnez **SUPPORT** > **Outils** > **topologie de grille**.
2. Sélectionnez ***site*** > ***Storage Node***.
3. Développez le nœud de stockage et sélectionnez le service ou le composant.
4. Sélectionnez l'onglet **Configuration**.

Les tableaux suivants résument les paramètres de configuration du nœud de stockage.

LDR

Nom d'attribut	Code	Description
État HTTP	HSTE	État actuel du protocole HTTP pour S3, Swift et tout autre trafic StorageGRID interne : • Hors ligne : aucune opération n'est autorisée et toute application client qui tente d'ouvrir une session HTTP au service LDR reçoit un message d'erreur. Les sessions actives sont normalement fermées. • En ligne : le fonctionnement se poursuit normalement
Démarrage automatique HTTP	HTA	• Si cette option est sélectionnée, l'état du système au redémarrage dépend de l'état du composant **LDR** > **Storage**. Si le composant **LDR** > **Storage** est en lecture seule au redémarrage, l'interface HTTP est également en lecture seule. Si le composant **LDR** > **Storage** est en ligne, HTTP est également en ligne. Dans le cas contraire, l'interface HTTP reste à l'état hors ligne. • Si elle n'est pas sélectionnée, l'interface HTTP reste hors ligne jusqu'à ce qu'elle soit explicitement activée.

LDR > datastore

Nom d'attribut	Code	Description
Réinitialiser le nombre d'objets perdus	RCOR	Réinitialisez le compteur du nombre d'objets perdus sur ce service.

LDR > stockage

Nom d'attribut	Code	Description
État de stockage — souhaité	SSD	Paramètre configurable par l'utilisateur pour l'état souhaité du composant de stockage. Le service LDR lit cette valeur et tente de faire correspondre l'état indiqué par cet attribut. La valeur est persistante entre les redémarrages. Par exemple, vous pouvez utiliser ce paramètre pour forcer le stockage à devenir en lecture seule, même en présence d'un espace de stockage disponible suffisant. Ceci peut être utile pour le dépannage. L'attribut peut prendre l'une des valeurs suivantes : • Hors ligne : lorsque l'état souhaité est hors ligne, le service LDR met le composant **LDR** > **Storage** hors ligne. • Lecture seule : lorsque l'état souhaité est en lecture seule, le service LDR déplace l'état du stockage en lecture seule et arrête d'accepter le nouveau contenu. Notez que le contenu peut continuer à être enregistré sur le nœud de stockage pendant une courte période jusqu'à la fermeture des sessions ouvertes. • En ligne : conservez la valeur sur Online pendant le fonctionnement normal du système. L'état de stockage — le courant du composant de stockage sera défini de manière dynamique par le service en fonction de l'état du service LDR, comme le volume de l'espace de stockage objet disponible. Si l'espace est faible, le composant devient lecture seule.
Délai de vérification de l'état dépassé	SHCT	La limite de temps en secondes pendant laquelle un test de vérification de l'état doit s'effectuer pour que le volume de stockage soit considéré comme sain. Ne modifiez cette valeur que si vous y êtes invité par le support.

LDR > Vérification

Nom d'attribut	Code	Description
Réinitialiser le nombre d'objets manquants	VCMI	Réinitialise le nombre d'objets manquants détectés (OMIS). Utiliser uniquement une fois la vérification de l'existence d'objet terminée. Les données d'objet répliqué manquantes sont restaurées automatiquement par le système StorageGRID.

Nom d'attribut	Code	Description
Taux de vérification	VPRI	Définissez la vitesse à laquelle la vérification des antécédents a lieu. Voir les informations sur la configuration du taux de vérification en arrière-plan.
Réinitialiser le nombre d'objets corrompus	VCCR	Réinitialisez le compteur pour les données d'objet répliqué corrompues trouvées lors de la vérification en arrière-plan. Cette option peut être utilisée pour effacer la condition d'alarme des objets corrompus détectés (OCOR).
Supprimer des objets en quarantaine	OQRT	Supprimez des objets corrompus du répertoire de quarantaine, réinitialisez le nombre d'objets mis en quarantaine et effacez l'alarme OQRT (Quarquarantaine Objects détectés). Cette option est utilisée après la restauration automatique par le système StorageGRID d'objets corrompus. Si une alarme objets perdus est déclenchée, le support technique peut vouloir accéder aux objets mis en quarantaine. Dans certains cas, les objets mis en quarantaine peuvent être utiles pour la récupération des données ou pour le débogage des problèmes sous-jacents à l'origine des copies d'objet corrompues.

LDR > codage d'effacement

Nom d'attribut	Code	Description
Réinitialiser le nombre d'échecs d'écriture	RSWF	Réinitialisez le compteur pour les échecs d'écriture des données d'objet avec code d'effacement sur le nœud de stockage.
Réinitialiser le nombre d'échecs de lecture	RSRF	Réinitialisez le compteur pour les échecs de lecture des données d'objet avec code d'effacement à partir du nœud de stockage.
Réinitialiser supprime le nombre d'échecs	RSDF	Réinitialisez le compteur pour les échecs de suppression des données d'objet avec code d'effacement du nœud de stockage.
Réinitialiser le nombre de copies corrompues détectées	RSCC	Réinitialisez le compteur du nombre de copies corrompues de données d'objet avec code d'effacement sur le nœud de stockage.
Réinitialiser le nombre de fragments corrompus détectés	RSCD	Réinitialisez le compteur en cas de fragments endommagés de données d'objet avec code d'effacement sur le nœud de stockage.

Nom d’attribut	Code	Description
Réinitialiser le nombre de fragments manquants détectés	RSMD	Réinitialisez le compteur en cas de fragments manquants de données d’objet avec code d’effacement sur le nœud de stockage. Utiliser uniquement une fois la vérification de l’existence d’objet terminée.

LDR > réplication

Nom d’attribut	Code	Description
Réinitialiser le nombre d’échecs de réplication entrante	RICR	Réinitialisez le compteur pour les échecs de réplication entrants. Il peut être utilisé pour effacer l’alarme RIRF (réplication entrante — échouée).
Réinitialiser le nombre d’échecs de réplication sortante	ROCR	Réinitialisez le compteur pour les échecs de réplication sortants. Cette fonction permet d’effacer l’alarme RORF (réplications sortantes — en échec).
Désactiver la réplication entrante	DSIR	Sélectionnez cette option pour désactiver la réplication entrante dans le cadre d’une procédure de maintenance ou de test. Laisser non vérifié pendant le fonctionnement normal. Lorsque la réplication entrante est désactivée, les objets peuvent être extraits du nœud de stockage pour être copiés vers d’autres emplacements du système StorageGRID, mais les objets ne peuvent pas être copiés sur ce nœud de stockage à partir d’autres emplacements : le service LDR est en lecture seule.
Désactiver la réplication sortante	DSOR	Sélectionnez cette option pour désactiver la réplication sortante (y compris les demandes de contenu pour les récupérations HTTP) dans le cadre d’une procédure de maintenance ou de test. Laisser non vérifié pendant le fonctionnement normal. Lorsque la réplication sortante est désactivée, les objets peuvent être copiés vers ce nœud de stockage, mais les objets ne peuvent pas être récupérés depuis le nœud de stockage pour être copiés vers d’autres emplacements du système StorageGRID. Le service LDR est en écriture seule.

Gérer des nœuds de stockage complets

Lorsque les nœuds de stockage atteignent leur capacité maximale, ils doivent étendre le système StorageGRID en ajoutant du nouveau stockage. Trois options sont disponibles : ajout de volumes de stockage, ajout de tiroirs d’extension de stockage et ajout de nœuds

de stockage.

Ajout de volumes de stockage

Chaque nœud de stockage prend en charge un nombre maximal de volumes de stockage. Le maximum défini varie selon la plate-forme. Si un nœud de stockage contient moins de volumes de stockage que le nombre maximum, vous pouvez ajouter des volumes pour augmenter sa capacité. Reportez-vous aux instructions pour "Extension d'un système StorageGRID".

Ajout de tiroirs d'extension de stockage

Certains nœuds de stockage StorageGRID, comme le SG6060, peuvent prendre en charge des tiroirs de stockage supplémentaires. Si vos appliances StorageGRID bénéficient de fonctionnalités d'extension qui n'ont pas encore été étendues à leur capacité maximale, vous pouvez ajouter des tiroirs de stockage pour augmenter la capacité. Reportez-vous aux instructions pour "Extension d'un système StorageGRID".

Ajouter des nœuds de stockage

L'ajout de nœuds de stockage permet d'augmenter la capacité de stockage. L'ajout de stockage nécessite de prendre en compte les règles ILM et les exigences de capacité actuellement actives. Reportez-vous aux instructions pour "Extension d'un système StorageGRID".

Gérer les nœuds d'administration

Qu'est-ce qu'un nœud d'administration ?

Des nœuds d'administration qui assurent les services de gestion tels que la configuration du système, la surveillance et la journalisation. Chaque grid doit être connecté à un nœud d'administration principal et doit comporter un nombre quelconque de nœuds d'administration non primaires pour assurer la redondance.

Lorsque vous vous connectez à Grid Manager ou au Gestionnaire de locataires, vous vous connectez à un noeud d'administration. Vous pouvez vous connecter à n'importe quel nœud d'administration et chaque nœud d'administration affiche une vue similaire du système StorageGRID. Cependant, les procédures de maintenance doivent être effectuées à l'aide du nœud d'administration principal.

Les nœuds d'administration peuvent également être utilisés pour équilibrer la charge du trafic des clients S3 et Swift.

Quel est l'expéditeur préféré

Si votre déploiement StorageGRID inclut plusieurs nœuds d'administration, le nœud d'administration principal est l'expéditeur préféré pour les notifications d'alerte, les messages AutoSupport, les traps et les notifications SNMP et les notifications d'alarme héritées.

Dans le cadre des opérations système normales, seul l'expéditeur préféré envoie des notifications. Cependant, tous les autres nœuds d'administration contrôlent l'expéditeur préféré. Si un problème est détecté, les autres nœuds d'administration agissent en tant que *expéditeurs de secours*.

Plusieurs notifications peuvent être envoyées dans les cas suivants :

- Si les nœuds d'administration sont « débarqués » les uns des autres, l'expéditeur préféré et les expéditeurs en veille essayeront d'envoyer des notifications et plusieurs copies de notifications peuvent être reçues.

- Si l’expéditeur en veille détecte des problèmes avec l’expéditeur préféré et commence à envoyer des notifications, l’expéditeur préféré peut retrouver sa capacité à envoyer des notifications. Dans ce cas, des notifications en double peuvent être envoyées. L’expéditeur en attente interrompt l’envoi des notifications lorsqu’il ne détecte plus d’erreurs sur l’expéditeur préféré.

> Lorsque vous testez des messages AutoSupport, tous les nœuds d’administration envoient l’e-mail de test. Lorsque vous testez les notifications d’alertes, vous devez vous connecter à chaque nœud d’administration pour vérifier la connectivité.

Services primaires pour les nœuds d’administration

Le tableau ci-dessous présente les services principaux pour les nœuds d’administration, mais ce tableau ne répertorie pas tous les services de nœud.

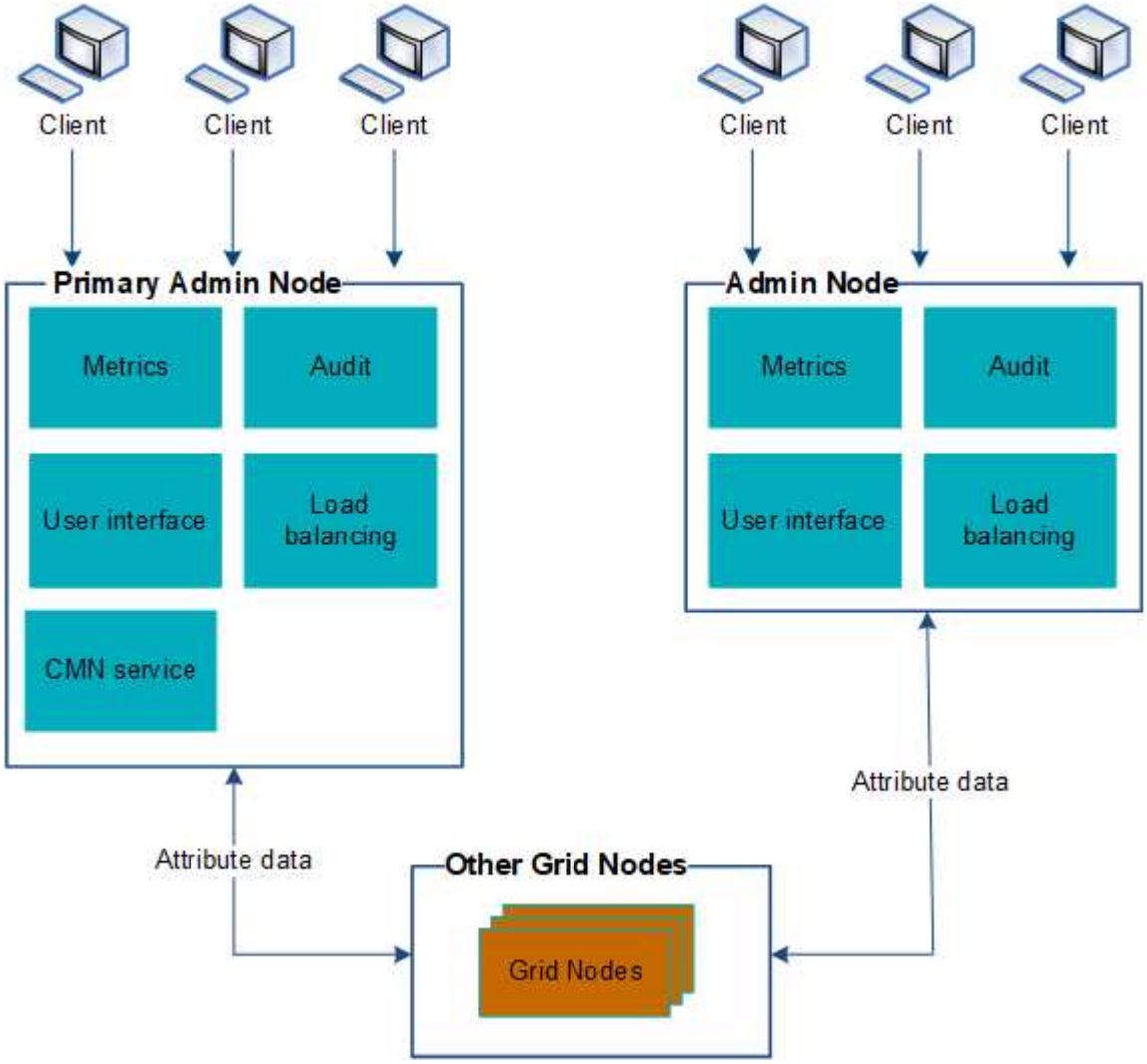
Service	Fonction de touche
Système de gestion des audits (AMS)	Suit l’activité et les événements du système.
Nœud de gestion de la configuration (CMN)	Gestion de la configuration à l’échelle du système. Nœud d’administration principal uniquement.
Interface de gestion du programme d’applications de gestion (api)	Traite les requêtes à partir de l’API de gestion Grid et de l’API de gestion des locataires.
Haute disponibilité	Gère les adresses IP virtuelles haute disponibilité pour les groupes de nœuds d’administration et de nœuds de passerelle. **Remarque :** ce service se trouve également sur les nœuds de passerelle.
Équilibreur de charge	Équilibrage de la charge du trafic S3 et Swift entre les clients et les nœuds de stockage. **Remarque :** ce service se trouve également sur les nœuds de passerelle.
Système de gestion de réseau (NMS)	Fournit des fonctionnalités pour le gestionnaire de grille.
Prometheus	Collecte et stocke les mesures de séries chronologiques des services sur tous les nœuds.
Moniteur d’état du serveur (SSM)	Surveille le système d’exploitation et le matériel sous-jacent.

Utiliser plusieurs nœuds d’administration

Un système StorageGRID peut inclure plusieurs nœuds d’administration pour vous permettre de contrôler et de configurer en continu votre système StorageGRID, même en

cas de panne d'un nœud d'administration.

Si un nœud d'administration devient indisponible, le traitement des attributs continue, les alertes et les alarmes (système hérité) sont toujours déclenchées et les notifications par e-mail et les messages AutoSupport sont toujours envoyés. Toutefois, plusieurs nœuds d'administration n'assurent pas la protection du basculement, à l'exception des notifications et des messages AutoSupport. En particulier, les accusés de réception d'alarme effectués à partir d'un nœud d'administration ne sont pas copiés sur d'autres nœuds d'administration.



Deux options s'offrent à vous pour continuer à afficher et à configurer le système StorageGRID en cas de défaillance d'un nœud d'administration :

- Les clients Web peuvent se reconnecter à tout autre nœud d'administration disponible.
- Si un administrateur système a configuré un groupe de nœuds d'administration haute disponibilité, les clients Web peuvent continuer à accéder à Grid Manager ou au Gestionnaire de locataires à l'aide de l'adresse IP virtuelle du groupe HA. Voir "Gérez les groupes haute disponibilité".

> En cas d'utilisation d'un groupe haute disponibilité, l'accès est interrompu en cas de panne du nœud d'administration actif. Les utilisateurs doivent se reconnecter une fois que l'adresse IP virtuelle du groupe HA bascule vers un autre noeud d'administration du groupe.

Certaines tâches de maintenance peuvent uniquement être effectuées à l'aide du nœud d'administration

principal. En cas de panne du nœud d'administration principal, celui-ci doit être restauré avant que le système StorageGRID ne fonctionne à nouveau entièrement.

Identifiez le nœud d'administration principal

Le nœud d'administration principal héberge le service CMN. Certaines procédures de maintenance peuvent uniquement être effectuées à l'aide du nœud d'administration principal.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous disposez d'autorisations d'accès spécifiques.

Étapes

1. Sélectionnez **SUPPORT** > **Outils** > **topologie de grille**.
2. Sélectionnez ***site*** > **Admin Node**, puis sélectionnez ➕ Pour développer l'arborescence de la topologie et afficher les services hébergés sur ce nœud d'administration.

   Le nœud d'administration principal héberge le service CMN.

3. Si ce nœud d'administration n'héberge pas le service CMN, vérifiez les autres nœuds d'administration.

Afficher l'état des notifications et les files d'attente

Le service Network Management System (NMS) sur les nœuds Admin envoie des notifications au serveur de messagerie. Vous pouvez afficher l'état actuel du service NMS ainsi que la taille de sa file d'attente de notifications sur la page moteur d'interface.

Pour accéder à la page moteur d'interface, sélectionnez **SUPPORT** > **Outils** > **topologie de grille**. Enfin, sélectionnez ***site*** > ***Admin Node*** > **NMS** > **interface Engine**.

Les notifications sont traitées via la file d'attente de notifications par e-mail et sont envoyées au serveur de messagerie l'une après l'autre dans l'ordre dans lequel elles sont déclenchées. En cas de problème (par exemple, une erreur de connexion réseau) et si le serveur de messagerie n'est pas disponible lors de la tentative d'envoi de la notification, une tentative de renvoi de la notification au serveur de messagerie se poursuit pendant une période de 60 secondes. Si la notification n'est pas envoyée au serveur de messagerie après 60 secondes, elle est supprimée de la file d'attente de notifications et une tentative d'envoi de la notification suivante dans la file d'attente est effectuée.

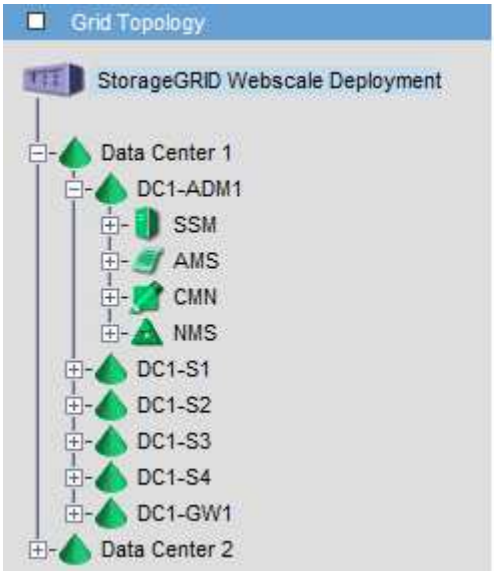
Comme les notifications peuvent être supprimées de la file d'attente de notifications sans être envoyées, il est possible qu'une alarme puisse être déclenchée sans qu'une notification soit envoyée. Si une notification est supprimée de la file d'attente sans être envoyée, l'alarme mineure MIN (État de la notification par e-mail) est déclenchée.

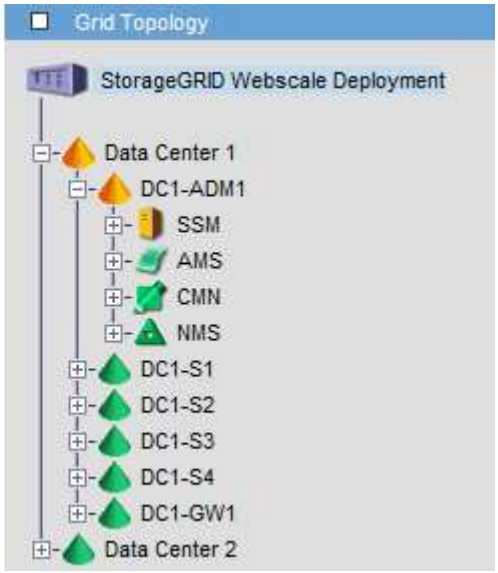
Affichage des alarmes acquittées par les nœuds d'administration (système hérité)

Lorsque vous accusez réception d'une alarme sur un nœud d'administration, l'alarme acquittée n'est copiée sur aucun autre nœud d'administration. Étant donné que les accusés de réception ne sont pas copiés sur d'autres nœuds d'administration, l'arborescence de la topologie de la grille peut ne pas être identique pour chaque nœud

d’administration.

Cette différence peut être utile lors de la connexion de clients Web. Les clients Web peuvent avoir différentes vues du système StorageGRID selon les besoins de l’administrateur.





Notez que les notifications sont envoyées depuis le nœud d’administration où l’accusé de réception a lieu.

Configurez l’accès client d’audit

Configurer l’accès client d’audit pour NFS

Le nœud d’administration, via le service AMS (Audit Management System), consigne tous les événements système vérifiés dans un fichier journal disponible via le partage d’audit, qui est ajouté à chaque nœud d’administration lors de l’installation. Le partage d’audit est automatiquement activé en tant que partage en lecture seule.

Pour accéder aux journaux d’audit, vous pouvez configurer l’accès client aux partages d’audit pour NFS. Ou bien, c’est possible "utilisez un serveur syslog externe".

Le système StorageGRID utilise une reconnaissance positive pour éviter toute perte de messages d’audit avant qu’ils ne soient écrits dans le fichier journal. Un message reste placé dans la file d’attente d’un service jusqu’à ce que le service AMS ou un service de relais d’audit intermédiaire en ait reconnu le contrôle. Pour plus d’informations, voir "Examiner les journaux d’audit".

Avant de commencer

- Vous avez le `Passwords.txt` avec le mot de passe root/admin.
- Vous avez le `Configuration.txt` Fichier (disponible dans le progiciel de récupération).
- Le client d’audit utilise NFS version 3 (NFSv3).

Description de la tâche

Effectuez cette procédure pour chaque nœud d’administration d’un déploiement StorageGRID à partir duquel vous souhaitez récupérer des messages d’audit.

Étapes

1. Connectez-vous au nœud d'administration principal :
   a. Saisissez la commande suivante : `ssh admin@primary_Admin_Node_IP`
   b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
   c. Entrez la commande suivante pour passer à la racine : `su -`
   d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

      Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

2. Vérifiez que tous les services sont en cours d'exécution ou vérifiés. Entrez : `storagegrid-status`

   Si certains services ne sont pas répertoriés comme étant en cours d'exécution ou vérifiés, résolvez les problèmes avant de continuer.

3. Revenez à la ligne de commande. Appuyez sur **Ctrl+C**.
4. Démarrez l'utilitaire de configuration NFS. Entrez : `config_nfs.rb`

```
------------------------------------------------------------------
| Shares                | Clients              | Config          |
------------------------------------------------------------------
| add-audit-share       | add-ip-to-share      | validate-config |
| enable-disable-share  | remove-ip-from-share | refresh-config  |
|                       |                      | help            |
|                       |                      | exit            |
------------------------------------------------------------------
```

5. Ajouter le client d'audit : `add-audit-share`
   a. Lorsque vous y êtes invité, entrez l'adresse IP ou la plage d'adresses IP du client d'audit pour le partage d'audit : `client_IP_address`
   b. Lorsque vous y êtes invité, appuyez sur **entrée**.
6. Si plusieurs clients d'audit sont autorisés à accéder au partage d'audit, ajoutez l'adresse IP de l'utilisateur supplémentaire : `add-ip-to-share`
   a. Entrez le numéro du partage d'audit : *`audit_share_number`*
   b. Lorsque vous y êtes invité, entrez l'adresse IP ou la plage d'adresses IP du client d'audit pour le partage d'audit : *`client_IP_address`*
   c. Lorsque vous y êtes invité, appuyez sur **entrée**.

      L'utilitaire de configuration NFS s'affiche.

   d. Répétez ces sous-étapes pour chaque client d'audit supplémentaire ayant accès au partage d'audit.
7. Vérifiez éventuellement votre configuration.
   a. Saisissez les informations suivantes : `validate-config`

      Les services sont vérifiés et affichés.

b. Lorsque vous y êtes invité, appuyez sur **entrée**.

   L'utilitaire de configuration NFS s'affiche.

c. Fermez l'utilitaire de configuration NFS : `exit`

8. Déterminez si vous devez activer des partages d'audit sur d'autres sites.
   - Si le déploiement de StorageGRID est un site unique, passez à l'étape suivante.
   - Si le déploiement de StorageGRID inclut des nœuds d'administration sur d'autres sites, activez ces partages d'audit si nécessaire :
     i. Connectez-vous à distance au nœud d'administration du site :
        A. Saisissez la commande suivante : `ssh admin@grid_node_IP`
        B. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
        C. Entrez la commande suivante pour passer à la racine : `su -`
        D. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
     ii. Répétez cette procédure pour configurer les partages d'audit pour chaque nœud d'administration supplémentaire.
     iii. Fermez la connexion du shell sécurisé distant au nœud d'administration distant. Entrez : `exit`
9. Déconnectez-vous du shell de commande : `exit`

Les clients d'audit NFS ont accès à un partage d'audit en fonction de leur adresse IP. Accordez l'accès au partage d'audit à un nouveau client d'audit NFS en ajoutant son adresse IP au partage ou supprimez un client d'audit existant en supprimant son adresse IP.

Ajouter un client d'audit NFS à un partage d'audit

Les clients d'audit NFS ont accès à un partage d'audit en fonction de leur adresse IP. Accorder l'accès au partage d'audit à un nouveau client d'audit NFS en ajoutant son adresse IP au partage d'audit.

Avant de commencer

- Vous avez le `Passwords.txt` avec le mot de passe du compte root/admin.
- Vous avez le `Configuration.txt` Fichier (disponible dans le progiciel de récupération).
- Le client d'audit utilise NFS version 3 (NFSv3).

Étapes

1. Connectez-vous au nœud d'administration principal :
   a. Saisissez la commande suivante : `ssh admin@primary_Admin_Node_IP`
   b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
   c. Entrez la commande suivante pour passer à la racine : `su -`
   d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

      Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

2. Démarrez l'utilitaire de configuration NFS : `config_nfs.rb`

```
------------------------------------------------------------------
| Shares               | Clients              | Config          |
------------------------------------------------------------------
| add-audit-share      | add-ip-to-share      | validate-config |
| enable-disable-share | remove-ip-from-share | refresh-config  |
|                      |                      | help            |
|                      |                      | exit            |
------------------------------------------------------------------
```

3. Entrez : `add-ip-to-share`

   La liste des partages d'audit NFS activés sur le nœud d'administration s'affiche. Le partage d'audit est répertorié comme suit : `/var/local/audit/export`

4. Entrez le numéro du partage d'audit : *`audit_share_number`*
5. Lorsque vous y êtes invité, entrez l'adresse IP ou la plage d'adresses IP du client d'audit pour le partage d'audit : *`client_IP_address`*

   Le client d'audit est ajouté au partage d'audit.

6. Lorsque vous y êtes invité, appuyez sur **entrée**.

   L'utilitaire de configuration NFS s'affiche.

7. Répétez les étapes pour chaque client d'audit qui doit être ajouté au partage d'audit.
8. Vérifiez éventuellement votre configuration : `validate-config`

   Les services sont vérifiés et affichés.

   a. Lorsque vous y êtes invité, appuyez sur **entrée**.

      L'utilitaire de configuration NFS s'affiche.

9. Fermez l'utilitaire de configuration NFS : `exit`
10. Si le déploiement de StorageGRID est un site unique, passez à l'étape suivante.

    Si le déploiement StorageGRID inclut des nœuds d'administration sur d'autres sites, activez éventuellement ces partages d'audit si nécessaire :

    a. Connectez-vous à distance au nœud d'administration d'un site :
       i. Saisissez la commande suivante : `ssh admin@`*`grid_node_IP`*
       ii. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
       iii. Entrez la commande suivante pour passer à la racine : `su -`
       iv. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
    b. Répétez cette procédure pour configurer les partages d'audit pour chaque nœud d'administration.

c. Fermez la connexion du shell sécurisé distant au nœud d'administration distant : `exit`

11. Déconnectez-vous du shell de commande : `exit`

Vérifier l'intégration de l'audit NFS

Après avoir configuré un partage d'audit et ajouté un client d'audit NFS, vous pouvez monter le partage client d'audit et vérifier que les fichiers sont disponibles à partir du partage d'audit.

Étapes

1. Vérifiez la connectivité (ou la variante du système client) à l'aide de l'adresse IP côté client du nœud d'administration hébergeant le service AMS. Entrez : `ping IP_address`

   Vérifiez que le serveur répond, indiquant la connectivité.

2. Montez le partage d'audit en lecture seule à l'aide d'une commande appropriée au système d'exploitation client. Un exemple de commande Linux est (entrez sur une ligne) :

   `mount -t nfs -o hard,intr Admin_Node_IP_address:/var/local/audit/export myAudit`

   Utilisez l'adresse IP du nœud d'administration hébergeant le service AMS et le nom de partage prédéfini pour le système d'audit. Le point de montage peut être n'importe quel nom sélectionné par le client (par exemple, *myAudit* dans la commande précédente).

3. Vérifiez que les fichiers sont disponibles à partir du partage d'audit. Entrez : `ls myAudit /*`

   où *myAudit* est le point de montage du partage d'audit. Au moins un fichier journal doit être répertorié.

Supprimer un client d'audit NFS du partage d'audit

Les clients d'audit NFS ont accès à un partage d'audit en fonction de leur adresse IP. Vous pouvez supprimer un client d'audit existant en supprimant son adresse IP.

Avant de commencer

- Vous avez le `Passwords.txt` avec le mot de passe du compte root/admin.
- Vous avez le `Configuration.txt` Fichier (disponible dans le progiciel de récupération).

Description de la tâche

Vous ne pouvez pas supprimer la dernière adresse IP autorisée pour accéder au partage d'audit.

Étapes

1. Connectez-vous au nœud d'administration principal :
   a. Saisissez la commande suivante : `ssh admin@primary_Admin_Node_IP`
   b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
   c. Entrez la commande suivante pour passer à la racine : `su -`
   d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

2. Démarrez l'utilitaire de configuration NFS : `config_nfs.rb`

```
------------------------------------------------------------------
| Shares                | Clients               | Config          |
------------------------------------------------------------------
| add-audit-share       | add-ip-to-share       | validate-config |
| enable-disable-share  | remove-ip-from-share  | refresh-config  |
|                       |                       | help            |
|                       |                       | exit            |
------------------------------------------------------------------
```

3. Supprimez l'adresse IP du partage d'audit : `remove-ip-from-share`

   Une liste numérotée de partages d'audit configurés sur le serveur s'affiche. Le partage d'audit est répertorié comme suit : `/var/local/audit/export`

4. Saisissez le numéro correspondant au partage d'audit : *`audit_share_number`*

   Une liste numérotée d'adresses IP autorisées à accéder au partage d'audit s'affiche.

5. Saisissez le numéro correspondant à l'adresse IP que vous souhaitez supprimer.

   Le partage d'audit est mis à jour et l'accès n'est plus autorisé à partir d'un client d'audit possédant cette adresse IP.

6. Lorsque vous y êtes invité, appuyez sur **entrée**.

   L'utilitaire de configuration NFS s'affiche.

7. Fermez l'utilitaire de configuration NFS : `exit`
8. Si votre déploiement StorageGRID est un déploiement de plusieurs sites de data Center avec des nœuds d'administration supplémentaires sur les autres sites, désactivez les partages d'audit suivants :
   a. Connectez-vous à distance au nœud d'administration de chaque site :
      i. Saisissez la commande suivante : `ssh admin@`*`grid_node_IP`*
      ii. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
      iii. Entrez la commande suivante pour passer à la racine : `su -`
      iv. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
   b. Répétez cette procédure pour configurer les partages d'audit pour chaque nœud d'administration supplémentaire.
   c. Fermez la connexion du shell sécurisé distant au nœud d'administration distant : `exit`
9. Déconnectez-vous du shell de commande : `exit`

Modifier l'adresse IP d'un client d'audit NFS

Procédez comme suit si vous devez modifier l'adresse IP d'un client d'audit NFS.

Étapes

1. Ajouter une nouvelle adresse IP à un partage d'audit NFS existant.
2. Supprimez l'adresse IP d'origine.

Informations associées

- "Ajouter un client d'audit NFS à un partage d'audit"
- "Supprimer un client d'audit NFS du partage d'audit"

Gérer les nœuds d'archivage

Qu'est-ce qu'un nœud d'archivage ?

En option, chaque site de data Center StorageGRID peut être déployé avec un nœud d'archivage, ce qui vous permet de vous connecter à un système de stockage d'archivage externe ciblé, tel que Tivoli Storage Manager (TSM).

> ! La prise en charge des nœuds d'archivage (pour l'archivage dans le cloud à l'aide de l'API S3 et l'archivage sur bande à l'aide du middleware TSM) est obsolète et sera supprimée dans une prochaine version. Le déplacement d'objets d'un nœud d'archivage vers un système de stockage d'archives externe a été remplacé par les pools de stockage cloud ILM pour offrir davantage de fonctionnalités.
>
> Voir :
>
> - "Migration des objets vers un pool de stockage cloud"
> - "Utilisation des pools de stockage cloud"
>
> De plus, vous devez supprimer les nœuds d'archivage de la règle ILM active dans StorageGRID 11.7 ou version antérieure. La suppression des données d'objet stockées sur les nœuds d'archivage simplifie les mises à niveau futures. Voir "Utilisation des règles ILM et des règles ILM".

Le nœud d'archivage fournit une interface par le biais de laquelle vous pouvez cibler un système de stockage d'archives externe pour le stockage à long terme des données d'objet. Le nœud d'archivage surveille également cette connexion et le transfert des données d'objet entre le système StorageGRID et le système de stockage d'archives externes ciblé.

Après avoir configuré les connexions à la cible externe, vous pouvez configurer le nœud d'archivage pour optimiser les performances TSM, mettre un nœud d'archivage hors ligne lorsqu'un serveur TSM atteint sa capacité ou est indisponible, et configurer les paramètres de réplication et de récupération. Vous pouvez également définir des alarmes personnalisées pour le nœud d'archivage.

Les données d'objet qui ne peuvent pas être supprimées, mais qui ne sont pas régulièrement consultées, peuvent à tout moment être déplacées depuis les disques rotatifs d'un nœud de stockage et vers un stockage d'archivage externe tel que le cloud ou la bande. Cet archivage des données d'objet s'effectue via la configuration du nœud d'archivage d'un site de data Center, puis la configuration des règles ILM sur lesquelles ce nœud d'archivage est sélectionné comme « cible » pour les instructions de placement de contenu. Le nœud d'archivage ne gère pas les données d'objet archivées lui-même, ce qui est réalisé par le dispositif d'archivage

externe.

Les métadonnées de l'objet ne sont pas archivées, mais restent sur les nœuds de stockage.

Qu'est-ce que le service ARC

Le service d'archivage (ARC) sur les nœuds d'archivage fournit l'interface de gestion que vous pouvez utiliser pour configurer les connexions au système de stockage d'archivage externe, comme les bandes via le middleware TSM.

Il s'agit du service ARC qui interagit avec un système de stockage d'archives externe, en envoyant des données d'objet pour le stockage secondaire et en effectuant des récupérations lorsqu'une application client demande un objet archivé. Lorsqu'une application client demande un objet archivé, un nœud de stockage demande les données de l'objet au service ARC. Le service ARC envoie une demande au système de stockage d'archives externe, qui récupère les données de l'objet demandé et les envoie au service ARC. Le service ARC vérifie les données de l'objet et les transfère au nœud de stockage, qui renvoie alors l'objet à l'application client requérant.

Les demandes de données d'objet archivées sur bande via un middleware TSM sont gérées pour optimiser les récupérations. Les demandes peuvent être commandées de façon à ce que les objets stockés dans l'ordre séquentiel sur bande soient demandés dans le même ordre séquentiel. Les demandes sont alors mises en file d'attente pour soumission à l'unité de stockage. En fonction du périphérique d'archivage, plusieurs demandes d'objets sur différents volumes peuvent être traitées simultanément.

Archivez vos données dans le cloud via l'API S3

Vous pouvez configurer un nœud d'archivage pour qu'il se connecte directement à Amazon Web Services (AWS) ou à tout autre système capable de s'interfacer avec le système StorageGRID via l'API S3.

La prise en charge des nœuds d'archivage (pour l'archivage dans le cloud à l'aide de l'API S3 et l'archivage sur bande à l'aide du middleware TSM) est obsolète et sera supprimée dans une prochaine version. Le déplacement d'objets d'un nœud d'archivage vers un système de stockage d'archives externe a été remplacé par les pools de stockage cloud ILM pour offrir davantage de fonctionnalités.

Voir "Utilisation des pools de stockage cloud".

Configurez les paramètres de connexion pour l'API S3

Si vous vous connectez à un noeud d'archivage à l'aide de l'interface S3, vous devez configurer les paramètres de connexion de l'API S3. Tant que ces paramètres ne sont pas configurés, le service ARC reste dans un état d'alarme majeur car il ne parvient pas à communiquer avec le système de stockage d'archives externe.

La prise en charge des nœuds d'archivage (pour l'archivage dans le cloud à l'aide de l'API S3 et l'archivage sur bande à l'aide du middleware TSM) est obsolète et sera supprimée dans une prochaine version. Le déplacement d'objets d'un nœud d'archivage vers un système de stockage d'archives externe a été remplacé par les pools de stockage cloud ILM pour offrir davantage de fonctionnalités.

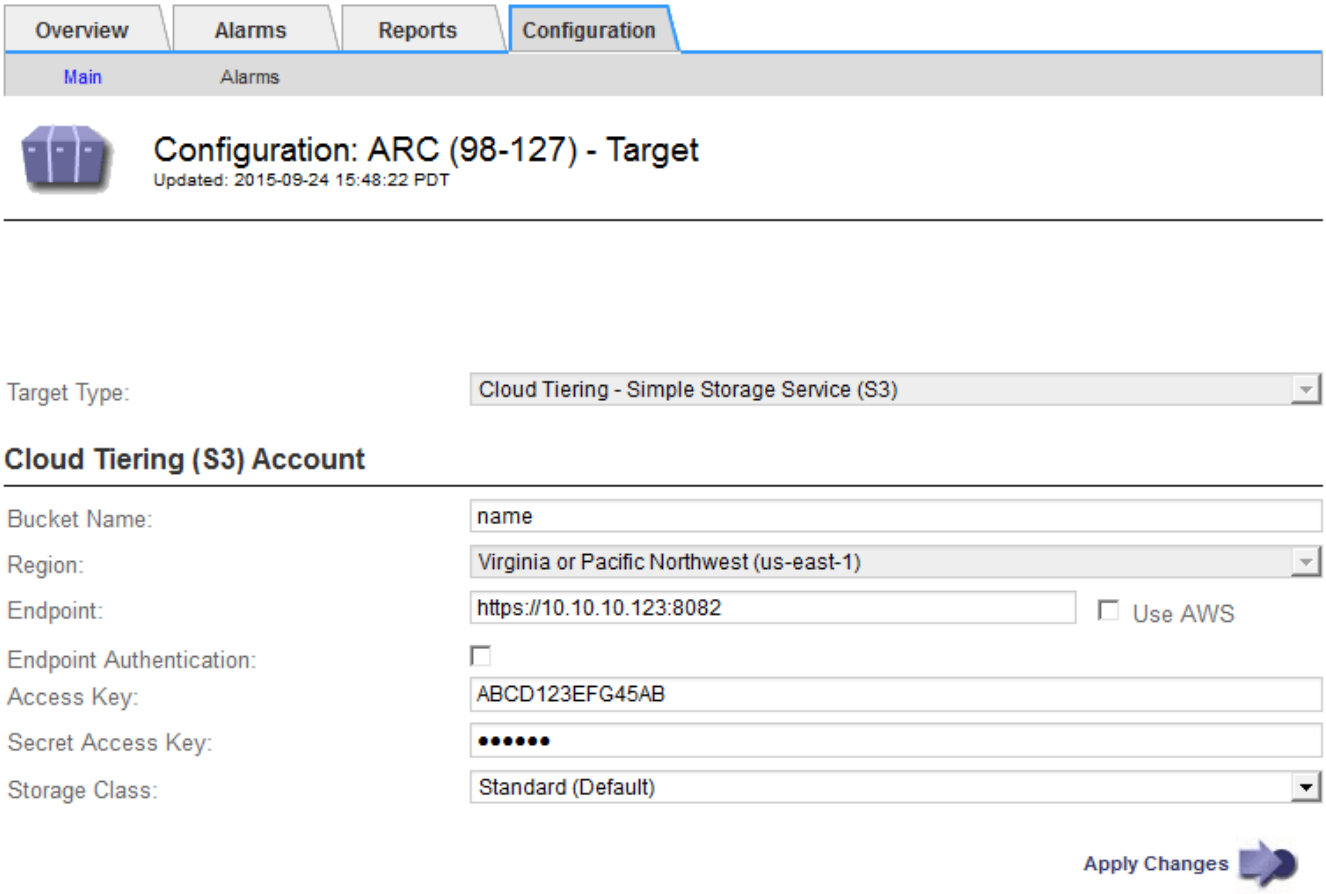
Voir "Utilisation des pools de stockage cloud".

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous disposez d'autorisations d'accès spécifiques.
- Vous avez créé un compartiment sur le système de stockage d'archivage cible :
  - Le compartiment est dédié à un seul nœud d'archivage. Il ne peut pas être utilisé par d'autres nœuds d'archivage ou d'autres applications.
  - La région du compartiment est sélectionnée pour votre emplacement.
  - Le compartiment doit être configuré avec une gestion des versions suspendue.
- La segmentation d'objet est activée et la taille de segment maximale est inférieure ou égale à 4.5 Gio (4,831,838,208 octets). Les demandes d'API S3 qui dépassent cette valeur échouent si S3 est utilisé comme système de stockage d'archivage externe.

Étapes

1. Sélectionnez **SUPPORT** > **Outils** > **topologie de grille**.
2. Sélectionnez **Archive Node** > **ARC** > **Target**.
3. Sélectionnez **Configuration** > **main**.



4. Sélectionnez **Cloud Tiering - simple Storage Service (S3)** dans la liste déroulante Type de cible.

> Les paramètres de configuration ne sont pas disponibles tant que vous n'avez pas sélectionné de type cible.

5. Configurez le compte de Tiering cloud (S3) via lequel le nœud d'archivage se connecte au système de

stockage d'archivage externe cible compatible S3.

La plupart des champs de cette page sont explicites. La section suivante décrit les champs pour lesquels vous avez peut-être besoin d'aide.

- **Région** : disponible uniquement si **Use AWS** est sélectionné. La région que vous sélectionnez doit correspondre à la région du compartiment.
- **Endpoint** et **use AWS** : pour Amazon Web Services (AWS), sélectionnez **use AWS**. **Endpoint** est alors automatiquement renseigné avec une URL de point de terminaison en fonction des attributs Nom du compartiment et région. Par exemple :

  ```
  https://bucket.region.amazonaws.com
  ```

  Pour une cible non AWS, entrez l'URL du système hébergeant le compartiment, y compris le numéro de port. Par exemple :

```
https://system.com:1080
```

- **Authentification par point de terminaison** : activée par défaut. Si le réseau vers le système de stockage d'archives externe est approuvé, vous pouvez décocher la case pour désactiver la vérification du certificat SSL de point final et du nom d'hôte pour le système de stockage d'archives externe ciblé. Si une autre instance d'un système StorageGRID est le périphérique de stockage d'archives cible et que le système est configuré avec des certificats signés publiquement, vous pouvez garder la case cochée.
- **Classe de stockage** : sélectionnez **Standard (par défaut)** pour le stockage normal. Sélectionnez **réduction de redondance** uniquement pour les objets qui peuvent être facilement recréés. **Redondance réduite** fournit un stockage moins coûteux et moins fiable. Si le système de stockage d'archives cible est une autre instance du système StorageGRID, **Storage Class** contrôle le nombre de copies intermédiaires de l'objet à l'entrée sur le système cible, si la double validation est utilisée lors de l'ingestion d'objets.

6. Sélectionnez **appliquer les modifications**.

   Les paramètres de configuration spécifiés sont validés et appliqués à votre système StorageGRID. Une fois configuré, la cible ne peut pas être modifiée.

Modifiez les paramètres de connexion de l'API S3

Une fois que le nœud d'archivage est configuré pour se connecter à un système de stockage d'archives externe via l'API S3, vous pouvez modifier certains paramètres en cas de modification de la connexion.

Avant de commencer

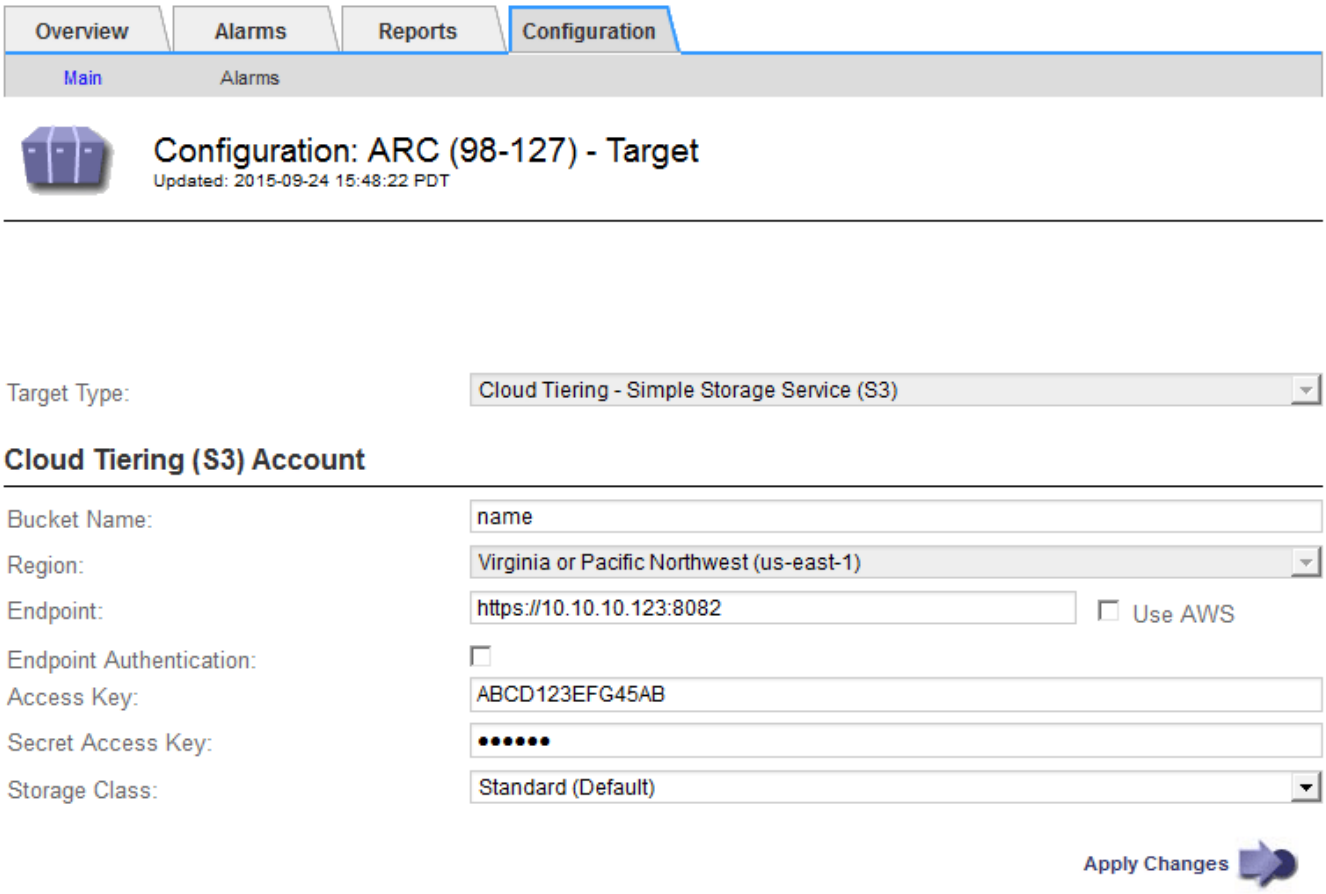
- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous disposez d'autorisations d'accès spécifiques.

Description de la tâche

Si vous modifiez le compte Cloud Tiering (S3), vous devez vous assurer que les identifiants d'accès utilisateur ont un accès en lecture/écriture au compartiment, y compris tous les objets précédemment ingérées par le nœud d'archivage vers le compartiment.

Étapes

1. Sélectionnez **SUPPORT** > **Outils** > **topologie de grille**.
2. Sélectionnez ***Archive Node*** > **ARC** > **cible**.
3. Sélectionnez **Configuration** > **main**.



4. Modifiez les informations de compte si nécessaire.

   Si vous modifiez la classe de stockage, les nouvelles données d'objet sont stockées avec la nouvelle classe de stockage. Un objet existant reste stocké sous la classe de stockage définie lors de l'ingestion.

   > Le nom de compartiment, la région et le terminal, utilisent des valeurs AWS et ne peuvent pas être modifiés.

5. Sélectionnez **appliquer les modifications**.

Modifiez l'état du service NetApp Cloud Tiering

Vous pouvez contrôler la capacité de lecture et d'écriture du nœud d'archivage sur le système de stockage d'archives externe ciblé qui se connecte via l'API S3 en modifiant l'état du service de Tiering cloud.

Avant de commencer

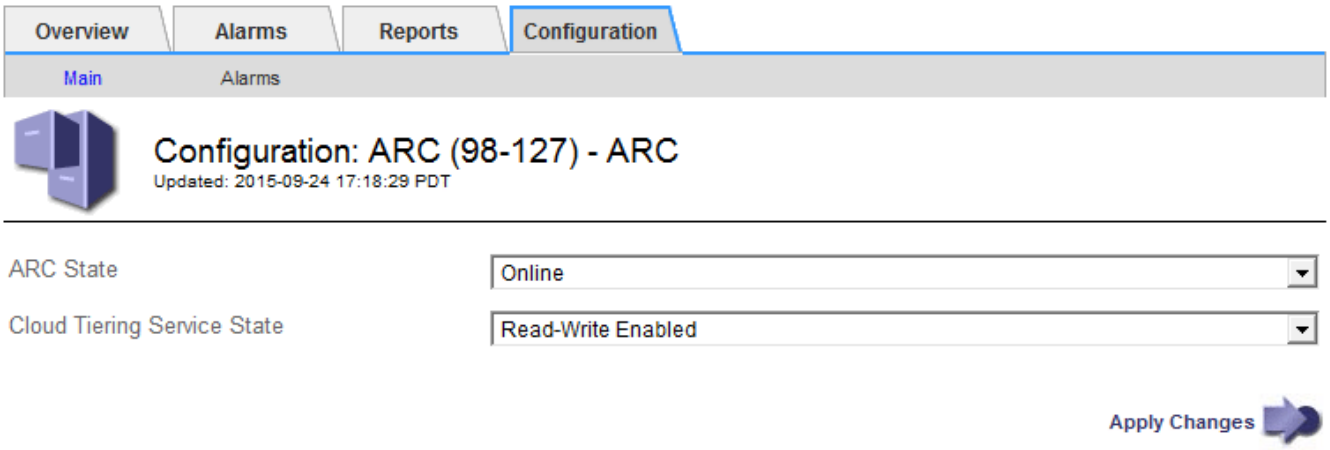
- Vous devez être connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous devez disposer d'autorisations d'accès spécifiques.
- Le nœud d'archivage doit être configuré.

Description de la tâche

Vous pouvez mettre le nœud d'archivage hors ligne en changeant l'état du service de Tiering cloud sur **Read-Write Disabled**.

Étapes

1. Sélectionnez **SUPPORT** > **Outils** > **topologie de grille**.
2. Sélectionnez ***Archive Node*** > **ARC**.
3. Sélectionnez **Configuration** > **main**.



4. Sélectionnez un **Cloud Tiering Service State**.
5. Sélectionnez **appliquer les modifications**.

Réinitialisez le nombre d'échecs de stockage pour la connexion API S3

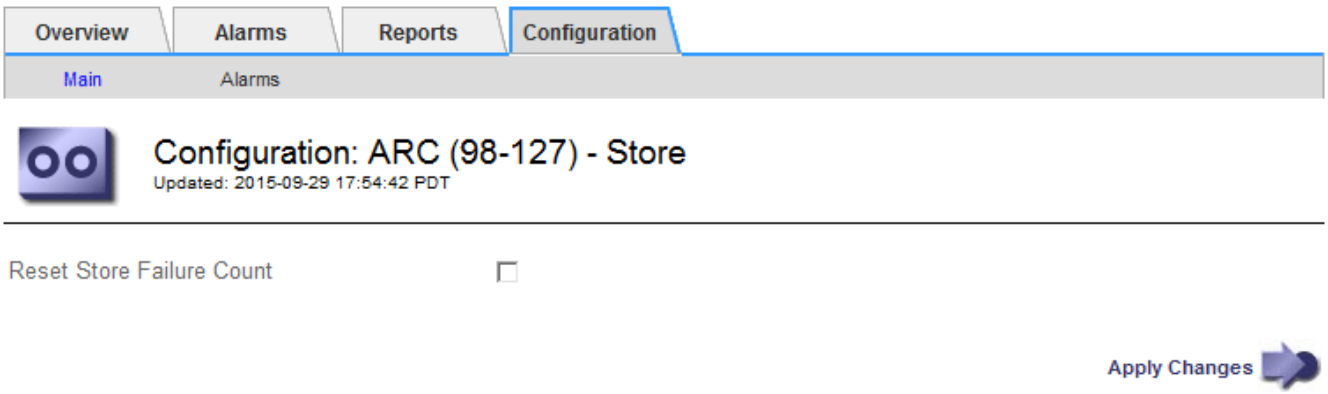
Si votre nœud d'archivage se connecte à un système de stockage d'archives via l'API S3, vous pouvez réinitialiser le nombre d'échecs de stockage, qui peut être utilisé pour effacer l'alarme ARVF (échecs de stockage).

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous disposez d'autorisations d'accès spécifiques.

Étapes

1. Sélectionnez **SUPPORT** > **Outils** > **topologie de grille**.
2. Sélectionnez ***Archive Node*** > **ARC** > **Store**.
3. Sélectionnez **Configuration** > **main**.



4. Sélectionnez **Réinitialiser le nombre d'échecs de stockage**.
5. Sélectionnez **appliquer les modifications**.

   L'attribut Store Failures se réinitialise sur zéro.

Migrer des objets depuis Cloud Tiering - S3 vers un pool de stockage cloud

Si vous utilisez actuellement la fonctionnalité **Cloud Tiering - simple Storage Service (S3)** pour hiérarchiser les données d'objet vers un compartiment S3, vous devez migrer vos objets vers un pool de stockage cloud. Les pools de stockage cloud offrent une approche évolutive qui tire parti de tous les nœuds de stockage dans votre système StorageGRID.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous disposez d'autorisations d'accès spécifiques.
- Des objets sont déjà stockés dans le compartiment S3 configuré pour le Tiering dans le cloud.

> Avant de migrer les données d'objet, contactez votre ingénieur commercial NetApp pour comprendre et gérer les coûts éventuels associés.

Description de la tâche

Le pool de stockage cloud est similaire à celui d'un pool de stockage du point de vue ILM. Toutefois, si les pools de stockage sont constitués de nœuds de stockage ou de nœuds d'archivage dans le système StorageGRID, un pool de stockage cloud est constitué d'un compartiment S3 externe.

Avant de migrer les objets depuis Cloud Tiering - S3 vers un pool de stockage cloud, vous devez d'abord créer un compartiment S3, puis créer le pool de stockage cloud dans StorageGRID. Vous pouvez ensuite créer une nouvelle règle ILM et remplacer la règle ILM utilisée pour stocker les objets dans le compartiment Cloud Tiering par une règle ILM clonée qui stocke les mêmes objets dans le pool de stockage cloud.

> Lorsque des objets sont stockés dans un pool de stockage cloud, des copies de ces objets ne peuvent pas non plus être stockées dans StorageGRID. Si la règle ILM que vous utilisez actuellement pour Cloud Tiering est configurée pour stocker les objets en même temps, déterminez si vous souhaitez toujours effectuer cette migration facultative, car elle sera perdue. Si vous continuez cette migration, vous devez créer de nouvelles règles au lieu de cloner les règles existantes.

Étapes

1. Création d'un pool de stockage cloud.

   Utilisez un nouveau compartiment S3 pour le pool de stockage cloud afin de garantir que celui-ci contient uniquement les données gérées par le pool de stockage cloud.

2. Recherchez toutes les règles ILM de la règle ILM active qui entraîne le stockage des objets dans le compartiment de NetApp Cloud Tiering.
3. Clonez chacune de ces règles.
4. Dans les règles clonées, modifiez l'emplacement de placement dans le nouveau pool de stockage cloud.
5. Enregistrez les règles clonées.
6. Création d'une nouvelle règle qui utilise les nouvelles règles
7. Simuler et activer la nouvelle règle.

   Lorsque la nouvelle règle est activée et que l'évaluation ILM est effectuée, les objets sont déplacés du compartiment S3 configuré pour NetApp Cloud Tiering vers le compartiment S3 configuré pour le pool de stockage cloud. L'espace utilisable sur la grille n'est pas affecté. Une fois les objets déplacés vers le pool de stockage cloud, ils sont supprimés du compartiment de NetApp Cloud Tiering.

Informations associées

"Gestion des objets avec ILM"

Archivez vos données sur bande via le logiciel médiateur TSM

Vous pouvez configurer un nœud d'archivage pour qu'il cible un serveur Tivoli Storage Manager (TSM) qui fournit une interface logique permettant de stocker et de récupérer des données d'objet sur des unités de stockage à accès aléatoire ou séquentiel, y compris des librairies de bandes.

Le service ARC du nœud d'archivage sert de client au serveur TSM, utilisant Tivoli Storage Manager comme logiciel médiateur pour communiquer avec le système de stockage d'archives.

> La prise en charge des nœuds d'archivage (pour l'archivage dans le cloud à l'aide de l'API S3 et l'archivage sur bande à l'aide du middleware TSM) est obsolète et sera supprimée dans une prochaine version. Le déplacement d'objets d'un nœud d'archivage vers un système de stockage d'archives externe a été remplacé par les pools de stockage cloud ILM pour offrir davantage de fonctionnalités.
>
> Voir "Utilisation des pools de stockage cloud".

Cours de gestion TSM

Les classes de gestion définies par le middleware TSM décrivent le fonctionnement des opérations de sauvegarde et d'archivage de TSM's et peuvent être utilisées pour spécifier les règles du contenu appliqué par le serveur TSM. Ces règles fonctionnent indépendamment de la politique ILM du système StorageGRID et doivent rester cohérentes avec StorageGRID la condition que les objets soient stockés de manière permanente et soient toujours disponibles pour la récupération par le nœud d'archivage. Une fois les données d'objet envoyées à un serveur TSM par le nœud d'archivage, les règles de cycle de vie et de conservation TSM sont appliquées pendant que les données de l'objet sont stockées sur bande gérée par le serveur TSM.

La classe de gestion TSM est utilisée par le serveur TSM pour appliquer des règles pour l'emplacement ou la conservation des données après que les objets soient envoyés au serveur TSM par le nœud d'archivage. Par exemple, les objets identifiés comme sauvegardes de bases de données (contenu temporaire pouvant être remplacé par des données plus récentes) peuvent être traités différemment des données d'application (contenu fixe qui doit être conservé indéfiniment).

Configurer les connexions au middleware TSM

Avant que le nœud d'archivage puisse communiquer avec le middleware Tivoli Storage Manager (TSM), vous devez configurer plusieurs paramètres.

Avant de commencer

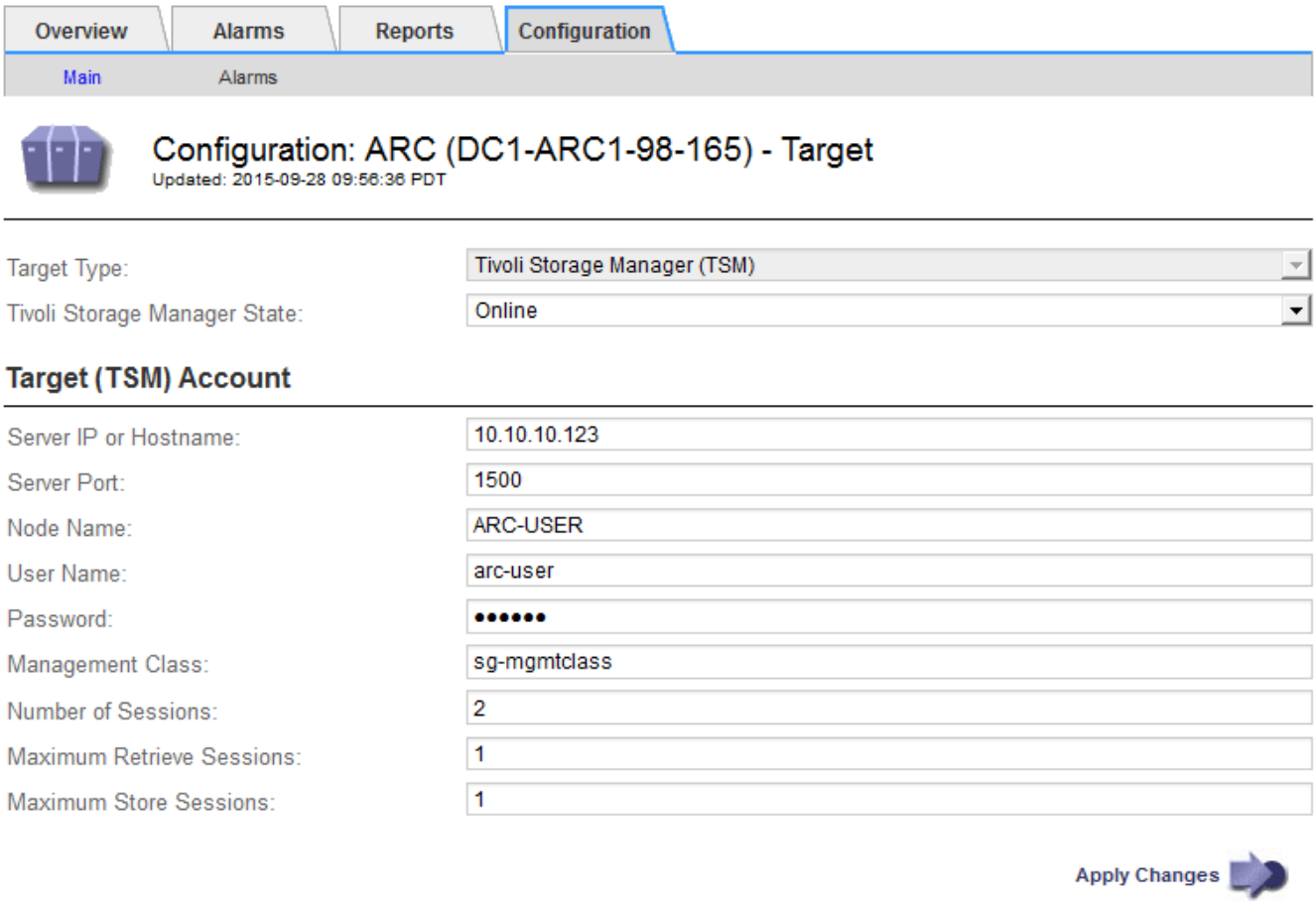
- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous disposez d'autorisations d'accès spécifiques.

Description de la tâche

Tant que ces paramètres ne sont pas configurés, le service ARC reste dans un état d'alarme majeur car il ne peut pas communiquer avec Tivoli Storage Manager.

Étapes

1. Sélectionnez **SUPPORT** > **Outils** > **topologie de grille**.
2. Sélectionnez ***Archive Node*** > **ARC** > **cible**.
3. Sélectionnez **Configuration** > **main**.



4. Dans la liste déroulante **Type cible**, sélectionnez **Tivoli Storage Manager (TSM)**.

5. Pour l'état **Tivoli Storage Manager**, sélectionnez **Offline** pour empêcher les récupérations du serveur middleware TSM.

   Par défaut, l'état Tivoli Storage Manager est défini sur en ligne, ce qui signifie que le noeud d'archivage peut récupérer des données d'objet à partir du serveur middleware TSM.

6. Complétez les informations suivantes :

   - **IP ou Nom d'hôte du serveur** : spécifiez l'adresse IP ou le nom de domaine complet du serveur middleware TSM utilisé par le service ARC. L'adresse IP par défaut est 127.0.0.1.
   - **Port serveur** : spécifiez le numéro de port sur le serveur middleware TSM auquel le service ARC se connectera. La valeur par défaut est 1500.
   - **Nom du noeud** : spécifiez le nom du noeud d'archive. Vous devez entrer le nom (utilisateur d'arc) que vous avez enregistré sur le serveur middleware TSM.
   - **Nom d'utilisateur** : spécifiez le nom d'utilisateur utilisé par le service ARC pour se connecter au serveur TSM. Entrez le nom d'utilisateur par défaut (utilisateur d'arc) ou l'utilisateur administratif spécifié pour le noeud d'archivage.
   - **Mot de passe** : Indiquez le mot de passe utilisé par le service ARC pour se connecter au serveur TSM.
   - **Classe de gestion** : spécifiez la classe de gestion par défaut à utiliser si une classe de gestion n'est pas spécifiée lors de l'enregistrement de l'objet sur le système StorageGRID ou si la classe de gestion spécifiée n'est pas définie sur le serveur middleware TSM.
   - **Nombre de sessions** : spécifiez le nombre de lecteurs de bande sur le serveur middleware TSM dédié au nœud d'archivage. Le nœud d'archivage crée simultanément un maximum d'une session par point de montage et un petit nombre de sessions supplémentaires (moins de cinq).

     Vous devez modifier cette valeur pour qu'elle soit identique à la valeur définie pour MAXNUMMP (nombre maximal de points de montage) lorsque le nœud d'archivage a été enregistré ou mis à jour. (Dans la commande REGISTER, la valeur par défaut de MAXNUMMP utilisée est 1, si aucune valeur n'est définie.)

   Vous devez également modifier la valeur de MAXSESSIONS pour le serveur TSM à un nombre au moins aussi important que le nombre de sessions défini pour le service ARC. La valeur par défaut de MAXSESSIONS sur le serveur TSM est 25.

   - **Nombre maximal de sessions de récupération** : spécifiez le nombre maximal de sessions que le service ARC peut ouvrir sur le serveur middleware TSM pour les opérations de récupération. Dans la plupart des cas, la valeur appropriée est le nombre de sessions moins le nombre maximal de sessions en magasin. Si vous devez partager un lecteur de bande pour le stockage et la récupération, spécifiez une valeur égale au nombre de sessions.
   - **Nombre maximal de sessions de stockage** : spécifiez le nombre maximal de sessions simultanées que le service ARC peut ouvrir sur le serveur middleware TSM pour les opérations d'archivage.

     Cette valeur doit être définie sur une seule, sauf lorsque le système de stockage d'archives ciblé est plein et que seules les récupérations peuvent être effectuées. Définissez cette valeur sur zéro pour utiliser toutes les sessions pour les récupérations.

7. Sélectionnez **appliquer les modifications**.

Optimisez un nœud d'archivage pour les sessions middleware TSM

Vous pouvez optimiser les performances d'un noeud d'archivage qui se connecte à Tivoli

Server Manager (TSM) en configurant les sessions du noeud d'archivage.

Avant de commencer

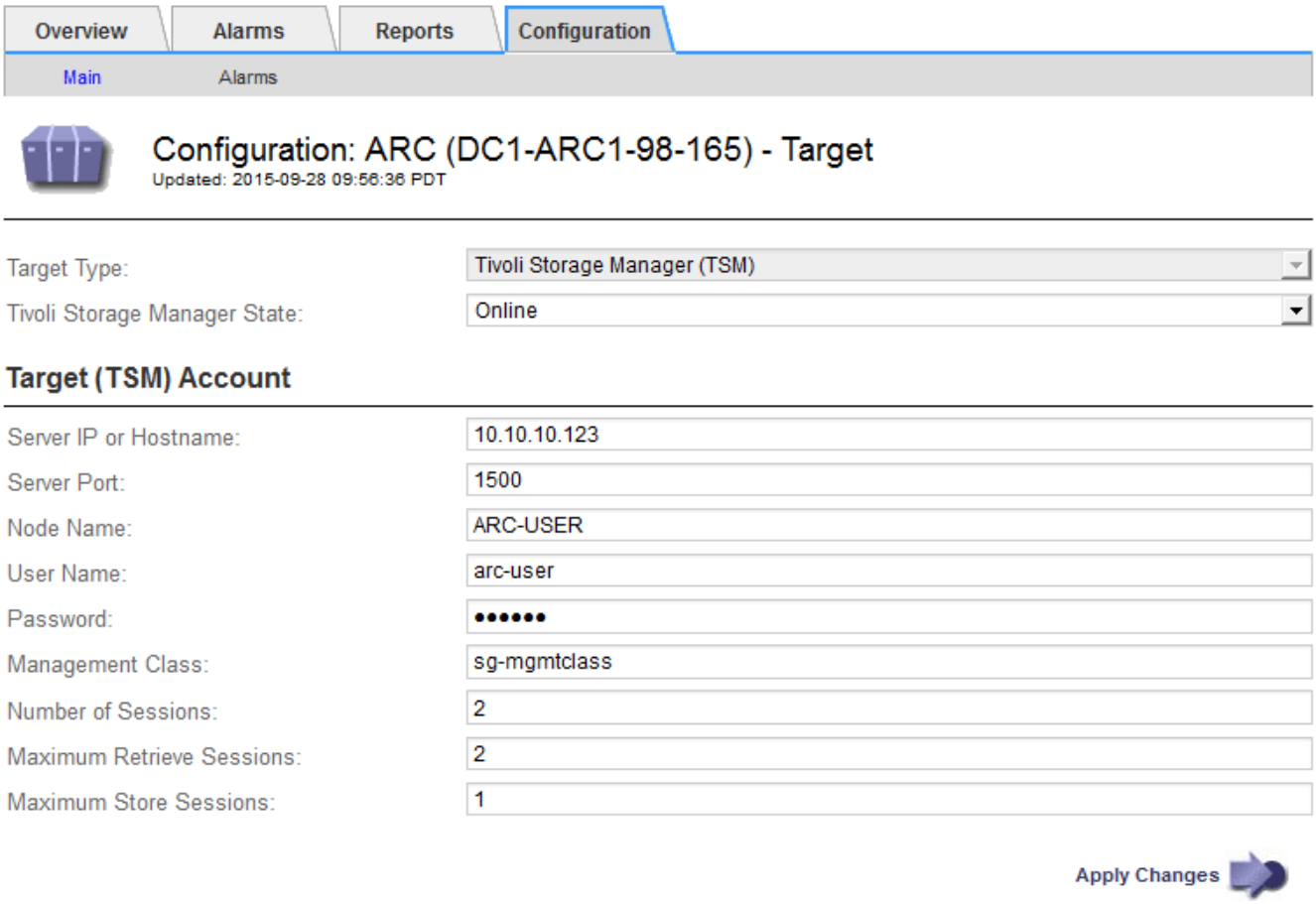
- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous disposez d'autorisations d'accès spécifiques.

Description de la tâche

En général, le nombre de sessions simultanées que le nœud d'archivage a ouvertes au serveur middleware TSM est défini sur le nombre de lecteurs de bande que le serveur TSM a dédiés au nœud d'archivage. Un lecteur de bande est alloué au stockage tandis que le reste est alloué à la récupération. Toutefois, lorsqu'un nœud de stockage est en cours de reconstruction à partir de copies de nœud d'archivage ou que le nœud d'archivage fonctionne en mode lecture seule, vous pouvez optimiser les performances du serveur TSM en définissant le nombre maximal de sessions d'extraction à identique au nombre de sessions simultanées. Il en résulte que tous les disques peuvent être utilisés simultanément pour la récupération et, au plus, un de ces lecteurs peut également être utilisé pour le stockage, le cas échéant.

Étapes

1. Sélectionnez **SUPPORT** > **Outils** > **topologie de grille**.
2. Sélectionnez ***Archive Node*** > **ARC** > **cible**.
3. Sélectionnez **Configuration** > **main**.
4. Modifier **nombre maximal de sessions de récupération** pour être le même que **nombre de sessions**.



5. Sélectionnez **appliquer les modifications**.

Configurer l'état d'archivage et les compteurs pour TSM

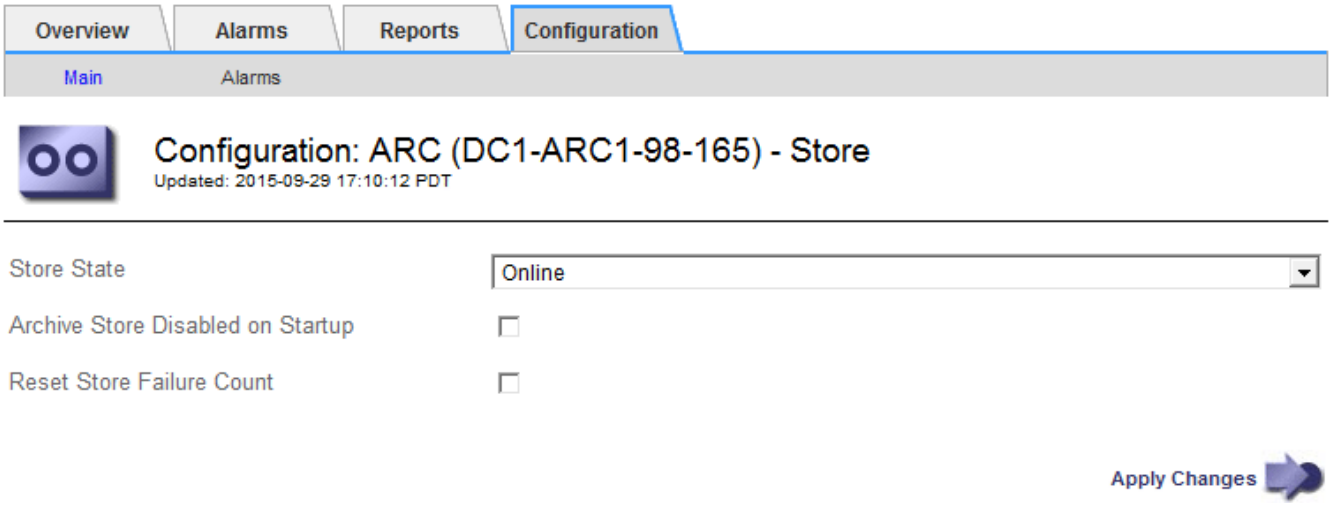
Si votre nœud d'archivage se connecte à un serveur middleware TSM, vous pouvez configurer l'état du magasin d'archives d'un nœud d'archivage sur en ligne ou hors ligne. Vous pouvez également désactiver le magasin d'archives lors du premier démarrage du nœud d'archivage ou réinitialiser le nombre d'échecs en cours de suivi pour l'alarme associée.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous disposez d'autorisations d'accès spécifiques.

Étapes

1. Sélectionnez **SUPPORT** > **Outils** > **topologie de grille**.
2. Sélectionnez ***Archive Node*** > **ARC** > **Store**.
3. Sélectionnez **Configuration** > **main**.



4. Modifiez les paramètres suivants, si nécessaire :
   - État du stockage : définissez l'état du composant sur :
     - En ligne : le nœud d'archivage est disponible pour traiter les données d'objet pour le stockage vers le système de stockage d'archivage.
     - Hors ligne : le nœud d'archivage n'est pas disponible pour traiter les données d'objet pour le stockage vers le système de stockage d'archives.
   - Magasin d'archives désactivé au démarrage : lorsque cette option est sélectionnée, le composant stockage d'archives reste en lecture seule lors du redémarrage. Utilisé pour désactiver de manière persistante le stockage vers le système cible de stockage d'archives. Utile lorsque le système de stockage d'archives ciblé ne peut pas accepter de contenu.
   - Réinitialiser le nombre d'échecs du magasin : réinitialisez le compteur pour les échecs du magasin. Il peut être utilisé pour effacer l'alarme ARVF (Store Failure).
5. Sélectionnez **appliquer les modifications**.

Informations associées

"Gérer un nœud d'archivage lorsque le serveur TSM atteint sa capacité"

Gérer un nœud d'archivage lorsque le serveur TSM atteint sa capacité

Le serveur TSM n'a aucun moyen d'informer le nœud d'archivage lorsque la base de données TSM ou le stockage des supports d'archivage gérés par le serveur TSM atteint sa capacité maximale. Cette situation peut être évitée grâce à la surveillance proactive du serveur TSM.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous disposez d'autorisations d'accès spécifiques.

Description de la tâche

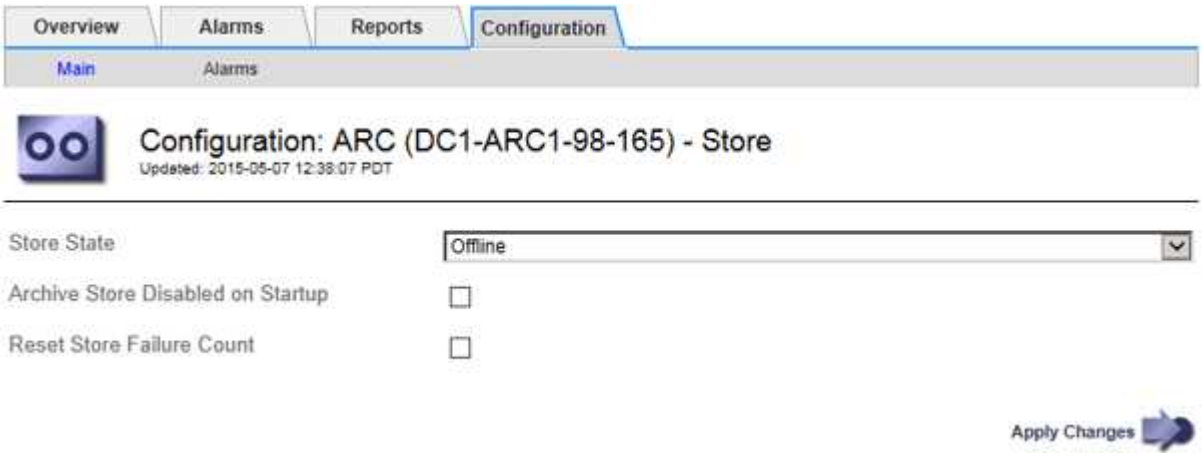
Le nœud d'archivage continue à accepter les données d'objet pour le transfert vers le serveur TSM une fois que le serveur TSM a arrêté d'accepter le nouveau contenu. Ce contenu ne peut pas être écrit sur un support géré par le serveur TSM. Une alarme est déclenchée si cela se produit.

Empêcher le service ARC d'envoyer du contenu au serveur TSM

Pour empêcher le service ARC d'envoyer du contenu supplémentaire au serveur TSM, vous pouvez mettre le nœud d'archivage hors ligne en mettant hors ligne son composant **ARC** > **Store**. Cette procédure peut également être utile pour empêcher les alarmes lorsque le serveur TSM n'est pas disponible pour la maintenance.

Étapes

1. Sélectionnez **SUPPORT** > **Outils** > **topologie de grille**.
2. Sélectionnez ***Archive Node*** > **ARC** > **Store**.
3. Sélectionnez **Configuration** > **main**.



4. Définissez **Etat du magasin** sur `Offline`.
5. Sélectionnez **Archive Store Disabled au démarrage**.
6. Sélectionnez **appliquer les modifications**.

Définissez le nœud d'archivage sur lecture seule si le middleware TSM atteint sa capacité

Si le serveur middleware TSM cible atteint sa capacité, le nœud d'archivage peut être optimisé pour effectuer uniquement des récupérations.

Étapes

1. Sélectionnez **SUPPORT** > **Outils** > **topologie de grille**.
2. Sélectionnez ***Archive Node*** > **ARC** > **cible**.
3. Sélectionnez **Configuration** > **main**.
4. Modifiez le nombre maximal de sessions de récupération pour qu'il soit identique au nombre de sessions simultanées répertoriées dans nombre de sessions.
5. Définissez le nombre maximum de sessions de stockage sur 0.

> Il n'est pas nécessaire de modifier le nombre maximal de sessions de stockage sur 0 si le nœud d'archivage est en lecture seule. Les sessions de magasin ne seront pas créées.

6. Sélectionnez **appliquer les modifications**.

Configurer les paramètres de récupération du nœud d'archivage

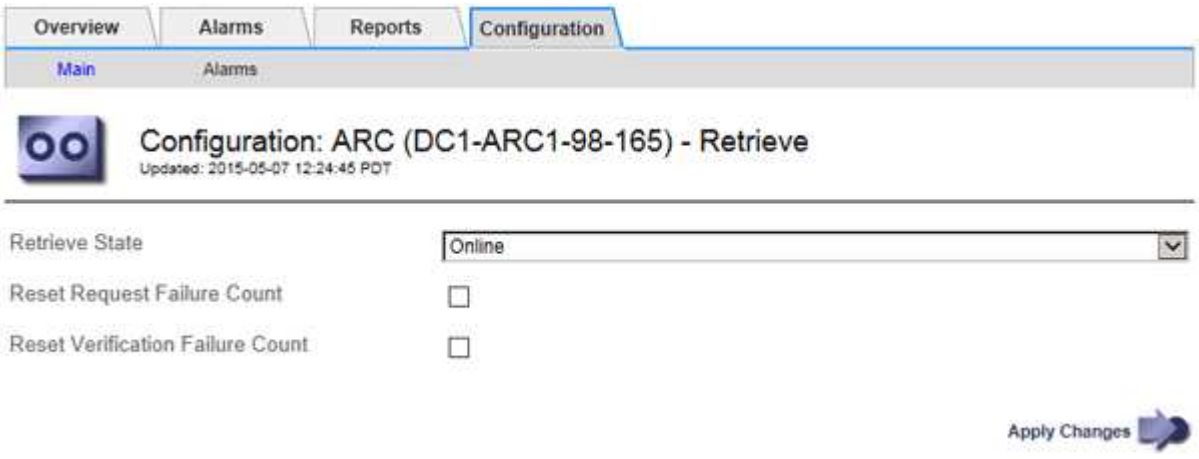
Vous pouvez configurer les paramètres de récupération d'un nœud d'archivage pour définir l'état en ligne ou hors ligne, ou réinitialiser le nombre d'échecs en cours de suivi pour les alarmes associées.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous disposez d'autorisations d'accès spécifiques.

Étapes

1. Sélectionnez **SUPPORT** > **Outils** > **topologie de grille**.
2. Sélectionnez **Archive Node** > **ARC** > **Retrieve**.
3. Sélectionnez **Configuration** > **main**.



4. Modifiez les paramètres suivants, si nécessaire :
   - **Récupérer l'état** : définissez l'état du composant sur :
     - En ligne : le nœud de grille est disponible pour récupérer les données d'objet à partir du périphérique de support d'archivage.
     - Hors ligne : le nœud grid n'est pas disponible pour récupérer les données d'objet.

- Réinitialiser le nombre d'échecs de demande : cochez cette case pour réinitialiser le compteur des échecs de demande. Il peut être utilisé pour effacer l'alarme ARRF (demandes d'échecs).
- Réinitialiser le nombre d'échecs de vérification : cochez cette case pour réinitialiser le compteur des échecs de vérification sur les données d'objet récupérées. Il peut être utilisé pour effacer l'alarme ARRV (échecs de vérification).

5. Sélectionnez **appliquer les modifications**.

Configurer la réplication du noeud d'archivage

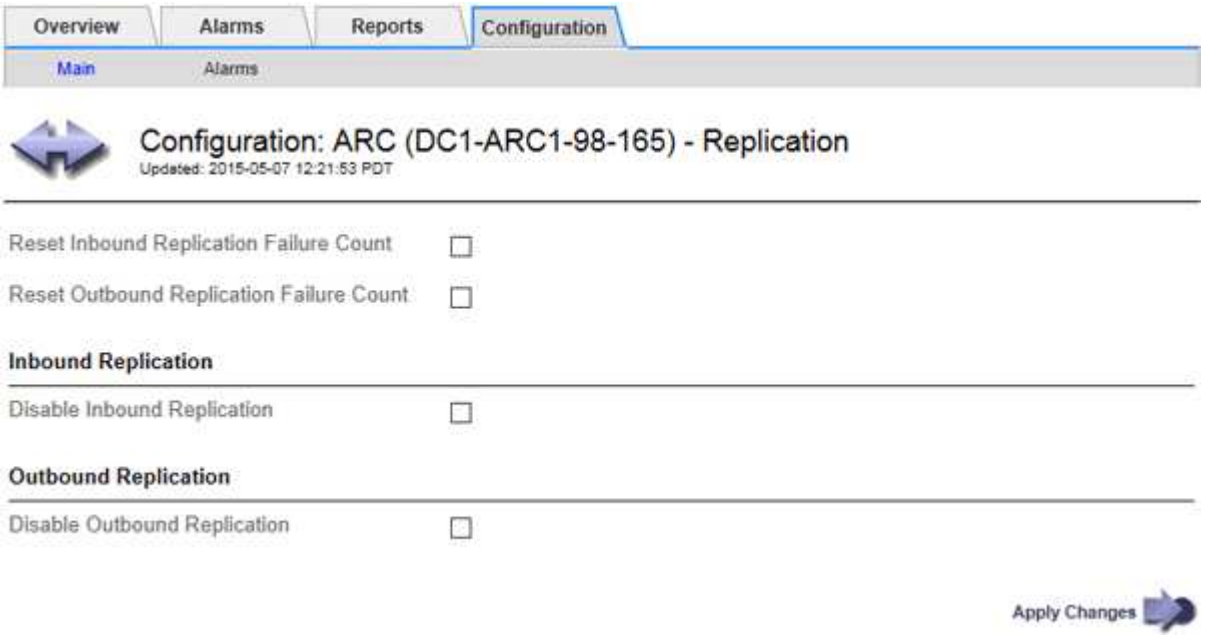
Vous pouvez configurer les paramètres de réplication d'un nœud d'archivage et désactiver la réplication entrante et sortante, ou réinitialiser le nombre d'échecs en cours de suivi pour les alarmes associées.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous disposez d'autorisations d'accès spécifiques.

Étapes

1. Sélectionnez **SUPPORT** > **Outils** > **topologie de grille**.
2. Sélectionnez ***Archive Node*** > **ARC** > **Replication**.
3. Sélectionnez **Configuration** > **main**.



4. Modifiez les paramètres suivants, si nécessaire :
   - **Réinitialiser le nombre d'échecs de réplication entrant** : sélectionnez cette option pour réinitialiser le compteur pour les échecs de réplication entrants. Cette fonction permet d'effacer l'alarme RRF (Replications entrantes — FAILED).
   - **Réinitialiser le nombre d'échecs de réplication sortante** : sélectionnez cette option pour réinitialiser le compteur des échecs de réplication sortants. Cette fonction permet d'effacer l'alarme RORF (réplications sortantes — en échec).
   - **Désactiver la réplication entrante** : sélectionnez cette option pour désactiver la réplication entrante

dans le cadre d'une procédure de maintenance ou de test. Laisser effacé pendant le fonctionnement normal.

Lorsque la réplication entrante est désactivée, les données d'objet peuvent être extraites du service ARC pour être répliquées vers d'autres emplacements du système StorageGRID, mais les objets ne peuvent pas être répliqués vers ce service ARC à partir d'autres emplacements système. Le service ARC est en lecture seule.

- **Désactiver la réplication sortante** : cochez cette case pour désactiver la réplication sortante (y compris les demandes de contenu pour les récupérations HTTP) dans le cadre d'une procédure de maintenance ou de test. Laisser non vérifié pendant le fonctionnement normal.

  Lorsque la réplication sortante est désactivée, les données d'objet peuvent être copiées vers ce service ARC pour respecter les règles ILM, mais les données d'objet ne peuvent pas être récupérées du service ARC pour être copiées vers d'autres emplacements du système StorageGRID. Le service ARC est en écriture uniquement.

5. Sélectionnez **appliquer les modifications**.

Définissez les alarmes personnalisées pour le nœud d'archivage

Vous devez établir des alarmes personnalisées pour les attributs ARQL et ARRL utilisés pour surveiller la vitesse et l'efficacité de la récupération des données d'objet à partir du système de stockage d'archives par le nœud d'archivage.

- ARQL : longueur moyenne de la file d'attente. Durée moyenne, en microsecondes, de la mise en file d'attente des données de cet objet pour la récupération à partir du système de stockage d'archivage.
- ARRL : latence moyenne de la requête. Temps moyen, en microsecondes, requis par le nœud d'archivage pour récupérer les données d'objet à partir du système de stockage d'archivage.

Les valeurs acceptables pour ces attributs dépendent de la configuration et de l'utilisation du système de stockage d'archives. (Allez à **ARC** > **Retrieve** > **Présentation** > **main**.) Les valeurs définies pour les délais de requête et le nombre de sessions disponibles pour les demandes de récupération sont particulièrement influentes.

Une fois l'intégration terminée, surveillez les récupérations de données d'objet du nœud d'archivage pour établir des valeurs pour les temps de récupération normaux et la longueur de file d'attente. Ensuite, créez des alarmes personnalisées pour ARQL et ARRL qui se déclencheront en cas de condition de fonctionnement anormale. Reportez-vous aux instructions pour "gestion des alarmes (système hérité)".

Intégrez Tivoli Storage Manager

Configuration et fonctionnement du nœud d'archivage

Votre système StorageGRID gère le nœud d'archivage comme un emplacement dans lequel les objets sont stockés indéfiniment et sont toujours accessibles.

À l'ingestion d'un objet, des copies sont effectuées dans tous les emplacements nécessaires, y compris les nœuds d'archivage, en fonction des règles de gestion du cycle de vie des informations (ILM) définies pour votre système StorageGRID. Le nœud d'archivage agit comme un client sur un serveur TSM, et les bibliothèques clientes TSM sont installées sur le nœud d'archivage par le processus d'installation du logiciel StorageGRID. Les données d'objet dirigées vers le nœud d'archivage pour le stockage sont enregistrées directement sur le serveur TSM au moment de leur réception. Le nœud d'archivage n'exécute pas les données

d’objet avant de les enregistrer sur le serveur TSM, ni l’agrégation d’objets. Cependant, le nœud d’archivage peut envoyer plusieurs copies au serveur TSM en une seule transaction lorsque le taux de données le garantit.

Une fois que le nœud d’archivage enregistre les données d’objet sur le serveur TSM, les données d’objet sont gérées par le serveur TSM à l’aide de ses politiques de cycle de vie/rétention. Ces règles de conservation doivent être définies pour être compatibles avec le fonctionnement du nœud d’archivage. En d’autres termes, les données d’objet enregistrées par le nœud d’archivage doivent être stockées indéfiniment et doivent toujours être accessibles par le nœud d’archivage, à moins qu’elles ne soient supprimées par le nœud d’archivage.

Il n’y a aucune connexion entre les règles ILM du système StorageGRID et les politiques de cycle de vie/conservation du serveur TSM. Chaque système fonctionne de manière indépendante ; cependant, lorsque chaque objet est ingéré dans le système StorageGRID, vous pouvez lui attribuer une classe de gestion TSM. Cette classe de gestion est transmise au serveur TSM avec les données d’objet. L’affectation de classes de gestion à différents types d’objets vous permet de configurer le serveur TSM pour placer les données d’objet dans différents pools de stockage, ou d’appliquer différentes règles de migration ou de conservation, le cas échéant. Par exemple, les objets identifiés comme sauvegardes de bases de données (le contenu temporaire pouvant être remplacé par des données plus récentes) peuvent être traités différemment des données applicatives (contenu fixe qui doit être conservé indéfiniment).

Le nœud d’archivage peut être intégré à un nouveau serveur TSM ou à un serveur TSM existant ; il ne nécessite pas de serveur TSM dédié. Les serveurs TSM peuvent être partagés avec d’autres clients, à condition que la taille du serveur TSM soit adaptée à la charge maximale attendue. TSM doit être installé sur un serveur ou une machine virtuelle distincte du nœud d’archivage.

Il est possible de configurer plusieurs nœuds d’archivage pour écrire sur le même serveur TSM. Cependant, cette configuration n’est recommandée que si les nœuds d’archivage écrivent différents ensembles de données sur le serveur TSM. Il n’est pas recommandé de configurer plusieurs nœuds d’archivage pour écrire sur le même serveur TSM lorsque chaque nœud d’archivage écrit des copies des mêmes données d’objet dans l’archive. Dans ce dernier scénario, les deux copies sont soumises à un point de défaillance unique (le serveur TSM), pour les copies redondantes et indépendantes des données d’objet.

Les nœuds d’archivage n’utilisent pas le composant HSM (Hierarchical Storage Management) de TSM.

Bonnes pratiques pour la configuration

Lorsque vous dimensionnez et configurez votre serveur TSM, il existe les meilleures pratiques que vous devez appliquer pour l’optimiser afin qu’il fonctionne avec le nœud d’archivage.

Lors du dimensionnement et de la configuration du serveur TSM, il est important de prendre en compte les facteurs suivants :

- Comme le nœud d’archivage ne agrège pas les objets avant de les enregistrer sur le serveur TSM, la base de données TSM doit être dimensionnée pour contenir les références à tous les objets qui seront écrits sur le nœud d’archivage.
- Le logiciel de nœud d’archivage ne peut pas tolérer la latence liée à l’écriture d’objets directement sur bande ou sur un autre support amovible. Par conséquent, le serveur TSM doit être configuré avec un pool de stockage sur disque pour le stockage initial des données sauvegardées par le nœud d’archivage chaque fois que des supports amovibles sont utilisés.
- Vous devez configurer les règles de conservation TSM pour utiliser la conservation basée sur les événements. Le nœud d’archivage ne prend pas en charge les politiques de conservation TSM basées sur la création. Utilisez les paramètres recommandés suivants de retmin=0 et retver=0 dans la stratégie de rétention (ce qui indique que la rétention commence lorsque le noeud d’archivage déclenche un

événement de rétention et est conservé pendant 0 jours après cela). Toutefois, ces valeurs pour le retmin et le retver sont facultatives.

Le pool de disques doit être configuré pour migrer les données vers le pool de bandes (c'est-à-dire que le pool de bandes doit être le NXTSTGPOOL du pool de disques). Le pool de bandes ne doit pas être configuré en tant que pool de copies du pool de disques avec une écriture simultanée sur les deux pools (le pool de bandes ne peut pas être un COPYSTGPOOL pour le pool de disques). Pour créer des copies hors ligne des bandes contenant les données du nœud d'archivage, configurez le serveur TSM avec un deuxième pool de bandes qui est un pool de copies du pool de bandes utilisé pour les données du nœud d'archivage.

Terminez la configuration du nœud d'archivage

Le nœud d'archivage ne fonctionne pas après avoir terminé le processus d'installation. Avant que le système StorageGRID puisse enregistrer des objets sur le nœud d'archivage TSM, vous devez terminer l'installation et la configuration du serveur TSM et configurer le nœud d'archivage pour qu'il communique avec le serveur TSM.

Si nécessaire, reportez-vous à la documentation IBM suivante lorsque vous préparez votre serveur TSM pour l'intégration au nœud d'archivage d'un système StorageGRID :

- "Guide d'installation et d'utilisation des pilotes de périphérique de bande IBM"
- "Référence de programmation des pilotes de périphériques de bande IBM"

Installez un nouveau serveur TSM

Vous pouvez intégrer le nœud d'archivage à un nouveau serveur TSM ou à un serveur TSM existant. Si vous installez un nouveau serveur TSM, suivez les instructions de la documentation TSM pour terminer l'installation.

> ⓘ Un nœud d'archivage ne peut pas être co-hébergé avec un serveur TSM.

Configurer le serveur TSM

Cette section comprend des exemples d'instructions pour préparer un serveur TSM conformément aux meilleures pratiques TSM.

Les instructions suivantes vous guident tout au long du processus :

- Définition d'un pool de stockage sur disque et d'un pool de stockage sur bandes (le cas échéant) sur le serveur TSM
- Définition d'une stratégie de domaine qui utilise la classe de gestion TSM pour les données enregistrées à partir du nœud d'archivage et enregistrement d'un nœud pour utiliser cette stratégie de domaine

Ces instructions sont fournies à titre indicatif uniquement ; elles ne sont pas destinées à remplacer la documentation TSM ou à fournir des instructions complètes adaptées à toutes les configurations. Des instructions spécifiques à un déploiement doivent être fournies par un administrateur TSM qui connaît à la fois vos exigences détaillées et la documentation complète de TSM Server.

Définir les pools de stockage sur bande et sur disque TSM

Le nœud d'archivage écrit dans un pool de stockage sur disque. Pour archiver du

contenu sur bande, vous devez configurer le pool de stockage sur disque afin de déplacer le contenu vers un pool de stockage sur bande.

Description de la tâche

Pour un serveur TSM, vous devez définir un pool de stockage sur bandes et un pool de stockage sur disque dans Tivoli Storage Manager. Une fois le pool de disques défini, créez un volume de disque et affectez-le au pool de disques. Un pool de bandes n'est pas nécessaire si votre serveur TSM utilise du stockage sur disque uniquement.

Vous devez effectuer plusieurs étapes sur votre serveur TSM avant de pouvoir créer un pool de stockage sur bandes. (Créez une bibliothèque de bandes et au moins un lecteur dans la bibliothèque de bandes. Définissez un chemin entre le serveur et la bibliothèque et entre le serveur et les lecteurs, puis définissez une classe de périphériques pour les lecteurs.) Les détails de ces étapes peuvent varier en fonction de la configuration matérielle et des besoins de stockage du site. Pour plus d'informations, consultez la documentation TSM.

Le jeu d'instructions ci-dessous illustre le processus. Vous devez savoir que les besoins spécifiques à votre site peuvent varier en fonction des besoins de votre déploiement. Pour plus d'informations sur la configuration et pour obtenir des instructions, consultez la documentation TSM.

Vous devez vous connecter au serveur avec des privilèges d'administration et utiliser l'outil dsmadmc pour exécuter les commandes suivantes.

Étapes

1. Créez une bibliothèque de bandes.

   `define library` *`tapelibrary`* `libtype=`*`scsi`*

   Où *`tapelibrary`* est un nom arbitraire choisi pour la bibliothèque de bandes et la valeur de `libtype` peut varier selon le type de bibliothèque de bandes.

2. Définissez un chemin entre le serveur et la bibliothèque de bandes.

   `define path` *`servername tapelibrary`* `srctype=server desttype=library device=`*`lib-devicename`*

   - *`servername`* Est le nom du serveur TSM
   - *`tapelibrary`* est le nom de bibliothèque de bandes que vous avez défini
   - *`lib-devicename`* est le nom du périphérique de la bibliothèque de bandes

3. Définissez un lecteur pour la bibliothèque.

   `define drive` *`tapelibrary drivename`*

   - *`drivename`* est le nom que vous souhaitez spécifier pour le lecteur
   - *`tapelibrary`* est le nom de bibliothèque de bandes que vous avez défini

     Il est possible que vous souhaitiez configurer un ou plusieurs lecteurs supplémentaires, en fonction de la configuration de votre matériel. (Par exemple, si le serveur TSM est connecté à un commutateur Fibre Channel qui comporte deux entrées d'une bibliothèque de bandes, vous pouvez définir un lecteur pour chaque entrée.)

4. Définissez un chemin entre le serveur et le lecteur que vous avez défini.

   ```
   define path servername drivename srctype=server desttype=drive
   library=tapelibrary device=drive-dname
   ```

   - *drive-dname* est le nom du périphérique du lecteur
   - *tapelibrary* est le nom de bibliothèque de bandes que vous avez défini

     Répétez l'opération pour chaque lecteur que vous avez défini pour la bibliothèque de bandes à l'aide d'un lecteur distinct *drivename* et *drive-dname* pour chaque lecteur.

5. Définir une classe de périphérique pour les lecteurs.

   ```
   define devclass DeviceClassName devtype=lto library=tapelibrary
   format=tapetype
   ```

   - *DeviceClassName* est le nom de la classe de périphérique
   - *lto* est le type de lecteur connecté au serveur
   - *tapelibrary* est le nom de bibliothèque de bandes que vous avez défini
   - *tapetype* est le type de bande ; par exemple, ultrium3

6. Ajoutez des volumes de bande à l'inventaire de la bibliothèque.

   ```
   checkin libvolume tapelibrary
   ```

   tapelibrary est le nom de bibliothèque de bandes que vous avez défini.

7. Créez le pool de stockage sur bande primaire.

   ```
   define stgpool SGWSTapePool DeviceClassName description=description
   collocate=filespace maxscratch=XX
   ```

   - *SGWSTapePool* Est le nom du pool de stockage de bandes du nœud d'archivage. Vous pouvez sélectionner n'importe quel nom pour le pool de stockage de bandes (tant que le nom utilise les conventions de syntaxe attendues par le serveur TSM).
   - *DeviceClassName* est le nom de la classe de périphérique pour la bibliothèque de bandes.
   - *description* Est une description du pool de stockage qui peut être affichée sur le serveur TSM à l'aide de `query stgpool` commande. Par exemple : « pool de stockage sur bande pour le nœud d'archivage ».
   - *collocate=filespace* Spécifie que le serveur TSM doit écrire des objets à partir du même espace de fichiers dans une seule bande.
   - `XX` est l'une des suivantes :
     - Nombre de bandes vides dans la bibliothèque de bandes (dans le cas où le nœud d'archivage est la seule application utilisant la bibliothèque).
     - Nombre de bandes allouées pour l'utilisation par le système StorageGRID (dans les cas où la bibliothèque de bandes est partagée).

8. Sur un serveur TSM, créez un pool de stockage sur disque. Sur la console d'administration du serveur TSM, entrez

```
define stgpool SGWSDiskPool disk description=description
maxsize=maximum_file_size nextstgpool=SGWSTapePool highmig=percent_high
lowmig=percent_low
```

- *SGWSDiskPool* Est le nom du pool de disques du nœud d'archivage. Vous pouvez sélectionner n'importe quel nom pour le pool de stockage sur disque (tant que le nom utilise les conventions de syntaxe attendues par le TSM).
- *description* Est une description du pool de stockage qui peut être affichée sur le serveur TSM à l'aide de `query stgpool` commande. Par exemple, "disque de stockage pool pour le noeud d'archivage".
- *maximum_file_size* force les objets de plus grande taille à être écrits directement sur bande, au lieu d'être mis en cache dans le pool de disques. Il est recommandé de le régler *maximum_file_size* À 10 Go.
- *nextstgpool=SGWSTapePool* Désigne le pool de stockage sur disque au pool de stockage sur bandes défini pour le nœud d'archivage.
- *percent_high* définit la valeur à laquelle le pool de disques commence à migrer son contenu vers le pool de bandes. Il est recommandé de le régler *percent_high* sur 0, pour que la migration des données commence immédiatement
- *percent_low* définit la valeur à laquelle la migration vers le pool de bandes s'arrête. Il est recommandé de le régler *percent_low* à 0 pour effacer le pool de disques.

9. Sur un serveur TSM, créez un ou plusieurs volumes de disque et affectez-les au pool de disques.

```
define volume SGWSDiskPool volume_name formatsize=size
```

- *SGWSDiskPool* est le nom du pool de disques.
- *volume_name* est le chemin complet vers l'emplacement du volume (par exemple, `/var/local/arc/stage6.dsm`) Sur le serveur TSM où il écrit le contenu du pool de disques en préparation du transfert sur bande.
- *size* Est la taille, en Mo, du volume de disque.

  Par exemple, pour créer un volume de disque unique de sorte que le contenu d'un pool de disques remplisse une seule bande, définissez la valeur de la taille sur 200000 lorsque le volume de bande a une capacité de 200 Go.

  Cependant, il est préférable de créer plusieurs volumes de disque de taille inférieure, car le serveur TSM peut écrire sur chaque volume du pool de disques. Par exemple, si la taille de la bande est de 250 Go, créez 25 volumes de disque d'une taille de 10 Go (10000) chacun.

Le serveur TSM préalloue de l'espace dans le répertoire du volume de disque. Cette opération peut prendre un certain temps (plus de trois heures pour un volume de disque de 200 Go).

Définissez une stratégie de domaine et enregistrez un nœud

Vous devez définir une stratégie de domaine qui utilise la classe de gestion TSM pour les données enregistrées à partir du nœud d'archivage, puis enregistrer un nœud pour utiliser cette stratégie de domaine.

Les processus du nœud d'archivage peuvent fuir de mémoire si le mot de passe client du nœud d'archivage dans Tivoli Storage Manager (TSM) expire. Assurez-vous que le serveur TSM est configuré de sorte que le nom d'utilisateur/mot de passe du client pour le nœud d'archivage n'expire jamais.

Lors de l'enregistrement d'un noeud sur le serveur TSM pour l'utilisation du noeud d'archivage (ou la mise à jour d'un noeud existant), vous devez spécifier le nombre de points de montage que le noeud peut utiliser pour les opérations d'écriture en spécifiant le paramètre MAXNUMMP à la commande ENREGISTRER NOEUD. Le nombre de points de montage est généralement équivalent au nombre de têtes de lecteur de bande attribuées au nœud d'archivage. Le nombre spécifié pour MAXNUMMP sur le serveur TSM doit être au moins aussi grand que la valeur définie pour **ARC** > **Target** > **Configuration** > **main** > **maximum Store sessions** pour le nœud d'archivage, Qui est défini sur 0 ou 1, car les sessions de stockage simultanées ne sont pas prises en charge par le nœud d'archivage.

La valeur MAXSESSIONS définie pour le serveur TSM contrôle le nombre maximal de sessions qui peuvent être ouvertes sur le serveur TSM par toutes les applications clientes. La valeur de MAXSESSIONS spécifiée sur TSM doit être au moins aussi grande que la valeur spécifiée pour **ARC** > **Target** > **Configuration** > **main** > **nombre de sessions** dans le gestionnaire de grille pour le noeud d'archives. Le nœud d'archivage crée simultanément au plus une session par point de montage et un petit nombre (< 5) de sessions supplémentaires.

Le nœud TSM affecté au nœud d'archivage utilise une stratégie de domaine personnalisée `tsm-domain`. Le `tsm-domain` La politique de domaine est une version modifiée de la politique de domaine « standard », configurée pour écrire sur bande et avec la destination d'archivage définie comme pool de stockage du système StorageGRID (*`SGWSDiskPool`*).

Vous devez vous connecter au serveur TSM avec des privilèges d'administration et utiliser l'outil dsmadmc pour créer et activer la stratégie de domaine.

Créez et activez la stratégie de domaine

Vous devez créer une stratégie de domaine, puis l'activer pour configurer le serveur TSM afin d'enregistrer les données envoyées à partir du noeud d'archivage.

Étapes

1. Créer une stratégie de domaine.

   ```
   copy domain standard tsm-domain
   ```

2. Si vous n'utilisez pas de classe de gestion existante, entrez l'une des options suivantes :

   ```
   define policyset tsm-domain standard
   ```

   ```
   define mgmtclass tsm-domain standard default
   ```

   `default` est la classe de gestion par défaut pour le déploiement.

3. Créez un groupe de copie dans le pool de stockage approprié. Entrer (sur une ligne) :

   ```
   define copygroup tsm-domain standard default type=archive
   destination=SGWSDiskPool retinit=event retmin=0 retver=0
   ```

default Est la classe de gestion par défaut du nœud d'archivage. Les valeurs de `retinit`, `retmin`, et `retver` Ont été choisis pour refléter le comportement de rétention actuellement utilisé par le noeud d'archivage

> Ne pas configurer `retinit` à `retinit=create`. Réglage `retinit=create` Empêche le nœud d'archivage de supprimer du contenu, car les événements de rétention sont utilisés pour supprimer du contenu du serveur TSM.

4. Attribuez la classe de gestion à la valeur par défaut.

   ```
   assign defmgmtclass tsm-domain standard default
   ```

5. Définissez la nouvelle règle sur active.

   ```
   activate policyset tsm-domain standard
   ```

   Ignorez l'avertissement « aucun groupe de copie de sauvegarde » qui s'affiche lorsque vous entrez la commande Activer.

6. Enregistrez un nœud pour utiliser le nouvel ensemble de règles sur le serveur TSM. Sur le serveur TSM, entrez (sur une ligne) :

   ```
   register node arc-user arc-password passexp=0 domain=tsm-domain
   MAXNUMMP=number-of-sessions
   ```

   Arc-user et arc-mot-de-passe sont les mêmes nom de noeud client et mot de passe que ceux définis sur le noeud d'archivage, et la valeur MAXNUMMP est définie sur le nombre de lecteurs de bande réservés pour les sessions de magasin de noeud d'archivage.

   > Par défaut, l'enregistrement d'un nœud crée un ID utilisateur administratif avec l'autorité propriétaire du client, avec le mot de passe défini pour le nœud.

Migrer les données vers StorageGRID

Vous pouvez migrer d'importants volumes de données vers le système StorageGRID tout en utilisant le système StorageGRID pour les opérations quotidiennes.

Ce guide vous aidera à planifier une migration de grands volumes de données vers le système StorageGRID. Ce n'est pas un guide général de la migration des données et n'inclut pas des étapes détaillées pour effectuer une migration. Suivez les instructions de cette section pour assurer une migration efficace des données dans le système StorageGRID sans perturber les opérations quotidiennes et que les données migrées sont correctement gérées par le système StorageGRID.

Vérifier la capacité du système StorageGRID

Avant de migrer d'importants volumes de données vers le système StorageGRID, vérifiez que le système StorageGRID dispose des capacités de disque nécessaires pour gérer le volume prévu.

Si le système StorageGRID inclut un nœud d'archivage et qu'une copie des objets migrés a été enregistrée sur un stockage secondaire (par exemple, une bande), assurez-vous que le stockage du nœud d'archivage dispose de suffisamment de capacité pour le volume prévu de données migrées.

Dans le cadre de l'évaluation de la capacité, examinez le profil de données des objets que vous prévoyez de migrer et calculez la capacité de disque requise. Pour plus d'informations sur la surveillance de la capacité du disque de votre système StorageGRID, reportez-vous à la section "Gérer des nœuds de stockage" et les instructions pour "Surveillance StorageGRID".

Détermination de la règle ILM pour les données migrées

La règle ILM du système StorageGRID détermine le nombre de copies effectuées, l'emplacement des copies stockées et la durée de conservation de ces copies. Une règle ILM comprend un ensemble de règles ILM décrit la procédure de filtrage des objets et de gestion des données d'objet au fil du temps.

Selon l'utilisation des données migrées et vos exigences concernant les données migrées, vous pouvez définir des règles ILM uniques pour les données migrées qui ne sont pas les règles ILM utilisées pour les opérations quotidiennes. Par exemple, si la gestion quotidienne des données implique différentes exigences réglementaires que les données incluses dans la migration, il est possible de vouloir créer un nombre différent de copies des données migrées sur un niveau de stockage différent.

Vous pouvez configurer des règles qui s'appliquent exclusivement aux données migrées si une distinction unique entre les données migrées et les données objet enregistrées au quotidien.

Si vous faites la distinction de manière fiable entre les types de données en utilisant l'un des critères de métadonnées, ce critère vous permet de définir une règle ILM qui ne s'applique qu'aux données migrées.

Avant de commencer la migration des données, veillez à bien comprendre la règle ILM du système StorageGRID et la manière dont elle s'applique aux données migrées, et à effectuer et tester toutes les modifications apportées à la règle ILM. Voir "Gestion des objets avec ILM".

> Une règle ILM incorrecte peut entraîner une perte de données irrécupérable. Examinez attentivement toutes les modifications apportées à une stratégie ILM avant de l'activer pour vous assurer que celle-ci fonctionne comme prévu.

Évaluez l'impact de la migration sur les opérations

Le système StorageGRID permet un fonctionnement efficace du stockage objet et de la récupération. Il offre une excellente protection contre la perte de données grâce à la création transparente de copies redondantes des données d'objet et des métadonnées.

Cependant, la migration des données doit être gérée avec soin conformément aux instructions de ce guide afin d'éviter tout impact sur les opérations quotidiennes du système ou, dans des cas extrêmes, le risque de perte des données en cas de défaillance du système StorageGRID.

La migration de volumes importants de données impose une charge supplémentaire au système. Lorsque le système StorageGRID est lourdement chargé, il répond plus lentement aux demandes de stockage et de récupération d'objets. Cela peut interférer avec les demandes de stockage et de récupération qui font partie intégrante des opérations quotidiennes. La migration peut également entraîner d'autres problèmes opérationnels. Par exemple, lorsqu'un nœud de stockage arrive à saturation de la capacité, la charge intermittente importante due à l'ingestion par lots peut faire basculer le nœud de stockage entre la lecture seule et la lecture-écriture, générant des notifications.

Si le chargement persiste, les files d'attente peuvent développer différentes opérations que le système StorageGRID doit exécuter pour assurer la redondance complète des données d'objet et des métadonnées.

La migration des données doit être gérée avec soin conformément aux directives présentées dans ce document afin de garantir un fonctionnement sûr et efficace du système StorageGRID pendant la migration. Lors de la migration des données, ingestion d'objets par lots ou ingestion continue. Ensuite, surveillez en

permanence le système StorageGRID pour vous assurer que les différentes valeurs d'attribut ne sont pas dépassées.

Planifiez et surveillez la migration des données

La migration des données doit être planifiée et contrôlée si nécessaire pour assurer le placement des données conformément à la politique ILM dans les délais impartis.

Planification de la migration des données

Évitez la migration des données pendant les heures de fonctionnement essentielles. Limitez la migration des données aux soirées, week-ends et autres fois que l'utilisation du système est faible.

Si possible, ne planifiez pas la migration des données pendant les périodes d'activité élevée. Toutefois, s'il n'est pas pratique d'éviter complètement la période d'activité élevée, il est sûr de procéder aussi longtemps que vous surveillez attentivement les attributs pertinents et que vous prenez des mesures s'ils dépassent les valeurs acceptables.

Surveiller la migration des données

Ce tableau répertorie les attributs que vous devez contrôler lors de la migration des données, ainsi que les problèmes qu'ils représentent.

Si vous utilisez des stratégies de classification du trafic avec des limites de taux pour accélérer l'entrée, vous pouvez surveiller le taux observé en conjonction avec les statistiques décrites dans le tableau suivant et réduire les limites si nécessaire.

Superviser	Description
Nombre d'objets en attente de l'évaluation ILM	1. Sélectionnez **SUPPORT** > **Outils** > **topologie de grille**. 2. Sélectionnez ***déploiement*** > **Présentation** > **main**. 3. Dans la section ILM Activity, surveillez le nombre d'objets affichés pour les attributs suivants : ◦ **Attente - tous (XQUZ)**: Le nombre total d'objets en attente d'évaluation ILM. ◦ **Attente - client (XCQZ)** : nombre total d'objets en attente d'évaluation ILM des opérations client (par exemple, transfert). 4. Si le nombre d'objets affichés pour l'un de ces attributs dépasse 100,000, réduisez la vitesse d'entrée des objets afin de réduire la charge sur le système StorageGRID.
Capacité de stockage des systèmes d'archivage ciblés	Si la règle ILM enregistre une copie des données migrées vers un système de stockage d'archives ciblé (bande ou cloud), surveillez la capacité du système de stockage d'archivage ciblé pour s'assurer que la capacité disponible est suffisante.
Archive Node > **ARC** > **Store**	Si une alarme pour l'attribut **Store Failures (ARVF)** est déclenchée, le système de stockage d'archives ciblé a peut-être atteint sa capacité. Vérifiez le système de stockage d'archives ciblé et résolvez tout problème ayant déclenché une alarme.

Gestion des objets avec ILM

Gérez les objets avec ILM : présentation

Vous gérez les objets dans un système StorageGRID en configurant une règle de gestion du cycle de vie des informations (ILM) constituée d'une ou plusieurs règles ILM. Les règles ILM indiquent à StorageGRID comment créer et distribuer des copies de données en mode objet et comment gérer ces copies au fil du temps.

À propos de ces instructions

La conception et la mise en œuvre de règles ILM et de la politique ILM nécessitent une planification minutieuse. Vous devez connaître vos exigences opérationnelles, la topologie de votre système StorageGRID, vos besoins en matière de protection des objets et les types de stockage disponibles. Ensuite, vous devez déterminer comment vous voulez que différents types d'objets soient copiés, distribués et stockés.

Suivez ces instructions pour :

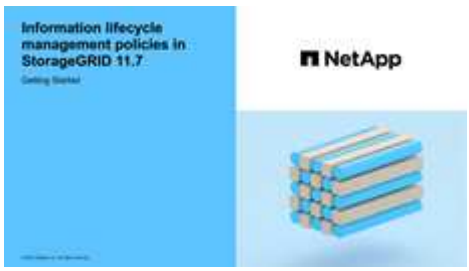
- En savoir plus sur la solution ILM de StorageGRID, notamment "ILM fonctionne tout au long de la vie d'un objet".
- Découvrez comment configurer "pools de stockage", "Pools de stockage cloud", et "Règles ILM".
- Découvrez comment "Créez, simulez et activez une règle ILM" qui protégeront les données d'objet sur un ou plusieurs sites.
- Découvrez comment "Gestion des objets avec le verrouillage objet S3", Qui permet de s'assurer que les objets de compartiments S3 spécifiques ne sont pas supprimés ou écrasés pendant une durée spécifiée.

En savoir plus >>

Pour en savoir plus, consultez ces vidéos :

- "Vidéo : règles de gestion du cycle de vie de l'information dans StorageGRID 11.7".

- "Vidéo : politiques de gestion du cycle de vie de l'information dans StorageGRID 11.7"



ILM et cycle de vie des objets

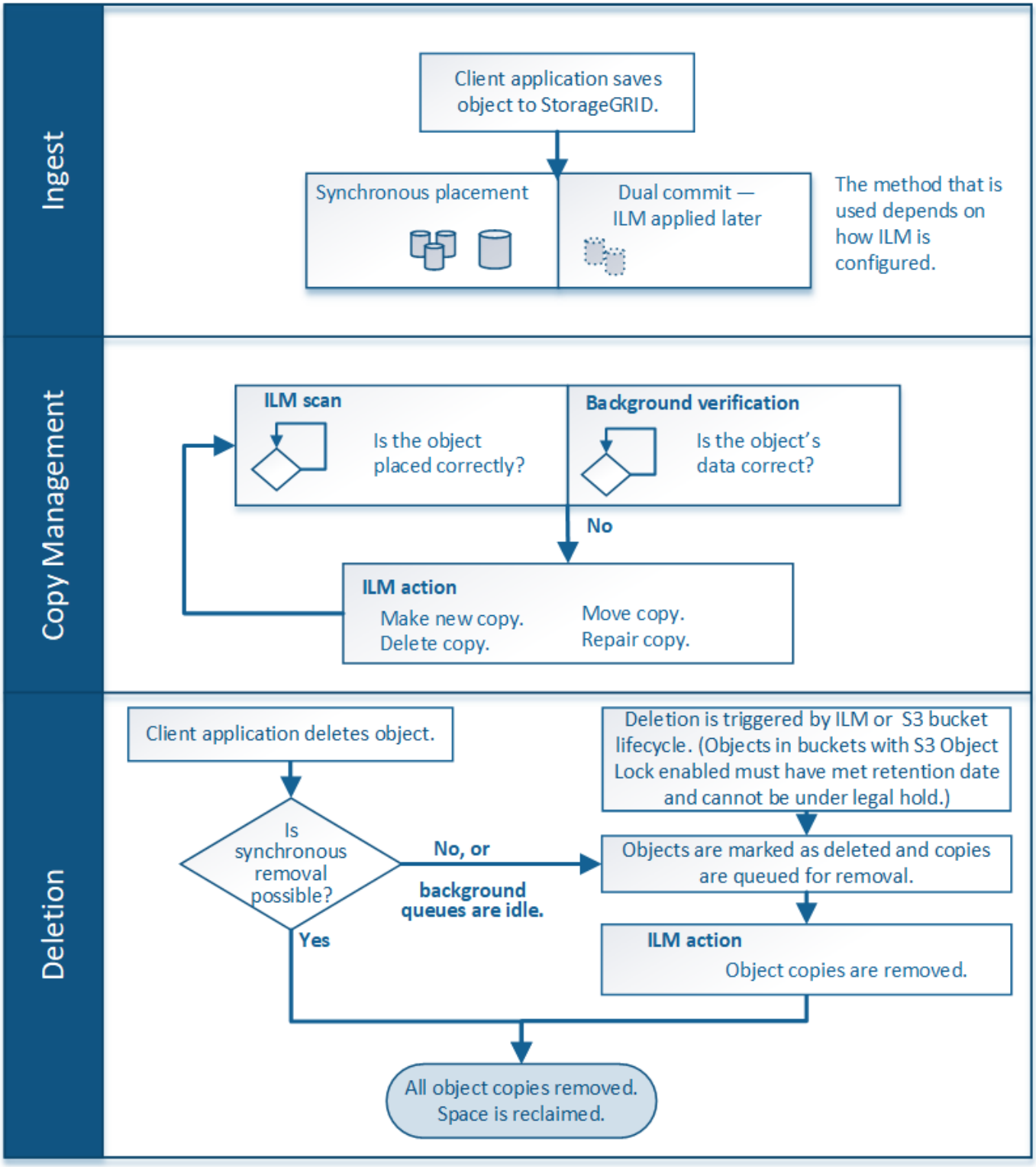
Fonctionnement de ILM tout au long de la vie d'un objet

La compréhension de la façon dont StorageGRID utilise les règles ILM pour gérer les objets à chaque étape de leur vie peut vous aider à concevoir des règles plus efficaces.

- **InGest** : l'entrée commence lorsqu'une application client S3 ou Swift établit une connexion pour enregistrer un objet dans le système StorageGRID et est terminée lorsque StorageGRID renvoie un message « entrée réussie » au client. Les données d'objet sont protégées pendant l'ingestion, soit par application immédiate d'instructions ILM (placement synchrone), soit par création de copies intermédiaires et application de la règle ILM (double allocation), en fonction de la spécification des exigences ILM.
- **Gestion des copies** : après la création du nombre et du type de copies d'objets spécifiés dans les instructions de placement de l'ILM, StorageGRID gère les emplacements des objets et protège les objets contre les pertes.
  - Analyse et évaluation ILM : StorageGRID analyse en continu la liste des objets stockés dans la grille et vérifie si les copies actuelles répondent aux exigences ILM. Lorsque différents types, nombres ou emplacements de copies d'objets sont requis, StorageGRID crée, supprime ou déplace des copies selon les besoins.
  - Vérification en arrière-plan : StorageGRID effectue en permanence une vérification en arrière-plan afin de vérifier l'intégrité des données d'objet. En cas de problème, StorageGRID crée automatiquement une nouvelle copie objet ou un fragment d'objet de code d'effacement de remplacement à un emplacement conforme aux exigences ILM actuelles. Voir "Vérifiez l'intégrité de l'objet".
- **Suppression d'objet** : la gestion d'un objet se termine lorsque toutes les copies sont supprimées du système StorageGRID. La suppression d'objets peut être due à une demande de suppression d'un client, ou à la suppression d'un ILM ou d'un programme de suppression provoqué par l'expiration du cycle de vie d'un compartiment S3.

> Les objets d'un compartiment pour lequel le verrouillage objet S3 est activé ne peuvent pas être supprimés s'ils sont soumis à une conservation légale ou si une date de conservation jusqu'à a été spécifiée, mais pas encore remplie.

Le diagramme résume le fonctionnement de ILM tout au long du cycle de vie d'un objet.



Mode d'ingestion des objets

Options d'ingestion

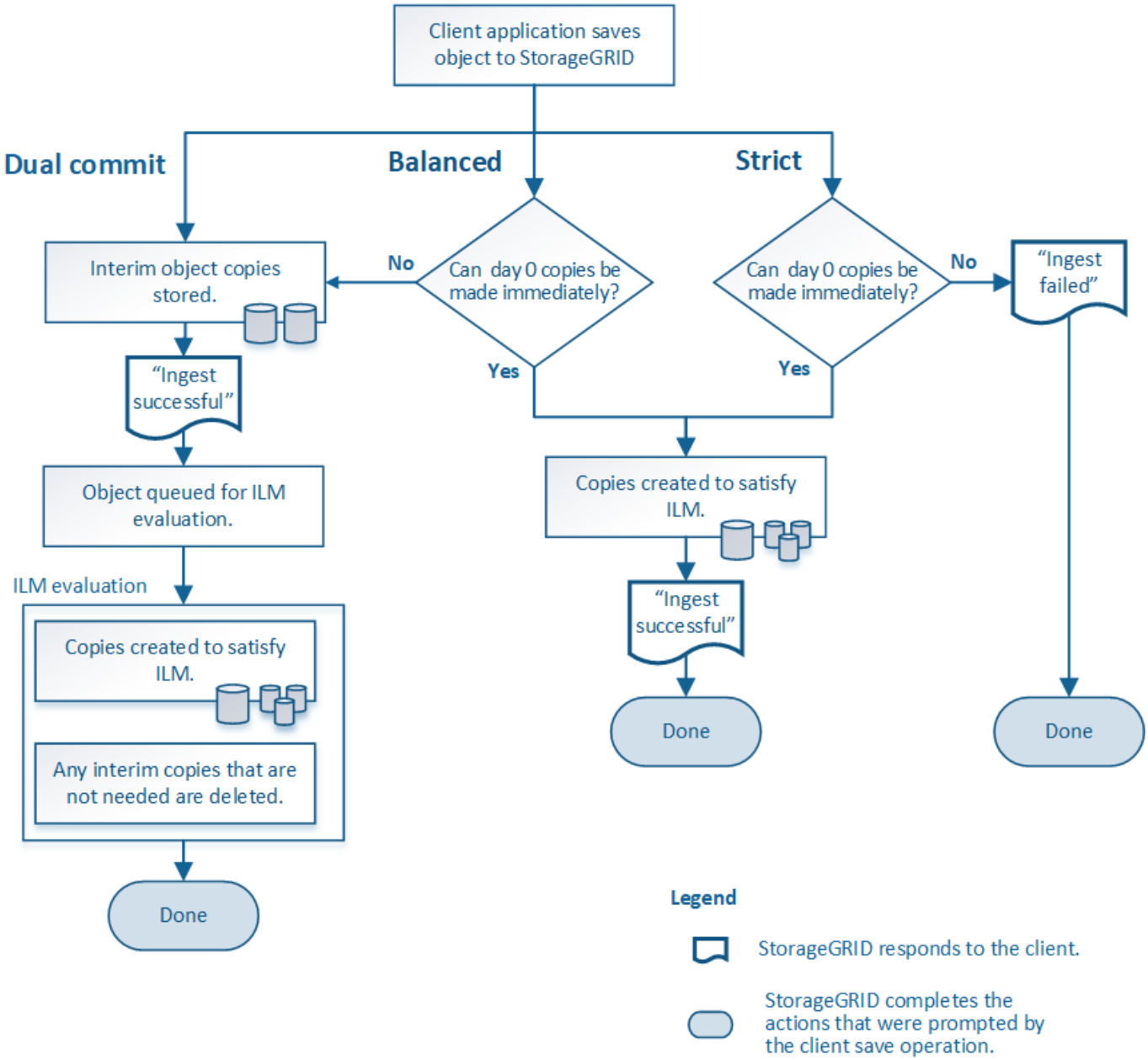
Lorsque vous créez une règle ILM, vous spécifiez l'une des trois options suivantes pour la protection des objets à leur entrée : double allocation, stricte ou équilibrée.

Selon votre choix, StorageGRID effectue des copies intermédiaires et met les objets en file d'attente pour

l'évaluation ILM. De plus, il utilise un placement synchrone et effectue immédiatement des copies pour répondre aux besoins de la solution ILM.

Organigramme des options d'ingestion

L'organigramme indique ce qui se passe lorsque les objets sont mis en correspondance par une règle ILM qui utilise chacune des trois options d'ingestion.



Double allocation

Lorsque vous sélectionnez l'option Dual commit, StorageGRID effectue immédiatement des copies d'objet provisoires sur deux nœuds de stockage différents et renvoie un message « acquisition réussie » au client. L'objet est placé dans la file d'attente pour l'évaluation ILM et les copies correspondant aux instructions de placement de la règle sont créées ultérieurement.

Quand utiliser l'option Double validation

Utilisez l'option Dual commit dans l'un des cas suivants :

- Vous utilisez des règles ILM multisites et la latence d'ingestion du client est votre élément principal. Lorsque vous utilisez la fonctionnalité Dual Commit, vous devez vous assurer que votre grid peut effectuer le travail supplémentaire de création et de suppression des copies à double allocation si elles ne respectent pas la règle ILM. Détails :
  - La charge sur la grille doit être suffisamment faible pour éviter un backlog ILM.
  - La grille doit disposer de ressources matérielles excessives (IOPS, processeur, mémoire, bande passante réseau, etc.).
- Vous utilisez des règles ILM multisites et la connexion WAN entre les sites présente généralement une latence élevée ou une bande passante limitée. Dans ce scénario, l'utilisation de l'option de double engagement permet d'éviter les délais d'attente du client. Avant de choisir l'option Dual commit, il est recommandé de tester l'application cliente avec des charges de travail réalistes.

Stricte

Lorsque vous sélectionnez une option stricte, StorageGRID utilise le placement synchrone pour l'ingestion et immédiatement toutes les copies d'objet spécifiées dans les instructions de placement de la règle. L'ingestion échoue si StorageGRID ne peut pas créer toutes les copies, par exemple, car l'emplacement de stockage requis est temporairement indisponible. Le client doit recommencer l'opération.

Quand utiliser l'option stricte

Utilisez l'option stricte si vous devez respecter des exigences opérationnelles ou réglementaires pour stocker immédiatement les objets aux emplacements définis dans la règle ILM. Par exemple, pour satisfaire aux exigences réglementaires, vous devrez peut-être utiliser l'option strict et un filtre avancé de contrainte d'emplacement pour garantir que les objets ne sont jamais stockés dans certains data centers.

Voir "Exemple 5 : règles et règles ILM pour un comportement d'ingestion strict".

Équilibré (par défaut)

Lorsque vous sélectionnez l'option équilibrée, StorageGRID utilise également le placement synchrone lors de l'ingestion et immédiatement toutes les copies spécifiées dans les instructions de placement de la règle. Contrairement à l'option la plus stricte, si StorageGRID ne peut pas immédiatement effectuer toutes les copies, il utilise la fonction Dual commit.

Quand utiliser l'option équilibrée

Utilisez l'option équilibrée afin de bénéficier de la meilleure combinaison possible de protection des données, de performances de grid et d'ingestion. Balanced est l'option par défaut de l'assistant de création de règles ILM.

Avantages, inconvénients et limites des options d'acquisition

Découvrez les avantages et les inconvénients de chacune des trois options de protection des données à l'entrée (équilibre, stricte ou double engagement). Vous pouvez décider de la règle ILM à sélectionner.

Pour une vue d'ensemble des options d'acquisition, reportez-vous à la section "Options d'ingestion".

Avantages des options équilibrées et strictes

Par rapport à la double allocation qui crée des copies intermédiaires lors de l'ingestion, les deux options de placement synchrone offrent plusieurs avantages :

- **Meilleure sécurité des données**: Les données d'objet sont immédiatement protégées comme spécifié dans les instructions de placement de la règle ILM, qui peuvent être configurées de façon à protéger contre un large éventail de conditions de défaillance, y compris la défaillance de plusieurs emplacements de stockage. La double validation ne peut protéger que contre la perte d'une copie locale unique.
- * Opération de grille plus efficace*: Chaque objet est traité une seule fois, comme il est ingéré. Comme StorageGRID il n'est pas nécessaire de suivre ou de supprimer les copies intermédiaires, la charge de traitement est réduite et l'espace de base de données est consommé.
- **(équilibré) recommandé**: L'option équilibrée offre une efficacité ILM optimale. L'utilisation de l'option Equilibré est recommandée sauf si un comportement d'ingestion strict est requis ou si la grille répond à tous les critères d'utilisation de la double validation.
- * (Strict) certitude sur les emplacements des objets*: L'option stricte garantit que les objets sont immédiatement stockés conformément aux instructions de placement de la règle ILM.

Inconvénients des options équilibrées et strictes

Par rapport à Dual commit, les options équilibrées et strictes présentent quelques inconvénients :

- **Le client ingère plus longtemps**: Les latences d'entrée du client peuvent être plus longues. Lorsque vous utilisez les options équilibrées ou strictes, le message « ingest successful » n'est pas renvoyé au client tant que tous les fragments avec code d'effacement ou les copies répliquées ne sont pas créés et stockés. Néanmoins, les données d'objet atteindront leur placement final beaucoup plus vite.
- **(strict) taux plus élevés d'échec d'ingestion**: Avec l'option stricte, l'ingestion échoue lorsque StorageGRID ne peut pas immédiatement effectuer toutes les copies spécifiées dans la règle ILM. Si un emplacement de stockage requis est temporairement hors ligne ou si un problème réseau entraîne des retards dans la copie des objets entre les sites, des défaillances sont parfois à l'origine de taux élevés.
- **(strict) les parutions de téléchargement partitionné S3 peuvent ne pas être comme prévu dans certaines circonstances**: Avec strict, vous attendez que les objets soient placés comme décrit par la règle ILM ou pour que l'entrée échoue. Toutefois, avec un téléchargement partitionné S3, ILM est évalué pour chaque partie de l'objet lors de son ingestion, et pour l'objet dans son ensemble lorsque le téléchargement partitionné est terminé. Dans les circonstances suivantes, cela peut entraîner des placements qui sont différents de ceux que vous attendez :
  - **Si le ILM change alors qu'un téléchargement partitionné S3 est en cours**: Parce que chaque pièce est placée conformément à la règle qui est active lors de l'ingestion de la pièce, certaines parties de l'objet peuvent ne pas répondre aux exigences ILM actuelles une fois le téléchargement partitionné terminé. Dans ce cas, l'ingestion de l'objet n'a pas échoué. Toute pièce qui n'est pas correctement placée est placée dans la file d'attente pour une réévaluation ILM et sera déplacée ultérieurement à l'emplacement correct.
  - **Lorsque les règles ILM filtrent sur la taille** : lors de l'évaluation de ILM pour une pièce, StorageGRID filtre la taille de la pièce, et non la taille de l'objet. Ainsi, certaines parties d'un objet peuvent être stockées dans des emplacements qui ne respectent pas les exigences de la règle ILM pour l'ensemble de l'objet. Par exemple, si une règle indique que tous les objets de 10 Go ou plus sont stockés dans DC1 alors que tous les objets plus petits sont stockés dans DC2, à l'acquisition chaque partie de 1 Go d'un téléchargement partitionné en 10 parties est stockée dans DC2. Lorsque ILM est évalué pour l'objet, toutes les parties de l'objet sont déplacées vers DC1.
- **(strict) l'ingestion n'échoue pas lorsque les balises d'objet ou les métadonnées sont mises à jour et les nouveaux placements ne peuvent pas être effectués** : avec stricte, les objets doivent être placés

comme décrit par la règle ILM ou l'ingestion pour échouer. Toutefois, lorsque vous mettez à jour les métadonnées ou les balises d'un objet déjà stocké dans la grille, l'objet n'est pas réingéré. Cela signifie que toute modification du placement d'objet déclenchée par la mise à jour n'est pas effectuée immédiatement. Les changements de placement sont apportés lorsqu'ILM est réévaluée par des processus ILM en arrière-plan normaux. Si les modifications de positionnement requises ne peuvent pas être effectuées (par exemple, parce qu'un nouvel emplacement requis n'est pas disponible), l'objet mis à jour conserve son positionnement actuel jusqu'à ce que les modifications de positionnement soient possibles.

Limitations sur les placements d'objets avec les options équilibrées et strictes

Les options équilibrées ou strictes ne peuvent pas être utilisées pour les règles ILM avec l'une des instructions de positionnement suivantes :

- Placement dans un pool de stockage cloud au premier jour.
- Placement dans un nœud d'archivage au jour 0.
- Placements dans un pool de stockage cloud ou un nœud d'archivage lorsque l'heure de création définie par l'utilisateur est l'heure de référence de la règle.

Ces restrictions existent, car StorageGRID ne peut pas effectuer de copies synchrones vers un pool de stockage cloud ou un nœud d'archivage, et une heure de création définie par l'utilisateur pourrait résoudre le problème actuel.

L'interaction des règles ILM et des contrôles de cohérence sur la protection des données

La règle ILM et le contrôle de cohérence de votre choix affectent la protection des objets. Ces paramètres peuvent interagir.

Par exemple, le comportement d'ingestion sélectionné dans une règle ILM affecte le placement initial des copies d'objet, tandis que le contrôle de cohérence utilisé lors du stockage d'un objet affecte le placement initial des métadonnées d'objet. Étant donné que StorageGRID requiert l'accès aux données et aux métadonnées d'un objet pour répondre aux demandes des clients, le choix de niveaux de protection correspondants au niveau de cohérence et au comportement d'ingestion permet une meilleure protection initiale des données et des réponses système plus prévisibles.

Voici un résumé des contrôles de cohérence disponibles dans StorageGRID :

- **Tous** : tous les nœuds reçoivent immédiatement des métadonnées d'objet ou la demande échouera.
- **Strong-global**: Les métadonnées d'objet sont immédiatement distribuées à tous les sites. Garantit une cohérence de lecture après écriture pour toutes les demandes client sur tous les sites.
- **Site fort**: Les métadonnées d'objet sont immédiatement distribuées aux autres nœuds du site. Garantit la cohérence de lecture après écriture pour toutes les demandes client dans un site.
- **Lecture-après-nouvelle-écriture** : offre une cohérence lecture-après-écriture pour les nouveaux objets et une cohérence éventuelle pour les mises à jour d'objets. Offre une haute disponibilité et une protection des données garanties. Recommandé dans la plupart des cas.
- **Disponible** : assure la cohérence finale pour les nouveaux objets et les mises à jour d'objets. Pour les compartiments S3, utilisez uniquement si nécessaire (par exemple, pour un compartiment qui contient des valeurs de journal rarement lues ou pour les opérations HEAD ou GET sur des clés qui n'existent pas). Non pris en charge pour les compartiments FabricPool S3.

Avant de sélectionner un niveau de cohérence, lisez la description complète des contrôles de cohérence dans les instructions pour "UTILISEZ L'API REST S3". Vous devez comprendre les avantages et les limites avant de modifier la valeur par défaut.

Exemple d'interaction du contrôle de cohérence et de la règle ILM

Supposons que vous disposez d'une grille à deux sites avec la règle ILM suivante et le paramètre de niveau de cohérence suivant :

- **Règle ILM** : créez deux copies d'objet, une sur le site local et une sur un site distant. Le comportement d'entrée strict est sélectionné.
- **Niveau de cohérence**: "Sept-global" (les métadonnées d'objet sont immédiatement distribuées à tous les sites).

Lorsqu'un client stocke un objet dans la grille, StorageGRID effectue à la fois des copies d'objet et distribue les métadonnées aux deux sites avant de rétablir la réussite du client.

L'objet est entièrement protégé contre la perte au moment du message d'ingestion. Par exemple, si le site local est perdu peu de temps après l'ingestion, des copies des données de l'objet et des métadonnées de l'objet existent toujours sur le site distant. L'objet est entièrement récupérable.

Si vous utilisez à la place la même règle ILM et le niveau de cohérence "sept-site", le client peut recevoir un message de réussite après la réplication des données d'objet vers le site distant, mais avant que les métadonnées d'objet ne soient distribuées sur ce site. Dans ce cas, le niveau de protection des métadonnées d'objet ne correspond pas au niveau de protection des données d'objet. Si le site local est perdu peu de temps après l'ingestion, les métadonnées d'objet sont perdues. Impossible de récupérer l'objet.

L'interdépendance entre les niveaux de cohérence et les règles ILM peut être complexe. Contactez NetApp si vous avez besoin d'aide.

Informations associées

- "Exemple 5 : règles et règles ILM pour un comportement d'ingestion strict"

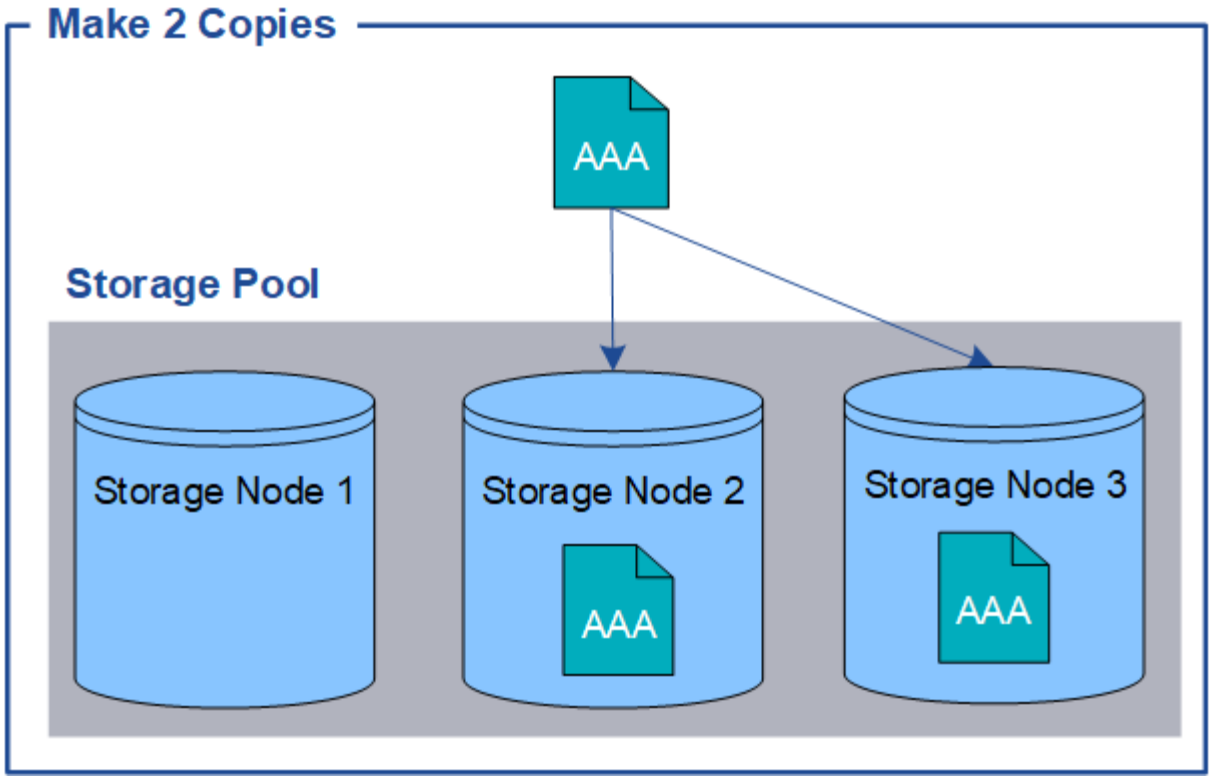
Le mode de stockage des objets (réplication ou code d'effacement)

Qu'est-ce que la réplication ?

La réplication est l'une des deux méthodes utilisées par StorageGRID pour stocker les données d'objet. Lorsque les objets correspondent à une règle ILM utilisant la réplication, le système crée des copies exactes des données d'objet et stocke les copies sur les nœuds de stockage ou les nœuds d'archivage.

Lorsque vous configurez une règle ILM pour créer des copies répliquées, vous spécifiez le nombre de copies à créer, l'emplacement où elles doivent être stockées, ainsi que la durée de stockage de ces copies à chaque emplacement.

L'exemple de règle ILM décrit deux copies répliquées de chaque objet placées dans un pool de stockage contenant trois nœuds de stockage.



Lorsque StorageGRID met les objets en correspondance avec cette règle, elle crée deux copies de l'objet, en plaçant chaque copie sur un autre nœud de stockage du pool. Les deux copies peuvent être placées sur deux des trois nœuds de stockage disponibles. Dans ce cas, la règle a placé des copies d'objet sur les nœuds de stockage 2 et 3. Comme il existe deux copies, l'objet peut être récupéré en cas de défaillance de l'un des nœuds du pool de stockage.

> StorageGRID ne peut stocker qu'une seule copie répliquée d'un objet sur un nœud de stockage donné. Si le grid inclut trois nœuds de stockage et que vous créez une règle ILM de 4 copies, seules trois copies sont effectuées, une copie pour chaque nœud de stockage. L'alerte **ILM placement inaccessible** est déclenchée pour indiquer que la règle ILM n'a pas pu être complètement appliquée.

Informations associées

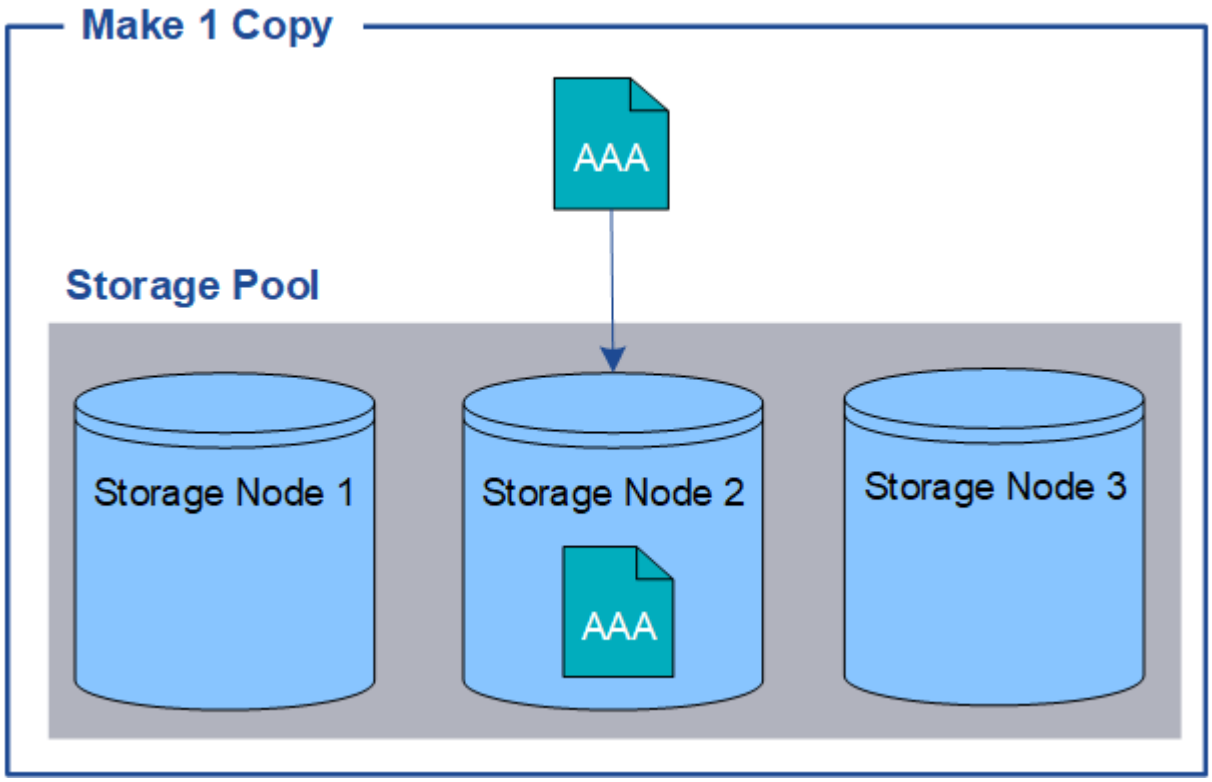
- "Qu'est-ce que le code d'effacement ?"
- "Qu'est-ce qu'un pool de stockage ?"
- "Protection contre la perte de site à l'aide de la réplication et du code d'effacement"

Pourquoi ne pas utiliser la réplication à copie unique

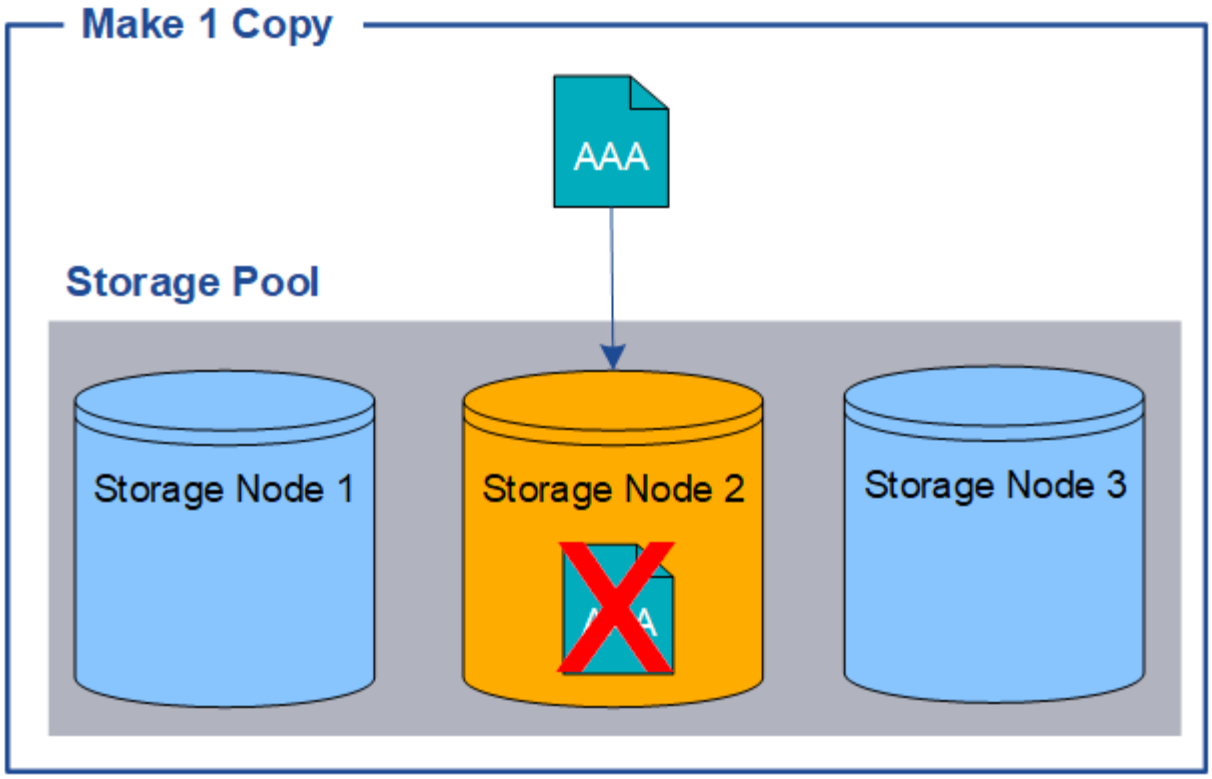
Lors de la création d'une règle ILM pour créer des copies répliquées, vous devez toujours spécifier au moins deux copies pour une période donnée dans les instructions de placement.

> N'utilisez pas de règle ILM pour créer une seule copie répliquée pour une période donnée. Si une seule copie répliquée d'un objet existe, cet objet est perdu en cas de défaillance ou d'erreur importante d'un noeud de stockage. De plus, lors des procédures de maintenance telles que les mises à niveau, l'accès à l'objet est temporairement perdu.

Dans l'exemple suivant, la règle ILM Make 1 copie spécifie qu'une copie répliquée d'un objet doit être placée dans un pool de stockage contenant trois nœuds de stockage. Lors de l'ingestion d'un objet qui correspond à cette règle, StorageGRID place une copie unique sur un seul nœud de stockage.



Lorsqu'une règle ILM ne crée qu'une seule copie répliquée d'un objet, cet objet devient inaccessible lorsque le nœud de stockage est indisponible. Dans cet exemple, vous perdrez temporairement l'accès à l'objet AAA chaque fois que le nœud de stockage 2 est hors ligne, par exemple lors d'une procédure de mise à niveau ou de maintenance. Vous perdrez entièrement l'objet AAA en cas de défaillance du nœud de stockage 2.



Pour éviter de perdre des données d'objet, vous devez toujours effectuer au moins deux copies de tous les objets à protéger par la réplication. Si deux copies ou plus existent, vous pouvez toujours accéder à l'objet en cas de panne ou de mise hors ligne d'un nœud de stockage.

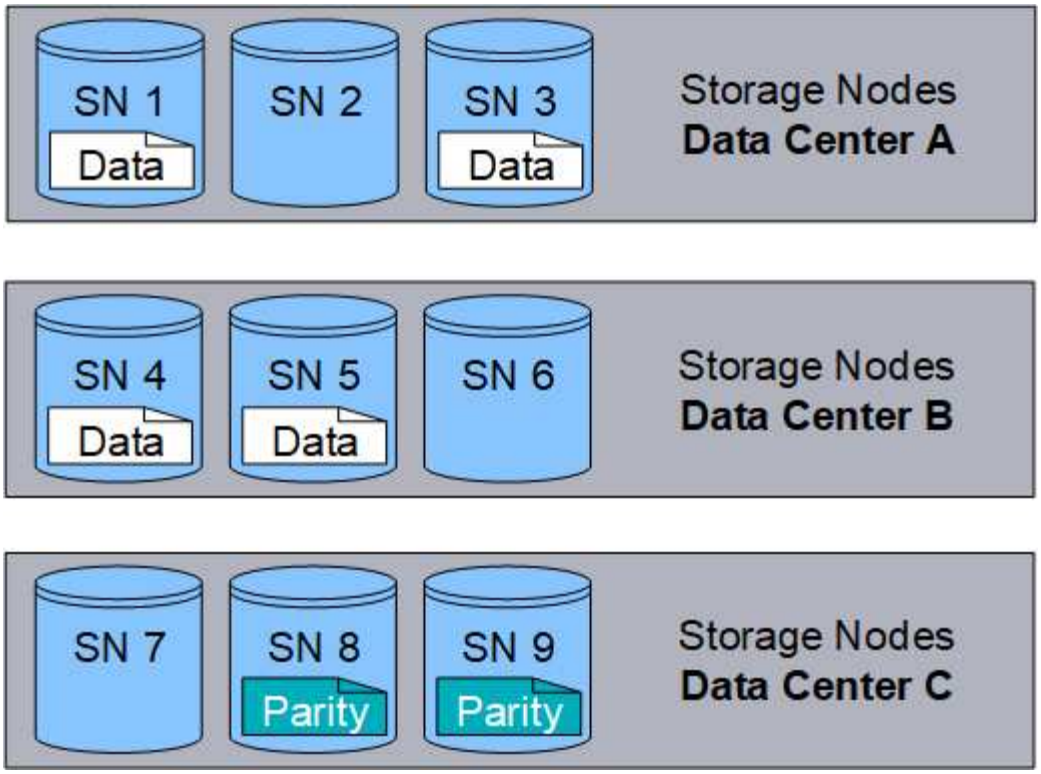
Qu'est-ce que le code d'effacement ?

Le code d'effacement est l'une des deux méthodes utilisées par StorageGRID pour stocker des données en mode objet. Lorsque les objets correspondent à une règle ILM utilisant le code d'effacement, ces objets sont découpés en fragments de données, des fragments de parité supplémentaires sont calculés et chaque fragment est stocké sur un autre nœud de stockage.

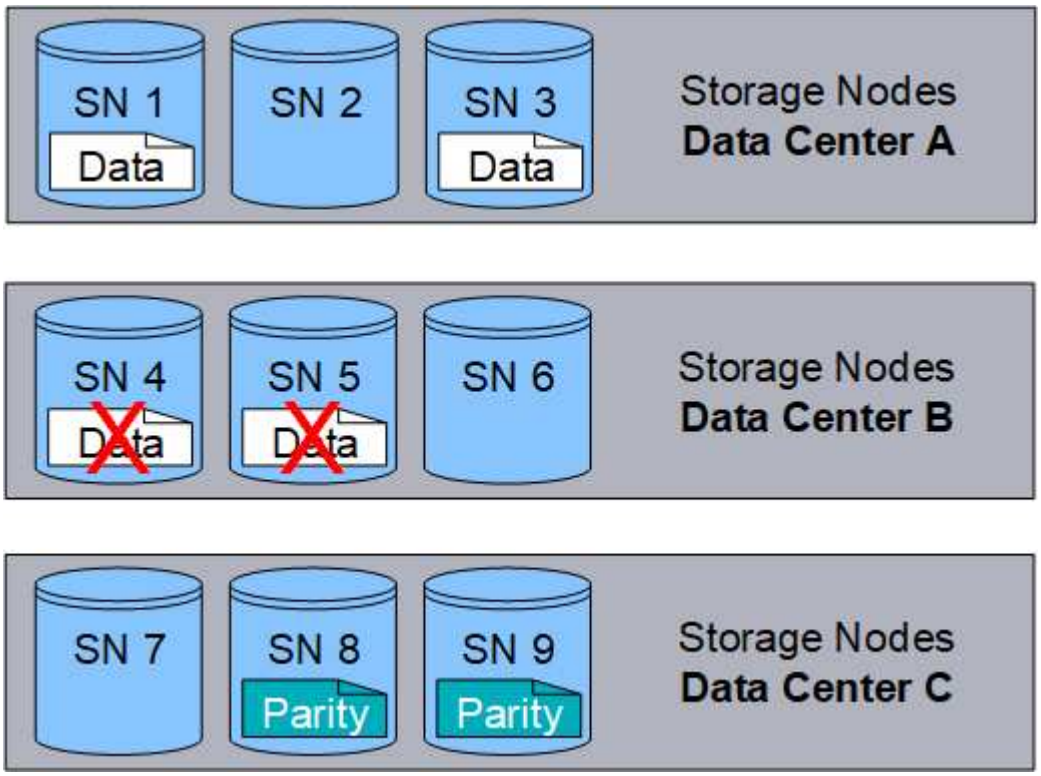
Lorsqu'un objet est accédé, il est réassemblé à l'aide des fragments stockés. En cas de corruption ou de perte d'un fragment de parité, l'algorithme de code d'effacement peut recréer ce fragment à l'aide d'un sous-ensemble des données restantes et des fragments de parité.

Au fur et à mesure que vous créez des règles ILM, StorageGRID crée des profils de code d'effacement qui prennent en charge ces règles. Vous pouvez afficher la liste des profils de code d'effacement, "renommer un profil de code d'effacement", ou "Désactivez un profil de code d'effacement s'il n'est actuellement utilisé dans aucune règle ILM".

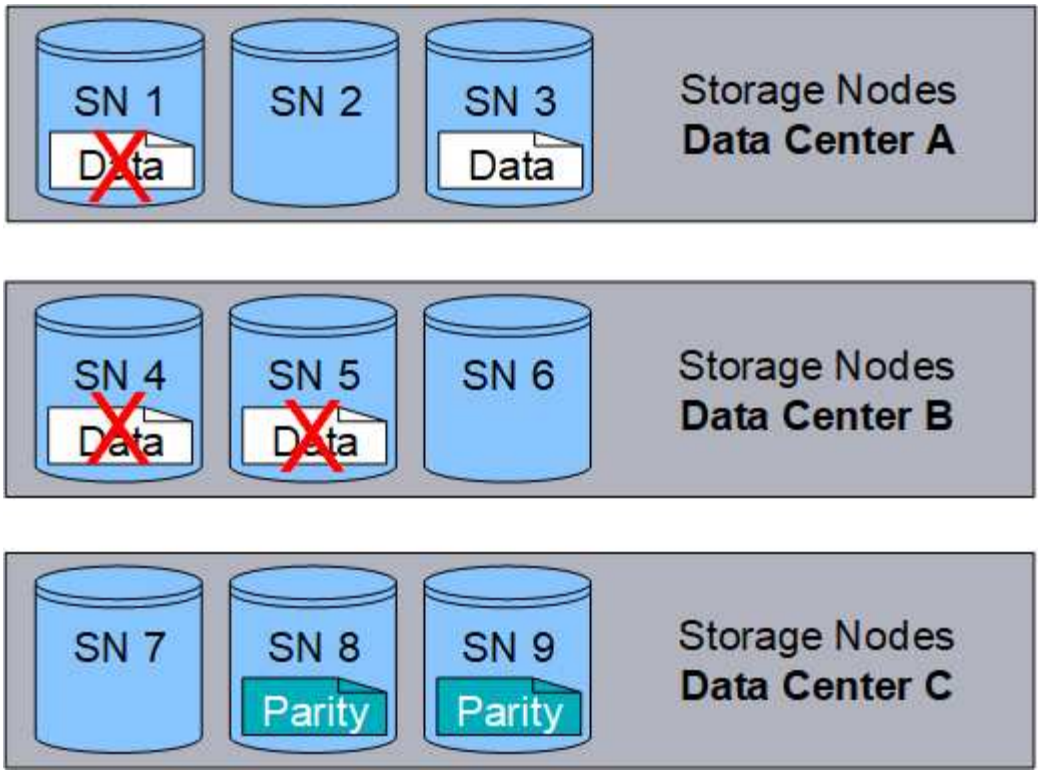
L'exemple suivant illustre l'utilisation d'un algorithme de code d'effacement sur les données d'un objet. Dans cet exemple, la règle ILM utilise un schéma de code d'effacement 4+2. Chaque objet est tranché en quatre fragments de données égaux et deux fragments de parité sont calculés à partir des données d'objet. Chacun des six fragments est stocké sur un nœud différent sur trois sites du data Center pour assurer la protection des données en cas de défaillance d'un nœud ou de perte d'un site.



Le schéma de code d'effacement 4+2 peut être configuré de différentes manières. Par exemple, vous pouvez configurer un pool de stockage sur un seul site qui contient six nœuds de stockage. Pour "protection contre la perte de site", Vous pouvez utiliser un pool de stockage contenant trois sites avec trois nœuds de stockage sur chaque site. Un objet peut être récupéré tant que quatre des six fragments (données ou parité) restent disponibles. Jusqu'à deux fragments peuvent être perdus sans perte des données de l'objet. Si un site entier est perdu, l'objet peut toujours être récupéré ou réparé, tant que tous les autres fragments restent accessibles.



Si plus de deux nœuds de stockage sont perdus, l'objet n'est pas récupérable.



Informations associées

- "Qu'est-ce que la réplication ?"
- "Qu'est-ce qu'un pool de stockage ?"
- "Que sont les schémas de code d'effacement ?"
- "Renommer un profil de code d'effacement"
- "Désactiver un profil de code d'effacement"

Que sont les schémas de code d'effacement ?

Les schémas de codage d'effacement contrôlent le nombre de fragments de données et le nombre de fragments de parité créés pour chaque objet.

Lorsque vous configurez le profil de code d'effacement d'une règle ILM, vous sélectionnez un schéma de code d'effacement disponible en fonction du nombre de nœuds et de sites qui composent le pool de stockage à utiliser.

Le système StorageGRID utilise l'algorithme de codage d'effacement Reed-Solomon. L'algorithme tranche un objet en `k` fragments de données et calculs `m` fragments de parité. Le `k + m = n` les fragments sont répartis à travers `n` Des nœuds de stockage pour assurer la protection des données. Un objet peut supporter jusqu'à `m` fragments perdus ou corrompus. Pour récupérer ou réparer un objet, `k` des fragments sont nécessaires.

Lorsque vous sélectionnez le pool de stockage à utiliser pour une règle qui crée une copie avec code d'effacement, suivez les consignes suivantes pour les pools de stockage :

- Le pool de stockage doit inclure trois sites ou plus, ou exactement un site.

> Le code d'effacement ne peut pas être utilisé si le pool de stockage comprend deux sites.

    - Schémas de code d'effacement pour les pools de stockage contenant au moins trois sites
    - Schémas de code d'effacement pour pools de stockage sur un site
- N'utilisez pas de pool de stockage incluant le site par défaut, tous les sites.
- Le pool de stockage doit inclure au moins `k+m +1` Nœuds de stockage.

  Le nombre minimal de nœuds de stockage requis est de `k+m`. Toutefois, il est possible de disposer d'au moins un nœud de stockage supplémentaire pour empêcher les défaillances d'entrée et les arriérés ILM en cas d'indisponibilité temporaire d'un nœud de stockage requis.

La surcharge du stockage d'un schéma de code d'effacement est calculée en divisant le nombre de fragments de parité (`m`) par le nombre de fragments de données (`k`). Vous pouvez utiliser la surconsommation de stockage pour calculer la quantité d'espace disque requise par chaque objet avec code d'effacement :

```
disk space = object size + (object size * storage overhead)
```

Par exemple, si vous stockez un objet de 10 Mo avec le schéma 4+2 (qui affiche une surcharge du stockage de 50 %), l'objet utilise 15 Mo de stockage grid. Si vous stockez le même objet de 10 Mo avec le schéma 6+2 (qui affiche une surcharge de stockage de 33 %), l'objet consomme environ 13.3 Mo.

Sélectionnez le schéma de code d'effacement dont la valeur totale est la plus faible `k+m` qui répond à vos besoins. Les schémas de code d'effacement avec un nombre réduit de fragments sont globalement plus efficaces sur le plan de la capacité de calcul. En effet, un nombre réduit de fragments est créé et distribué (ou récupéré) par objet, ils offrent de meilleures performances en raison de la taille de fragment plus importante et nécessitent moins de nœuds lors d'une extension lorsque davantage de stockage est nécessaire. (Pour plus d'informations sur la planification d'une extension de stockage, reportez-vous au "Instructions d'extension de StorageGRID".)

Schémas de code d'effacement pour les pools de stockage contenant au moins trois sites

Le tableau ci-dessous décrit les schémas de code d'effacement actuellement pris en charge par StorageGRID pour les pools de stockage incluant au moins trois sites. Tous ces programmes offrent une protection contre les pertes de site. Un site peut être perdu et l'objet sera toujours accessible.

Pour les schémas de code d'effacement qui assurent une protection contre la perte de site, le nombre recommandé de nœuds de stockage dans le pool de stockage est supérieur à `k+m +1` Car chaque site requiert au moins trois nœuds de stockage.

Schéma de code d'effacement (*k+m*)	Nombre minimal de sites déployés	Nombre recommandé de nœuds de stockage sur chaque site	Nombre total recommandé de nœuds de stockage	Protection contre la perte de site ?	Surcharge du stockage
4+2	3	3	9	Oui.	50 %
6+2	4	3	12	Oui.	33 %
8+2	5	3	15	Oui.	25 %
6+3	3	4	12	Oui.	50 %

Schéma de code d'effacement (*k*+*m*)	Nombre minimal de sites déployés	Nombre recommandé de nœuds de stockage sur chaque site	Nombre total recommandé de nœuds de stockage	Protection contre la perte de site ?	Surcharge du stockage
9+3	4	4	16	Oui.	33 %
2+1	3	3	9	Oui.	50 %
4+1	5	3	15	Oui.	25 %
6+1	7	3	21	Oui.	17 %
7+5	3	5	15	Oui.	71 %

StorageGRID requiert au moins trois nœuds de stockage par site. Pour utiliser le schéma 7+5, chaque site requiert au moins quatre nœuds de stockage. Il est recommandé d'utiliser cinq nœuds de stockage par site.

Lors de la sélection d'un schéma de code d'effacement assurant la protection du site, équilibrez l'importance relative des facteurs suivants :

- **Nombre de fragments**: La performance et la flexibilité d'expansion sont généralement meilleures quand le nombre total de fragments est plus faible.
- **Tolérance aux pannes** : la tolérance aux pannes est augmentée en ayant plus de segments de parité (c'est-à-dire quand `m` a une valeur plus élevée.)
- **Trafic réseau**: Lors de la récupération après des pannes, en utilisant un schéma avec plus de fragments (c'est-à-dire, un total plus élevé pour `k+m`) crée plus de trafic réseau.
- **Surcharge de stockage** : les schémas qui génèrent une surcharge plus élevée requièrent davantage d'espace de stockage par objet.

Par exemple, lorsque vous décidez d'un schéma 4+2 et 6+3 (qui ont tous deux des frais de stockage de 50 %), sélectionnez le schéma 6+3 si une tolérance de panne supplémentaire est nécessaire. Sélectionnez le schéma 4+2 si les ressources réseau sont limitées. Si tous les autres facteurs sont égaux, sélectionnez 4+2 parce qu'il a un nombre total de fragments inférieur.

Si vous n'êtes pas certain du schéma à utiliser, sélectionnez 4+2 ou 6+3, ou contactez le support technique.

Schémas de code d'effacement pour pools de stockage sur un site

Un pool de stockage sur un site prend en charge tous les schémas de codage d'effacement définis pour trois sites ou plus, à condition que le site dispose de suffisamment de nœuds de stockage.

Le nombre minimal de nœuds de stockage requis est de `k+m`, mais un pool de stockage avec `k+m +1` Nœuds de stockage recommandés. Par exemple, le schéma de code d'effacement 2+1 requiert un pool de stockage avec au moins trois nœuds de stockage, mais quatre nœuds de stockage sont recommandés.

Schéma de code d'effacement (*k*+*m*)	Nombre minimal de nœuds de stockage	Nombre recommandé de nœuds de stockage	Surcharge du stockage
4+2	6	7	50 %
6+2	8	9	33 %
8+2	10	11	25 %
6+3	9	10	50 %
9+3	12	13	33 %
2+1	3	4	50 %
4+1	5	6	25 %
6+1	7	8	17 %
7+5	12	13	71 %

Avantages, inconvénients et exigences du code d'effacement

Avant de décider s'il est nécessaire d'utiliser la réplication ou le codage d'effacement pour protéger les données d'objet contre la perte, vous devez connaître les avantages, les inconvénients et les exigences du codage d'effacement.

Avantages du code d'effacement

Par rapport à la réplication, le codage d'effacement assure une fiabilité, une disponibilité et une efficacité du stockage supérieures.

- **Fiabilité**: La fiabilité est évaluée en termes de tolérance de pannes, c'est-à-dire le nombre de défaillances simultanées qui peuvent être soutenues sans perte de données. Avec la réplication, plusieurs copies identiques sont stockées sur différents nœuds et entre plusieurs sites. Avec le codage d'effacement, un objet est codé en données et fragments de parité, puis distribué sur de nombreux nœuds et sites. Cette dispersion assure à la fois la protection des pannes sur le site et sur les nœuds. Par rapport à la réplication, le codage d'effacement améliore la fiabilité pour des coûts de stockage comparables.
- **Disponibilité** : la disponibilité peut être définie comme la possibilité de récupérer des objets en cas de défaillance ou d'accès aux nœuds de stockage. Par rapport à la réplication, le codage d'effacement assure une disponibilité supérieure et un coût de stockage comparable.
- **Efficacité du stockage** : pour des niveaux similaires de disponibilité et de fiabilité, les objets protégés par le codage d'effacement consomment moins d'espace disque que les mêmes objets s'ils sont protégés par la réplication. Par exemple, un objet de 10 Mo répliqué sur deux sites consomme 20 Mo d'espace disque (deux copies), tandis qu'un objet dont le code d'effacement est appliqué à trois sites et dont le schéma de code d'effacement 6+3 n'utilise que 15 Mo d'espace disque.

L'espace disque des objets avec code d'effacement est calculé selon la taille de l'objet et la surcharge du stockage. Le pourcentage de surcharge de stockage est le nombre de fragments de parité divisé par le nombre de fragments de données.

Inconvénients du code d'effacement

Par rapport à la réplication, le code d'effacement présente les inconvénients suivants :

- En fonction du schéma de code d'effacement, une augmentation du nombre de sites et de nœuds de stockage est recommandée. En revanche, si vous répliquez les données d'objet, vous n'avez besoin que d'un seul nœud de stockage pour chaque copie. Voir "Schémas de code d'effacement pour pools de stockage contenant au moins trois sites" et "Schémas de code d'effacement pour pools de stockage sur un site".
- Coût et complexité accrus de l'expansion du stockage. Pour étendre un déploiement qui utilise la réplication, vous ajoutez de la capacité de stockage à chaque emplacement où les copies d'objet sont effectuées. Pour étendre un déploiement qui utilise le code d'effacement, vous devez tenir compte à la fois du schéma de code d'effacement utilisé et de la façon dont les nœuds de stockage existants sont complets. Par exemple, si vous attendez que les nœuds existants soient pleins à 100 %, vous devez ajouter au moins `k+m` Nœuds de stockage. Toutefois, si vous étendez cette infrastructure lorsque les nœuds existants sont pleins à 70 %, vous pouvez ajouter deux nœuds par site tout en optimisant la capacité de stockage utilisable. Pour plus d'informations, voir "Ajoutez de la capacité de stockage pour les objets avec code d'effacement".
- Le codage d'effacement entre sites répartis géographiquement augmente la latence de récupération. Les fragments d'objet d'un objet dont le code d'effacement est codé et distribué sur des sites distants sont plus longs à extraire les connexions WAN que les objets répliqués et disponibles localement (sur le même site que celui sur lequel le client se connecte).
- Lorsque vous utilisez le codage d'effacement sur des sites répartis géographiquement, le trafic réseau WAN est plus important pour les récupérations et les réparations, en particulier pour les objets fréquemment récupérés ou pour la réparation d'objets via les connexions réseau WAN.
- Lorsque vous utilisez le codage d'effacement sur plusieurs sites, le débit maximal d'objets diminue considérablement à mesure que la latence du réseau entre les sites augmente. Cette diminution est due à la diminution correspondante du débit du réseau TCP, ce qui affecte la rapidité avec laquelle le système StorageGRID peut stocker et récupérer des fragments d'objet.
- Plus grande utilisation des ressources de calcul.

Quand utiliser le code d'effacement

Le code d'effacement convient mieux aux exigences suivantes :

- Objets dont la taille est supérieure à 1 Mo.

Le codage d'effacement convient mieux aux objets de plus de 1 Mo. N'utilisez pas le code d'effacement pour les objets inférieurs à 200 Ko afin d'éviter la surcharge liée à la gestion de très petits fragments de code d'effacement.

- Stockage à long terme ou à froid pour le contenu rarement récupéré.
- Haute disponibilité et fiabilité des données.
- Protégez-vous contre les défaillances complètes du site et des nœuds.
- Efficacité du stockage.

- Les déploiements sur un seul site exigent une protection efficace des données avec une seule copie avec code d'effacement plutôt que plusieurs copies répliquées.
- Déploiements sur plusieurs sites pour lesquels la latence inter-site est inférieure à 100 ms.

Méthode de détermination de la conservation des objets

StorageGRID fournit aux administrateurs du grid et aux utilisateurs de locataires individuels les options permettant de spécifier la durée de stockage des objets. En général, les instructions de conservation fournies par un utilisateur locataire ont priorité sur les instructions de conservation fournies par l'administrateur de la grille.

Contrôle de la conservation des objets par les utilisateurs locataires

Les locataires disposent de trois méthodes principales pour contrôler la durée de stockage de leurs objets dans StorageGRID :

- Si le paramètre global S3 Object Lock est activé pour la grille, les locataires S3 peuvent créer des compartiments avec le verrouillage d'objet S3 activé, puis utiliser l'API REST S3 pour spécifier les paramètres de conservation à la date et la conservation légale de chaque version d'objet ajoutée dans ce compartiment.
  - Aucune méthode ne permet de supprimer une version d'objet faisant l'objet d'une conservation légale.
  - Avant que la date de conservation d'une version d'objet ne soit atteinte, cette version ne peut pas être supprimée par aucune méthode.
  - Les objets des compartiments où le verrouillage d'objet S3 est activé sont conservés par ILM « Forever ». Une fois la date de conservation atteinte, une version d'objet peut être supprimée par une demande client ou l'expiration du cycle de vie du compartiment. Voir "Gestion des objets avec le verrouillage d'objets S3".
- Les locataires S3 peuvent ajouter une configuration du cycle de vie à leurs compartiments pour définir une action d'expiration. En cas de cycle de vie d'un compartiment, StorageGRID stocke un objet jusqu'à ce que la date ou le nombre de jours spécifiés dans l'action expiration soit atteint, à moins que le client ne supprime d'abord l'objet. Voir "Création de la configuration du cycle de vie S3".
- Un client S3 ou Swift peut émettre une demande de suppression d'objet. StorageGRID privilégie toujours les demandes de suppression client sur le cycle de vie du compartiment S3 ou la ILM pour déterminer si supprimer ou conserver un objet.

Comment les administrateurs du grid contrôlent-ils la conservation des objets

Les administrateurs du grid utilisent des instructions de placement ILM pour contrôler la durée de stockage des objets. Lorsque les objets sont comparés par une règle ILM, StorageGRID les stocke jusqu'à la dernière période de la règle ILM. Les objets sont conservés indéfiniment si « toujours » est spécifié pour les instructions de placement.

Quelle que soit la durée de conservation des objets, les paramètres ILM contrôlent les types de copies d'objet (répliquées ou avec code d'effacement) stockés et l'emplacement des copies (nœuds de stockage, pools de stockage cloud ou nœuds d'archivage).

Interaction du cycle de vie des compartiments S3 et de la ILM

L'action d'expiration dans un cycle de vie des compartiments S3 remplace toujours les paramètres ILM. Par conséquent, un objet peut être conservé dans la grille même après l'expiration des instructions ILM de placement de l'objet.

Exemples de conservation d'objets

Pour mieux comprendre les interactions entre le verrouillage objet S3, les paramètres du cycle de vie des compartiments, les demandes de suppression de clients et la gestion des règles ILM, prenez en compte ces exemples.

Exemple 1 : le cycle de vie des compartiments S3 permet de conserver les objets plus longtemps que ILM

ILM

Stockez deux copies pendant 1 an (365 jours)

Cycle de vie des compartiments

Expire les objets dans 2 ans (730 jours)

Résultat

StorageGRID stocke l'objet pendant 730 jours. StorageGRID utilise les paramètres du cycle de vie du compartiment pour déterminer s'il faut supprimer ou conserver un objet.

> Si le cycle de vie des compartiments précise que les objets doivent être conservés plus longtemps que spécifié par l'ILM, StorageGRID continue d'utiliser les instructions de placement du ILM pour déterminer le nombre et le type de copies à stocker. Dans cet exemple, deux copies de l'objet continueront à être stockées dans StorageGRID au lieu de 366 à 730 jours.

Exemple 2 : le cycle de vie des compartiments S3 expire les objets avant la gestion du cycle de vie des règles

ILM

Stockage de deux copies pendant 2 ans (730 jours)

Cycle de vie des compartiments

Expiration des objets en 1 an (365 jours)

Résultat

StorageGRID supprime les deux copies de l'objet après le jour 365.

Exemple 3 : la suppression du client annule le cycle de vie du compartiment et la ILM

ILM

Stockage de deux copies sur des nœuds de stockage « toujours »

Cycle de vie des compartiments

Expire les objets dans 2 ans (730 jours)

Demande de suppression du client

Émis le jour 400

Résultat

StorageGRID supprime les deux copies de l'objet le jour 400 en réponse à la requête de suppression du client.

Exemple 4 : le verrouillage d'objet S3 remplace la demande de suppression du client

Verrouillage d'objet S3

Conserver jusqu'à ce jour pour une version d'objet : 2026-03-31. Une obligation légale n'est pas en vigueur.

Règle ILM conforme

Stockez deux copies sur des nœuds de stockage « toujours ».

Demande de suppression du client

Émis le 2024-03-31.

Résultat

StorageGRID ne supprimera pas la version de l'objet car la date de conservation est encore à 2 ans.

Comment supprimer les objets

StorageGRID peut supprimer des objets en réponse directe à une requête d'un client ou automatiquement à la suite de l'expiration du cycle de vie d'un compartiment S3 ou des exigences de la politique ILM. Pour gérer plus efficacement les objets, il est important de comprendre les différentes méthodes de suppression des objets et la façon dont StorageGRID les gère.

StorageGRID peut utiliser l'une des deux méthodes suivantes pour supprimer les objets :

- Suppression synchrone : lorsque StorageGRID reçoit une demande de suppression de client, toutes les copies d'objet sont supprimées immédiatement. Le client est informé que la suppression a réussi une fois les copies supprimées.
- Les objets sont placés en file d'attente pour suppression : lorsque StorageGRID reçoit une requête de suppression, l'objet est mis en attente pour suppression et le client est immédiatement informé de l'réussie de cette suppression. Les copies d'objet sont supprimées ultérieurement par le traitement ILM en arrière-plan.

Lors de la suppression d'objets, StorageGRID utilise la méthode qui optimise les performances de suppression, réduit les retards de suppression et libère de l'espace le plus rapidement possible.

Le tableau résume le moment où StorageGRID utilise chaque méthode.

Méthode d'exécution de la suppression	Lorsqu'il est utilisé
Les objets sont placés en file d'attente pour suppression	Lorsque **l'une** des conditions suivantes est vraie : • La suppression automatique d'objet a été déclenchée par l'un des événements suivants : ◦ La date d'expiration ou le nombre de jours pendant la configuration du cycle de vie d'un compartiment S3 est atteint. ◦ La dernière période spécifiée dans une règle ILM s'écoule. **Remarque :** les objets d'un compartiment pour lequel le verrouillage d'objet S3 est activé ne peuvent pas être supprimés s'ils sont en attente légale ou si une date de conservation jusqu'à a été spécifiée mais pas encore remplie. • Un client S3 ou Swift demande la suppression d'une ou plusieurs des conditions suivantes : ◦ Les copies ne peuvent pas être supprimées dans les 30 secondes qui suivent, car, par exemple, un emplacement d'objet est temporairement indisponible. ◦ Les files d'attente de suppression d'arrière-plan sont inactives.
Suppression immédiate d'objets (suppression synchrone)	Lorsqu'un client S3 ou Swift effectue une demande de suppression et **toutes** des conditions suivantes sont remplies : • Toutes les copies peuvent être supprimées en 30 secondes. • Les files d'attente de suppression d'arrière-plan contiennent des objets à traiter.

Lorsque des clients S3 ou Swift font des demandes de suppression, StorageGRID commence par ajouter des objets à la file d'attente de suppression. Il passe ensuite en mode suppression synchrone. S'assurer que la file d'attente de suppression en arrière-plan contient des objets à traiter, ce qui permet à StorageGRID de traiter les suppressions plus efficacement, en particulier pour les clients à faible simultanéité, tout en aidant à empêcher la suppression des arriérés du client.

Temps nécessaire à la suppression des objets

La façon dont StorageGRID supprime des objets peut avoir un impact sur le fonctionnement du système :

- Lorsque StorageGRID effectue une suppression synchrone, StorageGRID peut donner jusqu'à 30 secondes pour renvoyer un résultat au client. Cela signifie que la suppression peut se produire plus lentement, même si les copies sont réellement supprimées plus rapidement que lors de la mise en file d'attente d'objets StorageGRID pour suppression.
- Si vous surveillez de près les performances de suppression lors d'une suppression en bloc, vous remarquerez que ce taux de suppression semble ralentir après la suppression d'un certain nombre d'objets. Ce changement survient lorsque StorageGRID passe d'objets de mise en file d'attente pour suppression à des fins de suppression synchrone. La réduction apparente du taux de suppression ne signifie pas que les copies d'objet sont supprimées plus lentement. Au contraire, elle indique qu'en moyenne, l'espace est maintenant libéré plus rapidement.

Si vous supprimez un grand nombre d'objets et que vous souhaitez libérer rapidement de l'espace, pensez à utiliser une requête client pour supprimer des objets au lieu de les supprimer à l'aide d'ILM ou d'autres méthodes. En général, l'espace est libéré plus rapidement lors de la suppression d'espace par les clients, car StorageGRID peut utiliser la suppression synchrone.

Le temps nécessaire pour libérer de l'espace après la suppression d'un objet dépend de plusieurs facteurs :

- Si les copies d'objet sont supprimées de manière synchrone ou mises en file d'attente pour être supprimées ultérieurement (pour les demandes de suppression de client).
- D'autres facteurs, tels que le nombre d'objets dans la grille ou la disponibilité des ressources de la grille lorsque les copies d'objet sont mises en file d'attente pour suppression (pour les suppressions de clients et d'autres méthodes).

Suppression d'objets avec version S3

Lorsque le contrôle de version est activé pour un compartiment S3, StorageGRID suit un comportement Amazon S3 pour répondre aux demandes de suppression, qu'elles proviennent d'un client S3, de l'expiration d'un cycle de vie d'un compartiment S3 ou des exigences de la règle ILM.

Lorsque des objets sont versionnés, les demandes de suppression d'objets ne suppriment pas la version actuelle de l'objet et ne libèrent pas d'espace. Une demande de suppression d'objet crée un marqueur de suppression en tant que version actuelle de l'objet, ce qui rend la version précédente de l'objet « non actuelle ».

Bien que l'objet n'ait pas été supprimé, StorageGRID se comporte comme si la version actuelle de l'objet n'est plus disponible. Les requêtes à cet objet renvoient 404 NotFound. Cependant, les données d'objet non actuelles n'ayant pas été supprimées, les demandes qui spécifient une version non actuelle de l'objet peuvent réussir.

Pour libérer de l'espace lors de la suppression d'objets multiversion, utilisez l'une des méthodes suivantes :

- **Demande client S3** : spécifiez l'ID de version de l'objet dans la demande de SUPPRESSION d'objet S3 (`DELETE /object?versionId=ID`). Notez que cette demande ne supprime que les copies d'objet pour la version spécifiée (les autres versions occupent toujours de l'espace).
- **Cycle de vie du godet** : utilisez le `NoncurrentVersionExpiration` l'action en termes de configuration du cycle de vie des compartiments. Lorsque le nombre de NonactuelDays spécifié est atteint, StorageGRID supprime définitivement toutes les copies des versions d'objets non courants. Ces versions d'objet ne peuvent pas être restaurées.

  Le `NewerNoncurrentVersions` L'action dans la configuration du cycle de vie du compartiment spécifie le nombre de versions non actuelles conservées dans un compartiment S3 versionné. S'il existe plus de versions non actuelles que `NewerNoncurrentVersions` Spécifie que StorageGRID supprime les anciennes versions une fois la valeur NoncurrentDays écoulée. Le `NewerNoncurrentVersions` Le seuil remplace les règles de cycle de vie fournies par ILM, ce qui signifie qu'un objet non actuel avec une version dans le système `NewerNoncurrentVersions` Le seuil est conservé si la requête ILM de suppression le requiert.

- **ILM** : "Cloner la règle active" Et ajouter deux règles ILM à la nouvelle politique proposée :
  - Première règle : utilisez « temps non courant » comme temps de référence pour correspondre aux versions non actuelles de l'objet. Dans "Étape 1 (entrer les détails) de l'assistant de création de règles ILM", Sélectionnez **Oui** pour la question, ""appliquer cette règle aux anciennes versions d'objet uniquement (dans les compartiments S3 avec gestion des versions activée)?"
  - Deuxième règle : utilisez **le temps d'ingestion** pour correspondre à la version actuelle. La règle «

Noncurrent Time » doit apparaître dans la police au-dessus de la règle **Ingest Time**.

Suppression des marqueurs de suppression S3

Lorsqu'un objet versionné est supprimé, StorageGRID crée un marqueur de suppression en tant que version actuelle de l'objet. Pour supprimer le marqueur de suppression de zéro octet du compartiment, le client S3 doit supprimer explicitement la version de l'objet. Les marqueurs de suppression ne sont pas supprimés par ILM, les règles de cycle de vie des compartiments ou la suppression d'objets dans les opérations de compartiment.

Informations associées

- "UTILISEZ L'API REST S3"
- "Exemple 4 : règles et règles ILM pour les objets avec version S3"

Créer et attribuer des notes de stockage

Les niveaux de stockage identifient le type de stockage utilisé par un nœud de stockage. Vous pouvez créer des classes de stockage si vous souhaitez que les règles ILM placent certains objets sur certains nœuds de stockage.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous disposez d'autorisations d'accès spécifiques.

Description de la tâche

Lorsque vous installez StorageGRID pour la première fois, le niveau de stockage **par défaut** est automatiquement attribué à chaque nœud de stockage de votre système. Si nécessaire, vous pouvez définir des niveaux de stockage personnalisés et les attribuer à différents nœuds de stockage.

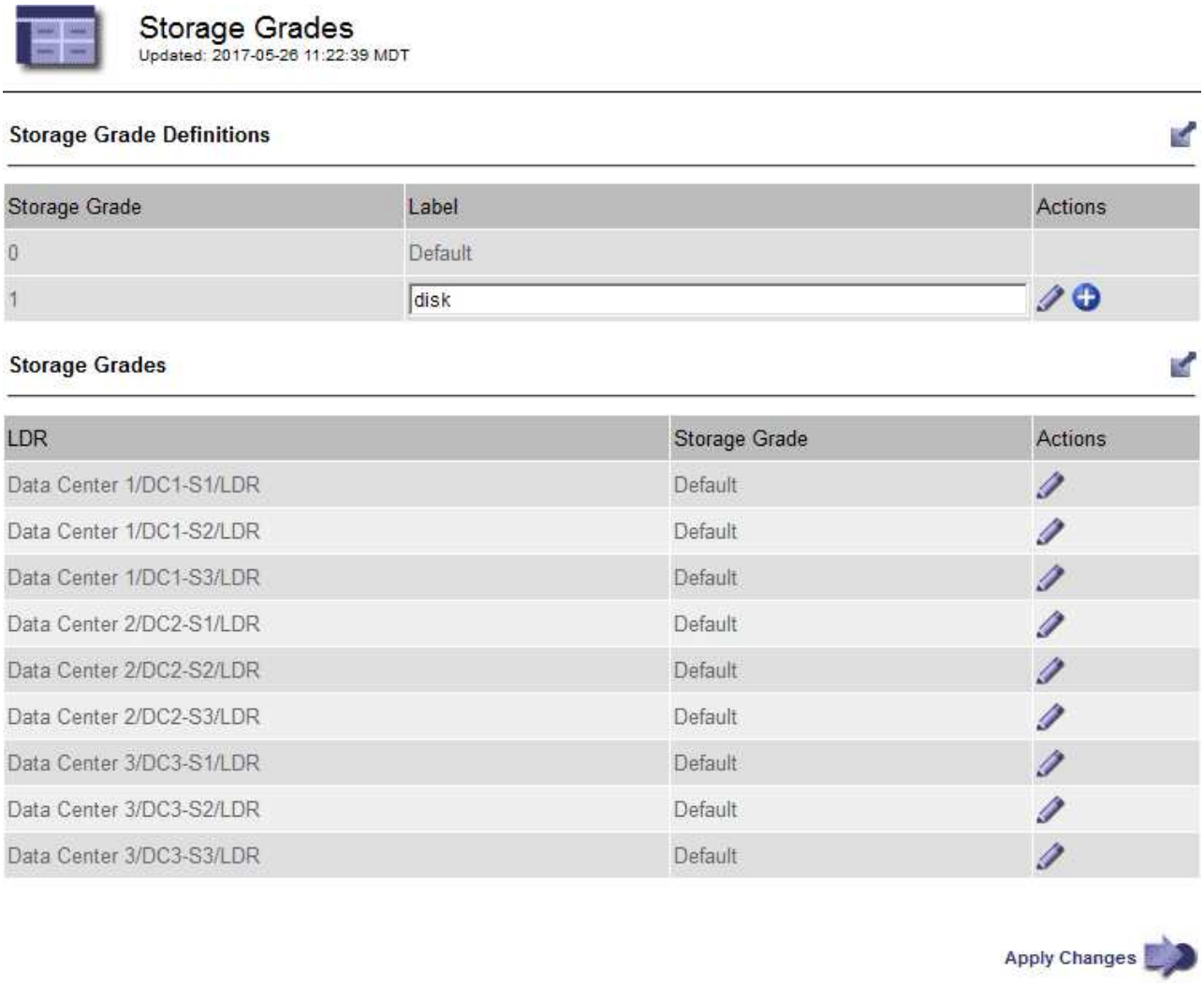
L'utilisation de niveaux de stockage personnalisés vous permet de créer des pools de stockage ILM qui ne contiennent qu'un type spécifique de nœud de stockage. Vous pouvez, par exemple, stocker certains objets sur les nœuds de stockage les plus rapides, comme les appliances de stockage 100 % Flash StorageGRID.

Si le niveau de stockage n'est pas un problème (par exemple, tous les nœuds de stockage sont identiques), vous pouvez ignorer cette procédure et utiliser la sélection **inclut tous les niveaux de stockage** pour le niveau de stockage lorsque vous le souhaitez "créer des pools de stockage". Cette sélection permet de s'assurer que le pool de stockage inclura chaque nœud de stockage sur le site, quel que soit son niveau de stockage.

> Ne créez pas plus de niveaux de stockage que nécessaire. Par exemple, ne créez pas de niveau de stockage pour chaque nœud de stockage. Attribuez plutôt chaque catégorie de stockage à deux nœuds ou plus. Des types de stockage attribués à un seul nœud peuvent entraîner des backlog ILM si ce nœud est indisponible.

Étapes

1. Sélectionnez **ILM** > **grades de stockage**.
2. Définissez des niveaux de stockage personnalisés :
   a. Pour chaque classe de stockage personnalisée que vous souhaitez ajouter, sélectionnez **Insérer** pour ajouter une ligne.
   b. Saisissez un libellé descriptif.



c. Sélectionnez **appliquer les modifications**.

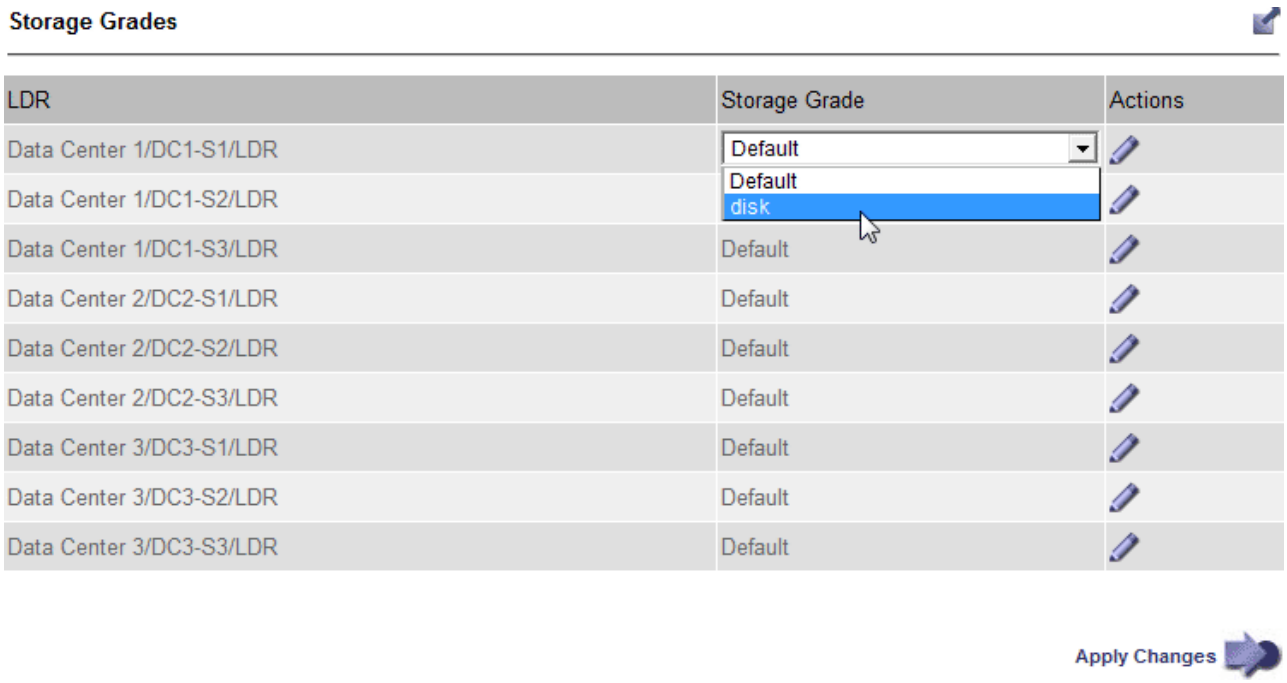
d. Si vous souhaitez modifier une étiquette enregistrée, sélectionnez **Modifier** Et sélectionnez **appliquer les modifications**.

Vous ne pouvez pas supprimer des niveaux de stockage.

3. Attribuez de nouveaux niveaux de stockage aux nœuds de stockage :

a. Localisez le noeud de stockage dans la liste LDR et sélectionnez son icône **Edit** .

b. Sélectionnez le niveau de stockage approprié dans la liste.



Attribuez une note de stockage à un nœud de stockage donné une seule fois. La récupération d'un nœud de stockage suite à une défaillance permet de conserver la qualité de stockage précédemment attribuée. Ne modifiez pas cette affectation une fois la politique ILM activée. Si l'affectation est modifiée, les données sont stockées selon le nouveau niveau de stockage.

a. Sélectionnez **appliquer les modifications**.

Utiliser des pools de stockage

Qu'est-ce qu'un pool de stockage ?

Un pool de stockage est un groupe logique de nœuds de stockage ou de nœuds d'archivage.

Lorsque vous installez StorageGRID, un pool de stockage par site est automatiquement créé. Vous pouvez configurer des pools de stockage supplémentaires selon vos besoins en stockage.

La prise en charge des nœuds d'archivage (pour l'archivage dans le cloud à l'aide de l'API S3 et l'archivage sur bande à l'aide du middleware TSM) est obsolète et sera supprimée dans une prochaine version. Le déplacement d'objets d'un nœud d'archivage vers un système de stockage d'archives externe a été remplacé par les pools de stockage cloud ILM pour offrir davantage de fonctionnalités.

Voir "Utilisation des pools de stockage cloud".

Les pools de stockage ont deux attributs :

- **Stockage** : pour les nœuds de stockage, les performances relatives du stockage de support.
- **Site** : le centre de données où les objets seront stockés.

Les pools de stockage sont utilisés dans les règles ILM pour déterminer l'emplacement du stockage des

données en mode objet et le type de stockage utilisé. Lorsque vous configurez des règles ILM pour la réplication, vous sélectionnez un ou plusieurs pools de stockage incluant des nœuds de stockage ou des nœuds d'archivage. Lorsque vous créez des profils de code d'effacement, vous sélectionnez un pool de stockage qui inclut les nœuds de stockage.

Instructions pour la création de pools de stockage

Configurez et utilisez les pools de stockage pour vous protéger contre les pertes de données, en distribuant les données entre plusieurs sites. Les copies répliquées et les copies avec code d'effacement nécessitent différentes configurations de pool de stockage.

Voir "Exemples d'activation de la protection contre la perte sur site à l'aide de la réplication et du code d'effacement".

Instructions pour tous les pools de stockage

- Simplifiez au maximum les configurations de vos pools de stockage. Ne créez pas plus de pools de stockage que nécessaire.
- Créez des pools de stockage avec autant de nœuds que possible. Chaque pool de stockage doit contenir deux nœuds ou plus. Un pool de stockage ne disposant pas de nœuds suffisants peut générer des arriérés ILM en cas d'indisponibilité d'un nœud.
- Évitez de créer ou d'utiliser des pools de stockage qui se chevauchent (contiennent un ou plusieurs des mêmes nœuds). Si les pools de stockage se chevauchent, il est possible d'enregistrer plusieurs copies des données d'objet sur le même nœud.
- En général, n'utilisez pas le pool de stockage tous les nœuds (StorageGRID 11.6 et versions antérieures) ni le site tous les sites. Ces éléments sont automatiquement mis à jour pour inclure les nouveaux sites que vous ajoutez dans une extension, ce qui peut ne pas être le comportement que vous voulez.

Instructions relatives aux pools de stockage utilisés pour les copies répliquées

- Pour une protection contre les pertes de site à l'aide de "la réplication", spécifiez un ou plusieurs pools de stockage spécifiques au site dans le "Instructions de placement pour chaque règle ILM".

  Un pool de stockage est automatiquement créé pour chaque site lors de l'installation de StorageGRID.

  L'utilisation d'un pool de stockage pour chaque site permet de placer les copies d'objets répliquées exactement là où vous en avez besoin (par exemple, une copie de chaque objet sur chaque site pour une protection contre les pertes au niveau du site).

- Si vous ajoutez un site dans une extension, créez un nouveau pool de stockage qui ne contient que le nouveau site. Puis, "Mise à jour des règles ILM" pour contrôler les objets stockés sur le nouveau site.
- Si le nombre de copies est inférieur au nombre de pools de stockage, le système distribue les copies pour équilibrer l'utilisation des disques entre les pools.
- Si les pools de stockage se chevauchent (contiennent les mêmes nœuds de stockage), toutes les copies de l'objet peuvent être enregistrées sur un seul site. Vous devez vous assurer que les pools de stockage sélectionnés ne contiennent pas les mêmes nœuds de stockage.

Instructions relatives aux pools de stockage utilisés pour les copies avec code d'effacement

- Pour une protection contre les pertes de site à l'aide de "le code d'effacement", créez des pools de stockage composés d'au moins trois sites. Si un pool de stockage ne comprend que deux sites, vous ne

pouvez pas l'utiliser pour le code d'effacement. Aucun schéma de code d'effacement n'est disponible pour un pool de stockage possédant deux sites.

- Le nombre de nœuds de stockage et de sites contenus dans le pool de stockage détermine lesquels "schémas de code d'effacement" sont disponibles.
- Si possible, un pool de stockage doit inclure plus que le nombre minimum de nœuds de stockage requis pour le schéma de code d'effacement sélectionné. Par exemple, si vous utilisez un schéma de code d'effacement 6+3, vous devez avoir au moins neuf nœuds de stockage. Toutefois, il est recommandé de disposer d'au moins un nœud de stockage supplémentaire par site.
- Distribuez les nœuds de stockage sur tous les sites de façon aussi homogène que possible. Par exemple, pour prendre en charge un schéma de code d'effacement 6+3, configurez un pool de stockage qui inclut au moins trois nœuds de stockage sur trois sites.
- Si vos besoins en débit sont élevés, il n'est pas recommandé d'utiliser un pool de stockage comprenant plusieurs sites si la latence réseau entre les sites est supérieure à 100 ms. Au fur et à mesure que la latence augmente, la vitesse à laquelle StorageGRID peut créer, placer et récupérer des fragments d'objet diminue considérablement en raison de la diminution du débit du réseau TCP.

  La diminution du débit affecte les taux maximaux d'entrée et de récupération d'objets (lorsqu'un comportement d'ingestion est sélectionné pour être équilibré ou strict) ou peut entraîner des retards de file d'attente ILM (lorsque la double validation est sélectionnée comme comportement d'ingestion). Voir "Comportement d'ingestion des règles ILM".

  > ⓘ Si votre grid ne comprend qu'un seul site, vous ne pouvez pas utiliser le pool de stockage tous les nœuds (StorageGRID 11.6 et versions antérieures) ou le site par défaut tous les sites dans un profil de code d'effacement. Ce comportement empêche le profil de devenir non valide si un second site est ajouté.

- Les nœuds d'archivage ne peuvent pas être utilisés pour des données avec code d'effacement.

Instructions relatives aux pools de stockage utilisés pour les copies archivées

> ⚠ La prise en charge des nœuds d'archivage (pour l'archivage dans le cloud à l'aide de l'API S3 et l'archivage sur bande à l'aide du middleware TSM) est obsolète et sera supprimée dans une prochaine version. Le déplacement d'objets d'un nœud d'archivage vers un système de stockage d'archives externe a été remplacé par les pools de stockage cloud ILM pour offrir davantage de fonctionnalités.
>
> Voir "Migration des objets vers un pool de stockage cloud".
>
> De plus, vous devez supprimer les nœuds d'archivage de la règle ILM active dans StorageGRID 11.7 ou version antérieure. La suppression des données d'objet stockées sur les nœuds d'archivage simplifie les mises à niveau futures. Voir "Utilisation des règles ILM et des règles ILM".

- Vous ne pouvez pas créer de pool de stockage incluant à la fois des nœuds de stockage et des nœuds d'archivage. Les copies archivées nécessitent un pool de stockage incluant uniquement les noeuds d'archivage.
- Lorsque vous utilisez un pool de stockage incluant des nœuds d'archivage, vous devez également conserver au moins une copie répliquée ou codée d'effacement dans un pool de stockage incluant des nœuds de stockage.
- Si le paramètre global S3 Object Lock est activé et que vous créez une règle ILM conforme, vous ne pouvez pas utiliser de pool de stockage incluant des nœuds d'archivage. Voir les instructions de gestion

des objets avec le verrouillage d'objet S3.

- Si le type cible d'un nœud d'archivage est Cloud Tiering - simple Storage Service (S3), le nœud d'archivage doit se trouver dans son propre pool de stockage.

Activer la protection contre la perte de site

Si votre déploiement StorageGRID inclut plusieurs sites, vous pouvez utiliser la réplication et le code d'effacement avec des pools de stockage configurés de manière appropriée pour assurer la protection contre la perte de site.

Le code d'effacement et la réplication nécessitent différentes configurations de pools de stockage :

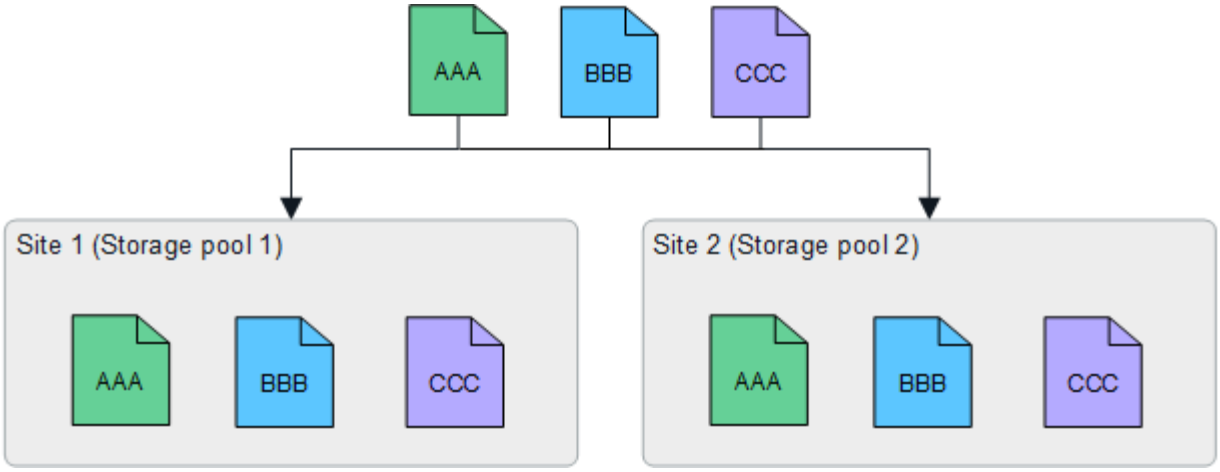
- Pour utiliser la réplication pour la protection contre les pertes sur site, utilisez les pools de stockage spécifiques au site qui sont automatiquement créés lors de l'installation de StorageGRID. Créez ensuite les règles ILM avec "instructions de positionnement" qui spécifient plusieurs pools de stockage afin qu'une copie de chaque objet soit placée sur chaque site.
- D'utiliser le code d'effacement pour la protection contre la perte d'un site, "créez des pools de stockage composés de plusieurs sites". Ensuite, créez des règles ILM qui utilisent un pool de stockage composé de plusieurs sites et n'importe quel schéma de code d'effacement disponible.

Exemple de réplication

Par défaut, un pool de stockage est créé pour chaque site lors de l'installation de StorageGRID. Avec des pools de stockage composés d'un seul site, vous pouvez configurer des règles ILM qui utilisent la réplication pour la protection contre la perte de site. Dans cet exemple :

- Le pool de stockage 1 contient le site 1
- Le pool de stockage 2 contient le site 2
- La règle ILM contient deux emplacements :
  - Stocker les objets en répliquant 1 copie sur le site 1
  - Stockez les objets en répliquant 1 copie sur le site 2

Placement des règles ILM :



Si un site est perdu, des copies des objets sont disponibles sur l'autre site.

Exemple de code d'effacement

Les pools de stockage comprenant plusieurs sites par pool de stockage vous permettent de configurer des règles ILM qui utilisent le code d'effacement pour la protection contre la perte de site. Dans cet exemple :

- Le pool de stockage 1 contient les sites 1 à 3
- La règle ILM contient un emplacement : stockage des objets par code d'effacement à l'aide d'un schéma EC 4+2 au niveau du pool de stockage 1, qui contient trois sites

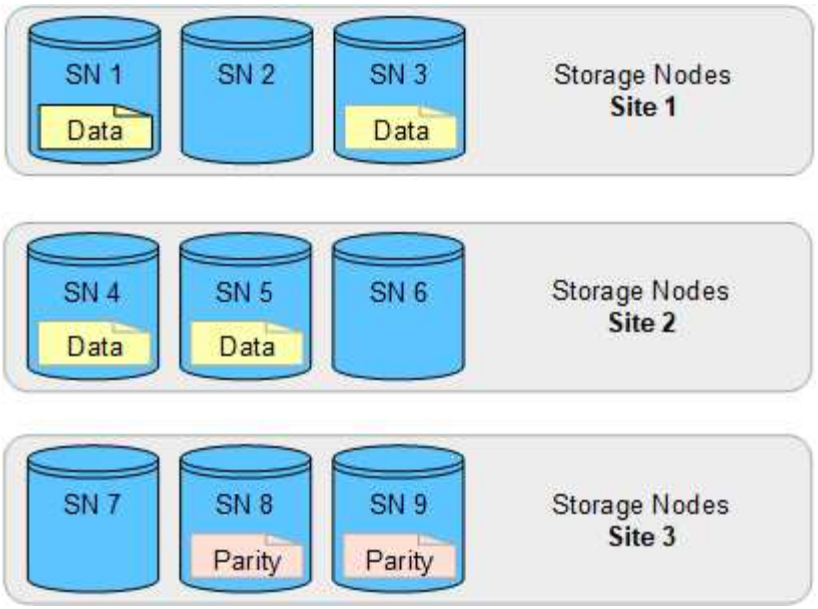
Placement des règles ILM :

Dans cet exemple :

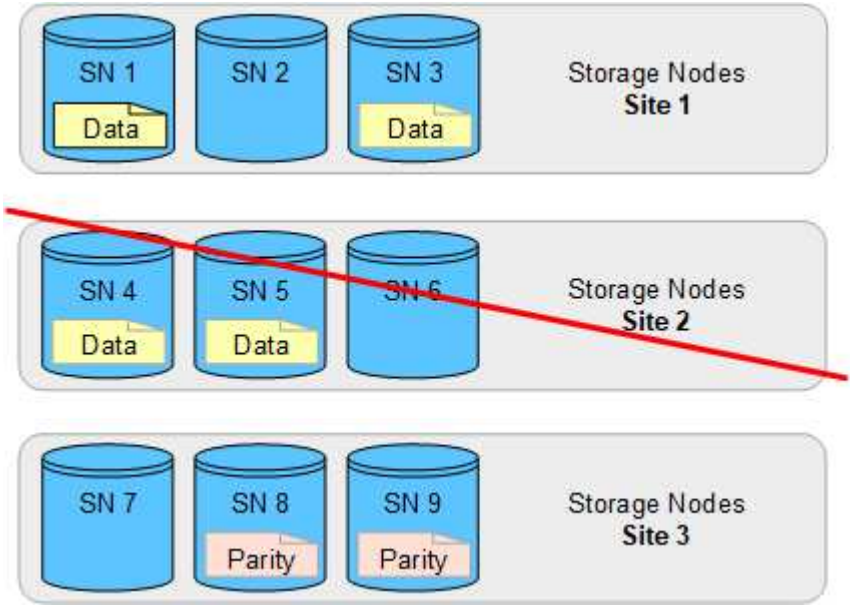
- La règle ILM utilise un schéma de code d'effacement 4+2.
- Chaque objet est tranché en quatre fragments de données égaux et deux fragments de parité sont calculés à partir des données d'objet.
- Chacun des six fragments est stocké sur un nœud différent sur trois sites du data Center pour assurer la protection des données en cas de défaillance d'un nœud ou de perte d'un site.

> Le code d'effacement est autorisé dans les pools de stockage contenant un nombre quelconque de sites *excepté* deux sites.

Règle ILM basée sur un schéma de code d'effacement 4+2 :



En cas de perte d'un site, les données peuvent toujours être restaurées :



Créer un pool de stockage

Vous créez des pools de stockage afin de déterminer où le système StorageGRID stocke les données d'objet et le type de stockage utilisé. Chaque pool de stockage comprend un ou plusieurs sites et une ou plusieurs catégories de stockage.

> Lorsque vous installez StorageGRID 11.7 sur une nouvelle grille, des pools de stockage sont automatiquement créés pour chaque site afin de réduire le nombre d'étapes requises pour créer de nouvelles règles ILM. Toutefois, lors des mises à niveau vers StorageGRID 11.7, les pools de stockage ne sont pas créés pour chaque site.

Si vous souhaitez créer des pools de stockage cloud pour stocker des données d'objet en dehors de votre système StorageGRID, reportez-vous au "Informations sur l'utilisation des pools de stockage cloud".

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous disposez d'autorisations d'accès spécifiques.
- Vous avez passé en revue les instructions relatives à la création de pools de stockage.

Description de la tâche

Les pools de stockage déterminent l'emplacement de stockage des données d'objet. Le nombre de pools de stockage dont vous avez besoin dépend du nombre de sites de votre grid et des types de copies que vous souhaitez : répliquées ou avec code d'effacement.

- Pour la réplication et le code d'effacement à un seul site, créez un pool de stockage pour chaque site. Par exemple, si vous souhaitez stocker les copies d'objets répliquées sur trois sites, créez trois pools de stockage.
- Pour le codage d'effacement sur trois sites ou plus, créez un pool de stockage comprenant une entrée pour chaque site. Par exemple, si vous souhaitez effacement d'objets de code sur trois sites, créez un pool de stockage.

> N'incluez pas le site All sites dans un pool de stockage qui sera utilisé dans un profil de code d'effacement. Ajoutez plutôt une entrée distincte au pool de stockage pour chaque site qui stocke les données codées d'effacement. Voir cette étape par exemple.

- Si vous avez plusieurs niveaux de stockage, ne créez pas de pool de stockage qui inclut différents niveaux de stockage sur un seul site. Voir la "Instructions pour la création de pools de stockage".

Étapes

1. Sélectionnez **ILM** > **pools de stockage**.

   L'onglet Storage pools répertorie tous les pools de stockage définis.

   > Pour les nouvelles installations de StorageGRID 11.6 ou version antérieure, le pool de stockage tous les nœuds est automatiquement mis à jour chaque fois que vous ajoutez de nouveaux sites de data Center. N'utilisez pas ce pool dans les règles ILM.

2. Pour créer un nouveau pool de stockage, sélectionnez **Créer**.
3. Entrez un nom unique pour le pool de stockage. Utilisez un nom facile à identifier lorsque vous configurez les profils de code d'effacement et les règles ILM.
4. Dans la liste déroulante **site**, sélectionnez un site pour ce pool de stockage.

   Lorsque vous sélectionnez un site, le nombre de nœuds de stockage et de nœuds d'archivage dans le tableau est automatiquement mis à jour.

   En général, n'utilisez pas le site tous les sites dans un pool de stockage. Les règles ILM utilisées par un pool de stockage tous les sites placent les objets sur n'importe quel site disponible, ce qui vous permet de réduire le contrôle du placement des objets. En outre, un pool de stockage tous les sites utilise immédiatement les nœuds de stockage sur un nouveau site, ce qui peut ne pas être le comportement que vous attendez.

5. Dans la liste déroulante **Storage grade**, sélectionnez le type de stockage qui sera utilisé si une règle ILM utilise ce pool de stockage.

   La qualité de stockage, inclut toutes les nuances de stockage, inclut tous les nœuds de stockage sur le site

sélectionné. Le niveau de stockage par défaut des nœuds d'archivage inclut tous les nœuds d'archivage du site sélectionné. Si vous avez créé des notes de stockage supplémentaires pour les nœuds de stockage de votre grille, elles sont répertoriées dans la liste déroulante.

6. si vous souhaitez utiliser le pool de stockage dans un profil de code d'effacement multi-site, sélectionnez **Ajouter plus de nœuds** pour ajouter une entrée pour chaque site au pool de stockage.

> Vous ne pouvez pas créer d'entrées dupliquées ou créer un pool de stockage qui inclut à la fois le niveau de stockage des nœuds d'archivage et tout niveau de stockage contenant des nœuds de stockage.
>
> Vous êtes averti si vous ajoutez plusieurs entrées avec différents niveaux de stockage pour un site.

Pour supprimer une entrée, sélectionnez l'icône de suppression ✕.

7. Lorsque vous êtes satisfait de vos sélections, sélectionnez **Enregistrer**.

Le nouveau pool de stockage est ajouté à la liste.

Afficher les détails du pool de stockage

Vous pouvez afficher les détails d'un pool de stockage pour déterminer où le pool de stockage est utilisé et pour voir quels nœuds et niveaux de stockage sont inclus.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous disposez d'autorisations d'accès spécifiques.

Étapes

1. Sélectionnez **ILM** > **pools de stockage**.

Le tableau Storage pools contient les informations suivantes pour chaque pool de stockage incluant des nœuds de stockage :

- **Nom** : nom d'affichage unique du pool de stockage.
- **Node count** : nombre de nœuds dans le pool de stockage.
- **Utilisation du stockage** : pourcentage de l'espace utilisable total utilisé pour les données d'objet sur ce nœud. Cette valeur n'inclut pas les métadonnées d'objet.
- **Capacité totale** : taille du pool de stockage, qui correspond à la quantité totale d'espace utilisable pour les données d'objet pour tous les nœuds du pool de stockage.
- **Utilisation ILM**: Comment le pool de stockage est actuellement utilisé. Un pool de stockage peut être inutilisé ou être utilisé dans une ou plusieurs règles ILM, profils de code d'effacement, ou les deux.

> Vous ne pouvez pas supprimer un pool de stockage s'il est utilisé.

2. Pour afficher des détails sur un pool de stockage spécifique, sélectionnez son nom.

La page de détails du pool de stockage s'affiche.

3. Consultez l'onglet **nœuds** pour en savoir plus sur les nœuds de stockage ou les nœuds d'archivage inclus dans le pool de stockage.

   Le tableau inclut les informations suivantes pour chaque nœud :

   - Nom du nœud
   - Nom du site
   - Qualité de stockage
   - Utilisation du stockage (%) : pourcentage de l'espace total utilisable pour les données d'objet utilisé pour le nœud de stockage. Ce champ n'est pas visible pour les pools de nœuds d'archivage.

   > La même valeur d'utilisation du stockage (%) est également affichée dans le graphique stockage utilisé - données d'objet pour chaque nœud de stockage (sélectionnez **NŒUDS** > ***nœud de stockage*** > **stockage**).

4. Sélectionnez l'onglet **ILM usage** pour déterminer si le pool de stockage est actuellement utilisé dans des règles ILM ou des profils de code d'effacement.
5. Vous pouvez également accéder à la page **ILM rules** pour en savoir plus sur les règles qui utilisent le pool de stockage et les gérer.

   Voir la "Instructions d'utilisation des règles ILM".

Modifier le pool de stockage

Vous pouvez modifier un pool de stockage pour modifier son nom ou mettre à jour des sites et des notes de stockage.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous disposez d'autorisations d'accès spécifiques.
- Vous avez passé en revue le "instructions pour la création de pools de stockage".
- Si vous prévoyez de modifier un pool de stockage utilisé par une règle de la règle ILM active, vous savez comment vos modifications affectent le placement des données d'objet.

Description de la tâche

Si vous ajoutez un nouveau site ou une nouvelle classe de stockage à un pool de stockage utilisé dans la règle ILM active, sachez que les nœuds de stockage du nouveau site ou de la nouvelle classe de stockage ne seront pas utilisés automatiquement. Pour forcer StorageGRID à utiliser un nouveau site ou une nouvelle classe de stockage, vous devez activer une nouvelle règle ILM après avoir enregistré le pool de stockage modifié.

Étapes

1. Sélectionnez **ILM** > **pools de stockage**.
2. Cochez la case du pool de stockage à modifier.

   Vous ne pouvez pas modifier le pool de stockage tous les nœuds (StorageGRID 11.6 et versions antérieures).

3. Sélectionnez **Modifier**.

4. Si nécessaire, modifiez le nom du pool de stockage.
5. Selon les besoins, sélectionnez d'autres sites et niveaux de stockage.

> Vous ne pouvez pas modifier le site ou le niveau de stockage si le pool de stockage est utilisé dans un profil de code d'effacement et si cette modification entraînerait la non-validité du schéma de code d'effacement. Par exemple, si un pool de stockage utilisé dans un profil de code d'effacement inclut actuellement une classe de stockage avec un seul site, il est impossible d'utiliser une classe de stockage avec deux sites, car la modification rendrait le schéma de code d'effacement non valide.

6. Sélectionnez **Enregistrer**.

Une fois que vous avez terminé

Si vous avez ajouté un nouveau site ou une nouvelle classe de stockage à un pool de stockage utilisé dans la règle ILM active, activez une nouvelle règle ILM pour forcer StorageGRID à utiliser le nouveau site ou la nouvelle classe de stockage. Par exemple, clonez votre règle ILM existante, puis activez le clone. Voir "Utilisation des règles ILM et des règles ILM".

Retirez un pool de stockage

Vous pouvez supprimer un pool de stockage qui n'est pas utilisé.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous avez le "autorisations d'accès requises".

Étapes

1. Sélectionnez **ILM** > **pools de stockage**.
2. Consultez la colonne utilisation d'ILM du tableau pour déterminer si vous pouvez supprimer le pool de stockage.

   Vous ne pouvez pas supprimer un pool de stockage s'il est utilisé dans une règle ILM ou dans un profil de code d'effacement. Si nécessaire, sélectionnez ***Storage pool name*** > **ILM usage** pour déterminer où le pool de stockage est utilisé.

3. Si le pool de stockage que vous souhaitez supprimer n'est pas utilisé, cochez la case.
4. Sélectionnez **Supprimer**.
5. Sélectionnez **OK**.

Utilisation des pools de stockage cloud

Qu'est-ce qu'un pool de stockage cloud ?

Un pool de stockage cloud permet d'utiliser des règles ILM pour déplacer des données d'objet en dehors de votre système StorageGRID. Par exemple, vous pouvez déplacer les objets rarement consultés vers un stockage cloud moins coûteux, comme Amazon S3 Glacier, S3 Glacier Deep Archive, Google Cloud ou le Tier d'accès Archive dans le stockage Microsoft Azure Blob. Vous pouvez également conserver une sauvegarde dans le cloud des objets StorageGRID pour améliorer la reprise d'activité.

Le pool de stockage cloud est similaire à celui d'un pool de stockage du point de vue ILM. Pour stocker des objets à l'un ou l'autre des emplacements, sélectionnez le pool lors de la création des instructions de placement pour une règle ILM. Toutefois, alors que les pools de stockage sont constitués de nœuds de stockage ou de nœuds d'archivage dans le système StorageGRID, un pool de stockage cloud est constitué d'un compartiment externe (S3) ou d'un conteneur (stockage Azure Blob Storage).

> Le déplacement d'objets d'un nœud d'archivage vers un système de stockage d'archives externe via l'API S3 est déconseillé et a été remplacé par les pools de stockage cloud ILM, qui offrent davantage de fonctionnalités. Si vous utilisez actuellement un nœud d'archivage avec l'option Cloud Tiering - simple Storage Service (S3), "Migrez vos objets vers un pool de stockage cloud" à la place.

Le tableau compare les pools de stockage aux pools de stockage cloud et montre les similarités et les différences de haut niveau.

	Pool de stockage	**Pool de stockage cloud**
Comment est-elle créée ?	Utilisation de l'option **ILM** > **Storage pools** dans Grid Manager.	Utilisation de l'option **ILM** > **Storage pools** > **Cloud Storage pools** dans Grid Manager. Vous devez configurer le compartiment ou le conteneur externe avant de pouvoir créer le pool de stockage cloud.
Combien de pools pouvez-vous créer ?	Illimitée.	Jusqu'à 10.
Où sont stockés les objets ?	Sur un ou plusieurs nœuds de stockage ou d'archivage dans StorageGRID.	Dans un compartiment Amazon S3, un conteneur de stockage Azure Blob ou Google Cloud externe au système StorageGRID. Si le pool de stockage cloud est un compartiment Amazon S3 : • Vous pouvez configurer un cycle de vie de compartiment pour la transition des objets vers un stockage à long terme à faible coût, comme Amazon S3 Glacier ou S3 Glacier Deep Archive. Le système de stockage externe doit prendre en charge la classe de stockage Glacier et l'API S3 POST-restauration objet. • Vous pouvez créer des pools de stockage cloud à utiliser avec AWS commercial Cloud Services (C2S), qui prend en charge la région secrète AWS. Si le pool de stockage cloud est un conteneur de stockage Azure Blob, StorageGRID transfère l'objet vers le Tier d'archivage. **Remarque :** en général, ne configurez pas la gestion du cycle de vie du stockage Azure Blob pour le conteneur utilisé pour un pool de stockage cloud. Les opérations DE restauration POST-objet des objets dans le pool de stockage cloud peuvent être affectées par le cycle de vie configuré.

	Pool de stockage	Pool de stockage cloud
Quels sont les contrôles du placement des objets ?	Règle ILM de la politique ILM active.	Règle ILM de la politique ILM active.
Quelle est la méthode de protection des données utilisée ?	La réplication ou le code d'effacement.	La réplication.
Combien de copies de chaque objet sont autorisées ?	Plusieurs.	Une copie dans le pool de stockage cloud et, éventuellement, une ou plusieurs copies dans StorageGRID. **Remarque :** vous ne pouvez pas stocker un objet dans plusieurs pools de stockage cloud à un moment donné.
Quels sont les avantages ?	Les objets sont rapidement accessibles à tout moment.	Stockage à moindre coût
		Remarque : les données FabricPool ne peuvent pas être hiérarchisées vers des pools de stockage cloud. Les objets avec le verrouillage d'objet S3 activé ne peuvent pas être placés dans les pools de stockage cloud.

Cycle de vie d'un objet de pool de stockage cloud

Avant d'implémenter les pools de stockage cloud, vérifiez le cycle de vie des objets stockés dans chaque type de pool de stockage cloud.

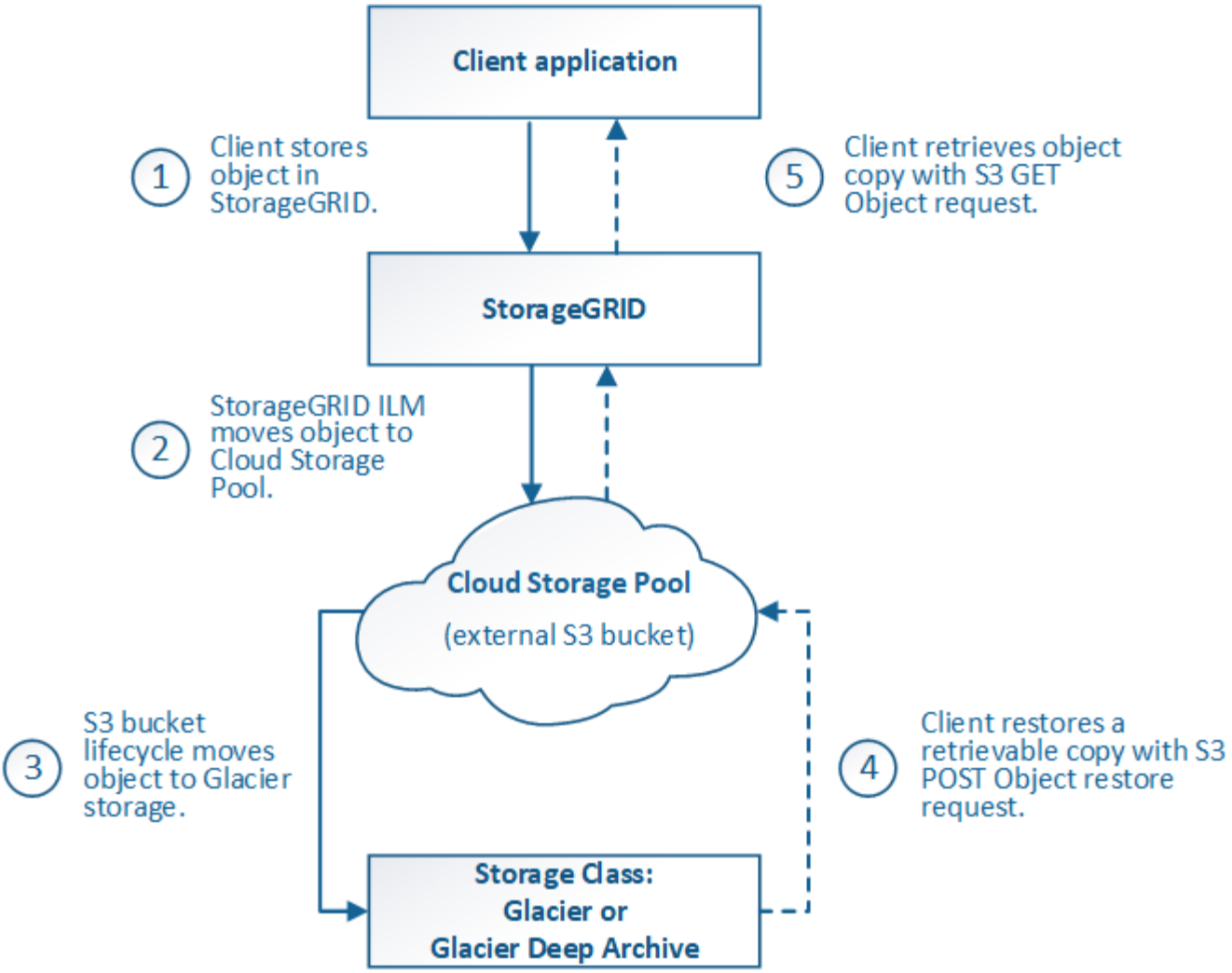
- S3 : cycle de vie d'un objet de pool de stockage cloud
- Azure : cycle de vie d'un objet de pool de stockage cloud

S3 : cycle de vie d'un objet de pool de stockage cloud

La figure représente les étapes du cycle de vie d'un objet stocké dans un pool de stockage cloud S3.

> Dans la figure et les explications, « Glacier » désigne à la fois la classe de stockage Glacier et la classe de stockage Glacier Deep Archive, à une exception près : la classe de stockage Glacier Deep Archive ne prend pas en charge le niveau de restauration accéléré. Seule la récupération en bloc ou standard est prise en charge.

> Google Cloud Platform (GCP) prend en charge la récupération d'objets à partir d'un stockage à long terme sans nécessiter de POST-restauration.



1. **Objet stocké dans StorageGRID**

   Pour démarrer le cycle de vie, une application client stocke un objet dans StorageGRID.

2. **Objet déplacé vers le pool de stockage cloud S3**
   - Lorsque l'objet est associé à une règle ILM utilisant un pool de stockage cloud S3 en tant qu'emplacement, StorageGRID déplace l'objet vers le compartiment S3 externe spécifié par le pool de stockage cloud.
   - Lorsque l'objet a été déplacé vers le pool de stockage cloud S3, l'application client peut la récupérer à l'aide d'une requête d'objet GET S3 de StorageGRID, à moins que l'objet n'ait été transféré vers le stockage Glacier.
3. **L'objet a été transféré vers Glacier (état non récupérable)**
   - L'objet peut également être transféré vers le stockage Glacier. Par exemple, un compartiment S3 externe peut utiliser la configuration du cycle de vie pour transférer un objet vers le stockage Glacier immédiatement ou après quelques jours.

> Si vous souhaitez effectuer la transition des objets, vous devez créer une configuration de cycle de vie pour le compartiment S3 externe. Pour ce faire, vous devez utiliser une solution de stockage implémentant la classe de stockage Glacier et prendre en charge l'API S3 POST-restauration objet.

> N’utilisez pas les pools de stockage cloud pour les objets qui ont été ingérés par les clients Swift. Swift ne prend pas en charge les demandes DE restauration POST-objet. StorageGRID ne pourra donc pas récupérer d’objets Swift ayant été transférés vers le stockage Glacier S3. L’émission d’une demande d’objet GET Swift pour récupérer ces objets échouera (403 interdit).

- Lors de la transition, l’application client peut utiliser une requête objet TÊTE S3 pour contrôler l’état de l’objet.

4. **Objet restauré à partir du stockage Glacier**

   Lorsqu’un objet est transféré vers le stockage Glacier, l’application client peut émettre une demande de restauration APRÈS objet S3 pour restaurer une copie récupérable dans le pool de stockage cloud S3. La demande spécifie le nombre de jours pendant lesquels la copie doit être disponible dans le pool de stockage cloud et le Tier d’accès aux données à utiliser pour l’opération de restauration (accéléré, Standard ou en bloc). Lorsque la date d’expiration de la copie récupérable est atteinte, la copie est automatiquement renvoyée à un état non récupérable.

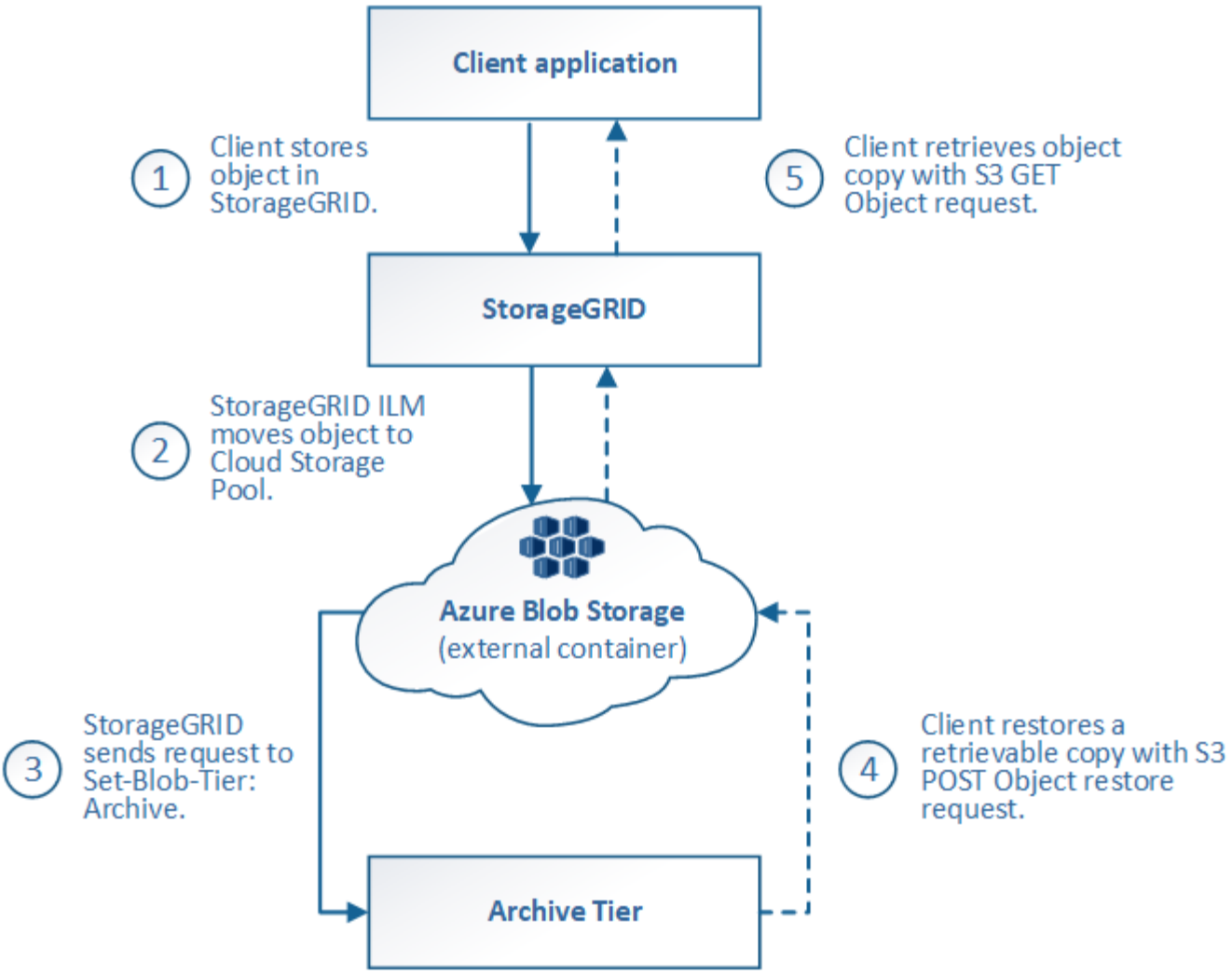
   > Si une ou plusieurs copies de l’objet existent également sur les nœuds de stockage dans StorageGRID, il n’est pas nécessaire de restaurer l’objet à partir de Glacier à l’aide d’une demande DE restauration POST-objet. En revanche, la copie locale peut être récupérée directement à l’aide d’une demande D’OBJET GET.

5. **Objet récupéré**

   Une fois qu’un objet a été restauré, l’application client peut émettre une requête GET Object pour récupérer l’objet restauré.

Azure : cycle de vie d’un objet de pool de stockage cloud

La figure représente les étapes du cycle de vie d’un objet stocké dans un pool de stockage cloud Azure.



1. **Objet stocké dans StorageGRID**

   Pour démarrer le cycle de vie, une application client stocke un objet dans StorageGRID.

2. **Objet déplacé vers Azure Cloud Storage Pool**

   Lorsque l'objet est associé à une règle ILM utilisant un pool de stockage cloud Azure comme emplacement, StorageGRID déplace l'objet vers le conteneur de stockage Azure Blob externe spécifié par le pool de stockage cloud

   > N'utilisez pas les pools de stockage cloud pour les objets qui ont été ingérés par les clients Swift. Swift ne prend pas en charge les demandes DE restauration POST-objet. StorageGRID ne pourra donc pas récupérer d'objets Swift ayant été transférés vers le niveau d'archivage du stockage Azure Blob Storage. L'émission d'une demande d'objet GET Swift pour récupérer ces objets échouera (403 interdit).

3. **L'objet a été transféré au niveau Archive (état non récupérable)**

   Immédiatement après le déplacement de l'objet vers le pool de stockage cloud Azure, StorageGRID transfère automatiquement l'objet vers le Tier d'archivage du stockage Azure Blob.

4. **Objet restauré à partir du niveau d'archive**

Si un objet a été migré vers le Tier d'archivage, l'application client peut lancer une demande de restauration S3 POST-objet pour restaurer une copie récupérable dans le pool de stockage cloud Azure.

Lorsqu'StorageGRID reçoit le POST-restauration d'objet, il transfère temporairement l'objet vers le Tier Azure Blob Storage Cool. Dès que la date d'expiration de la requête DE restauration POST-objet est atteinte, StorageGRID retransfère l'objet vers le niveau d'archivage.

> Si une ou plusieurs copies de l'objet existent également sur les nœuds de stockage dans StorageGRID, il n'est pas nécessaire de restaurer l'objet à partir du Tier d'accès Archive en émettant une demande de restauration POST-objet. En revanche, la copie locale peut être récupérée directement à l'aide d'une demande D'OBJET GET.

5. **Objet récupéré**

   Une fois qu'un objet a été restauré dans Azure Cloud Storage Pool, l'application client peut émettre une requête GET Object pour récupérer l'objet restauré.

Informations associées

"UTILISEZ L'API REST S3"

Quand utiliser les pools de stockage cloud

À l'aide des pools de stockage cloud, vous pouvez sauvegarder ou hiérarchiser les données vers un emplacement externe. En outre, vous pouvez sauvegarder ou déplacer des données vers plusieurs clouds.

Sauvegardez les données StorageGRID dans un emplacement externe

Vous pouvez utiliser un pool de stockage cloud pour sauvegarder des objets StorageGRID dans un emplacement externe.

Si les copies dans StorageGRID sont inaccessibles, vous pouvez utiliser les données objet du pool de stockage cloud pour transmettre les requêtes des clients. Cependant, vous devrez peut-être émettre une demande de restauration S3 POST-objet pour accéder à la copie d'objet de sauvegarde dans le pool de stockage cloud.

Les données d'objet d'un pool de stockage cloud peuvent également être utilisées pour restaurer des données perdues à partir de StorageGRID en raison d'un volume de stockage ou d'une défaillance du nœud de stockage. Si la seule copie restante d'un objet se trouve dans un pool de stockage cloud, StorageGRID restaure temporairement l'objet et crée une nouvelle copie sur le nœud de stockage restauré.

Pour implémenter une solution de sauvegarde :

1. Créez un pool de stockage cloud unique.
2. Configurez une règle ILM pour stocker simultanément les copies d'objets sur les nœuds de stockage (en tant que copies répliquées ou avec code d'effacement) et une seule copie objet dans le pool de stockage cloud.
3. Ajoutez la règle à votre règle ILM. Ensuite, simuler et activer la règle.

Déplacez les données de StorageGRID vers un emplacement externe

Vous pouvez utiliser un pool de stockage cloud pour stocker des objets en dehors du système StorageGRID.

Supposons par exemple que vous disposez d'un grand nombre d'objets que vous devez conserver, mais que vous prévoyez d'accéder rarement à ces objets. Un pool de stockage cloud permet de classer les objets en fonction de leur coût de stockage et de libérer de l'espace dans StorageGRID.

Pour implémenter une solution de hiérarchisation :

1. Créez un pool de stockage cloud unique.
2. Configurez une règle ILM pour déplacer les objets rarement utilisés depuis les nœuds de stockage vers le pool de stockage cloud.
3. Ajoutez la règle à votre règle ILM. Ensuite, simuler et activer la règle.

Possibilité de gérer plusieurs terminaux cloud

Vous pouvez configurer plusieurs terminaux de pool de stockage cloud si vous souhaitez effectuer le Tiering ou la sauvegarde des données d'objet vers plusieurs clouds. Les filtres de vos règles ILM permettent de spécifier les objets qui sont stockés dans chaque pool de stockage cloud. Par exemple, vous pouvez stocker des objets de certains locataires ou compartiments dans Amazon S3 Glacier et des objets d'autres locataires ou compartiments dans le stockage Azure Blob. Vous pouvez également déplacer des données entre Amazon S3 Glacier et le stockage Azure Blob.

> Lors de l'utilisation de plusieurs terminaux Cloud Storage Pool, n'oubliez pas qu'un objet ne peut être stocké que dans un seul pool de stockage cloud à la fois.

Pour implémenter plusieurs terminaux cloud :

1. Créez jusqu'à 10 pools de stockage cloud.
2. Configurez les règles ILM pour stocker les données d'objet appropriées au moment opportun dans chaque pool de stockage cloud. Stockez par exemple des objets à partir du compartiment A dans le pool de stockage cloud A et stockez des objets à partir du compartiment B dans le pool de stockage cloud B. Stockez les objets dans Cloud Storage Pool A pendant un certain temps, puis déplacez-les vers Cloud Storage Pool B.
3. Ajoutez les règles à votre politique ILM. Ensuite, simuler et activer la règle.

Considérations relatives aux pools de stockage cloud

Si vous envisagez d'utiliser un pool de stockage cloud pour déplacer les objets hors du système StorageGRID, vous devez étudier les critères de configuration et d'utilisation des pools de stockage cloud.

Considérations générales

- En général, le stockage d'archivage dans le cloud, comme Amazon S3 Glacier ou Azure Blob Storage, est un emplacement économique pour stocker les données d'objet. Mais le coût de la récupération des données à partir du stockage d'archivage dans le cloud est relativement élevé. Pour atteindre le coût global le plus bas, vous devez savoir quand et à quelle fréquence vous accéderez aux objets dans Cloud Storage Pool. L'utilisation d'un pool de stockage cloud est recommandée uniquement pour le contenu dont vous souhaitez accéder rarement.
- N'utilisez pas les pools de stockage cloud pour les objets qui ont été ingérés par les clients Swift. Swift ne prend pas en charge les demandes DE restauration POST-objet. StorageGRID ne pourra donc pas récupérer d'objets Swift ayant été transférés vers le stockage Glacier S3 ou le Tier d'archivage du stockage Azure Blob Storage. L'émission d'une demande d'objet GET Swift pour récupérer ces objets

échouera (403 interdit).

- L'utilisation de pools de stockage cloud avec FabricPool n'est pas prise en charge en raison de la latence ajoutée pour extraire un objet de la cible du pool de stockage cloud.
- Les objets avec le verrouillage d'objet S3 activé ne peuvent pas être placés dans les pools de stockage cloud.
- Si S3 Object Lock est activé pour le compartiment S3 de destination d'un pool de stockage cloud, la tentative de configuration de la réplication de compartiment (PutBucketReplication) échoue avec une erreur AccessDenied.

Considérations relatives aux ports utilisés pour les pools de stockage cloud

Pour s'assurer que les règles ILM peuvent déplacer des objets vers et depuis le pool de stockage cloud spécifié, vous devez configurer le ou les réseaux contenant les nœuds de stockage du système. Vous devez vous assurer que les ports suivants peuvent communiquer avec le pool de stockage cloud.

Par défaut, les pools de stockage cloud utilisent les ports suivants :

- **80**: Pour les URI de point final commençant par http
- **443**: Pour les URI de point final qui commencent par https

Vous pouvez spécifier un autre port lorsque vous créez ou modifiez un pool de stockage cloud.

Si vous utilisez un serveur proxy non transparent, vous devez également "Configurez un proxy de stockage" pour permettre l'envoi de messages vers des points de terminaison externes, tels qu'un point de terminaison sur internet.

Considérations relatives aux coûts

L'accès au stockage dans le cloud à l'aide d'un pool de stockage cloud requiert une connectivité réseau au cloud. Tenez compte des coûts de l'infrastructure réseau que vous utiliserez pour accéder au cloud et le provisionner de façon appropriée, en fonction de la quantité de données que vous prévoyez de déplacer entre StorageGRID et le cloud à l'aide du pool de stockage cloud.

Lorsque StorageGRID se connecte au terminal Cloud Storage Pool externe, plusieurs demandes de contrôle de la connectivité sont émises et les opérations nécessaires sont possibles. Un certain nombre de coûts supplémentaires seront associés à ces demandes, mais le coût de la surveillance d'un pool de stockage cloud ne doit être qu'une fraction du coût global du stockage d'objets dans S3 ou Azure.

Des coûts plus importants peuvent être encourus si vous devez déplacer des objets depuis un terminal externe de pool de stockage dans le cloud vers StorageGRID. Les objets peuvent être redéplacés vers StorageGRID dans l'un ou l'autre de ces cas :

- La seule copie de l'objet se trouve dans un pool de stockage cloud et vous décidez de le stocker dans StorageGRID à la place. Dans ce cas, vous reconfigurez vos règles et votre règle ILM. Lors de l'évaluation ILM, StorageGRID émet plusieurs demandes de récupération de l'objet à partir du pool de stockage cloud. StorageGRID crée ensuite le nombre spécifié de copies répliquées ou codées en local. Une fois que l'objet est de nouveau déplacé vers StorageGRID, la copie dans le pool de stockage cloud est supprimée.
- Les objets sont perdus en raison de la défaillance du nœud de stockage. Si la seule copie restante d'un objet se trouve dans un pool de stockage cloud, StorageGRID restaure temporairement l'objet et crée une nouvelle copie sur le nœud de stockage restauré.

Lorsque les objets sont déplacés vers StorageGRID à partir d'un pool de stockage cloud, StorageGRID émet plusieurs requêtes vers le terminal de pool de stockage cloud pour chaque objet. Avant de déplacer un grand nombre d'objets, contactez le support technique pour obtenir de l'aide pour estimer le délai et les coûts associés.

S3 : autorisations requises pour le compartiment de pool de stockage cloud

La politique de compartiment pour le compartiment S3 externe utilisé pour un pool de stockage cloud doit autoriser StorageGRID à déplacer un objet vers le compartiment, à obtenir l'état d'un objet et à restaurer un objet à partir du stockage Glacier, le cas échéant, et bien plus encore. Dans l'idéal, StorageGRID doit disposer d'un accès total au compartiment (`s3:*`) ; Cependant, si ce n'est pas possible, la politique de compartiment doit accorder les autorisations S3 suivantes à StorageGRID :

- `s3:AbortMultipartUpload`
- `s3:DeleteObject`
- `s3:GetObject`
- `s3:ListBucket`
- `s3:ListBucketMultipartUploads`
- `s3:ListMultipartUploadParts`
- `s3:PutObject`
- `s3:RestoreObject`

S3 : considérations sur le cycle de vie du compartiment externe

Le déplacement des objets entre le StorageGRID et le compartiment S3 externe spécifié dans le pool de stockage cloud est contrôlé par les règles ILM et la politique ILM active dans StorageGRID. À l'inverse, la transition des objets à partir du compartiment S3 externe spécifié dans le pool de stockage cloud vers Amazon S3 Glacier ou S3 Glacier Deep Archive (ou vers une solution de stockage implémentant la classe de stockage Glacier) est contrôlée par la configuration du cycle de vie de ce compartiment.

Si vous souhaitez migrer des objets depuis le pool de stockage cloud, vous devez créer la configuration de cycle de vie appropriée sur un compartiment S3 externe. Vous devez d'autre part utiliser une solution de stockage implémentant la classe de stockage Glacier et prendre en charge l'API DE restauration POST-objet S3.

Supposons par exemple que vous souhaitiez que tous les objets déplacés d'StorageGRID vers le pool de stockage cloud soient transférés immédiatement vers le stockage Amazon S3 Glacier. Vous devez créer une configuration de cycle de vie sur le compartiment S3 externe qui spécifie une seule action (**transition**) comme suit :

```
<LifecycleConfiguration>
  <Rule>
    <ID>Transition Rule</ID>
    <Filter>
       <Prefix></Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <Days>0</Days>
      <StorageClass>GLACIER</StorageClass>
    </Transition>
  </Rule>
</LifecycleConfiguration>
```

Cette règle consiste à basculer tous les objets de compartiment vers Amazon S3 Glacier le jour de leur création (à savoir le jour où ils ont été déplacés d'StorageGRID vers le pool de stockage cloud).

> Lors de la configuration du cycle de vie du compartiment externe, n'utilisez jamais les actions **expiration** pour définir quand les objets arrivent à expiration. Les actions d'expiration entraînent la suppression des objets expirés par le système de stockage externe. Si vous tentez par la suite d'accéder à un objet expiré à partir de StorageGRID, l'objet supprimé est introuvable.

Pour migrer les objets du pool de stockage cloud vers l'archivage profond S3 Glacier (au lieu d'Amazon S3 Glacier), spécifiez `<StorageClass>DEEP_ARCHIVE</StorageClass>` pendant le cycle de vie du compartiment. Cependant, sachez que vous ne pouvez pas utiliser le `Expedited` tiering pour restaurer des objets à partir d'une archive complète S3 Glacier.

Azure : considérations relatives au niveau d'accès

Lorsque vous configurez un compte de stockage Azure, vous pouvez définir le niveau d'accès par défaut sur chaud ou froid. Lorsque vous créez un compte de stockage à utiliser avec un pool de stockage cloud, vous devez utiliser le Tier actif comme niveau par défaut. Même si StorageGRID définit immédiatement le Tier sur Archive lors du déplacement d'objets vers le pool de stockage cloud, l'utilisation du paramètre par défaut de Hot garantit que vous ne serez pas facturé de frais de suppression anticipé pour les objets supprimés du Tier Cool avant le minimum de 30 jours.

Azure : gestion du cycle de vie non prise en charge

N'utilisez pas la gestion du cycle de vie du stockage Azure Blob pour le conteneur utilisé avec un pool de stockage cloud. Toute interférence entre les opérations du cycle de vie du système Cloud Storage Pool.

Informations associées

- "Création d'un pool de stockage cloud"

Comparaison des pools de stockage cloud et de la réplication CloudMirror

Lorsque vous commencez à utiliser les pools de stockage cloud, il peut être utile d'étudier les similarités et les différences entre les pools de stockage cloud et le service de réplication StorageGRID CloudMirror.

	Pool de stockage cloud	Service de réplication CloudMirror
Quel est l'objectif principal ?	Sert de cible d'archivage. La copie d'objet du pool de stockage cloud peut être la seule copie de l'objet ou une copie supplémentaire. Ainsi, au lieu de conserver deux copies sur site, vous pouvez conserver une copie dans StorageGRID et en envoyer une autre dans le pool de stockage cloud.	Permet à un locataire de répliquer automatiquement les objets à partir d'un compartiment dans StorageGRID (source) vers un compartiment S3 externe (destination). Crée une copie indépendante d'un objet dans une infrastructure S3 indépendante.
Comment est-il configuré ?	Défini de la même manière que les pools de stockage, à l'aide du gestionnaire de grille ou de l'API de gestion de grille. Peut être sélectionné comme emplacement dans une règle ILM. Lorsqu'un pool de stockage est constitué d'un groupe de nœuds de stockage, un pool de stockage cloud est défini à l'aide d'un terminal S3 ou Azure distant (adresse IP, identifiants, etc.).	Un utilisateur locataire "Configure la réplication CloudMirror" En définissant un terminal CloudMirror (adresse IP, identifiants, etc.) à l'aide du Gestionnaire des locataires ou de l'API S3. Une fois le terminal CloudMirror configuré, tous les compartiments appartenant à ce compte peuvent être configurés pour pointer vers le terminal CloudMirror.
Qui est responsable de sa configuration ?	En général, un administrateur grid	Généralement, un utilisateur locataire
Quelle est la destination ?	• Toute infrastructure S3 compatible (y compris Amazon S3) • Tier Azure Blob Archive • Google Cloud Platform (GCP)	• Toute infrastructure S3 compatible (y compris Amazon S3) • Google Cloud Platform (GCP)
Pourquoi déplacer des objets vers la destination ?	Une ou plusieurs règles ILM de la politique ILM active. Les règles ILM définissent le déplacement des objets StorageGRID vers le pool de stockage cloud et le déplacement des objets.	Acte d'ingestion d'un nouvel objet dans un compartiment source configuré avec un terminal CloudMirror. Les objets qui existaient dans le compartiment source avant la configuration du compartiment avec le point de terminaison CloudMirror ne sont pas répliqués, sauf s'ils ont été modifiés.

	Pool de stockage cloud	Service de réplication CloudMirror
Comment les objets sont-ils récupérés ?	Les applications doivent demander à StorageGRID de récupérer les objets qui ont été déplacés vers un pool de stockage cloud. Si la seule copie d'un objet a été transférée vers le stockage d'archivage, StorageGRID gère le processus de restauration de l'objet afin de pouvoir la récupérer.	Étant donné que la copie en miroir dans le compartiment de destination est une copie indépendante, les applications peuvent récupérer l'objet en effectuant des demandes vers StorageGRID ou vers la destination S3. Supposons, par exemple, que vous utilisiez la réplication CloudMirror pour mettre en miroir les objets dans une organisation partenaire. Le partenaire peut utiliser ses propres applications pour lire ou mettre à jour les objets directement à partir de la destination S3. Utiliser StorageGRID n'est pas nécessaire.
Pouvez-vous lire directement depuis la destination ?	Non Les objets déplacés vers un pool de stockage cloud sont gérés par StorageGRID. Les demandes de lecture doivent être dirigées vers StorageGRID (et StorageGRID sera responsable de la récupération à partir du pool de stockage cloud).	Oui, car la copie en miroir est une copie indépendante.
Que se passe-t-il si un objet est supprimé de la source ?	L'objet est également supprimé du pool de stockage cloud.	L'action de suppression n'est pas répliquée. Un objet supprimé n'existe plus dans le compartiment StorageGRID, mais il continue d'exister dans le compartiment de destination. De même, les objets du compartiment de destination peuvent être supprimés sans affecter la source.
Comment accéder aux objets après un incident (le système StorageGRID n'est pas opérationnel) ?	Les nœuds StorageGRID défaillants doivent être récupérés. Au cours de ce processus, les copies des objets répliqués peuvent être restaurées à l'aide de copies dans le pool de stockage cloud.	Les copies d'objets de la destination CloudMirror sont indépendantes de StorageGRID, ce qui permet d'y accéder directement avant la restauration des nœuds StorageGRID.

Création d'un pool de stockage cloud

Un pool de stockage cloud désigne un seul compartiment Amazon S3 externe, un autre fournisseur compatible avec S3 ou un conteneur de stockage Azure Blob.

Lorsque vous créez un pool de stockage cloud, vous spécifiez le nom et l'emplacement du compartiment ou conteneur externe que StorageGRID utilisera pour stocker les objets, le type de fournisseur cloud (Amazon S3/GCP ou Azure Blob Storage), ainsi que les informations dont StorageGRID a besoin pour accéder au compartiment ou conteneur externe.

StorageGRID valide le pool de stockage cloud dès que vous le sauvegardez. Vous devez donc vous assurer

que le compartiment ou le conteneur spécifié dans le pool de stockage cloud est accessible et qu'il existe.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous avez le "autorisations d'accès requises".
- Vous avez passé en revue le "Considérations relatives aux pools de stockage cloud".
- Le compartiment ou conteneur externe référencé par le pool de stockage cloud existe déjà, et vous connaissez son nom et son emplacement.
- Pour accéder au compartiment ou au conteneur, vous disposez des informations suivantes pour le type d'authentification que vous choisirez :

Clé d'accès S3

Pour le compartiment S3 externe

- ID de clé d'accès du compte propriétaire du compartiment externe.
- La clé d'accès secrète associée.

Vous pouvez également spécifier Anonyme pour le type d'authentification.

Portail d'accès C2S

Pour le service S3 de services cloud commerciaux (C2S)

Vous avez les éléments suivants :

- URL complète utilisée par StorageGRID pour obtenir des informations d'identification temporaires à partir du serveur du portail d'accès C2S (CAP), y compris tous les paramètres d'API requis et facultatifs attribués à votre compte C2S.
- Certificat d'autorité de certification du serveur émis par une autorité de certification du gouvernement (AC) appropriée. StorageGRID utilise ce certificat pour vérifier l'identité du serveur CAP. Le certificat d'autorité de certification du serveur doit utiliser le codage PEM.
- Certificat du client émis par une autorité de certification du gouvernement (AC) appropriée. StorageGRID utilise ce certificat pour s'identifier lui-même au serveur CAP. Le certificat client doit utiliser le codage PEM et avoir reçu l'accès à votre compte C2S.
- Clé privée codée PEM pour le certificat client.
- Phrase de passe pour le décryptage de la clé privée pour le certificat client, si elle est chiffrée.

> Si le certificat client est crypté, utilisez le format traditionnel pour le chiffrement. Le format chiffré PKCS #8 n'est pas pris en charge.

Stockage Azure Blob

Pour le conteneur externe

- URI (Uniform Resource identifier) utilisé pour accéder au conteneur de stockage Blob.
- Nom du compte de stockage et clé de compte. Utilisez le portail Azure pour trouver ces valeurs.

Étapes

1. Sélectionnez **ILM** > **Storage pools** > **Cloud Storage pools**.
2. Sélectionnez **Créer**, puis entrez les informations suivantes :

Champ	Description
Nom du pool de stockage cloud	Un nom qui décrit brièvement le pool de stockage cloud et son objectif. Nom facile à identifier lors de la configuration des règles ILM.
Type de fournisseur	Quel fournisseur de cloud utiliser pour ce pool de stockage cloud : • **Amazon S3/GCP** : sélectionnez cette option pour Amazon S3, commercial Cloud Services (C2S) S3, Google Cloud Platform (GCP) ou un autre fournisseur compatible avec S3. • **Stockage Azure Blob**
Seau ou conteneur	Nom du compartiment S3 ou du conteneur Azure externe. Vous ne pouvez pas modifier cette valeur une fois le pool de stockage cloud enregistré.

3. En fonction de votre sélection de type de fournisseur, entrez les informations de point de terminaison de service.

Amazon S3/GCP

a. Pour le protocole, sélectionnez HTTPS ou HTTP.

> N'utilisez pas de connexions HTTP pour les données sensibles.

b. Entrez le nom d'hôte. Exemple :

`s3-aws-region.amazonaws.com`

c. Sélectionnez le style d'URL :

Option	Description
Détection automatique	Essayez de détecter automatiquement le style d'URL à utiliser, en fonction des informations fournies. Par exemple, si vous spécifiez une adresse IP, StorageGRID utilise une URL de style de chemin d'accès. Sélectionnez cette option uniquement si vous ne savez pas quel style spécifique utiliser.
De type hébergement virtuel	Utilisez une URL de type hébergement virtuel pour accéder au compartiment. Les URL de type hébergement virtuel incluent le nom de compartiment dans le nom de domaine. Exemple : `https://bucket-name.s3.company.com/key-name`
Style de trajectoire	Utilisez une URL de style de chemin d'accès pour accéder au compartiment. Les URL de type chemin d'accès incluent le nom du compartiment à la fin Exemple : `https://s3.company.com/bucket-name/key-name` **Note:** l'option URL de style chemin d'accès n'est pas recommandée et sera obsolète dans une future version de StorageGRID.

d. Vous pouvez également saisir le numéro de port ou utiliser le port par défaut : 443 pour HTTPS ou 80 pour HTTP.

Stockage Azure Blob Storage

a. À l'aide de l'un des formats suivants, entrez l'URI du point de terminaison de service.

- `https://host:port`
- `http://host:port`

Exemple : `https://myaccount.blob.core.windows.net:443`

Si vous ne spécifiez pas de port, le port 443 est utilisé par défaut pour HTTPS et le port 80 pour HTTP.

4. Sélectionnez **Continuer**. Sélectionnez ensuite le type d'authentification et entrez les informations requises pour le terminal Cloud Storage Pool :

Touche d'accès

Pour le type de fournisseur Amazon S3/GCP uniquement

a. Pour **ID de clé d'accès**, entrez l'ID de clé d'accès du compte propriétaire du compartiment externe.

b. Pour **clé d'accès secrète**, entrez la clé d'accès secrète.

CAP (portail d'accès C2S)

Pour le service S3 de services cloud commerciaux (C2S)

a. Pour **URL d'informations d'identification temporaires**, entrez l'URL complète que StorageGRID utilisera pour obtenir des informations d'identification temporaires du serveur CAP, y compris tous les paramètres d'API requis et facultatifs attribués à votre compte C2S.

b. Pour **Server CA Certificate**, sélectionnez **Browse** et téléchargez le certificat d'autorité de certification codé PEM que StorageGRID utilisera pour vérifier le serveur CAP.

c. Pour **client Certificate**, sélectionnez **Parcourir** et téléchargez le certificat codé PEM que StorageGRID utilisera pour s'identifier sur le serveur CAP.

d. Pour **clé privée client**, sélectionnez **Parcourir** et téléchargez la clé privée codée PEM pour le certificat client.

e. Si la clé privée du client est cryptée, entrez la phrase de passe pour déchiffrer la clé privée du client. Sinon, laissez le champ **phrase de passe de clé privée client** vide.

Stockage Azure Blob Storage

a. Pour **Nom du compte**, entrez le nom du compte de stockage Blob qui possède le conteneur de services externes.

b. Pour **clé de compte**, entrez la clé secrète du compte de stockage Blob.

Anonyme

Aucune information supplémentaire n'est requise.

5. Sélectionnez **Continuer**. Choisissez ensuite le type de vérification du serveur que vous souhaitez utiliser :

Option	Description
Utilisez les certificats d'autorité de certification racine dans le système d'exploitation du nœud de stockage	Utilisez les certificats CA de la grille installés sur le système d'exploitation pour sécuriser les connexions.
Utiliser un certificat d'autorité de certification personnalisé	Utilisez un certificat d'autorité de certification personnalisé. Sélectionnez **Parcourir** et téléchargez le certificat codé PEM.
Ne vérifiez pas le certificat	Le certificat utilisé pour la connexion TLS n'est pas vérifié.

6. Sélectionnez **Enregistrer**.

Lorsque vous enregistrez un pool de stockage cloud, StorageGRID effectue les opérations suivantes :

- Vérifie que le compartiment ou le conteneur et le terminal de service existent et qu'ils peuvent être atteints à l'aide des informations d'identification que vous avez spécifiées.
- Écrit un fichier de marqueur dans le compartiment ou le conteneur pour l'identifier en tant que pool de stockage cloud. Ne supprimez jamais ce fichier nommé `x-ntap-sgws-cloud-pool-uuid`.

  Si la validation du pool de stockage cloud échoue, un message d'erreur s'affiche indiquant pourquoi la validation a échoué. Par exemple, une erreur peut être signalée en cas d'erreur de certificat ou si le compartiment ou le conteneur que vous avez spécifié n'existe pas déjà.

7. Si une erreur se produit, consultez le "Instructions de dépannage des pools de stockage cloud", Résolvez les problèmes, puis essayez à nouveau d'enregistrer le pool de stockage cloud.

Modifiez un pool de stockage cloud

Vous pouvez modifier un pool de stockage cloud pour modifier son nom, le point de terminaison de service ou d'autres informations. Cependant, vous ne pouvez pas modifier le compartiment S3 ou le conteneur Azure pour un pool de stockage cloud.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous disposez d'autorisations d'accès spécifiques.
- Vous avez passé en revue le "Considérations relatives aux pools de stockage cloud".

Étapes

1. Sélectionnez **ILM** > **Storage pools** > **Cloud Storage pools**.

   Le tableau Cloud Storage pools répertorie les pools de stockage cloud existants.

2. Cochez la case correspondant au pool de stockage cloud à modifier.
3. Sélectionnez **actions** > **Modifier**.
4. Si nécessaire, modifiez le nom d'affichage, le point de terminaison de service, les informations d'identification d'authentification ou la méthode de validation de certificat.

   > Vous ne pouvez pas modifier le type de fournisseur, le compartiment S3 ou le conteneur Azure pour un pool de stockage cloud.

   Si vous avez déjà téléchargé un certificat de serveur ou de client, vous pouvez sélectionner **Détails du certificat** pour vérifier le certificat en cours d'utilisation.

5. Sélectionnez **Enregistrer**.

   Lorsque vous enregistrez un pool de stockage cloud, StorageGRID valide la présence du compartiment ou du conteneur et du terminal de service, et qu'ils peuvent être atteints à l'aide des identifiants que vous avez spécifiés.

   Si la validation du pool de stockage cloud échoue, un message d'erreur s'affiche. Par exemple, une erreur peut être signalée en cas d'erreur de certificat.

   Reportez-vous aux instructions pour "Résolution des problèmes avec les pools de stockage cloud", Résolvez le problème, puis réessayez d'enregistrer le pool de stockage cloud.

Supprimez un pool de stockage cloud

Vous pouvez supprimer un pool de stockage cloud s'il n'est pas utilisé dans une règle ILM et s'il ne contient pas de données d'objet.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous avez le "autorisations d'accès requises".

Si nécessaire, utilisez la règles ILM pour déplacer les données d'objet

Si le pool de stockage cloud que vous souhaitez supprimer contient des données d'objet, vous devez utiliser ILM pour déplacer les données vers un autre emplacement. Par exemple, vous pouvez déplacer les données vers des nœuds de stockage sur votre grille ou vers un autre pool de stockage cloud.

Étapes

1. Sélectionnez **ILM** > **Storage pools** > **Cloud Storage pools**.
2. Consultez la colonne utilisation ILM du tableau pour déterminer si vous pouvez supprimer le pool de stockage cloud.

   Vous ne pouvez pas supprimer un pool de stockage cloud s'il est utilisé dans une règle ILM ou dans un profil de code d'effacement.

3. Si le pool de stockage cloud est utilisé, sélectionnez ***cloud Storage pool name*** > **ILM usage**.
4. "Clonez chaque règle ILM" Qui place actuellement les objets dans le pool de stockage cloud que vous souhaitez supprimer.
5. Déterminez l'emplacement où vous souhaitez déplacer les objets existants gérés par chaque règle clonée.

   Vous pouvez utiliser un ou plusieurs pools de stockage ou un autre pool de stockage cloud.

6. Editez chacune des règles que vous avez clonées.

   Pour l'étape 2 de l'assistant Créer une règle ILM, sélectionnez le nouvel emplacement dans le champ **copies AT**.

7. "Créez une nouvelle règle ILM proposée" et remplacez chacune des anciennes règles par une règle clonée.
8. Activer la nouvelle règle.
9. Attendez que ILM supprime les objets du pool de stockage cloud et les place à un nouvel emplacement.

Supprimer le pool de stockage cloud

Lorsque le pool de stockage cloud est vide et qu'il n'est utilisé dans aucune règle ILM, vous pouvez le supprimer.

Avant de commencer

- Vous avez supprimé toutes les règles ILM qui auraient pu utiliser le pool.
- Vous avez confirmé que le compartiment S3 ou le conteneur Azure ne contient aucun objet.

  Une erreur se produit si vous tentez de supprimer un pool de stockage cloud s'il contient des objets. Voir "Résoudre les problèmes liés aux pools de stockage cloud".

Lorsque vous créez un pool de stockage cloud, StorageGRID écrit un fichier de marqueur vers le compartiment ou le conteneur pour l'identifier comme un pool de stockage cloud. Ne supprimez pas ce fichier, qui est nommé `x-ntap-sgws-cloud-pool-uuid`.

Étapes

1. Sélectionnez **ILM** > **Storage pools** > **Cloud Storage pools**.
2. Si la colonne utilisation d'ILM indique que Cloud Storage Pool n'est pas utilisé, cochez la case.
3. Sélectionnez **actions** > **Supprimer**.
4. Sélectionnez **OK**.

Résoudre les problèmes liés aux pools de stockage cloud

Suivez ces étapes de dépannage pour résoudre les erreurs que vous pouvez rencontrer lors de la création, de la modification ou de la suppression d'un pool de stockage cloud.

Déterminez si une erreur s'est produite

StorageGRID effectue une vérification simple de l'état de santé de chaque pool de stockage cloud une fois par minute pour vérifier que celui-ci est accessible et qu'il fonctionne correctement. Si le contrôle de l'état détecte un problème, un message s'affiche dans la colonne dernière erreur du tableau pools de stockage cloud de la page pools de stockage cloud.

Le tableau indique la dernière erreur détectée pour chaque pool de stockage cloud et indique la durée de l'erreur.

En outre, une alerte **erreur** de connectivité de pool de stockage cloud est déclenchée si le contrôle d'intégrité détecte qu'une ou plusieurs nouvelles erreurs de pool de stockage cloud se sont produites au cours des 5 dernières minutes. Si vous recevez une notification par e-mail pour cette alerte, accédez à la page Storage pools (sélectionnez **ILM** > **Storage pools**), consultez les messages d'erreur dans la colonne Last error (dernière erreur) et reportez-vous aux instructions de dépannage ci-dessous.

Vérifiez si une erreur a été résolue

Après avoir résolu les problèmes sous-jacents, vous pouvez déterminer si l'erreur a été résolue. Sur la page Cloud Storage Pool, sélectionnez le noeud final, puis sélectionnez **Clear error**. Un message de confirmation indique que StorageGRID a résolu l'erreur pour le pool de stockage cloud.

Si le problème sous-jacent a été résolu, le message d'erreur ne s'affiche plus. Toutefois, si le problème sous-jacent n'a pas été résolu (ou si une erreur différente est rencontrée), le message d'erreur s'affiche dans la colonne dernière erreur dans les minutes qui suivent.

Erreur : ce pool de stockage cloud contient du contenu inattendu

Cette erreur peut se produire lorsque vous tentez de créer, modifier ou supprimer un pool de stockage cloud. Cette erreur se produit si le godet ou le conteneur inclut le `x-ntap-sgws-cloud-pool-uuid` Le fichier de marqueurs, mais ce fichier n'a pas l'UUID attendu.

En général, cette erreur s'affiche uniquement si vous créez un pool de stockage cloud et qu'une autre instance de StorageGRID utilise déjà le même pool de stockage cloud.

Essayez ces étapes pour corriger le problème :

- Assurez-vous que personne dans votre entreprise n'utilise également ce Cloud Storage Pool.
- Supprimez le `x-ntap-sgws-cloud-pool-uuid` Et essayez à nouveau de configurer le pool de stockage cloud.

Erreur : impossible de créer ou de mettre à jour le pool de stockage cloud. Erreur du noeud final

Cette erreur peut se produire lorsque vous tentez de créer ou de modifier un pool de stockage cloud. Cette erreur indique qu'un problème de connectivité ou de configuration empêche StorageGRID d'écrire dans le pool de stockage cloud.

Pour corriger le problème, consultez le message d'erreur du noeud final.

- Si le message d'erreur contient `Get *url*: EOF`, Vérifiez que le terminal de service utilisé pour le pool de stockage cloud n'utilise pas HTTP pour un conteneur ou un compartiment qui nécessite HTTPS.
- Si le message d'erreur contient `Get *url*: net/http: request canceled while waiting for connection`, Vérifiez que la configuration réseau autorise les nœuds de stockage à accéder au terminal de service utilisé pour le pool de stockage cloud.
- Pour tous les autres messages d'erreur de point final, essayez un ou plusieurs des éléments suivants :
  - Créez un conteneur ou un compartiment externe avec le même nom que vous avez saisi pour le Cloud Storage Pool, et essayez à nouveau d'enregistrer le nouveau pool de stockage cloud.
  - Corrigez le nom de conteneur ou de compartiment que vous avez spécifié pour le pool de stockage cloud, et essayez de sauvegarder à nouveau le nouveau pool de stockage cloud.

Erreur : échec de l'analyse du certificat CA

Cette erreur peut se produire lorsque vous tentez de créer ou de modifier un pool de stockage cloud. L'erreur se produit si StorageGRID n'a pas pu analyser le certificat que vous avez saisi lors de la configuration du pool de stockage cloud.

Pour corriger le problème, vérifiez si le certificat CA que vous avez fourni ne présente pas de problèmes.

Erreur : un pool de stockage cloud associé à cet ID est introuvable

Cette erreur peut se produire lorsque vous essayez de modifier ou de supprimer un pool de stockage cloud. Cette erreur se produit si le noeud final renvoie une réponse 404, ce qui peut signifier l'un des éléments suivants :

- Les identifiants utilisés pour le pool de stockage cloud ne disposent pas des autorisations de lecture pour le compartiment.
- Le compartiment utilisé pour le pool de stockage cloud n'inclut pas la `x-ntap-sgws-cloud-pool-uuid` fichier de marqueur.

Essayez une ou plusieurs des étapes suivantes pour corriger le problème :

- Vérifiez que l'utilisateur associé à la clé d'accès configurée possède les autorisations requises.
- Modifiez le pool de stockage cloud avec des identifiants disposant des autorisations requises.
- Si les autorisations sont correctes, contactez l'assistance technique.

Erreur : impossible de vérifier le contenu du pool de stockage cloud. Erreur du noeud final

Cette erreur peut se produire lorsque vous tentez de supprimer un pool de stockage cloud. Cette erreur

indique qu'un problème de connectivité ou de configuration empêche StorageGRID de lire le contenu du compartiment Cloud Storage Pool.

Pour corriger le problème, consultez le message d'erreur du noeud final.

Erreur : les objets ont déjà été placés dans ce compartiment

Cette erreur peut se produire lorsque vous tentez de supprimer un pool de stockage cloud. Vous ne pouvez pas supprimer un pool de stockage cloud s'il contient des données qui y ont été déplacées par ILM, des données qui se trouvait dans le compartiment avant la configuration du pool de stockage cloud, ou des données qui ont été placées dans le compartiment par une autre source après la création du pool de stockage cloud.

Essayez une ou plusieurs des étapes suivantes pour corriger le problème :

- Suivez les instructions pour déplacer de nouveau des objets vers StorageGRID dans la section « cycle de vie d'un objet de pool de stockage cloud ».
- Si vous êtes certain que les objets restants n'ont pas été placés dans le pool de stockage cloud par ILM, supprimez manuellement les objets du compartiment.

> ⓘ Ne supprimez jamais manuellement d'objets d'un pool de stockage cloud qui auraient pu y avoir été placés par ILM. Si vous tentez par la suite d'accéder à un objet supprimé manuellement à partir de StorageGRID, l'objet supprimé est introuvable.

Erreur : le proxy a rencontré une erreur externe lors de la tentative d'accès au pool de stockage cloud

Cette erreur peut se produire si vous avez configuré un proxy de stockage non transparent entre les nœuds de stockage et le terminal S3 externe utilisé pour le pool de stockage cloud. Cette erreur se produit si le serveur proxy externe ne parvient pas à atteindre le terminal Cloud Storage Pool. Par exemple, il se peut que le serveur DNS ne puisse pas résoudre le nom d'hôte ou qu'il existe un problème de réseau externe.

Essayez une ou plusieurs des étapes suivantes pour corriger le problème :

- Vérifiez les paramètres de Cloud Storage Pool (**ILM** > **Storage pools**).
- Vérifiez la configuration réseau du serveur proxy de stockage.

Informations associées

"Cycle de vie d'un objet de pool de stockage cloud"

Gestion des profils de code d'effacement

Si nécessaire, vous pouvez renommer un profil de code d'effacement. Vous pouvez désactiver un profil de code d'effacement s'il n'est actuellement utilisé dans aucune règle ILM.

Renommer un profil de code d'effacement

Vous pouvez renommer un profil de code d'effacement pour le rendre plus évident.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".

- Vous avez le "autorisations d'accès requises".

Étapes

1. Sélectionnez **ILM** > **code d'effacement**.
2. Sélectionnez le profil à renommer.
3. Sélectionnez **Renommer**.
4. Entrez un nom unique pour le profil de code d'effacement.

   Le nom du profil de code d'effacement est ajouté au nom du pool de stockage dans l'instruction de placement d'une règle ILM.

   > Les noms des profils de code d'effacement doivent être uniques. Une erreur de validation se produit si vous utilisez le nom d'un profil existant, même si ce profil a été désactivé.

5. Sélectionnez **Enregistrer**.

Désactiver un profil de code d'effacement

Vous pouvez désactiver un profil de code d'effacement si vous ne prévoyez plus de l'utiliser et si ce profil n'est pas utilisé dans les règles ILM.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous avez le "autorisations d'accès requises".
- Vous avez confirmé que aucune opération de réparation avec code d'effacement ou aucune procédure de désaffectation des données n'est en cours. Un message d'erreur s'affiche si vous tentez de désactiver un profil de code d'effacement alors que l'une de ces opérations est en cours.

Description de la tâche

Lorsque vous désactivez un profil de code d'effacement, le profil apparaît toujours sur la page profils de code d'effacement, mais son état est **DESACTIVE**.

	Profile	Status	Storage Pool	Storage Nodes	Sites	Erasure Code	Storage Overhead (%)	Storage Node Redundancy	Site Redundancy
○	2+1 Data Center 1	Used In ILM Rule	Data Center 1	3	1	2+1	50	1	No
◉	New profile	Deactivated	Data Center 1	3	1	2+1	50	1	No

Vous ne pouvez plus utiliser un profil de code d'effacement qui a été désactivé. Un profil désactivé n'apparaît pas lorsque vous créez les instructions de placement pour une règle ILM. Vous ne pouvez pas réactiver un profil désactivé.

StorageGRID vous empêche de désactiver un profil de code d'effacement si l'une des conditions suivantes est vraie :

- Le profil de code d'effacement est actuellement utilisé dans une règle ILM.
- Le profil de code d'effacement n'est plus utilisé dans les règles ILM, mais les données en objet et les fragments de parité du profil existent toujours.

Étapes

1. Sélectionnez **ILM** > **codage d'effacement**.

2. Consultez la colonne **Status** pour confirmer que le profil de code d'effacement que vous souhaitez désactiver n'est utilisé dans aucune règle ILM.

   Vous ne pouvez pas désactiver un profil de code d'effacement s'il est utilisé dans une règle ILM. Dans cet exemple, le profil **2+1 Data Center 1** est utilisé dans au moins une règle ILM.

Profile	Status	Storage Pool	Storage Nodes	Sites	Erasure Code	Storage Overhead (%)	Storage Node Redundancy	Site Redundancy
2+1 Data Center 1	Used In ILM Rule	Data Center 1	3	1	2+1	50	1	No
New profile	Deactivated	Data Center 1	3	1	2+1	50	1	No

3. Si le profil est utilisé dans une règle ILM, effectuez la procédure suivante :
   a. Sélectionnez **ILM** > **règles**.
   b. Sélectionnez chaque règle et consultez le diagramme de rétention pour déterminer si la règle utilise le profil de code d'effacement que vous souhaitez désactiver.
   c. Si la règle ILM utilise le profil de code d'effacement que vous souhaitez désactiver, déterminez si la règle est utilisée dans la règle ILM active ou dans une règle proposée.
   d. Complétez les étapes supplémentaires du tableau, en fonction de l'endroit où le profil de code d'effacement est utilisé.

Où le profil a-t-il été utilisé ?	**Étapes supplémentaires à effectuer avant la désactivation du profil**	**Reportez-vous à ces instructions supplémentaires**
Jamais utilisé dans une règle ILM	Aucune étape supplémentaire n'est requise. Poursuivre cette procédure.	*Aucun*
Les règles ILM n'ont jamais été utilisées dans toutes les règles ILM	i. Modifiez ou supprimez toutes les règles ILM affectées. Si vous modifiez la règle, supprimez tous les placements qui utilisent le profil de code d'effacement. ii. Poursuivre cette procédure.	"Utilisation des règles ILM et des règles ILM"

Où le profil a-t-il été utilisé ?	Étapes supplémentaires à effectuer avant la désactivation du profil	Reportez-vous à ces instructions supplémentaires
Règle ILM faisant actuellement partie de la politique ILM active	i. Cloner la règle active. ii. Suppression de la règle ILM utilisant le profil de code d'effacement iii. Ajoutez une ou plusieurs nouvelles règles ILM pour assurer la protection des objets. iv. Enregistrez, simulez et activez la nouvelle stratégie. v. Attendez que la nouvelle stratégie soit appliquée et que les objets existants soient déplacés vers de nouveaux emplacements en fonction des nouvelles règles que vous avez ajoutées. **Remarque :** en fonction du nombre d'objets et de la taille de votre système StorageGRID, le déplacement des objets vers de nouveaux emplacements peut prendre des semaines, voire des mois, en fonction des nouvelles règles ILM. Bien que vous puissiez tenter en toute sécurité de désactiver un profil de code d'effacement alors qu'il est toujours associé à des données, l'opération de désactivation échouera. Un message d'erreur vous informe si le profil n'est pas encore prêt à être désactivé. vi. Modifiez ou supprimez la règle que vous avez supprimée de la stratégie. Si vous modifiez la règle, supprimez tous les placements qui utilisent le profil de code d'effacement. vii. Poursuivre cette procédure.	"Création d'une règle ILM" "Utilisation des règles ILM et des règles ILM"
La règle ILM faisant actuellement partie d'une politique ILM proposée	i. Modifier la règle proposée. ii. Suppression de la règle ILM utilisant le profil de code d'effacement iii. Ajoutez une ou plusieurs nouvelles règles ILM pour protéger tous les objets. iv. Enregistrez la stratégie proposée. v. Modifiez ou supprimez la règle que vous avez supprimée de la stratégie. Si vous modifiez la règle, supprimez tous les placements qui utilisent le profil de code d'effacement. vi. Poursuivre cette procédure.	"Création d'une règle ILM" "Utilisation des règles ILM et des règles ILM"

Où le profil a-t-il été utilisé ?	Étapes supplémentaires à effectuer avant la désactivation du profil	Reportez-vous à ces instructions supplémentaires
La règle ILM d'une règle ILM historique	i. Modifiez ou supprimez la règle. Si vous modifiez la règle, supprimez tous les placements qui utilisent le profil de code d'effacement. (La règle apparaît désormais comme une règle historique dans la politique historique.) ii. Poursuivre cette procédure.	"Utilisation des règles ILM et des règles ILM"

e. Actualisez la page profils de code d'effacement pour vous assurer que le profil n'est pas utilisé dans une règle ILM.

4. Si le profil n'est pas utilisé dans une règle ILM, sélectionnez le bouton radio et sélectionnez **Désactiver**.

   La boîte de dialogue Désactiver le profil EC s'affiche.

5. Si vous êtes sûr de vouloir désactiver le profil, sélectionnez **Désactiver**.
   - Si StorageGRID peut désactiver le profil de code d'effacement, son état est **DESACTIVE**. Vous ne pouvez plus sélectionner ce profil pour une règle ILM.
   - Si StorageGRID ne peut pas désactiver le profil, un message d'erreur s'affiche. Par exemple, un message d'erreur s'affiche si les données d'objet sont toujours associées à ce profil. Vous devrez peut-être attendre plusieurs semaines avant d'essayer à nouveau le processus de désactivation.

Configuration des régions (facultatif et S3 uniquement)

Les règles ILM permettent de filtrer des objets en fonction des régions où des compartiments S3 sont créés, ce qui vous permet de stocker des objets provenant de différentes régions dans différents emplacements de stockage.

Si vous souhaitez utiliser une région de compartiment S3 comme filtre dans une règle, vous devez d'abord créer les régions à utiliser par les compartiments du système.

Vous ne pouvez pas modifier la région d'un compartiment après sa création.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous disposez d'autorisations d'accès spécifiques.

Description de la tâche

Lorsque vous créez un compartiment S3, vous pouvez spécifier une région La spécification d'une région permet au compartiment d'être géographiquement proche de ses utilisateurs, ce qui peut contribuer à optimiser la latence, réduire les coûts et satisfaire aux exigences réglementaires.

Lorsque vous créez une règle ILM, vous pouvez utiliser la région associée à un compartiment S3 comme filtre avancé. Par exemple, vous pouvez concevoir une règle qui s'applique uniquement aux objets des compartiments S3 créés dans la région US-West-2. Afin d'optimiser la latence, vous pouvez ensuite placer des copies de ces objets sur des nœuds de stockage sur un site de data Center dans cette région.

Lors de la configuration de régions, suivez les consignes suivantes :

- Par défaut, tous les compartiments sont considérés comme appartenant à la région US-East-1.
- Vous devez créer les régions à l'aide de Grid Manager avant de spécifier une région autre que celle par défaut lors de la création de compartiments à l'aide du Gestionnaire de locataires ou de l'API de gestion des locataires ou avec l'élément de demande LocationConstraint pour les requêtes d'API PUT S3. Une erreur se produit si une demande PUT Bucket utilise une région qui n'a pas été définie dans StorageGRID.
- Lors de la création du compartiment S3, vous devez utiliser le nom exact de la région. Les noms de région sont sensibles à la casse. Les caractères autorisés sont des chiffres, des lettres et des tirets.

> ⓘ L'UE n'est pas considérée comme un alias pour l'ue-Ouest-1. Si vous souhaitez utiliser la région UE ou eu-West-1, vous devez utiliser le nom exact.

- Vous ne pouvez pas supprimer ou modifier une région si elle est actuellement utilisée dans la règle ILM active ou la règle ILM proposée.
- Si la région utilisée comme filtre avancé dans une règle ILM n'est pas valide, il est toujours possible d'ajouter cette règle à la règle proposée. Cependant, une erreur se produit si vous tentez d'enregistrer ou d'activer la stratégie proposée.

  Une région non valide peut se produire si vous utilisez une région en tant que filtre avancé dans une règle ILM, mais que vous supprimez cette région ultérieurement, ou si vous utilisez l'API de gestion de grille pour créer une règle et spécifier une région que vous n'avez pas définie.

- Si vous supprimez une région après l'avoir utilisée pour créer un compartiment S3, vous devez ajouter de nouveau la région si vous souhaitez utiliser le filtre avancé contrainte d'emplacement pour trouver des objets dans ce compartiment.

Étapes

1. Sélectionnez **ILM** > **régions**.

   La page régions s'affiche, les régions actuellement définies étant répertoriées. **Région 1** affiche la région par défaut, `us-east-1`, qui ne peut pas être modifié ou supprimé.

2. Pour ajouter une région :
   a. Sélectionnez l'icône Insérer ➕ à droite de la dernière entrée.
   b. Entrez le nom d'une région à utiliser lors de la création de compartiments S3.

      Vous devez utiliser ce nom de région exact comme élément de demande LocationConstraint lorsque vous créez le compartiment S3 correspondant.

3. Pour supprimer une région inutilisée, sélectionnez l'icône de suppression ✕.

   Un message d'erreur s'affiche si vous tentez de supprimer une région actuellement utilisée dans la stratégie active ou la stratégie proposée.

4. Une fois les modifications effectuées, sélectionnez **Enregistrer**.

   Vous pouvez maintenant sélectionner ces régions dans la section filtres avancés de l'étape 1 de l'assistant de création de règles ILM. Voir "Utilisation de filtres avancés dans les règles ILM".

Création d'une règle ILM

Création d'une règle ILM : présentation

Pour gérer les objets, vous créez un ensemble de règles de gestion du cycle de vie des informations (ILM) et vous les organisez en une règle ILM.

Chaque objet ingéré dans le système est évalué par rapport à la règle active. Lorsqu'une règle de la règle correspond aux métadonnées d'un objet, les instructions de la règle déterminent les actions que StorageGRID prend pour copier et stocker cet objet.

> Les métadonnées de l'objet ne sont pas gérées par des règles ILM. Les métadonnées d'objet sont stockées dans la base de données Cassandra, dans ce qu'on appelle un magasin de métadonnées. Trois copies des métadonnées des objets sont automatiquement conservées sur chaque site afin de protéger les données contre les pertes.

Éléments d'une règle ILM

Une règle ILM comporte trois éléments :

- **Critères de filtrage** : les filtres de base et avancés d'une règle définissent les objets auxquels la règle s'applique. Si un objet correspond à tous les filtres, StorageGRID applique la règle et crée les copies d'objet spécifiées dans les instructions de placement de la règle.
- **Instructions de placement** : les instructions de placement d'une règle définissent le nombre, le type et l'emplacement des copies d'objet. Chaque règle peut inclure une séquence d'instructions de placement pour modifier le nombre, le type et l'emplacement des copies d'objet au fil du temps. À l'expiration de la période de temps pour un placement, les instructions du placement suivant sont automatiquement appliquées par l'évaluation ILM suivante.
- **Comportement d'ingestion** : le comportement d'ingestion d'une règle vous permet de choisir la façon dont les objets filtrés par la règle sont protégés lors de leur ingestion (lorsqu'un client S3 ou Swift enregistre un objet dans la grille).

Filtrage de règles ILM

Lorsque vous créez une règle ILM, vous spécifiez des filtres pour identifier les objets auxquels la règle s'applique.

Dans le cas le plus simple, une règle ne peut pas utiliser de filtres. Toute règle qui n'utilise pas de filtre s'applique à tous les objets. Elle doit donc être la dernière règle (par défaut) d'une politique ILM. La règle par défaut fournit des instructions de stockage pour les objets qui ne correspondent pas aux filtres d'une autre règle.

- Les filtres de base vous permettent d'appliquer différentes règles à de grands groupes d'objets distincts. Ces filtres vous permettent d'appliquer une règle à des comptes de locataire spécifiques, à des compartiments S3 ou des conteneurs Swift, ou les deux.

  Les filtres de base vous permettent d'appliquer facilement différentes règles à un grand nombre d'objets. Par exemple, les données financières de votre entreprise peuvent être stockées pour répondre à la réglementation, tandis que les données du service marketing doivent être stockées pour faciliter les opérations quotidiennes. Après avoir créé des comptes de tenant distincts pour chaque service ou après avoir séparé les données des différents services dans des compartiments S3 distincts, vous pouvez facilement créer une règle qui s'applique à tous les enregistrements financiers et une deuxième règle qui s'applique à toutes les données de marketing.

- Les filtres avancés vous offrent un contrôle granulaire. Vous pouvez créer des filtres pour sélectionner des objets en fonction des propriétés d'objet suivantes :
  - Temps d'ingestion
  - Heure du dernier accès
  - Tout ou partie du nom de l'objet (clé)
  - Contrainte d'emplacement (S3 uniquement)
  - Taille de l'objet
  - Métadonnées d'utilisateur
  - Balise objet (S3 uniquement)

Vous pouvez filtrer les objets selon des critères très spécifiques. Par exemple, les objets stockés par le service d'imagerie de l'hôpital peuvent être utilisés fréquemment s'ils ont moins de 30 jours et rarement par la suite, tandis que les objets contenant les informations relatives aux visites des patients peuvent devoir être copiés dans le service de facturation du siège social du réseau de santé. Vous pouvez créer des filtres qui identifient chaque type d'objet en fonction du nom, de la taille, des balises d'objet S3 ou de tout autre critère pertinent. Il crée ensuite des règles distinctes pour stocker chaque ensemble d'objets de façon appropriée.

Vous pouvez combiner des filtres selon vos besoins dans une seule règle. Par exemple, le service marketing pourrait souhaiter stocker des fichiers d'images volumineux différemment des dossiers de fournisseurs, tandis que le service des ressources humaines pourrait avoir besoin de stocker les dossiers du personnel dans une zone géographique spécifique et des informations sur les politiques de manière centralisée. Dans ce cas, vous pouvez créer des règles qui filtrent par compte de locataire pour séparer les enregistrements de chaque service, tout en utilisant des filtres dans chaque règle pour identifier le type spécifique d'objets auquel la règle s'applique.

Instructions de placement des règles ILM

Les instructions de placement déterminent l'emplacement, le moment et le mode de stockage des données objet. Une règle ILM peut inclure une ou plusieurs instructions de placement. Chaque instruction de placement s'applique à une seule période de temps.

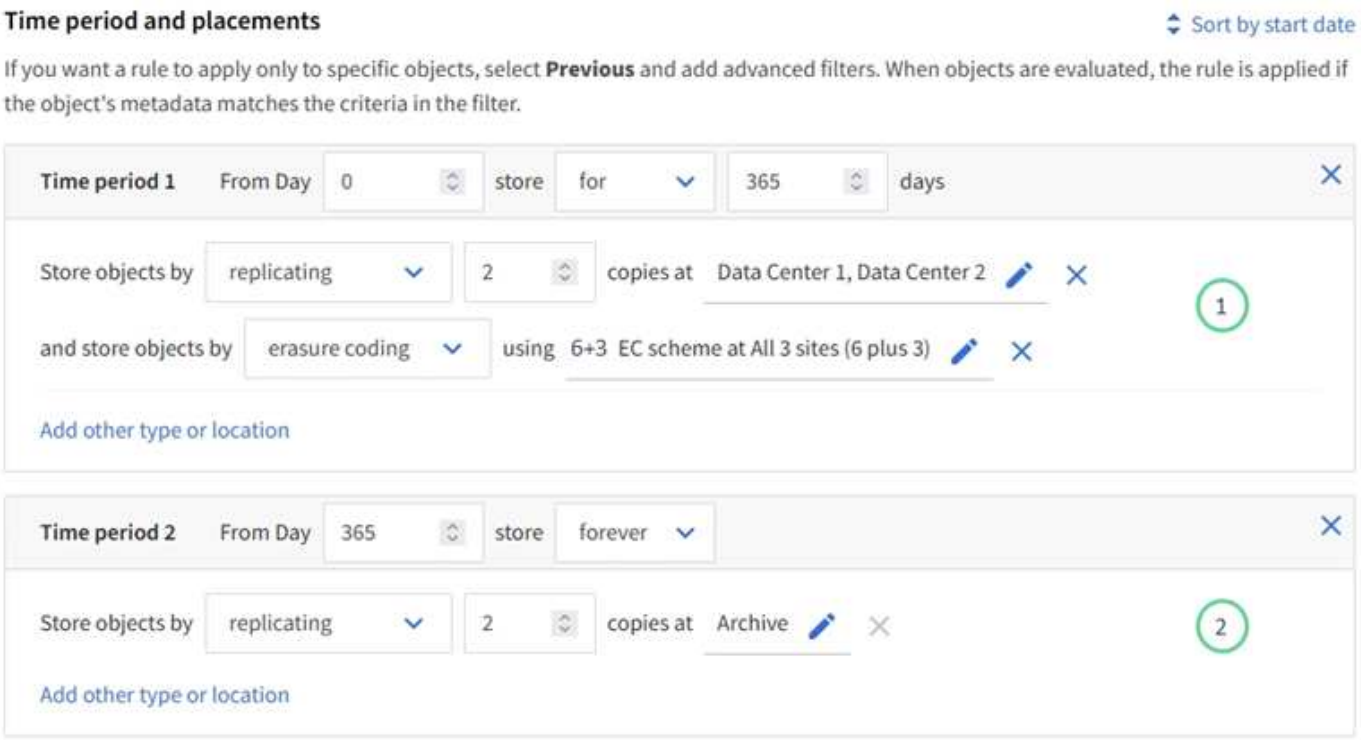
Lorsque vous créez des instructions de positionnement :

- Vous commencez par spécifier l'heure de référence, qui détermine le début des instructions de positionnement. L'heure de référence peut être lorsqu'un objet est ingéré, lorsqu'un objet est accédé, lorsqu'un objet versionné devient non courant ou une heure définie par l'utilisateur.
- Vous spécifiez ensuite le moment où le placement s'appliquera, par rapport à l'heure de référence. Par exemple, un placement peut commencer le jour 0 et se poursuivre pendant 365 jours, par rapport à l'ingestion de l'objet.
- Enfin, vous spécifiez le type de copies (réplication ou codage d'effacement) et l'emplacement de stockage des copies. Par exemple, vous pouvez stocker deux copies répliquées sur deux sites différents.

Chaque règle peut définir plusieurs placements pour une période unique et différents placements pour différentes périodes.

- Pour placer des objets à plusieurs emplacements pendant une seule période, sélectionnez **Ajouter un autre type ou un autre emplacement** pour ajouter plus d'une ligne pour cette période.
- Pour placer des objets à différents emplacements dans différentes périodes, sélectionnez **Ajouter une autre période** pour ajouter la période suivante. Spécifiez ensuite une ou plusieurs lignes dans la période.

L'exemple illustre deux instructions de positionnement sur la page Define stages de l'assistant Create ILM Rule.



Première instruction de positionnement (1) a deux lignes pour la première année :

- La première ligne crée deux copies d'objets répliquées sur deux sites de data Center.
- La seconde ligne crée une copie avec code d'effacement de 6 + 3 sur trois sites de data Center.

La deuxième instruction de positionnement (2) crée deux copies archivées au bout d'un an et les conserve indéfiniment.

Lorsque vous définissez l'ensemble des instructions de placement pour une règle, vous devez vous assurer qu'au moins une instruction de placement commence au jour 0, qu'il n'y a pas d'écart entre les périodes que vous avez définies, et que l'instruction de placement final continue soit indéfiniment ou jusqu'à ce que vous n'ayez plus besoin de copies d'objet.

À chaque expiration de la règle, les instructions de placement de contenu pour la période suivante sont appliquées. De nouvelles copies d'objet sont créées et les copies inutiles sont supprimées.

Comportement d'ingestion des règles ILM

Le comportement d'ingestion détermine si les copies d'objet sont immédiatement placées conformément aux instructions de la règle, ou si des copies intermédiaires sont effectuées et que les instructions de placement sont appliquées ultérieurement. Les comportements d'ingestion suivants sont disponibles pour les règles ILM :

- **Équilibré**: StorageGRID tente de faire toutes les copies spécifiées dans la règle ILM à l'entrée; si ce n'est pas possible, des copies intermédiaires sont faites et le succès est renvoyé au client. Les copies spécifiées dans la règle ILM sont effectuées lorsque cela est possible.
- **Strict** : toutes les copies spécifiées dans la règle ILM doivent être effectuées avant que le succès ne soit renvoyé au client.

- **Dual commit** : StorageGRID effectue immédiatement des copies intermédiaires de l'objet et renvoie le succès au client. Les copies spécifiées dans la règle ILM sont effectuées lorsque cela est possible.

Informations associées

- "Options d'ingestion"
- "Avantages, inconvénients et limites des options d'acquisition"
- "Interaction des contrôles de cohérence et des règles ILM pour la protection des données"

Exemple de règle ILM

À titre d'exemple, une règle ILM peut spécifier les éléments suivants :

- Appliquer uniquement aux objets appartenant au locataire A.
- Faites deux copies répliquées de ces objets et stockez chaque copie sur un site différent.
- Conservez les deux copies « pour toujours », ce qui signifie que StorageGRID ne les supprimera pas automatiquement. À la place, StorageGRID les conserve jusqu'à leur suppression par une demande de suppression de client ou avant l'expiration d'un cycle de vie de compartiment.
- Utilisez l'option équilibrée pour le comportement d'ingestion : l'instruction de placement sur deux sites est appliquée dès que le locataire A enregistre un objet dans StorageGRID, à moins qu'il ne soit pas possible d'effectuer immédiatement les deux copies requises.

  Par exemple, si le site 2 est injoignable lorsque le locataire A enregistre un objet, StorageGRID effectue deux copies provisoires sur les nœuds de stockage du site 1. Dès que le site 2 sera disponible, StorageGRID effectuera la copie requise sur ce site.

Informations associées

- "Qu'est-ce qu'un pool de stockage ?"
- "Qu'est-ce qu'un pool de stockage cloud ?"

Accédez à l'assistant de création de règles ILM

Les règles ILM permettent de gérer le placement des données d'objet au fil du temps. Pour créer une règle ILM, l'assistant de création d'une règle ILM est utilisé.

> Pour créer la règle ILM par défaut d'une règle, suivez la procédure "Instructions de création d'une règle ILM par défaut" à la place.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous disposez d'autorisations d'accès spécifiques.
- Si vous souhaitez spécifier les comptes de tenant auxquels cette règle s'applique, vous disposez de l'autorisation comptes de tenant ou vous connaissez l'ID de compte de chaque compte.
- Si vous souhaitez que la règle filtre les objets sur les métadonnées de l'heure du dernier accès, les mises à jour de l'heure du dernier accès doivent être activées par compartiment pour S3 ou par conteneur pour Swift.
- Vous avez configuré tous les pools de stockage cloud que vous prévoyez d'utiliser. Voir "Création d'un pool de stockage cloud".

- Vous connaissez le "options d'ingestion".
- Si vous devez créer une règle compatible pour une utilisation avec le verrouillage d'objet S3, vous connaissez le "Conditions requises pour le verrouillage d'objet S3".
- Vous pouvez également regarder la vidéo : "Vidéo : règles de gestion du cycle de vie de l'information dans StorageGRID 11.7".

Description de la tâche

Lors de la création de règles ILM :

- Comparez la topologie et les configurations de stockage du système StorageGRID.
- Déterminez les types de copies d'objet à effectuer (répliquées ou avec code d'effacement) et le nombre de copies de chaque objet requis.
- Déterminez les types de métadonnées d'objet utilisés dans les applications qui se connectent au système StorageGRID. Les règles ILM filtrent les objets en fonction de leurs métadonnées.
- Réfléchissez à l'emplacement souhaité pour le stockage des copies d'objets au fil du temps.
- Choisissez l'option d'ingestion à utiliser (équilibrée, stricte ou Dual commit).

Étapes

1. Sélectionnez **ILM** > **règles**.

   En fonction du nombre de sites dans la grille, la règle faire 2 copies ou la règle 1 copie par site s'affiche dans la liste des règles.

   > Si le paramètre global S3 Object Lock a été activé pour le système StorageGRID, la table récapitulative inclut une colonne **compatible** et les détails de la règle sélectionnée incluent un champ **compatible**.

2. Sélectionnez **Créer**. "Étape 1 (entrer les détails)" De l'assistant de création d'une règle ILM s'affiche.

Étape 1 sur 3 : saisissez les détails

L'étape **entrer détails** de l'assistant Créer une règle ILM vous permet d'entrer un nom et une description pour la règle et de définir des filtres pour la règle.

La saisie d'une description et la définition de filtres pour la règle sont facultatives.

Description de la tâche

Lors de l'évaluation d'un objet par rapport à un "Règle ILM", StorageGRID compare les métadonnées de l'objet aux filtres de la règle. Si les métadonnées correspondent à tous les filtres, StorageGRID utilise la règle pour placer l'objet. Vous pouvez concevoir une règle à appliquer à tous les objets, ou spécifier des filtres de base, tels qu'un ou plusieurs comptes de locataire, noms de compartiment ou filtres avancés, tels que la taille de

l'objet ou les métadonnées utilisateur.

Étapes

1. Entrez un nom unique pour la règle dans le champ **Nom**.
2. Vous pouvez également saisir une brève description de la règle dans le champ **Description**.

   Vous devez décrire le but ou la fonction de la règle afin de pouvoir reconnaître la règle ultérieurement.

3. Vous pouvez également sélectionner un ou plusieurs comptes de locataires S3 ou Swift auxquels s'applique cette règle. Si cette règle s'applique à tous les locataires, laissez ce champ vide.

   Si vous ne disposez pas de l'autorisation d'accès racine ou de compte de locataire, vous ne pouvez pas sélectionner de locataires dans la liste. Entrez plutôt l'ID de tenant ou entrez plusieurs ID comme une chaîne délimitée par des virgules.

4. Vous pouvez également spécifier les compartiments S3 ou les conteneurs Swift auxquels s'applique cette règle.

   Si **correspond à tout** est sélectionné (par défaut), la règle s'applique à tous les compartiments S3 ou conteneurs Swift.

5. Pour les locataires S3, sélectionnez **Oui** pour appliquer la règle uniquement aux anciennes versions d'objets dans des compartiments S3 pour lesquels la gestion de versions est activée.

   Si vous sélectionnez **Oui**, « temps non courant » sera automatiquement sélectionné pour l'heure de référence dans "Étape 2 de l'assistant de création de règles ILM".

   > Une heure non actuelle s'applique uniquement aux objets S3 dans des compartiments avec gestion des versions. Voir "Opérations sur les compartiments, GESTION des versions DES compartiments" et "Gestion des objets avec le verrouillage d'objets S3".

   Vous pouvez utiliser cette option pour réduire l'impact du stockage des objets multiversion en filtrant pour les versions d'objets non à jour. Voir "Exemple 4 : règles et règles ILM pour les objets avec version S3".

6. Si vous le souhaitez, sélectionnez **Ajouter un filtre avancé** pour spécifier des filtres supplémentaires.

   Si vous ne configurez pas le filtrage avancé, la règle s'applique à tous les objets correspondant aux filtres de base. Pour plus d'informations sur le filtrage avancé, reportez-vous à la section Utilisation de filtres avancés dans les règles ILM et Spécifiez plusieurs types et valeurs de métadonnées.

7. Sélectionnez **Continuer**. "Étape 2 (définir les placements)" De l'assistant de création d'une règle ILM s'affiche.

Utilisation de filtres avancés dans les règles ILM

Le filtrage avancé vous permet de créer des règles ILM qui s'appliquent uniquement à des objets spécifiques en fonction de leurs métadonnées. Lorsque vous configurez le filtrage avancé d'une règle, vous sélectionnez le type de métadonnées que vous souhaitez associer, sélectionnez un opérateur et spécifiez une valeur de métadonnées. Lors de l'évaluation des objets, la règle ILM s'applique uniquement aux objets dont les métadonnées correspondent au filtre avancé.

Le tableau indique les types de métadonnées que vous pouvez spécifier dans les filtres avancés, les opérateurs que vous pouvez utiliser pour chaque type de métadonnées et les valeurs de métadonnées attendues.

Type de métadonnées	Opérateurs pris en charge	Valeur des métadonnées
Temps d'ingestion	• est • n'est pas • est avant • est activé ou avant • est après • est activé ou après	Heure et date d'ingestion de l'objet. **Remarque :** pour éviter les problèmes de ressources lors de l'activation d'une nouvelle stratégie ILM, vous pouvez utiliser le filtre avancé heure d'ingestion dans toute règle susceptible de modifier l'emplacement d'un grand nombre d'objets existants. Définissez le temps d'ingestion sur une valeur supérieure ou égale à la durée approximative de l'entrée en vigueur de la nouvelle règle pour vous assurer que les objets existants ne sont pas déplacés inutilement.
Clé	• égal à • n'est pas égal • contient • ne contient pas • commence par • ne commence pas par • se termine par • ne se termine pas par	Une clé d'objet S3 ou Swift unique ou complète le système. Par exemple, vous pouvez faire correspondre les objets qui se terminent avec `.txt` ou commencez par `test-object/`.
Heure du dernier accès	• est • n'est pas • est avant • est activé ou avant • est après • est activé ou après	Heure et date de la dernière récupération de l'objet (lecture ou visualisation). **Note:** si vous prévoyez "utiliser l'heure du dernier accès" En tant que filtre avancé, les mises à jour de l'heure du dernier accès doivent être activées pour le compartiment S3 ou le conteneur Swift.
Contrainte d'emplacement (S3 uniquement)	• égal à • n'est pas égal	Région dans laquelle un compartiment S3 a été créé. Utilisez **ILM** > **régions** pour définir les régions affichées. **Note:** Une valeur US-est-1 fera correspondre des objets dans des compartiments créés dans la région US-est-1 ainsi que des objets dans des compartiments n'ayant pas de région spécifiée. Voir "Configuration des régions (facultatif et S3 uniquement)".

Type de métadonnées	Opérateurs pris en charge	Valeur des métadonnées
Taille de l'objet	• égal à • n'est pas égal • inférieur à • inférieur ou égal à • supérieur à • supérieur ou égal à	Taille de l'objet. Le codage d'effacement convient mieux aux objets de plus de 1 Mo. N'utilisez pas le code d'effacement pour les objets inférieurs à 200 Ko afin d'éviter la surcharge liée à la gestion de très petits fragments de code d'effacement. **Remarque :** pour filtrer les tailles d'objet inférieures à 1 Mo, entrez une valeur décimale. Le type de navigateur et les paramètres régionaux contrôlent si vous devez utiliser un point ou une virgule comme séparateur décimal.
Métadonnées d'utilisateur	• contient • se termine par • égal à • existe • ne contient pas • ne se termine pas par • n'est pas égal • n'existe pas • ne commence pas par • commence par	Paire clé-valeur, où **Nom métadonnées utilisateur** est la clé et **valeur métadonnées** la valeur. Par exemple, pour filtrer les objets dotés de métadonnées utilisateur de `color=blue`, spécifiez `color` Pour **Nom de métadonnées utilisateur**, `equals` pour l'opérateur, et `blue` Pour **valeur métadonnées**. **Remarque :** les noms de métadonnées de l'utilisateur ne sont pas sensibles à la casse; les valeurs de métadonnées de l'utilisateur sont sensibles à la casse.
Balise objet (S3 uniquement)	• contient • se termine par • égal à • existe • ne contient pas • ne se termine pas par • n'est pas égal • n'existe pas • ne commence pas par • commence par	Paire clé-valeur, où **Nom balise objet** est la clé et **valeur balise objet** est la valeur. Par exemple, pour filtrer les objets qui ont une balise d'objet de `Image=True`, spécifiez `Image` Pour **Nom de balise d'objet**, `equals` pour l'opérateur, et `True` Pour **valeur de balise d'objet**. **Remarque :** les noms de balise d'objet et les valeurs de balise d'objet sont sensibles à la casse. Vous devez entrer ces éléments exactement comme ils ont été définis pour l'objet.

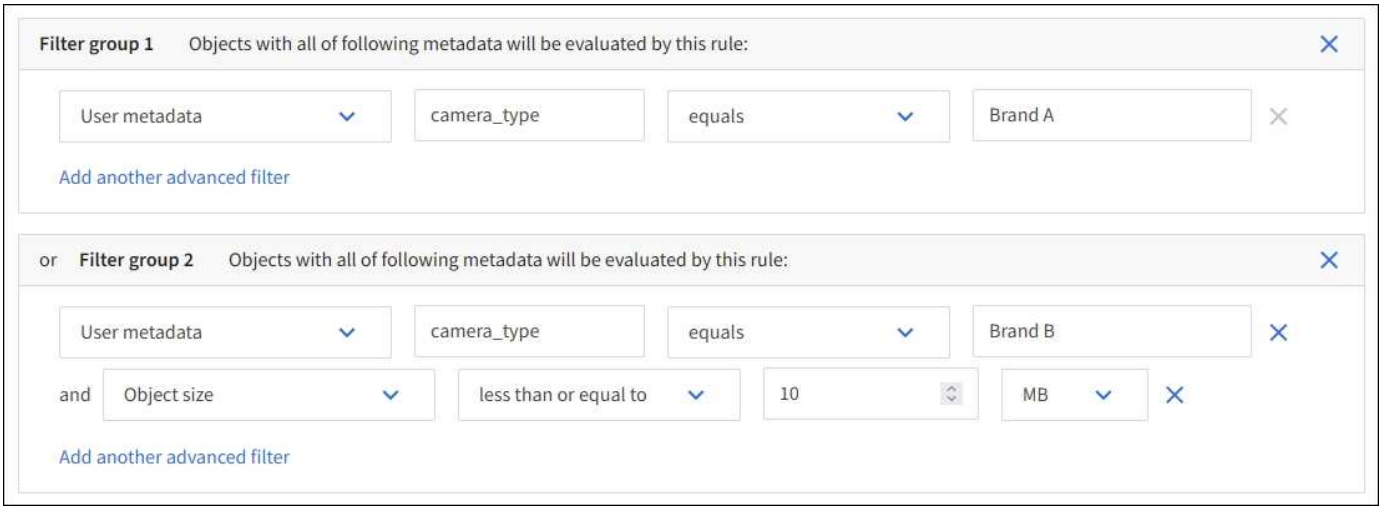
Spécifiez plusieurs types et valeurs de métadonnées

Lorsque vous définissez le filtrage avancé, vous pouvez spécifier plusieurs types de métadonnées et plusieurs valeurs de métadonnées. Par exemple, si vous souhaitez qu'une règle corresponde à des objets d'une taille comprise entre 10 Mo et 100 Mo, vous devez sélectionner le type de métadonnées **Object size** et spécifier

deux valeurs de métadonnées.

- La première valeur de métadonnées spécifie des objets supérieurs ou égaux à 10 Mo.
- La seconde valeur de métadonnées spécifie des objets inférieurs ou égaux à 100 Mo.

L'utilisation de plusieurs entrées vous permet d'avoir un contrôle précis sur les objets à associer. Dans l'exemple suivant, la règle s'applique aux objets dont la marque A ou la marque B est la valeur des métadonnées utilisateur Camera_type. Toutefois, la règle s'applique uniquement aux objets de marque B dont la taille est inférieure à 10 Mo.



Étape 2 sur 3 : définir les placements

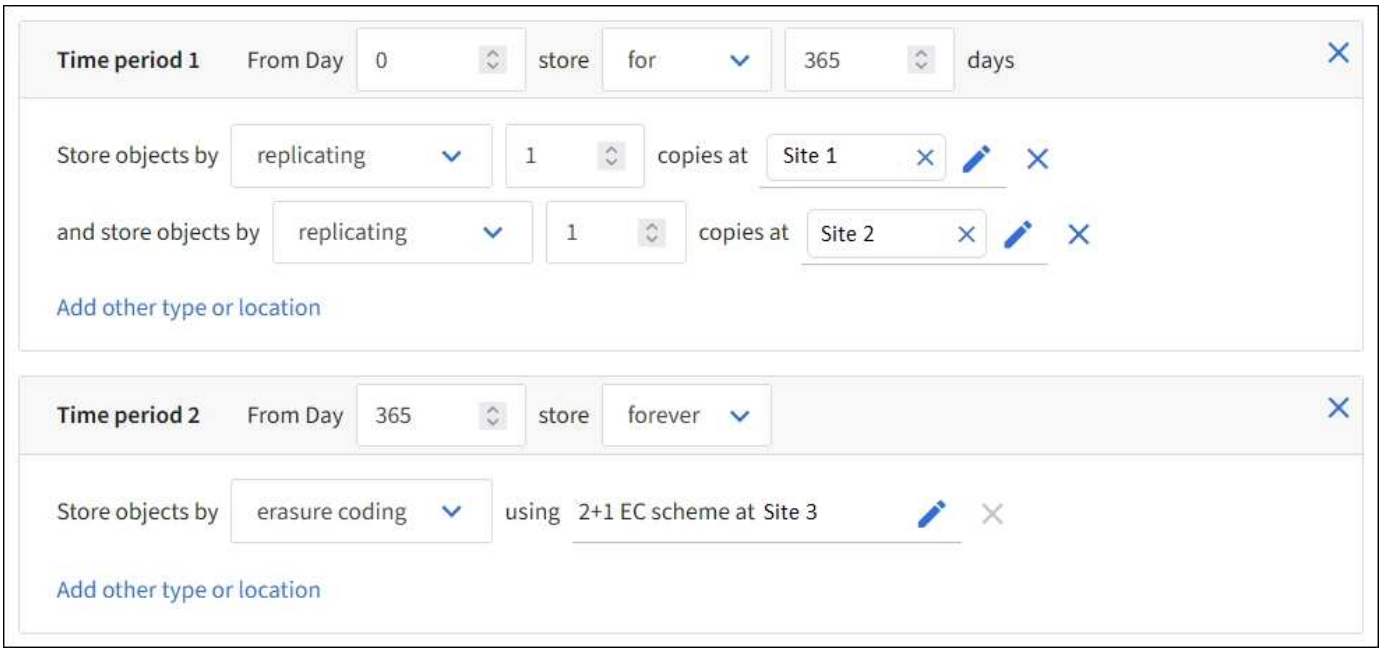
L'étape **Define stages** de l'assistant Create ILM Rule vous permet de définir les instructions de placement qui déterminent la durée de stockage des objets, le type de copies (répliquées ou avec code d'effacement), l'emplacement de stockage et le nombre de copies.

Description de la tâche

Une règle ILM peut inclure une ou plusieurs instructions de placement. Chaque instruction de placement s'applique à une seule période de temps. Lorsque vous utilisez plusieurs instructions, les périodes doivent être contiguës et au moins une instruction doit commencer le jour 0. Les instructions peuvent se poursuivre indéfiniment ou jusqu'à ce que vous n'ayez plus besoin de copies d'objet.

Chaque instruction de placement peut avoir plusieurs lignes si vous voulez créer différents types de copies ou utiliser différents emplacements au cours de cette période.

Dans cet exemple, la règle ILM stocke une copie répliquée sur le site 1 et une copie répliquée sur le site 2 pour la première année. Après un an, une copie avec code d'effacement pour 2+1 est effectuée et enregistrée sur un seul site.



Étapes

1. Pour **temps de référence**, sélectionnez le type de temps à utiliser lors du calcul de l'heure de début d'une instruction de placement.

Option	Description
Temps d'ingestion	Heure à laquelle l'objet a été ingéré.
Heure du dernier accès	Heure à laquelle l'objet a été récupéré pour la dernière fois (lu ou affiché). **Remarque :** pour utiliser cette option, les mises à jour de l'heure du dernier accès doivent être activées pour le compartiment S3 ou le conteneur Swift. Voir "Utiliser l'heure du dernier accès dans les règles ILM".
Heure de création définie par l'utilisateur	Heure spécifiée dans les métadonnées définies par l'utilisateur.
Heure non actuelle	« Noncurrent Time » est automatiquement sélectionné si vous avez sélectionné **Oui** pour la question, « appliquer cette règle aux anciennes versions d'objet uniquement (dans les compartiments S3 avec la gestion des versions activée) ? » po "Étape 1 de l'assistant de création de règles ILM".

> Si vous souhaitez créer une règle conforme, vous devez sélectionner **heure d'ingestion**. Voir "Gestion des objets avec le verrouillage d'objets S3".

2. Dans la section **période et placements**, entrez une heure de début et une durée pour la première période.

   Par exemple, vous pouvez spécifier l'emplacement de stockage des objets pour la première année (*du magasin du jour 0 pendant 365 jours*). Au moins une instruction doit commencer au jour 0.

3. Pour créer des copies répliquées :
   a. Dans la liste déroulante **stocker les objets par**, sélectionnez **répliquer**.
   b. Sélectionnez le nombre de copies à effectuer.

      Un avertissement s'affiche si vous changez le nombre de copies en 1. La règle ILM de création d'une seule copie répliquée pendant toute période met les données à risque de perte permanente. Voir "Pourquoi ne pas utiliser la réplication à copie unique".

      Pour éviter ce risque, effectuez une ou plusieurs des actions suivantes :

      - Augmentez le nombre de copies pour la période.
      - Ajoutez des copies à d'autres pools de stockage ou à un pool de stockage cloud.
      - Sélectionnez **code d'effacement** au lieu de **répliquer**.

        Vous pouvez ignorer cet avertissement en toute sécurité si cette règle crée déjà plusieurs copies pour toutes les périodes.

   c. Dans le champ **copies AT**, sélectionnez les pools de stockage à ajouter.

      Si vous spécifiez un seul pool de stockage, sachez que StorageGRID ne peut stocker qu'une seule copie répliquée d'un objet sur un nœud de stockage donné. Si votre grille comprend trois nœuds de stockage et que vous sélectionnez 4 comme nombre de copies, seules trois copies seront faites—une copie pour chaque nœud de stockage.

      > ⓘ L'alerte **ILM placement inaccessible** est déclenchée pour indiquer que la règle ILM n'a pas pu être complètement appliquée.

      Si vous spécifiez plus d'un pool de stockage, gardez ces règles à l'esprit :

      - Le nombre de copies ne peut pas être supérieur au nombre de pools de stockage.
      - Si le nombre de copies équivaut au nombre de pools de stockage, une copie de l'objet est stockée dans chaque pool de stockage.
      - Si le nombre de copies est inférieur au nombre de pools de stockage, une copie est stockée sur le site d'ingestion, puis le système distribue les copies restantes afin de maintenir un équilibre entre l'utilisation du disque dans les pools, tout en veillant à ce qu'aucun site ne reçoive plus d'une copie d'un objet.
      - Si les pools de stockage se chevauchent (contiennent les mêmes nœuds de stockage), toutes les copies de l'objet peuvent être enregistrées sur un seul site. Par conséquent, ne spécifiez pas le pool de stockage tous les nœuds (StorageGRID 11.6 et versions antérieures) et un autre pool de stockage.
4. Pour créer une copie avec code d'effacement :
   a. Dans la liste déroulante **stocker les objets par**, sélectionnez **code d'effacement**.

      > ⓘ Le codage d'effacement convient mieux aux objets de plus de 1 Mo. N'utilisez pas le code d'effacement pour les objets inférieurs à 200 Ko afin d'éviter la surcharge liée à la gestion de très petits fragments de code d'effacement.

   b. Si vous n'avez pas ajouté de filtre de taille d'objet pour une valeur supérieure à 0.2 Mo, sélectionnez **Précédent** pour revenir à l'étape 1. Ensuite, sélectionnez **Ajouter un filtre avancé** et définissez un filtre **taille de l'objet** sur une valeur supérieure à 0.2 Mo.

c. Sélectionnez le pool de stockage à ajouter et le schéma de code d'effacement à utiliser.

   L'emplacement de stockage d'une copie avec code d'effacement comprend le nom du schéma de code d'effacement, suivi du nom du pool de stockage.

5. Facultatif :
   a. Sélectionnez **Ajouter un autre type ou un autre emplacement** pour créer des copies supplémentaires à différents emplacements.
   b. Sélectionnez **Ajouter une autre période** pour ajouter différentes périodes.

   > Les objets sont automatiquement supprimés à la fin de la période finale, sauf si la période finale se termine par **Forever**.

6. Pour stocker des objets dans un pool de stockage cloud :
   a. Dans la liste déroulante **stocker les objets par**, sélectionnez **répliquer**.
   b. Sélectionnez le champ **copies at**, puis sélectionnez un pool de stockage cloud.

      Lorsque vous utilisez des pools de stockage cloud, gardez ces règles à l'esprit :

      - Vous ne pouvez pas sélectionner plusieurs pools de stockage cloud dans une instruction de placement unique. De même, vous ne pouvez pas sélectionner un pool de stockage cloud et un pool de stockage dans la même instruction de placement.
      - Vous ne pouvez stocker qu'une seule copie d'un objet dans un pool de stockage cloud donné. Un message d'erreur s'affiche si vous définissez **copies** sur 2 ou plus.
      - Vous ne pouvez pas stocker plusieurs copies d'objet simultanément dans un pool de stockage cloud. Un message d'erreur apparaît si plusieurs parutions utilisant un pool de stockage cloud présentent des dates redondantes ou si plusieurs lignes du même placement utilisent un pool de stockage cloud.
      - Vous pouvez stocker un objet dans un pool de stockage cloud simultanément dans lequel celui-ci est stocké sous forme de copies répliquées ou avec code d'effacement dans StorageGRID. Toutefois, vous devez inclure plusieurs lignes dans l'instruction de placement pour la période, afin de pouvoir spécifier le nombre et les types de copies pour chaque emplacement.

7. Dans le diagramme de conservation, confirmez vos instructions de placement.

   Chaque ligne du diagramme indique où et quand les copies d'objet seront placées. La couleur d'une ligne représente le type de copie :

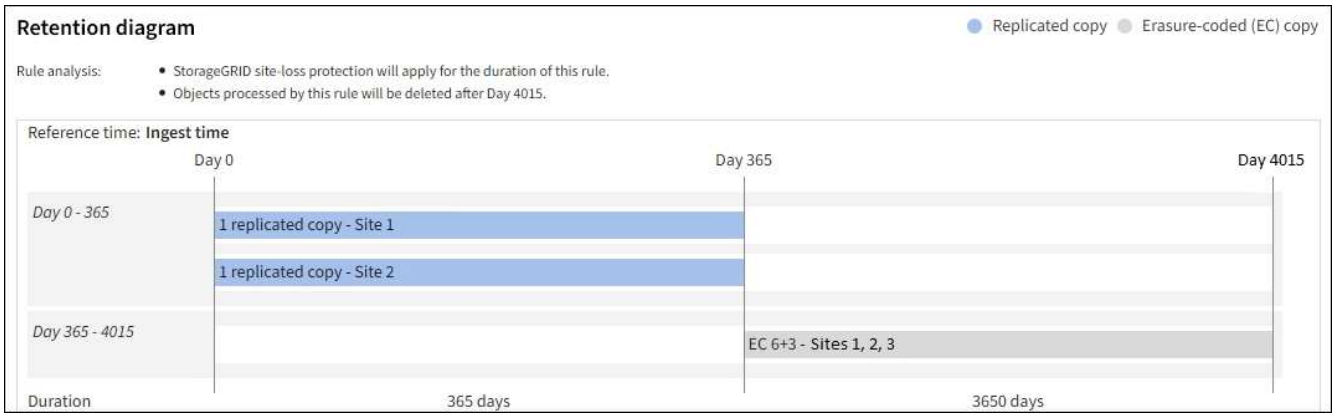
	La copie répliquée
	Copie avec code d'effacement
	Copie du pool de stockage cloud

   Dans cet exemple, la règle ILM stocke une copie répliquée sur le site 1 et une copie répliquée sur le site 2 pour la première année. Au bout d'un an et pendant 10 ans supplémentaires, une copie avec code d'effacement 6+3 sera sauvegardée sur trois sites. Au bout de 11 ans au total, les objets seront supprimés de StorageGRID.

   La section analyse des règles du diagramme de rétention indique :

- La protection contre la perte de site StorageGRID s'appliquera pendant toute la durée de cette règle.
- Les objets traités par cette règle seront supprimés après le jour 4015.

> Voir "Activer la protection contre la perte de site."



8. Sélectionnez **Continuer**. "Étape 3 (Sélectionner le comportement d'ingestion)" De l'assistant de création d'une règle ILM s'affiche.

Utiliser l'heure du dernier accès dans les règles ILM

Vous pouvez utiliser l'heure du dernier accès comme heure de référence dans une règle ILM. Il peut par exemple être nécessaire de conserver les objets qui ont été affichés au cours des trois derniers mois sur les nœuds de stockage locaux tout en déplaçant des objets qui n'ont pas été considérés comme récemment vers un emplacement hors site. Vous pouvez également utiliser l'heure du dernier accès en tant que filtre avancé si vous souhaitez qu'une règle ILM s'applique uniquement aux objets auxquels vous avez accédé pour la dernière fois à une date spécifique.

Description de la tâche

Avant d'utiliser l'heure du dernier accès dans une règle ILM, consultez les considérations suivantes :

- Lorsque vous utilisez l'heure du dernier accès comme heure de référence, sachez que la modification de l'heure du dernier accès d'un objet ne déclenche pas une évaluation ILM immédiate. Les placements de l'objet sont alors évalués et l'objet est déplacé selon les besoins lors de l'évaluation de l'objet par la ILM en arrière-plan. L'accès à l'objet peut prendre deux semaines ou plus.

  Prenez en compte cette latence lors de la création de règles ILM basées sur l'heure du dernier accès et évitez les placements qui utilisent des périodes courtes (moins d'un mois).

- Lorsque vous utilisez l'heure du dernier accès comme filtre avancé ou comme heure de référence, vous devez activer les mises à jour de l'heure du dernier accès pour les compartiments S3. Vous pouvez utiliser le "Gestionnaire de locataires" ou le "API de gestion des locataires".

> Les mises à jour du dernier accès sont toujours activées pour les conteneurs Swift, mais désactivées par défaut pour les compartiments S3.

Notez qu'en activant les mises à jour du dernier accès, vous pouvez réduire les performances, en particulier dans les systèmes dotés d'objets de petite taille. L'impact sur les performances a lieu, car StorageGRID doit mettre à jour les objets avec un nouvel horodatage chaque fois que les objets sont récupérés.

Le tableau suivant indique si l'heure du dernier accès est mise à jour pour tous les objets du compartiment pour différents types de demandes.

Type de demande	Indique si l'heure du dernier accès est mise à jour lorsque les mises à jour de l'heure du dernier accès sont désactivées	Indique si l'heure du dernier accès est mise à jour lorsque les mises à jour de l'heure du dernier accès sont activées
Demande de récupération d'un objet, de sa liste de contrôle d'accès ou de ses métadonnées	Non	Oui.
Demande de mise à jour des métadonnées d'un objet	Oui.	Oui.
Demander de copier un objet d'un compartiment à un autre	• Non, pour la copie source • Oui, pour la copie de destination	• Oui, pour la copie source • Oui, pour la copie de destination
Demander de terminer un téléchargement partitionné	Oui, pour l'objet assemblé	Oui, pour l'objet assemblé

Étape 3 sur 3 : sélectionnez le comportement d'ingestion

L'étape **Sélectionner le comportement d'ingestion** de l'assistant Créer une règle ILM vous permet de choisir la façon dont les objets filtrés par cette règle sont protégés lors de leur ingestion.

Description de la tâche

StorageGRID peut effectuer des copies intermédiaires et mettre en file d'attente les objets pour l'évaluation ILM, ou effectuer des copies pour répondre immédiatement aux instructions de placement de la règle.

Étapes

1. Sélectionner "comportement d'ingestion" à utiliser.

   Pour plus d'informations, voir "Avantages, inconvénients et limites des options d'acquisition".

Vous ne pouvez pas utiliser l'option équilibrée ou stricte si la règle utilise l'un des placements suivants :

- Un pool de stockage cloud dès le premier jour
- Un nœud d'archivage au jour 0
- Un pool de stockage cloud ou un nœud d'archivage lorsque la règle utilise une heure de création définie par l'utilisateur comme heure de référence

Voir "Exemple 5 : règles et règles ILM pour un comportement d'ingestion strict".

2. Sélectionnez **Créer**.

   La règle ILM est créée. La règle ne devient active que lorsqu'elle est ajoutée à un "Politique ILM" et cette règle est activée.

   Pour afficher les détails de la règle, sélectionnez son nom sur la page règles ILM.

Créez une règle ILM par défaut

Avant de créer une règle ILM, vous devez créer une règle par défaut afin de placer tous les objets qui ne correspondent pas à une autre règle de la politique. La règle par défaut ne peut pas utiliser de filtres. Elle doit s'appliquer à tous les locataires, à tous les compartiments et à toutes les versions d'objet.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous disposez d'autorisations d'accès spécifiques.

Description de la tâche

La règle par défaut est la dernière règle évaluée dans une politique ILM. Elle ne peut donc pas utiliser de filtres. Les instructions de placement de la règle par défaut sont appliquées à tous les objets qui ne sont pas associés par une autre règle de la règle.

Dans cet exemple de règle, la première règle s'applique uniquement aux objets appartenant à test-tenant-1. La règle par défaut, qui est la dernière, s'applique aux objets appartenant à tous les autres comptes de tenant.

Lorsque vous créez la règle par défaut, gardez ces exigences à l'esprit :

- La règle par défaut est automatiquement placée en tant que dernière règle de la stratégie.
- La règle par défaut ne peut pas utiliser de filtres de base ou avancés.
- La règle par défaut doit s'appliquer à toutes les versions d'objet.
- La règle par défaut doit créer des copies répliquées.

> N'utilisez pas de règle qui crée des copies avec code d'effacement comme règle par défaut d'une règle. Les règles de code d'effacement doivent utiliser un filtre avancé pour empêcher le codage d'effacement des objets de petite taille.

- En général, la règle par défaut doit conserver les objets à tout jamais.
- Si vous utilisez (ou si vous prévoyez d'activer) le paramètre de verrouillage d'objet S3 global, la règle par défaut de la stratégie active ou proposée doit être conforme.

Étapes

1. Sélectionnez **ILM** > **règles**.
2. Sélectionnez **Créer**.

   L'étape 1 (entrer les détails) de l'assistant de création de règle ILM s'affiche.

3. Entrez un nom unique pour la règle dans le champ **Nom de la règle**.
4. Vous pouvez également saisir une brève description de la règle dans le champ **Description**.
5. Laissez le champ **tenant accounts** vide.

   La règle par défaut doit s'appliquer à tous les comptes de tenant.

6. Laissez la liste déroulante Nom du compartiment comme **correspond à tous**.

   La règle par défaut doit s'appliquer à tous les compartiments S3 et les conteneurs Swift.

7. Conservez la réponse par défaut, **non**, pour la question, ""appliquer cette règle aux anciennes versions d'objet uniquement (dans les compartiments S3 avec gestion des versions activée)?"
8. N'ajoutez pas de filtres avancés.

   La règle par défaut ne peut pas spécifier de filtres.

9. Sélectionnez **Suivant**.

   L'étape 2 (définir les placements) s'affiche.

10. Pour heure de référence, sélectionnez une option.

    Si vous avez conservé la réponse par défaut, **non**, pour la question, ""appliquer cette règle aux anciennes versions d'objet uniquement?"" L'heure non actuelle ne sera pas incluse dans la liste déroulante. La règle par défaut doit appliquer toutes les versions d'objet.

11. Spécifiez les instructions de placement pour la règle par défaut.
    - La règle par défaut doit conserver les objets à tout jamais. Un avertissement s'affiche lorsque vous activez une nouvelle stratégie si la règle par défaut ne conserve pas les objets indéfiniment. Vous devez confirmer que c'est le comportement que vous attendez.
    - La règle par défaut doit créer des copies répliquées.

      > ⓘ N'utilisez pas de règle qui crée des copies avec code d'effacement comme règle par défaut d'une règle. Les règles de code d'effacement doivent inclure le filtre avancé **taille de l'objet (Mo) supérieure à 0.2** pour empêcher le codage d'effacement des objets plus petits.

    - Si vous utilisez (ou si vous avez l'intention d'activer) le paramètre global de verrouillage d'objet S3, la règle par défaut doit être conforme :
      - Les départements IT doivent créer au moins deux copies objet répliquées ou une copie avec code d'effacement.
      - Ces copies doivent exister sur les nœuds de stockage pendant toute la durée de chaque ligne dans les instructions de placement.
      - Les copies d'objet ne peuvent pas être enregistrées dans un pool de stockage cloud.
      - Les copies d'objet ne peuvent pas être enregistrées sur les nœuds d'archivage.
      - Au moins une ligne des instructions de placement doit commencer au jour 0, en utilisant l'heure d'ingestion comme heure de référence.
      - Au moins une ligne des instructions de placement doit être ""permanente".
12. Consultez le diagramme de conservation pour confirmer vos instructions de placement.
13. Sélectionnez **Continuer**.

    L'étape 3 (Sélectionner le comportement d'ingestion) s'affiche.

14. Sélectionnez l'option d'acquisition à utiliser, puis sélectionnez **Créer**.

Création de la règle ILM

Création d'une règle ILM : présentation

Une règle de gestion du cycle de vie des informations (ILM) est un ensemble ordonné de règles ILM qui détermine la façon dont le système StorageGRID gère les données d'objet au fil du temps.

Lorsque vous créez une règle ILM, vous commencez par sélectionner et organiser les règles ILM. Ensuite, vous vérifiez le comportement de votre stratégie proposée en la simulant contre des objets précédemment ingérés. Lorsque vous êtes satisfait du fait que la stratégie proposée fonctionne comme prévu, vous pouvez l'activer pour créer la stratégie active.

> Une règle ILM mal configurée peut entraîner une perte de données irrécupérable. Avant d'activer une politique ILM, examinez attentivement la politique ILM et ses règles ILM, puis simulez la politique ILM. Vérifiez toujours que la politique ILM fonctionne comme prévu.

Règle ILM par défaut

Lorsque vous installez StorageGRID et ajoutez des sites, une règle ILM par défaut est automatiquement créée. Si votre grille contient un site, la stratégie par défaut contient une règle par défaut qui réplique deux copies de chaque objet sur ce site. Si votre grille contient plusieurs sites, la règle par défaut réplique une copie de chaque objet sur chaque site.

Si la stratégie par défaut ne répond pas à vos besoins en stockage, vous pouvez créer vos propres règles et règles. Voir "Définition d'une règle ILM" et "Création d'une politique ILM proposée".

Comment une règle ILM évalue-t-elle les objets ?

La règle ILM active pour votre système StorageGRID permet de contrôler le placement, la durée et la protection des données de tous les objets.

Lorsque des clients enregistrent des objets dans StorageGRID, les objets sont évalués en fonction du jeu ordonné de règles ILM de la politique active, comme suit :

1. Si les filtres de la première règle de la règle correspondent à un objet, celui-ci est ingéré conformément au comportement d'ingestion de cette règle et stocké conformément aux instructions de placement de cette règle.
2. Si les filtres de la première règle ne correspondent pas à l'objet, l'objet est évalué par rapport à chaque règle ultérieure de la règle jusqu'à ce qu'une correspondance soit établie.
3. Si aucune règle ne correspond à un objet, les instructions de comportement d'ingestion et de placement de la règle par défaut de cette règle sont appliquées. La règle par défaut est la dernière règle d'une stratégie. La règle par défaut doit s'appliquer à tous les locataires, à tous les compartiments et à toutes les versions d'objet et ne peut pas utiliser de filtres avancés.

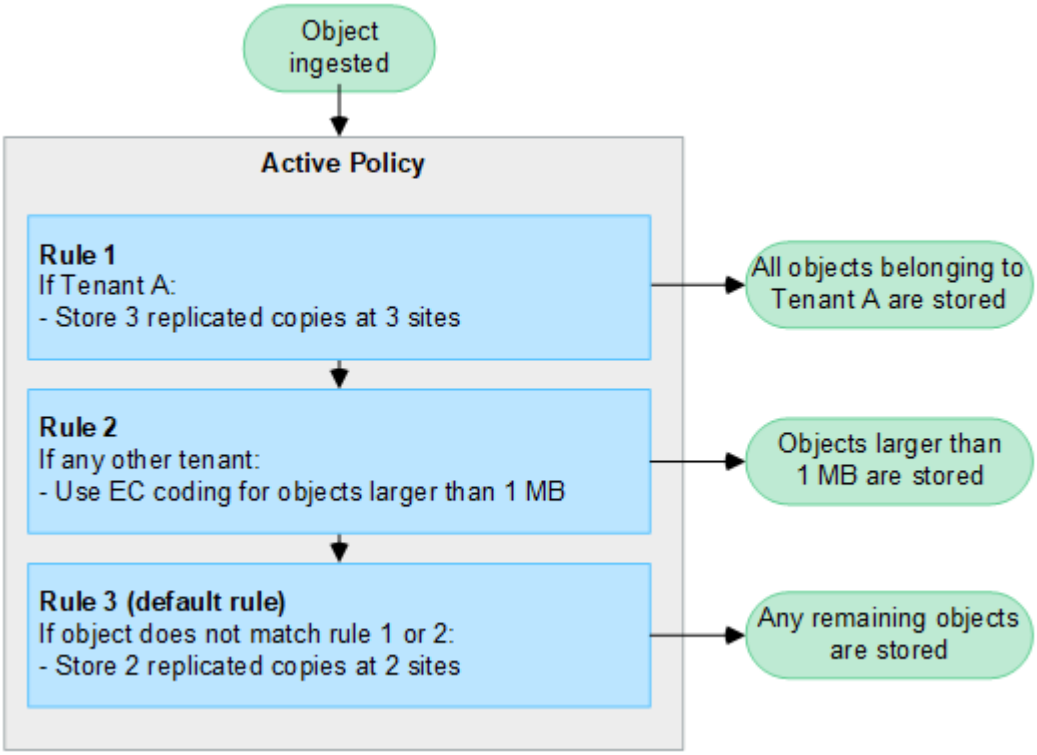
Exemple de règle ILM

À titre d'exemple, une politique ILM peut contenir trois règles ILM pour spécifier :

- **Règle 1 : copies répliquées pour le locataire A**
  - Faites correspondre tous les objets appartenant au locataire A.
  - Stockez ces objets sous forme de trois copies répliquées sur trois sites.

- Les objets appartenant à d'autres locataires ne correspondent pas à la règle 1, ils sont donc évalués par rapport à la règle 2.

- **Règle 2 : code d'effacement pour les objets supérieurs à 1 Mo**
  - Faites correspondre tous les objets d'autres locataires, mais uniquement s'ils sont supérieurs à 1 Mo. Ces objets plus volumineux sont stockés au moyen d'un code d'effacement de 6+3 sur trois sites.
  - Ne correspond pas aux objets de 1 Mo ou moins, ces objets sont donc évalués par rapport à la règle 3.
- **Règle 3 : 2 copies 2 centres de données** (par défaut)
  - Est la dernière règle et la règle par défaut de la règle. N'utilise pas de filtres.
  - Faites deux copies répliquées de tous les objets qui ne correspondent pas à la règle 1 ou à la règle 2 (objets qui n'appartiennent pas au locataire A de 1 Mo ou moins).



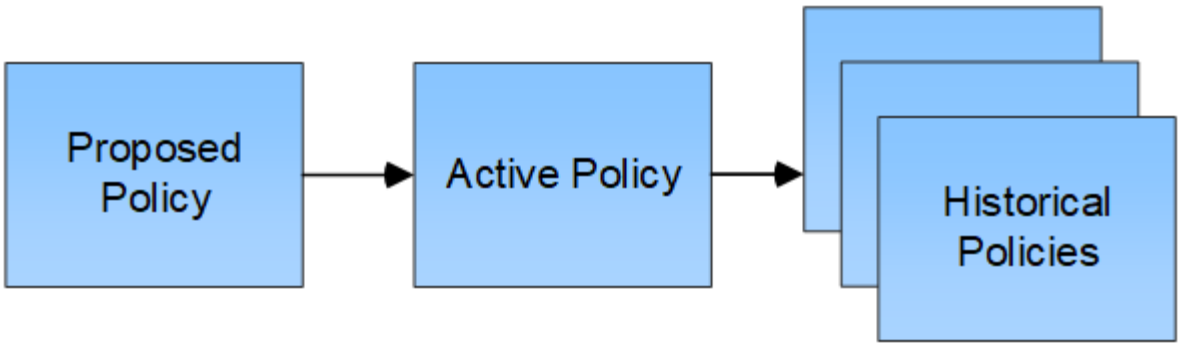
Quelles sont les politiques proposées, actives et historiques?

Chaque système StorageGRID doit disposer d'une règle ILM active. Un système StorageGRID peut également avoir une proposition de règle ILM et tout nombre de règles historiques.

Lorsque vous créez une règle ILM, vous créez une proposition de règle en sélectionnant une ou plusieurs règles ILM et en les organisant dans un ordre spécifique. Après avoir simulé la stratégie proposée pour confirmer son comportement, vous l'activez pour créer la stratégie active.

Lorsque vous activez une nouvelle règle ILM, StorageGRID utilise cette règle pour gérer tous les objets, y compris les objets existants et les objets récemment ingérées. Les objets existants peuvent être déplacés vers de nouveaux emplacements lorsque les règles ILM de la nouvelle règle sont mises en œuvre.

L'activation de la stratégie proposée fait de la stratégie précédemment active une stratégie historique. Impossible de supprimer les règles ILM historiques.



Facteurs à prendre en compte lors de la création d'une règle ILM

- Utilisez uniquement la règle de base 2 copies fournie par le système dans les systèmes de test. Pour StorageGRID 11.6 et les versions antérieures, la règle Make 2 copies de cette règle utilise le pool de stockage All Storage Nodes, qui contient tous les sites. Si votre système StorageGRID dispose de plusieurs sites, il est possible de placer deux copies d'un objet sur le même site.

> Le pool de stockage tous les nœuds de stockage est automatiquement créé lors de l'installation de StorageGRID 11.6 et des versions antérieures. Si vous effectuez une mise à niveau vers une version ultérieure de StorageGRID, le pool tous les nœuds de stockage existera toujours. Si vous installez StorageGRID 11.7 ou une version ultérieure en tant que nouvelle installation, le pool tous les nœuds de stockage n'est pas créé.

- Lors de la conception d'une nouvelle politique, tenez compte de tous les différents types d'objets pouvant être ingérés dans votre grille. Assurez-vous que la stratégie inclut des règles pour correspondre et placer ces objets selon les besoins.
- Privilégiez la simplicité des règles ILM. Cela permet d'éviter les situations dangereuses dans lesquelles les données d'objet ne sont pas protégées comme prévu lorsque des modifications sont apportées au système StorageGRID au fil du temps.
- Assurez-vous que les règles de la police sont dans le bon ordre. Lorsque la stratégie est activée, les objets nouveaux et existants sont évalués par les règles dans l'ordre indiqué, à partir du haut. Par exemple, si la première règle d'une règle correspond à un objet, cet objet ne sera évalué par aucune autre règle.
- La dernière règle de chaque politique ILM est la règle ILM par défaut, qui ne peut utiliser aucun filtre. Si un objet n'a pas été mis en correspondance par une autre règle, la règle par défaut contrôle l'emplacement de cet objet et la durée de conservation.
- Avant d'activer une nouvelle stratégie, vérifiez les modifications apportées par la stratégie au placement des objets existants. La modification de l'emplacement d'un objet existant peut entraîner des problèmes de ressources temporaires lorsque les nouveaux placements sont évalués et implémentés.

Création d'une règle ILM proposée

Vous pouvez créer de zéro une politique ILM proposée ou cloner la règle active actuelle si vous souhaitez commencer avec le même ensemble de règles.

Avant de créer votre propre stratégie, vérifiez que "Règle ILM par défaut" ne répond pas à vos besoins en stockage.

Si le "Le paramètre de verrouillage d'objet S3 global a été activé"Vous devez vous assurer que la règle ILM est conforme aux exigences des compartiments pour lesquels le verrouillage objet S3 est activé. Dans cette section, suivez les instructions qui mentionnent que le verrouillage d'objet S3 est activé.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous avez le "autorisations d'accès requises".
- Vous avez "Création de règles ILM" Selon que le verrouillage objet S3 est activé ou non.

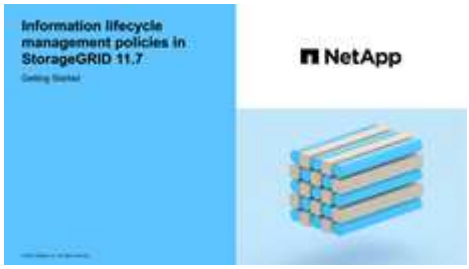
Verrouillage objet S3 non activé

- Vous avez "Création des règles ILM" vous souhaitez ajouter à la stratégie proposée. Si nécessaire, vous pouvez enregistrer une stratégie proposée, créer des règles supplémentaires, puis modifier la stratégie proposée pour ajouter les nouvelles règles.
- Vous avez "Une règle ILM par défaut a été créée" qui ne contient aucun filtre.

Verrouillage objet S3 activé

- Le "Le paramètre de verrouillage d'objet S3 global est déjà activé" Pour le système StorageGRID.
- Vous avez "Vous avez créé des règles ILM conformes et non conformes" vous souhaitez ajouter à la stratégie proposée. Si nécessaire, vous pouvez enregistrer une stratégie proposée, créer des règles supplémentaires, puis modifier la stratégie proposée pour ajouter les nouvelles règles.
- Vous avez "Une règle ILM par défaut a été créée" de la règle qui est conforme.

- Vous pouvez également regarder la vidéo : "Vidéo : politiques de gestion du cycle de vie de l'information dans StorageGRID 11.7"



Voir aussi "Création d'une règle ILM : présentation".

Description de la tâche

Les raisons principales de la création d'une politique ILM sont les suivantes :

- Vous avez ajouté un site et devez utiliser de nouvelles règles ILM pour placer les objets sur ce site.
- Vous désaffectez un site, vous devez supprimer toutes les règles ILM qui font référence au site.
- Vous avez ajouté un nouveau locataire qui présente des exigences spéciales de protection des données.
- Vous avez commencé à utiliser un pool de stockage cloud.

Utilisez uniquement la règle de base 2 copies fournie par le système dans les systèmes de test. Pour StorageGRID 11.6 et les versions antérieures, la règle par défaut de cette règle utilise le pool de stockage tous les nœuds de stockage, qui contient tous les sites. Si votre système StorageGRID dispose de plusieurs sites, il est possible de placer deux copies d'un objet sur le même site.

Étapes

1. Sélectionnez **ILM** > **stratégies**.

   Si le paramètre global S3 Object Lock est activé, la page des règles ILM indique les règles ILM compatibles.

2. Déterminez le mode de création de la règle ILM proposée. +

Commencez à zéro

1. Si une stratégie ILM proposée existe actuellement, sélectionnez **politique proposée** > **actions** > **Supprimer**.

   Vous ne pouvez pas créer de nouvelle stratégie proposée si une stratégie proposée existe déjà.

2. Sélectionnez **Créer la politique proposée** > **Créer une nouvelle politique**.

Commencez par les règles de la stratégie active

1. Si une stratégie ILM proposée existe actuellement, sélectionnez **politique proposée** > **actions** > **Supprimer**.

   Vous ne pouvez pas cloner la règle active si une règle proposée existe déjà.

2. Sélectionnez **Créer la stratégie proposée** > **Cloner la stratégie active**.

Modifier la stratégie proposée existante

1. Sélectionnez **politique proposée** > **actions** > **Modifier**.

1. Dans le champ **nom de la stratégie proposée**, entrez un nom unique pour la stratégie proposée.
2. Dans le champ **motif du changement**, entrez la raison pour laquelle vous créez une nouvelle stratégie proposée.
3. Pour ajouter des règles à la stratégie, sélectionnez **Sélectionner des règles**. Sélectionnez un nom de règle pour afficher les paramètres de cette règle.

   Périodiquement, la liste des règles est automatiquement mise à jour pour refléter les ajouts ou les suppressions. Si une règle est supprimée après sa sélection, un message d'erreur s'affiche.

   Si vous clonez une règle :

   - Vous sélectionnez les règles utilisées par la règle de clonage.
   - Si la stratégie que vous utilisez est une règle sans filtre qui n'était pas la règle par défaut, vous êtes invité à supprimer toutes ces règles, sauf une.
   - Si la règle par défaut utilise un filtre, vous êtes invité à sélectionner une nouvelle règle par défaut.

◦ Si la règle par défaut n'était pas la dernière, vous pouvez la déplacer vers la fin de la nouvelle règle.

Verrouillage objet S3 non activé

1. Sélectionnez une règle par défaut pour la stratégie proposée. Pour créer une nouvelle règle par défaut, sélectionnez **page règles ILM**.

   La règle par défaut s'applique aux objets qui ne correspondent pas à une autre règle de la stratégie. La règle par défaut ne peut pas utiliser de filtres et est toujours évaluée en dernier.

   > N'utilisez pas la règle Make 2 copies comme règle par défaut pour une stratégie. La règle Make 2 copies utilise un pool de stockage unique, tous les nœuds de stockage, qui contient tous les sites. Si votre système StorageGRID dispose de plusieurs sites, il est possible de placer deux copies d'un objet sur le même site.

Verrouillage objet S3 activé

1. Sélectionnez une règle par défaut pour la stratégie proposée. Pour créer une nouvelle règle par défaut, sélectionnez **page règles ILM**.

   La liste des règles contient uniquement les règles qui sont conformes et n'utilisent aucun filtre.

   > N'utilisez pas la règle Make 2 copies comme règle par défaut pour une stratégie. La règle Make 2 copies utilise un pool de stockage unique, tous les nœuds de stockage, qui contient tous les sites. Si vous utilisez cette règle, plusieurs copies d'un objet peuvent être placées sur le même site.

2. Si vous avez besoin d'une règle « par défaut » différente pour les objets dans des compartiments S3 non conformes, sélectionnez **inclure une règle sans filtres pour les compartiments S3 non conformes**, et sélectionnez une règle non conforme qui n'utilise pas de filtre.

   Par exemple, vous pouvez utiliser un pool de stockage cloud pour stocker des objets dans des compartiments pour lesquels le verrouillage d'objet S3 n'est pas activé.

   > Vous ne pouvez sélectionner qu'une règle non conforme qui n'utilise pas de filtre.

Voir aussi "Exemple 7 : règle ILM conforme pour le verrouillage d'objet S3".

1. Lorsque vous avez terminé de sélectionner la règle par défaut, sélectionnez **Continuer**.
2. Pour l'étape autres règles, sélectionnez toutes les autres règles que vous souhaitez ajouter à la stratégie. Ces règles utilisent au moins un filtre (compte de locataire, nom de compartiment, filtre avancé ou heure de référence non courante). Sélectionnez ensuite **Sélectionner**.

   La fenêtre Créer une stratégie proposée répertorie maintenant les règles que vous avez sélectionnées. La règle par défaut est à la fin, avec les autres règles au-dessus.

   Si le verrouillage d'objet S3 est activé et que vous avez également sélectionné une règle « par défaut » non conforme, cette règle est ajoutée en tant que règle de second en dernier dans la stratégie.

> Un avertissement s'affiche si une règle ne conserve pas les objets indéfiniment. Lorsque vous activez cette règle, vous devez confirmer que vous souhaitez que StorageGRID supprime des objets lorsque les instructions de placement pour la règle par défaut s'affichent (à moins qu'un cycle de vie de compartiment ne conserve les objets pendant une période plus longue).

3. Faites glisser les lignes des règles non par défaut pour déterminer l'ordre dans lequel ces règles seront évaluées.

   Vous ne pouvez pas déplacer la règle par défaut. Si le verrouillage d'objet S3 est activé, vous ne pouvez pas déplacer la règle « par défaut » non conforme si une règle a été sélectionnée.

   > Vous devez confirmer que les règles ILM sont dans l'ordre correct. Lorsque la stratégie est activée, les objets nouveaux et existants sont évalués par les règles dans l'ordre indiqué, à partir du haut.

4. Si nécessaire, sélectionnez **Sélectionner des règles** pour ajouter ou supprimer des règles.
5. Lorsque vous avez terminé, sélectionnez **Enregistrer**.
6. Accédez à "Simulation d'une règle ILM". Vous devez toujours simuler une stratégie proposée avant de l'activer pour vous assurer qu'elle fonctionne comme prévu.

Simulation d'une règle ILM

Simulez une stratégie proposée sur des objets test avant d'activer la stratégie et de l'appliquer à vos données de production. La fenêtre de simulation fournit un environnement autonome qui permet de tester les stratégies avant leur activation et leur application aux données de l'environnement de production.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous avez le "autorisations d'accès requises".
- Vous connaissez le compartiment S3/clé-objet ou le conteneur Swift/nom-objet pour chaque objet à tester.

Description de la tâche

Sélectionnez soigneusement les objets que vous souhaitez tester la stratégie proposée. Pour simuler une stratégie en profondeur, vous devez tester au moins un objet pour chaque filtre de chaque règle.

Par exemple, si une règle inclut une règle permettant de faire correspondre des objets dans le compartiment A et une autre règle pour faire correspondre des objets dans le compartiment B, vous devez sélectionner au moins un objet du compartiment A et un objet du compartiment B pour tester la règle en profondeur. Vous devez également sélectionner au moins un objet d'un autre compartiment pour tester la règle par défaut.

Lors de la simulation d'une règle, les considérations suivantes s'appliquent :

- Après avoir apporté des modifications à une police, enregistrez la stratégie proposée. Ensuite, simulez le comportement de la stratégie proposée enregistrée.
- Lorsque vous simulez une règle, les règles ILM de la règle filtrent les objets test. Vous pouvez ainsi voir la règle appliquée à chaque objet. Cependant, aucune copie d'objet n'est effectuée et aucun objet n'est placé. L'exécution d'une simulation ne modifie en aucune façon vos données, règles ou règles.

- La fenêtre simuler la stratégie proposée conserve les objets que vous avez testés jusqu'à ce que vous sélectionniez **Effacer tout** ou l'icône Supprimer ✕ Pour chaque objet de la liste des résultats de simulation.
- Simulation renvoie le nom de la règle lettrée. Pour déterminer quel pool de stockage ou profil de code d'effacement est en vigueur, sélectionnez le nom de la règle pour accéder à la page de détails de la règle, où vous pouvez afficher le diagramme de rétention et d'autres détails sur la règle.
- Si la gestion des versions S3 est activée, vous pouvez entrer l'ID de version de la version de l'objet que vous souhaitez utiliser pour la simulation.

Étapes

1. "Créez une règle proposée".
2. Utilisation d'un client S3, Swift ou "Console S3 expérimentale", Disponible dans le Gestionnaire de locataires pour chaque locataire, ingèrent les objets requis pour tester chaque règle.
3. Sur la page ILM policy, onglet policy proposée, sélectionnez **Simulate**.
4. Dans le champ **Object**, entrez S3 `bucket/object-key` Ou le Swift `container/object-name` pour un objet test. Par exemple : `bucket-01/filename.png`.
5. Si vous le souhaitez, entrez un ID de version pour l'objet dans le champ **ID de version**.
6. Sélectionnez **simuler**.
7. Dans la section Résultats de simulation, vérifiez que chaque objet a été mis en correspondance avec la règle correcte.

Exemple 1 : vérifiez les règles lors de la simulation d'une règle ILM proposée

Cet exemple décrit comment vérifier les règles lors de la simulation d'une stratégie proposée.

Dans cet exemple, la **exemple de règle ILM** est simulée contre les objets ingérés dans deux compartiments. La politique comprend trois règles, comme suit :

- La première règle, **deux copies, deux ans pour le compartiment a**, ne s'applique qu'aux objets du compartiment a.
- La deuxième règle, **objets EC > 1 Mo**, s'applique à tous les compartiments, mais aux filtres sur des objets supérieurs à 1 Mo.
- La troisième règle, **deux copies, deux centres de données**, est la règle par défaut. Il n'inclut aucun filtre et n'utilise pas l'heure de référence non actuelle.

Après avoir simulé la règle, confirmez que chaque objet a été mis en correspondance avec la règle appropriée.

Dans cet exemple :

- `bucket-a/bucket-a object.pdf` correspondance correcte de la première règle, qui filtre les objets dans `bucket-a`.
- `bucket-b/test object greater than 1 MB.pdf` est dans `bucket-b`, il ne correspond donc pas à la première règle. Au lieu de cela, il a été correctement mis en correspondance par la deuxième règle, qui filtre les objets de plus de 1 Mo.
- `bucket-b/test object less than 1 MB.pdf` ne correspond pas aux filtres des deux premières règles. il sera donc placé par la règle par défaut, qui ne comprend aucun filtre.

Exemple 2 : règles de réorganisation lors de la simulation d'une règle ILM proposée

Cet exemple montre comment vous pouvez réorganiser les règles pour modifier les résultats lors de la simulation d'une règle.

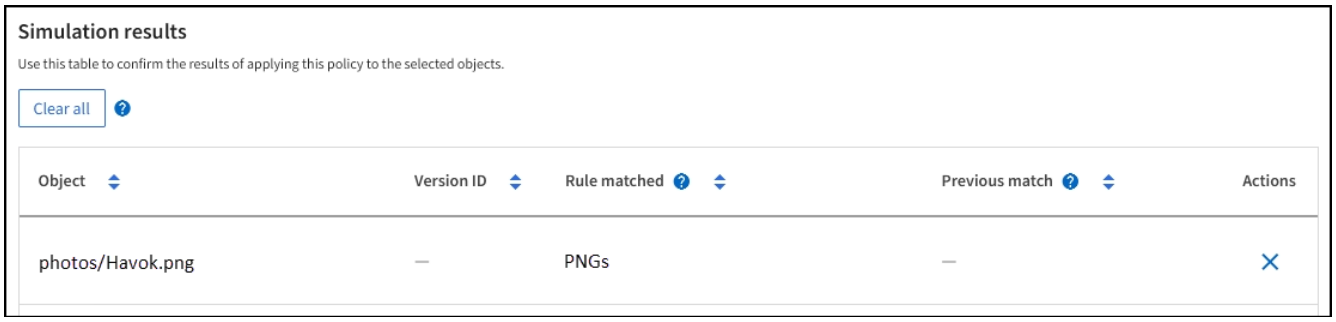
Dans cet exemple, la politique **Demo** est en cours de simulation. Cette règle, qui vise à trouver des objets qui ont des métadonnées utilisateur série=x-men, comprend trois règles, comme suit :

- La première règle, **PNG**, filtre les noms de clé qui se terminent dans `.png`.
- La deuxième règle, **X-men**, ne s'applique qu'aux objets pour le locataire A et les filtres pour `series=x-men` métadonnées d'utilisateur.
- La dernière règle, **deux copies deux centres de données**, est la règle par défaut, qui correspond à tous les objets qui ne correspondent pas aux deux premières règles.

Étapes

1. Après avoir ajouté les règles et enregistré la stratégie, sélectionnez **Simulate**.
2. Dans le champ **objet**, saisissez la clé de rubrique/objet S3 ou le nom-objet/conteneur Swift pour un objet test, puis sélectionnez **Simulate**.

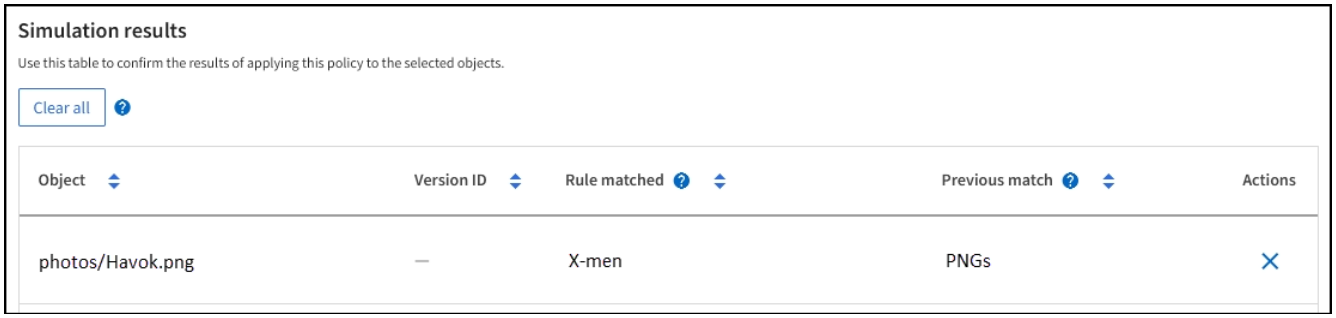
   Les résultats de la simulation s'affichent, indiquant que l' `Havok.png` L'objet a été associé à la règle **PNG**.



Cependant, `Havok.png` Était destiné à tester la règle **X-MEN**.

3. Pour résoudre le problème, réorganisez les règles.
   a. Sélectionnez **Terminer** pour fermer la fenêtre simuler une politique ILM.
   b. Sélectionnez **actions** > **Modifier** pour modifier la stratégie.
   c. Faites glisser la règle **X-men** en haut de la liste.
   d. Sélectionnez **Enregistrer**.
4. Sélectionnez **simuler**.

   Les objets que vous avez testés précédemment sont réévalués par rapport à la règle mise à jour et les nouveaux résultats de simulation sont affichés. Dans l'exemple, la colonne correspondance de règle indique que l' `Havok.png` L'objet correspond désormais à la règle des métadonnées X-men, comme prévu. La colonne comparaison précédente indique que la règle des PNG correspond à l'objet dans la simulation précédente.

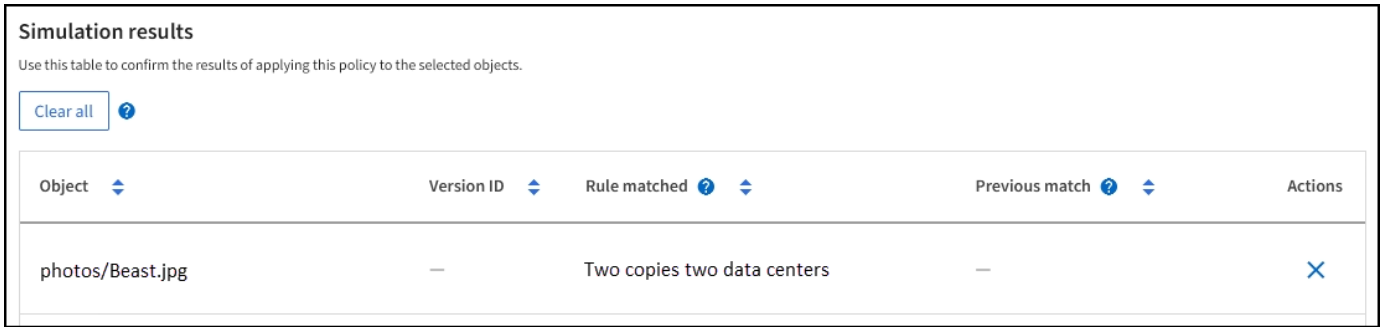


Si vous restez dans l'onglet Stratégie proposée, vous pouvez simuler à nouveau une stratégie après avoir apporté des modifications sans avoir à saisir à nouveau les noms des objets test.

Exemple 3 : corriger une règle lors de la simulation d'une politique ILM proposée

Cet exemple montre comment simuler une stratégie, corriger une règle dans la règle et poursuivre la simulation.

Dans cet exemple, la politique **Demo** est en cours de simulation. Cette politique a pour but de trouver des objets qui ont `series=x-men` métadonnées d'utilisateur. Toutefois, des résultats inattendus se sont produits lors de la simulation de cette politique contre le `Beast.jpg` objet. Au lieu de faire correspondre la règle de métadonnées X-Men, l'objet correspond à la règle par défaut, deux copies de deux centres de données.



Lorsqu'un objet test n'est pas associé à la règle attendue de la stratégie, vous devez examiner chaque règle de la stratégie et corriger les erreurs éventuelles.

Étapes

1. Sélectionnez **Terminer** pour fermer la boîte de dialogue simuler la stratégie. Dans l'onglet Stratégie proposée, sélectionnez **diagramme de rétention**. Sélectionnez ensuite **développer tout** ou **Afficher les détails** pour chaque règle selon les besoins.
2. Vérifiez le compte de locataire de la règle, l'heure de référence et les critères de filtrage.

   Supposons, par exemple, que les métadonnées de la règle X-MEN aient été saisies sous la forme « x-men01 » au lieu de « x-MEN ».

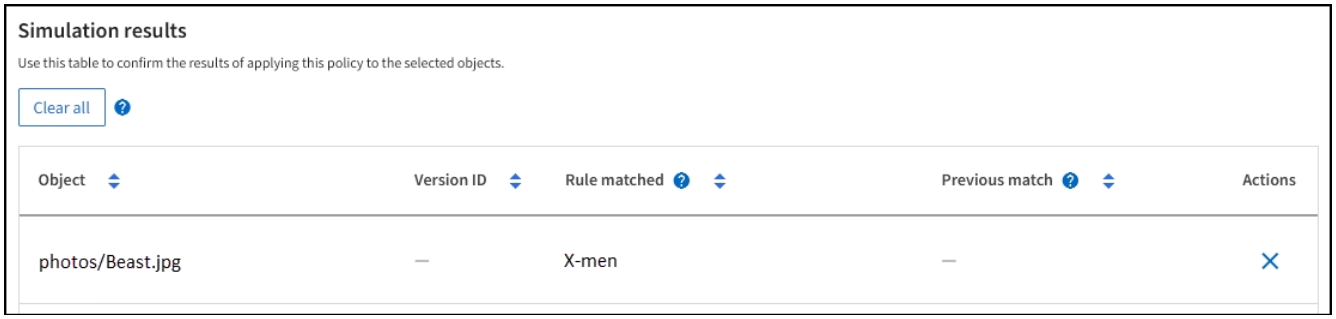
3. Pour résoudre l'erreur, corrigez la règle comme suit :
   - Si la règle fait partie de la stratégie proposée, vous pouvez soit cloner la règle, soit supprimer la règle de la stratégie, puis la modifier.
   - Si la règle fait partie de la stratégie active, vous devez cloner la règle. Vous ne pouvez pas modifier ou supprimer une règle de la stratégie active.

Option	Étapes
Clonez la règle	i. Sélectionnez **ILM** > **règles**. ii. Sélectionnez la règle incorrecte et sélectionnez **Clone**. iii. Entrez un nom pour la nouvelle règle, modifiez les informations incorrectes et sélectionnez **Create**. iv. Sélectionnez **ILM** > **politiques** > **politique proposée**. v. Sélectionnez **actions** > **Modifier**. vi. Sélectionnez **Sélectionner les règles**, puis **Continuer** pour accepter la même règle par défaut. vii. À l'étape Sélectionner autres règles, cochez la case de la nouvelle règle, décochez la case de la règle d'origine et sélectionnez **Sélectionner**. viii. Si nécessaire, réorganisez les règles en faisant glisser la nouvelle règle vers l'emplacement correct. ix. Sélectionnez **Enregistrer**.

Option	Étapes
Modifiez la règle	i. Sélectionnez **ILM** > **stratégies** > **stratégie proposée** et supprimez la règle que vous souhaitez modifier. ii. Sélectionnez **ILM** > **règles**. iii. Sélectionnez la règle à modifier et sélectionnez **Modifier**. Ou cochez la case de la règle et sélectionnez **actions** > **Modifier**. iv. Modifiez les informations incorrectes pour chaque partie de l'assistant, puis sélectionnez **mettre à jour**. v. Sélectionnez **ILM** > **politiques** > **politique proposée**. vi. Sélectionnez **actions** > **Modifier**. vii. Sélectionnez **Sélectionner les règles**, puis **Continuer** pour accepter la même règle par défaut. viii. Dans la boîte de dialogue Sélectionner d'autres règles, cochez la case correspondant à la règle corrigée, sélectionnez **Sélectionner**, puis **Enregistrer**. ix. Faites glisser les lignes des règles non par défaut pour déterminer l'ordre dans lequel ces règles seront évaluées.

4. Exécuter à nouveau la simulation.

   Dans cet exemple, la règle X-men corrigée correspond maintenant à l' `Beast.jpg` objet basé sur `series=x-men` les métadonnées d'utilisateur, comme prévu.



Activation de la règle ILM

Une fois que vous avez ajouté des règles ILM à une politique ILM proposée, que vous simulez la règle et que vous la confirmez, vous êtes prêt à activer la règle proposée.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous avez "autorisations d'accès spécifiques".
- Vous avez enregistré et simulé la règle ILM proposée.

Les erreurs de la règle ILM peuvent entraîner des pertes de données irrécupérables. Examinez attentivement et simulez la stratégie avant de l'activer pour confirmer qu'elle fonctionnera comme prévu. + lorsque vous activez une nouvelle règle ILM, StorageGRID l'utilise pour gérer tous les objets, y compris les objets existants et les objets nouvellement acquis. Avant d'activer une nouvelle règle ILM, vérifiez toutes les modifications du placement des objets répliqués et soumis au code d'effacement. La modification de l'emplacement d'un objet existant peut entraîner des problèmes de ressources temporaires lorsque les nouveaux placements sont évalués et implémentés.

Description de la tâche

Lorsque vous activez une règle ILM, le système distribue la nouvelle règle à tous les nœuds. Cependant, la nouvelle règle active peut ne pas être appliquée tant que tous les nœuds du grid ne sont pas disponibles pour recevoir la nouvelle règle. Dans certains cas, le système attend d'implémenter une nouvelle stratégie active pour s'assurer que les objets de grille ne sont pas accidentellement supprimés.

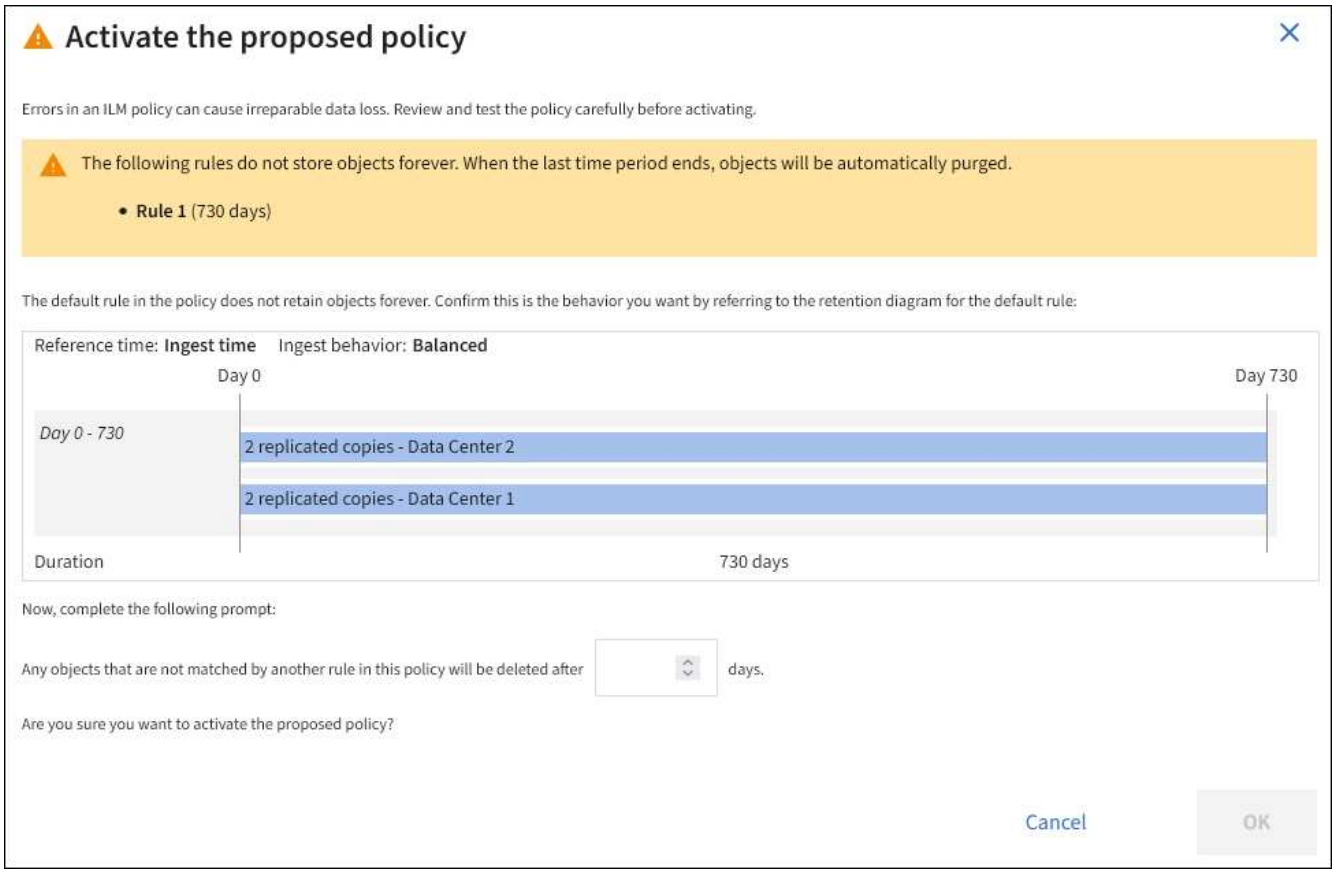
- Si vous apportez des modifications de règles qui augmentent la redondance ou la durabilité des données, ces modifications sont immédiatement mises en œuvre. Par exemple, si vous activez une nouvelle règle incluant une règle à trois copies au lieu d'une règle à deux copies, cette règle sera immédiatement implémentée car elle accroît la redondance des données.
- Si vous apportez des modifications à des règles susceptibles de réduire la redondance ou la durabilité des données, ces modifications ne seront pas implémentées tant que tous les nœuds de la grille ne sont pas disponibles. Par exemple, si vous activez une nouvelle stratégie qui utilise une règle à deux copies au lieu d'une règle à trois copies, la nouvelle stratégie s'affiche dans l'onglet Stratégie active, mais elle ne prend effet que lorsque tous les nœuds sont en ligne et disponibles.

Étapes

1. Lorsque vous êtes prêt à activer une stratégie proposée, sélectionnez **règles ILM** > **stratégie proposée**, puis **activer**.

   Un message d'avertissement s'affiche, vous invitant à confirmer que vous souhaitez activer la stratégie proposée.

   Une invite apparaît dans le message d'avertissement si la règle par défaut ne conserve pas les objets indéfiniment. Dans cet exemple, le diagramme de rétention montre que la règle par défaut supprimera les objets au bout de 730 jours (2 ans). Vous devez taper **730** dans la zone de texte pour confirmer que tous les objets qui ne correspondent pas à une autre règle de la stratégie seront supprimés de StorageGRID après 730 jours.



2. Sélectionnez **OK**.

Résultat

Lorsqu'une nouvelle règle ILM a été activée :

- La stratégie s'affiche dans l'onglet règle active. La date de début indique la date et l'heure d'activation de la police.
- La règle de gestion précédemment active apparaît dans l'onglet Historique des règles. Les entrées de date de début et de date de fin indiquent quand la police est devenue active et quand elle n'était plus en vigueur.

Informations associées

"Exemple 6 : modification d'une règle ILM"

Vérification d'une règle ILM avec la recherche de métadonnées d'objet

Une fois la règle ILM activée, vous devez ingérer des objets test représentatifs dans le système StorageGRID. Vous devez ensuite effectuer une recherche de métadonnées d'objet pour confirmer que les copies sont effectuées comme prévu et placées aux emplacements appropriés.

Avant de commencer

- Vous disposez d'un identificateur d'objet, qui peut être l'un des suivants :
  - **UUID** : identifiant unique universel de l'objet. Saisissez l'UUID en majuscules.
  - **CBID** : identifiant unique de l'objet dans StorageGRID. Vous pouvez obtenir le CBID d'un objet à partir du journal d'audit. Saisissez le CBID en majuscules.

- **Compartiment S3 et clé d'objet** : lors de l'ingestion d'un objet via l'interface S3, l'application client utilise une combinaison de compartiments et de clés d'objet pour stocker et identifier l'objet. Si le compartiment S3 est avec version et que vous souhaitez rechercher une version spécifique d'un objet S3 à l'aide du compartiment et de la clé d'objet, vous disposez de l'ID **version**.
- **Conteneur Swift et nom d'objet** : lorsqu'un objet est ingéré via l'interface Swift, l'application cliente utilise une combinaison de conteneur et de nom d'objet pour stocker et identifier l'objet.

Étapes

1. Ingestion de l'objet.
2. Sélectionnez **ILM** > **Object metadata Lookup**.
3. Saisissez l'identifiant de l'objet dans le champ **Identificateur**. Vous pouvez entrer un UUID, un CBID, un compartiment S3/une clé-objet ou un nom-objet/conteneur Swift.
4. Si vous le souhaitez, entrez un ID de version pour l'objet (S3 uniquement).

5. Sélectionnez **rechercher**.

   Les résultats de la recherche de métadonnées d'objet s'affichent. Cette page répertorie les types d'informations suivants :

   - Les métadonnées du système, y compris l'ID d'objet (UUID), le nom de l'objet, le nom du conteneur, le nom ou l'ID du compte de locataire, la taille logique de l'objet, la date et l'heure de la première création de l'objet, ainsi que la date et l'heure de la dernière modification de l'objet.
   - Toutes les paires de clé-valeur de métadonnées utilisateur personnalisées associées à l'objet.
   - Pour les objets S3, toutes les paires de clé-valeur de balise d'objet associées à l'objet.
   - Pour les copies d'objet répliquées, emplacement de stockage actuel de chaque copie.
   - Pour les copies d'objets avec code d'effacement, l'emplacement de stockage actuel de chaque fragment.
   - Pour les copies d'objet dans Cloud Storage Pool, l'emplacement de l'objet, notamment le nom du compartiment externe et l'identifiant unique de l'objet.
   - Pour les objets segmentés et les objets multisegments, une liste de segments d'objet, y compris les identificateurs de segments et la taille des données. Pour les objets de plus de 100 segments, seuls les 100 premiers segments sont affichés.
   - Toutes les métadonnées d'objet dans le format de stockage interne non traité. Ces métadonnées brutes incluent les métadonnées du système interne qui ne sont pas garanties de la version à la version.

     L'exemple suivant présente les résultats de la recherche de métadonnées d'objet pour un objet de test

S3 stocké sous forme de deux copies répliquées.

System Metadata

Object ID	A12E96FF-B13F-4905-9E9E-45373F6E7DA8
Name	testobject
Container	source
Account	t-1582139188
Size	5.24 MB
Creation Time	2020-02-19 12:15:59 PST
Modified Time	2020-02-19 12:15:59 PST

Replicated Copies

Node	Disk Path
99-97	/var/local/rangedb/2/p/06/0B/00nM8H$|TFbnQQ}|CV2E
99-99	/var/local/rangedb/1/p/12/0A/00nM8H$|TFboW28|CXG%

Raw Metadata


```
{
    "TYPE": "CTNT",
    "CHND": "A12E96FF-B13F-4905-9E9E-45373F6E7DA8",
    "NAME": "testobject",
    "CBID": "0x8823DE7EC7C10416",
    "PHND": "FEA0AE51-534A-11EA-9FCD-31FF00C36D56",
    "PPTH": "source",
    "META": {
        "BASE": {
            "PAWS": "2",
```


6. Vérifiez que l'objet est stocké à l'emplacement ou aux emplacements appropriés et qu'il s'agit du type de copie correct.

> Si l'option Audit est activée, vous pouvez également surveiller le journal d'audit du message règles objet respectées ORLM. Le message d'audit ORLM peut vous fournir davantage d'informations sur l'état du processus d'évaluation ILM, mais il ne peut pas vous fournir d'informations sur l'exactitude du placement des données de l'objet ou l'exhaustivité de la politique ILM. Vous devez évaluer cela vous-même. Pour plus de détails, voir "Examiner les journaux d'audit".

Informations associées

- "UTILISEZ L'API REST S3"
- "Utilisez l'API REST de Swift"

Utilisation des règles ILM et ILM

À mesure que vos besoins en stockage évoluent, vous devrez peut-être mettre en place une autre stratégie ou modifier les règles ILM associées à la règle. Vous pouvez consulter les metrics ILM pour déterminer les performances du système.

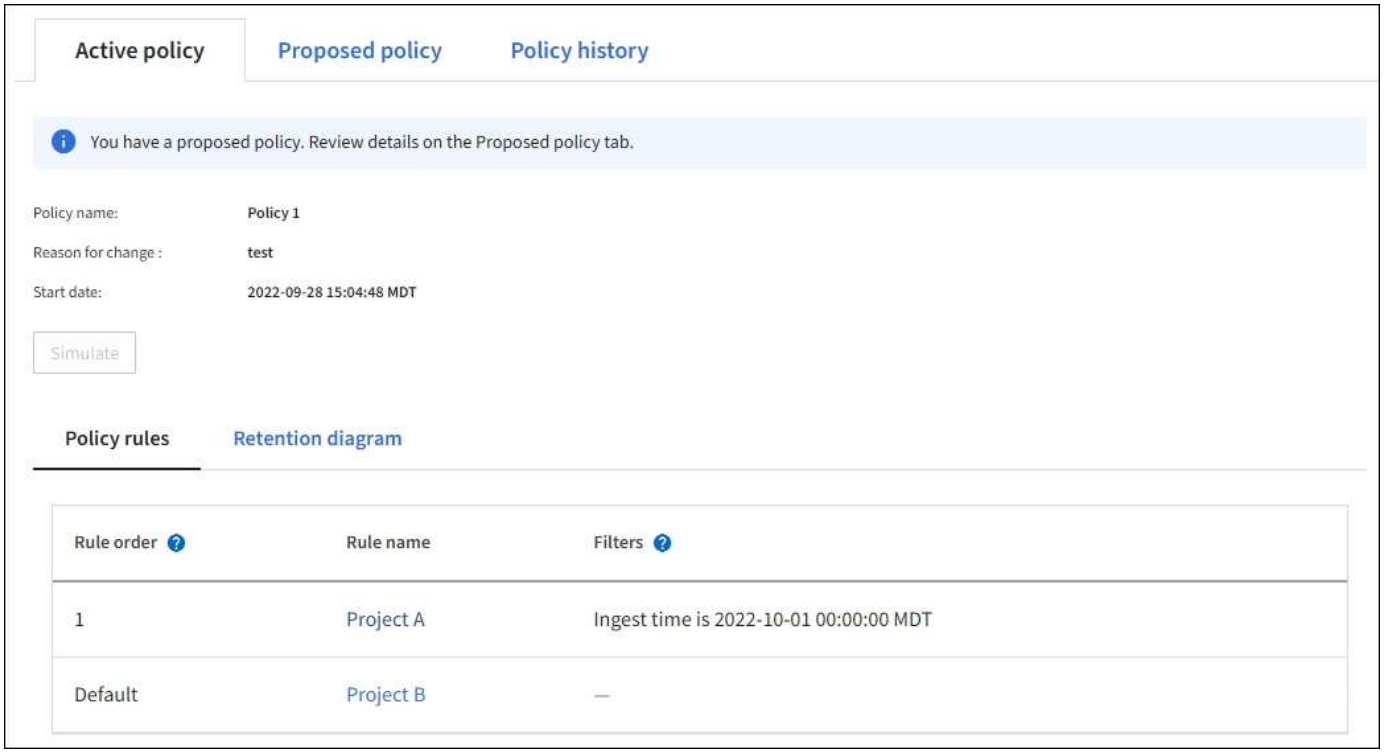
Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous disposez d'autorisations d'accès spécifiques.

Afficher les règles ILM

Pour afficher les règles ILM actives, proposées et historiques :

1. Sélectionnez **ILM** > **stratégies**.
2. Au besoin, sélectionnez **politique active**, **politique proposée** ou **Historique de la politique** pour afficher les détails de chacune d'elles. Dans chaque onglet, vous pouvez sélectionner **règles de stratégie** et **diagramme de rétention**.



Cloner une règle ILM historique

Pour cloner une règle ILM historique :

1. Sélectionnez **ILM** > **politiques** > **Historique des politiques**.
2. Supprimez la stratégie proposée, le cas échéant.
3. Sélectionnez le bouton radio de la stratégie à cloner, puis sélectionnez **Cloner la stratégie historique**.
4. Complétez les informations requises en suivant les instructions de la section "Création de la règle ILM proposée".

Une règle ILM mal configurée peut entraîner une perte de données irrécupérable. Avant d'activer une politique ILM, examinez attentivement la politique ILM et ses règles ILM, puis simulez la politique ILM. Vérifiez toujours que la politique ILM fonctionne comme prévu.

Suppression de la règle ILM proposée

Pour supprimer la règle proposée :

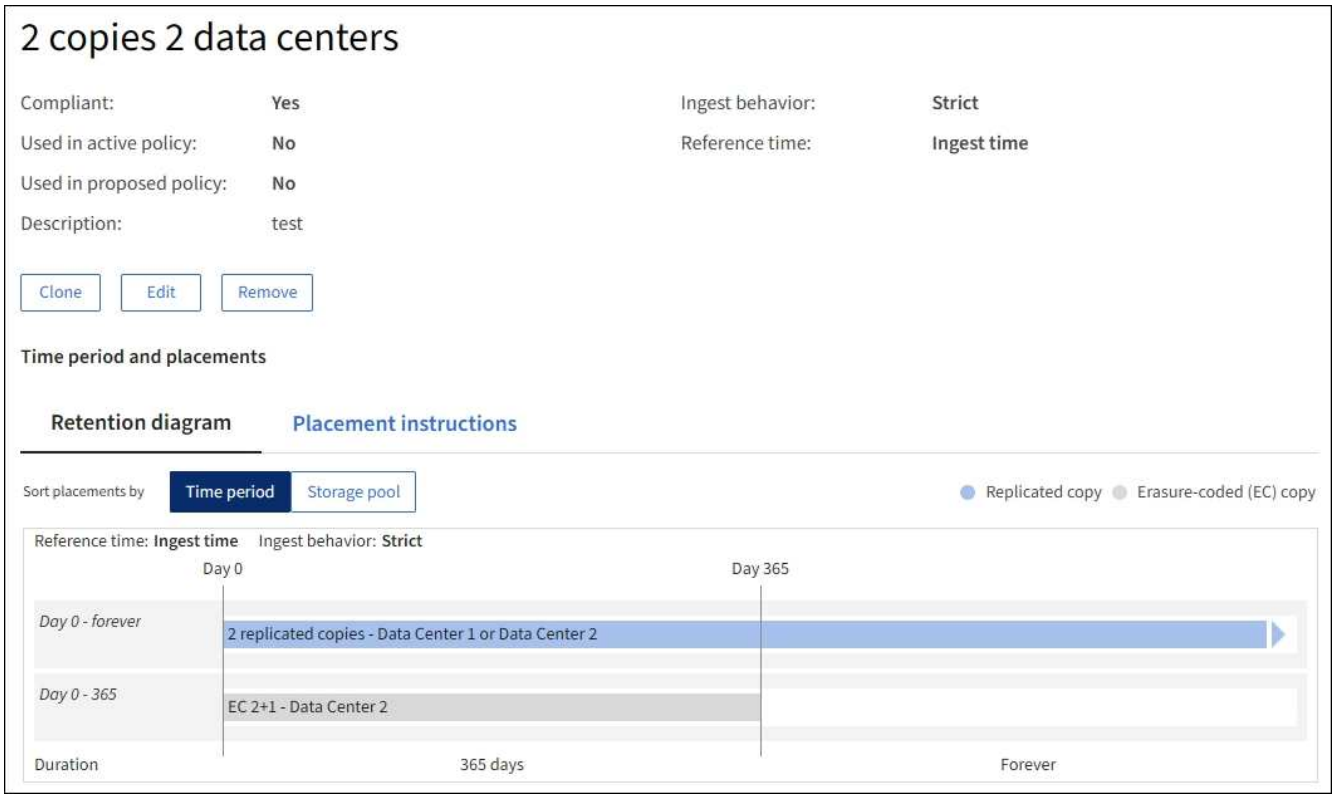
1. Sélectionnez **ILM** > **politiques** > **politique proposée**.
2. Sélectionnez **actions** > **Supprimer**.

La stratégie proposée et l'onglet de stratégie proposée sont supprimés.

Afficher le détail des règles ILM

Pour afficher les détails d'une règle ILM, y compris le diagramme de conservation et les instructions de placement de la règle :

1. Sélectionnez **ILM** > **règles**.
2. Sélectionnez la règle dont vous souhaitez afficher les détails. Exemple :



En outre, vous pouvez utiliser la page de détails pour cloner, modifier ou supprimer une règle.

Cloner une règle ILM

Vous ne pouvez pas modifier une règle si elle est utilisée dans la règle ILM proposée ou la règle ILM active. Vous pouvez plutôt cloner une règle et apporter les modifications nécessaires à la copie clonée. Ensuite, si nécessaire, vous pouvez supprimer la règle d'origine de la stratégie proposée et la remplacer par la version modifiée. Une règle ILM ne peut pas être clonée si elle a été créée à l'aide de StorageGRID version 10.2 ou

antérieure.

Avant d'ajouter une règle clonée à la règle ILM active, veuillez noter que la modification des instructions de placement d'un objet peut augmenter la charge appliquée au système.

Étapes

1. Sélectionnez **ILM** > **règles**.
2. Cochez la case correspondant à la règle à cloner, puis sélectionnez **Clone**. Vous pouvez également sélectionner le nom de la règle, puis sélectionner **Clone** dans la page des détails de la règle.
3. Mettez à jour la règle clonée en suivant les étapes de Modification d'une règle ILM et "Utilisation de filtres avancés dans les règles ILM".

   Lors du clonage d'une règle ILM, vous devez entrer un nouveau nom.

Modifiez une règle ILM

Vous devrez peut-être modifier une règle ILM pour modifier une instruction de filtre ou de placement.

Vous ne pouvez pas modifier une règle si elle est utilisée dans la règle ILM active ou la règle ILM proposée. Vous pouvez plutôt cloner ces règles et apporter les modifications nécessaires à la copie clonée. Vous ne pouvez pas non plus modifier la règle fournie par le système, effectuer 2 copies.

> Avant d'ajouter une règle modifiée à la règle ILM active, notez que toute modification des instructions de placement d'un objet peut entraîner une charge croissante sur le système.

Étapes

1. Sélectionnez **ILM** > **règles**.
2. Vérifiez que la règle à modifier n'est pas utilisée dans la règle ILM active ou la règle ILM proposée.
3. Si la règle que vous souhaitez modifier n'est pas utilisée, cochez la case correspondant à la règle et sélectionnez **actions** > **Modifier**. Vous pouvez également sélectionner le nom de la règle, puis sélectionner **Modifier** sur la page de détails de la règle.
4. Complétez les pages de l'assistant Modifier les règles ILM. Si nécessaire, suivez les étapes de "Création d'une règle ILM" et "Utilisation de filtres avancés dans les règles ILM".

   Lors de la modification d'une règle ILM, vous ne pouvez pas en modifier le nom.

> Si vous modifiez une règle utilisée dans une stratégie d'historique, le cette icône apparaît pour la règle lorsque vous affichez la stratégie, ce qui indique que la règle est devenue une règle historique.

Suppression d'une règle ILM

Pour gérer la liste des règles ILM actuelles, supprimez toutes les règles ILM que vous ne serez pas susceptible d'utiliser.

Étapes

Pour supprimer une règle ILM actuellement utilisée dans la règle active ou la règle proposée :

1. Clonez la règle active ou modifiez la règle proposée.

2. Supprimez la règle ILM de la règle.
3. Enregistrez, simulez et activez la nouvelle stratégie pour vous assurer que les objets sont protégés comme prévu.

Pour supprimer une règle ILM non utilisée actuellement :

1. Sélectionnez **ILM** > **règles**.
2. Confirmez que la règle que vous souhaitez supprimer n'est pas utilisée dans la stratégie active ou la stratégie proposée.
3. Si la règle que vous souhaitez supprimer n'est pas utilisée, sélectionnez-la et sélectionnez **Supprimer**. Vous pouvez sélectionner plusieurs règles et les supprimer toutes en même temps.
4. Sélectionnez **Oui** pour confirmer que vous souhaitez supprimer la règle ILM.

   La règle ILM est supprimée.

> Si vous supprimez une règle utilisée dans une stratégie d'historique, le ⊗ cette icône apparaît pour la règle lorsque vous affichez la stratégie, ce qui indique que la règle est devenue une règle historique.

Afficher les metrics ILM

Vous pouvez afficher les mesures de la règle ILM, telles que le nombre d'objets dans la file d'attente et la fréquence d'évaluation. Vous pouvez surveiller ces mesures afin de déterminer les performances du système. Une file d'attente ou un taux d'évaluation important peut indiquer que le système ne peut pas suivre le taux d'entrée, que la charge des applications clientes est excessive ou qu'il existe une condition anormale.

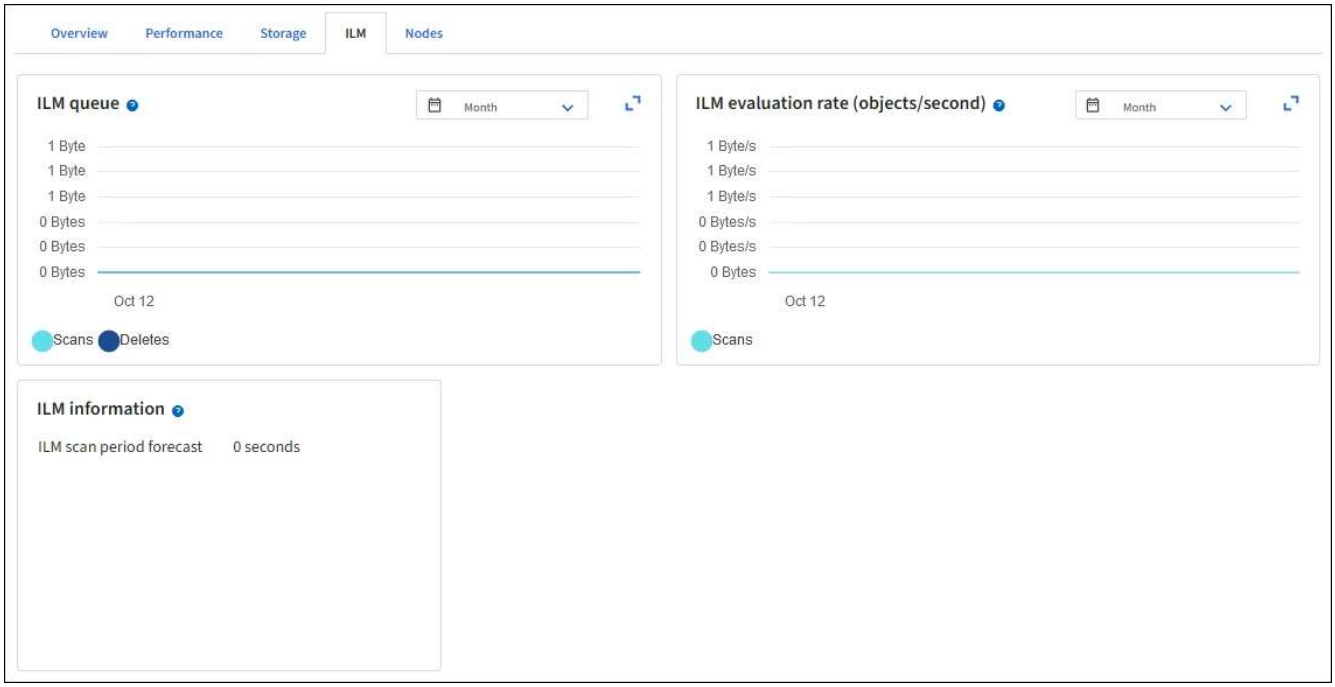
Étapes

1. Sélectionnez **Tableau de bord** > **ILM**.

> Le tableau de bord pouvant être personnalisé, l'onglet ILM peut ne pas être disponible.

2. Surveillez les mesures dans l'onglet ILM.

   Vous pouvez sélectionner le point d'interrogation ? Pour afficher une description des éléments de l'onglet ILM.



Utilisez le verrouillage d'objet S3

Gestion des objets avec le verrouillage d'objets S3

En tant qu'administrateur du grid, vous pouvez activer le verrouillage objet S3 sur votre système StorageGRID et mettre en œuvre une règle ILM conforme pour empêcher la suppression ou l'écrasement des objets de compartiments S3 spécifiques pendant une durée spécifiée.

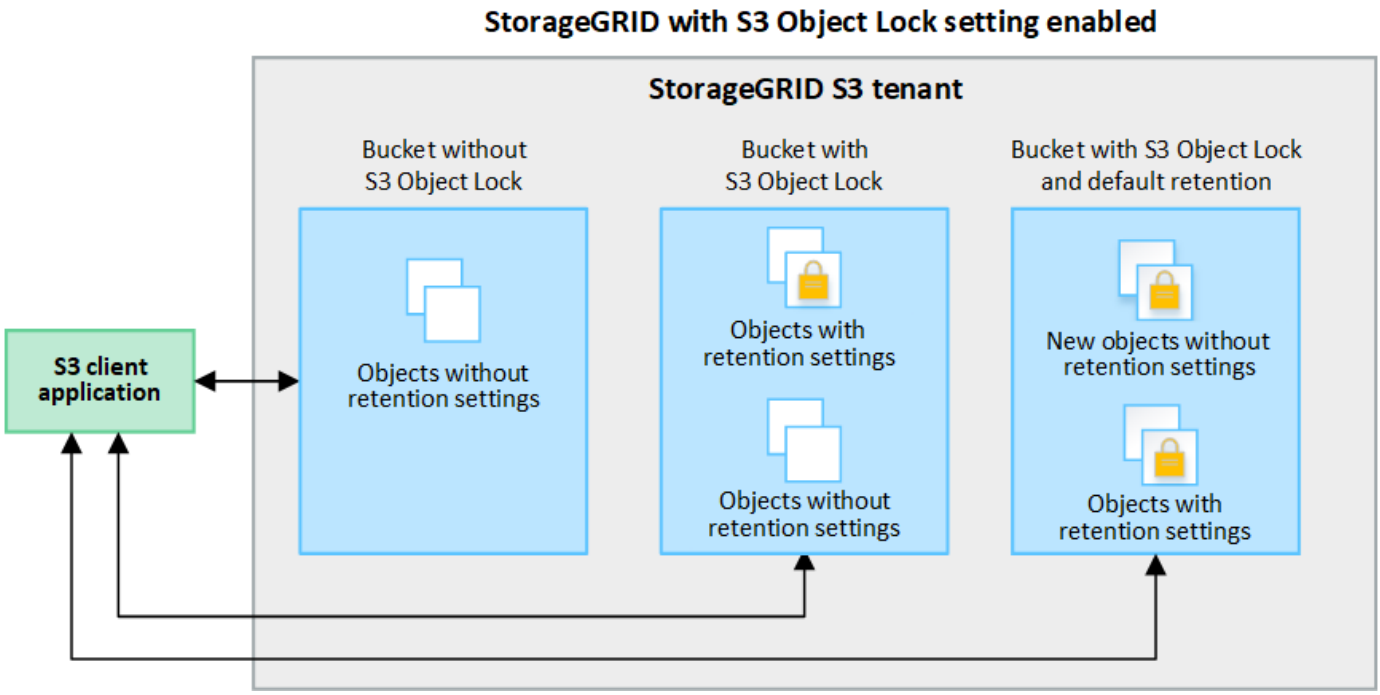
Qu'est-ce que le verrouillage objet S3 ?

La fonctionnalité de verrouillage objet StorageGRID S3 est une solution de protection des objets équivalente au verrouillage objet S3 dans Amazon simple Storage Service (Amazon S3).

Comme illustré dans la figure, lorsque le paramètre global de verrouillage d'objet S3 est activé pour un système StorageGRID, un compte de locataire S3 peut créer des compartiments avec ou sans verrouillage d'objet S3 activé. Si le verrouillage objet S3 est activé pour un compartiment, la gestion des versions de compartiment est requise et elle est automatiquement activée.

Si le verrouillage objet S3 est activé dans un compartiment, les applications client S3 peuvent spécifier des paramètres de conservation pour toute version d'objet enregistrée dans ce compartiment.

En outre, un compartiment dans lequel le verrouillage objet S3 est activé peut choisir entre un mode de conservation et une période de conservation par défaut. Les paramètres par défaut s'appliquent uniquement aux objets ajoutés au compartiment sans leurs propres paramètres de conservation.



Modes de rétention

La fonction de verrouillage d'objet StorageGRID S3 prend en charge deux modes de conservation pour appliquer différents niveaux de protection aux objets. Ces modes sont équivalents aux modes de conservation Amazon S3.

- En mode conformité :
  - L'objet ne peut pas être supprimé tant que sa date de conservation jusqu'à n'est pas atteinte.
  - La date de conservation de l'objet peut être augmentée, mais elle ne peut pas être réduite.
  - La date de conservation de l'objet jusqu'à ne peut pas être supprimée tant que cette date n'est pas atteinte.
- En mode gouvernance :
  - Les utilisateurs disposant d'une autorisation spéciale peuvent utiliser un en-tête de contournement dans les demandes pour modifier certains paramètres de conservation.
  - Ces utilisateurs peuvent supprimer une version d'objet avant d'atteindre sa date de conservation jusqu'à.
  - Ces utilisateurs peuvent augmenter, diminuer ou supprimer la date de conservation d'un objet.

Paramètres de conservation pour les versions d'objet

Si un compartiment est créé avec le verrouillage objet S3 activé, les utilisateurs peuvent utiliser l'application client S3 pour spécifier éventuellement les paramètres de conservation suivants pour chaque objet ajouté au compartiment :

- **Mode de conservation** : conformité ou gouvernance.
- **Conserver-jusqu'à-date**: Si la date de conservation d'une version d'objet est dans le futur, l'objet peut être récupéré, mais il ne peut pas être supprimé.
- **Mise en garde légale** : l'application d'une mise en garde légale à une version d'objet verrouille immédiatement cet objet. Par exemple, vous devrez peut-être mettre une obligation légale sur un objet lié

à une enquête ou à un litige juridique. Une obligation légale n'a pas de date d'expiration, mais reste en place jusqu'à ce qu'elle soit explicitement supprimée. Les dispositions légales sont indépendantes de la date de conservation.

> Si un objet fait l'objet d'une conservation légale, personne ne peut le supprimer, quel que soit son mode de conservation.

Pour plus d'informations sur les paramètres d'objet, reportez-vous à la section "Utilisez l'API REST S3 pour configurer le verrouillage objet S3".

Paramètre de rétention par défaut pour les compartiments

Si un compartiment est créé avec le verrouillage objet S3 activé, les utilisateurs peuvent spécifier les paramètres par défaut suivants pour le compartiment :

- **Mode de rétention par défaut** : conformité ou gouvernance.
- **Période de rétention par défaut** : durée pendant laquelle les nouvelles versions d'objets ajoutées à ce compartiment doivent être conservées, à partir du jour où elles sont ajoutées.

Les paramètres de compartiment par défaut s'appliquent uniquement aux nouveaux objets qui ne disposent pas de leurs propres paramètres de conservation. Les objets de compartiment existants ne sont pas affectés lorsque vous ajoutez ou modifiez ces paramètres par défaut.

Voir "Créer un compartiment S3" et "Mettre à jour la conservation par défaut du verrouillage d'objet S3".

Comparaison du verrouillage d'objet S3 à la conformité existante

Le verrouillage d'objet S3 remplace la fonctionnalité de conformité disponible dans les versions précédentes de StorageGRID. La fonctionnalité de verrouillage d'objet S3 conforme aux exigences Amazon S3 représente la fonctionnalité propriétaire de conformité StorageGRID, appelée désormais « conformité héritée ».

> Le paramètre conformité globale est obsolète. Si vous avez activé ce paramètre à l'aide d'une version précédente de StorageGRID, le paramètre verrouillage objet S3 est activé automatiquement. Vous pouvez continuer à utiliser StorageGRID pour gérer les paramètres des compartiments conformes existants ; cependant, vous ne pouvez pas créer de nouveaux compartiments conformes. Pour plus de détails, voir "Base de connaissances NetApp : comment gérer des compartiments conformes aux ancienne génération dans StorageGRID 11.5".

Si vous avez utilisé la fonctionnalité de conformité héritée dans une version précédente de StorageGRID, reportez-vous au tableau suivant pour savoir comment la comparer à la fonctionnalité de verrouillage d'objet S3 dans StorageGRID.

	Verrouillage d'objet S3	Conformité (existant)
Comment cette fonctionnalité est-elle activée dans le monde entier ?	Dans Grid Manager, sélectionnez **CONFIGURATION** > **système** > **verrouillage objet S3**.	N'est plus pris en charge.

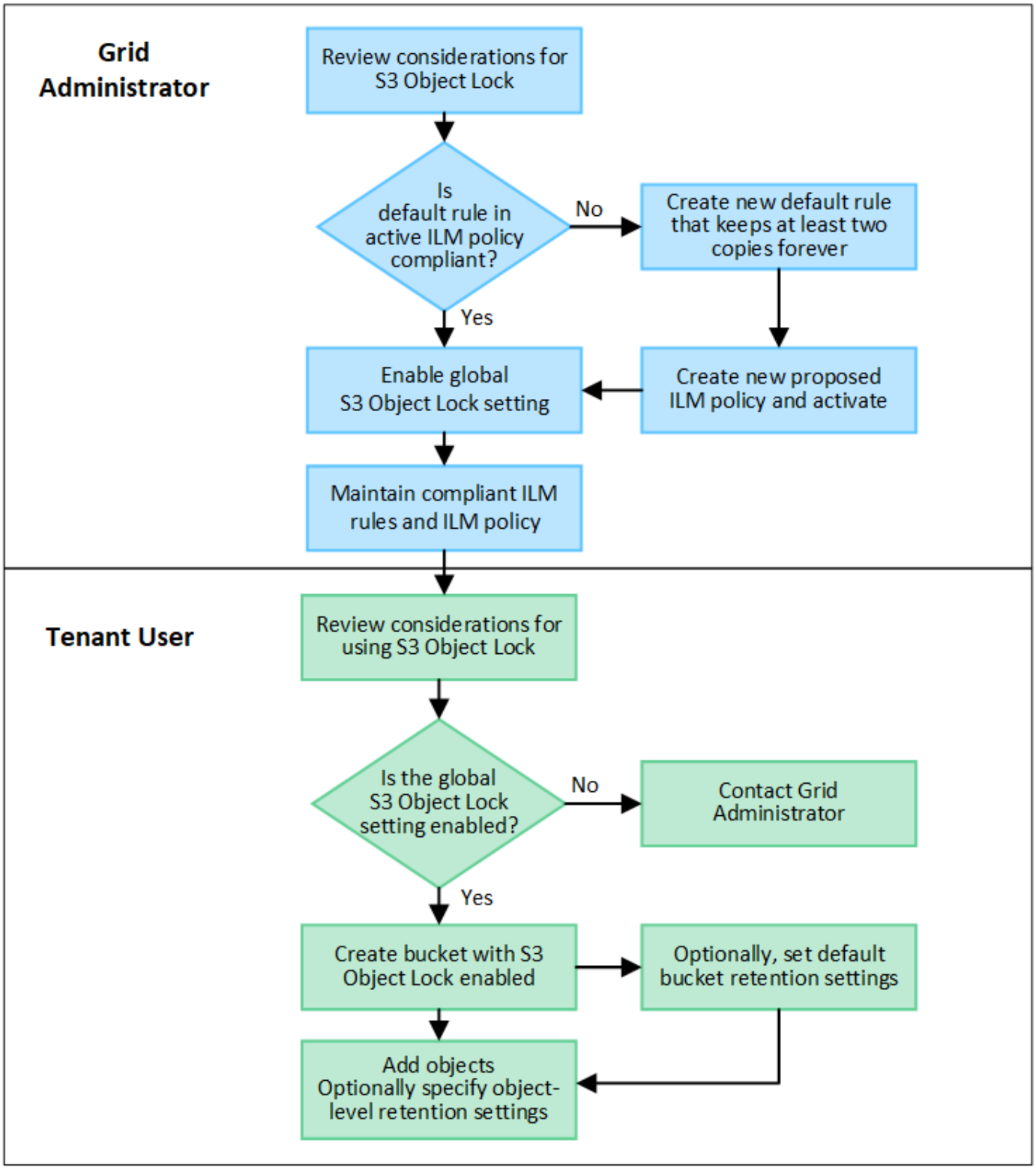
	Verrouillage d'objet S3	Conformité (existant)
Comment la fonctionnalité est-elle activée pour un compartiment ?	Les utilisateurs doivent activer le verrouillage objet S3 lors de la création d'un compartiment à l'aide du gestionnaire de locataires, de l'API de gestion des locataires ou de l'API REST S3.	N'est plus pris en charge.
Le contrôle de version des compartiments est-il pris en	Oui. Le contrôle de version des compartiments est requis et activé automatiquement lorsque le verrouillage des objets S3 est activé pour le compartiment.	Non
Comment la conservation d'objets est-elle définie ?	Les utilisateurs peuvent définir une date de conservation jusqu'à pour chaque version d'objet ou définir une période de conservation par défaut pour chaque compartiment.	Les utilisateurs doivent définir une période de conservation pour l'intégralité du compartiment. La période de conservation s'applique à tous les objets du compartiment.
La période de conservation peut-elle être modifiée ?	• En mode conformité, la date de conservation jusqu'à la date d'un objet peut être augmentée, mais jamais réduite. • En mode gouvernance, les utilisateurs disposant d'autorisations spéciales peuvent diminuer, voire supprimer les paramètres de conservation d'un objet.	La période de rétention d'un godet peut être augmentée, mais jamais réduite.
Où est contrôlé la suspension légale ?	Les utilisateurs peuvent placer une conservation légale ou lever une conservation légale pour toute version d'objet dans le compartiment.	Une retenue légale est placée sur le godet et affecte tous les objets du godet.

	Verrouillage d’objet S3	Conformité (existant)
Quand les objets peuvent-ils être supprimés ?	• En mode de conformité, une version d’objet peut être supprimée une fois la date de conservation jusqu’à atteinte, en supposant que l’objet n’est pas en attente légale. • En mode gouvernance, les utilisateurs disposant d’autorisations spéciales peuvent supprimer un objet avant que sa date de conservation jusqu’à soit atteinte, en supposant que l’objet ne soit pas en attente légale.	Un objet peut être supprimé après l’expiration de la période de conservation, en supposant que le compartiment n’est pas en conservation légale. Les objets peuvent être supprimés automatiquement ou manuellement.
La configuration du cycle de vie des compartiments est-elle prise en	Oui.	Non

Workflow pour le verrouillage d’objets S3

En tant qu’administrateur du grid, vous devez coordonner étroitement avec les utilisateurs des locataires pour assurer la protection des objets conformément aux exigences de conservation.

Le schéma des workflows représente les étapes générales d’utilisation du verrouillage d’objet S3. Ces étapes sont réalisées par l’administrateur du grid et les utilisateurs locataires.



Tâches d'administration du grid

Comme le montre le diagramme de workflow, un administrateur grid doit effectuer deux tâches générales avant que les locataires S3 ne puissent utiliser S3 Object Lock :

1. Créez au moins une règle ILM conforme et faites de cette règle la règle par défaut dans la politique ILM active.
2. Activez le paramètre global de verrouillage d'objet S3 pour l'ensemble du système StorageGRID.

Tâches des locataires

Une fois que le paramètre global de verrouillage d'objet S3 a été activé, les locataires peuvent effectuer les tâches suivantes :

1. Créez des compartiments dont le verrouillage d'objet S3 est activé.
2. Vous pouvez également spécifier les paramètres de conservation par défaut du compartiment. Les paramètres de compartiment par défaut sont appliqués uniquement aux nouveaux objets qui ne disposent pas de leurs propres paramètres de conservation.
3. Ajoutez des objets à ces compartiments, et spécifiez éventuellement des périodes de conservation au niveau objet et des paramètres de conservation légale.
4. Si nécessaire, mettez à jour la conservation par défaut du compartiment ou la période de conservation ou le paramètre de conservation légale d'un objet individuel.

Conditions requises pour le verrouillage d'objet S3

Vous devez connaître les exigences relatives à l'activation du paramètre global de verrouillage d'objet S3, les exigences de création de règles ILM et de règles ILM conformes, et les restrictions StorageGRID placées sur des compartiments et des objets qui utilisent le verrouillage d'objet S3.

Conditions requises pour l'utilisation du paramètre global de verrouillage d'objet S3

- Vous devez activer le paramètre global de verrouillage d'objet S3 à l'aide de Grid Manager ou de l'API Grid Management avant qu'un locataire S3 puisse créer un compartiment avec le verrouillage d'objet S3 activé.
- L'activation du paramètre global de verrouillage d'objet S3 permet à tous les comptes de locataires S3 de créer des compartiments avec le verrouillage d'objet S3 activé.
- Une fois que vous avez activé le paramètre global S3 Object Lock, vous ne pouvez pas le désactiver.
- Vous ne pouvez pas activer le verrouillage d'objet S3 global à moins que la règle par défaut de la règle ILM active ne soit *conforme* (c'est-à-dire que la règle par défaut doit respecter les exigences des compartiments avec le verrouillage d'objet S3 activé).
- Lorsque le paramètre global S3 Object Lock est activé, vous ne pouvez pas créer une nouvelle règle ILM proposée ni activer une règle ILM existante proposée, sauf si la règle par défaut de la règle est conforme. Une fois le paramètre S3 Object Lock global activé, les pages de règles ILM et de règles ILM indiquent les règles ILM compatibles.

Exigences relatives aux règles ILM conformes

Si vous souhaitez activer le paramètre global de verrouillage d'objet S3, vous devez vous assurer que la règle par défaut de votre stratégie ILM active est conforme. Une règle conforme répond aux exigences des deux compartiments avec le verrouillage de l'objet S3 activé et les compartiments existants pour lesquels la conformité de l'ancienne génération est activée :

- Les départements IT doivent créer au moins deux copies objet répliquées ou une copie avec code d'effacement.
- Ces copies doivent exister sur les nœuds de stockage pendant toute la durée de chaque ligne dans les instructions de placement.
- Les copies d'objet ne peuvent pas être enregistrées dans un pool de stockage cloud.
- Les copies d'objet ne peuvent pas être enregistrées sur les nœuds d'archivage.

- Au moins une ligne des instructions de placement doit commencer au jour 0, en utilisant **heure d'ingestion** comme heure de référence.
- Au moins une ligne des instructions de placement doit être ""permanente".

Exigences relatives aux règles ILM actives et proposées

Lorsque le paramètre global S3 Object Lock est activé, les règles ILM actives et proposées peuvent inclure des règles conformes et non conformes.

- La règle par défaut de la politique ILM active ou proposée doit être conforme.
- Les règles non conformes s'appliquent uniquement aux objets des compartiments qui ne disposent pas du verrouillage d'objet S3 ou qui ne disposent pas de la fonctionnalité conformité héritée.
- Les règles conformes peuvent s'appliquer aux objets dans n'importe quel compartiment. Il n'est pas nécessaire d'activer le verrouillage objet S3 ou la conformité héritée.

Une politique ILM conforme peut inclure ces trois règles :

1. Règle de conformité qui crée des copies avec code d'effacement des objets dans un compartiment spécifique lorsque le verrouillage objet S3 est activé. Les copies EC sont stockées sur les nœuds de stockage du premier jour vers toujours.
2. Une règle non conforme qui crée deux copies d'objets répliquées sur les nœuds de stockage pendant un an, puis déplace une copie d'objet vers les nœuds d'archivage et stocke cette copie indéfiniment. Cette règle s'applique uniquement aux compartiments pour lesquels le verrouillage d'objet S3 ou la conformité aux anciennes n'est pas activé, car il ne stocke qu'une seule copie d'objet indéfiniment et utilise des nœuds d'archivage.
3. Règle par défaut conforme qui crée deux copies d'objets répliquées sur les nœuds de stockage du jour 0 à l'infini. Cette règle s'applique à tout objet dans un compartiment qui n'a pas été filtré par les deux premières règles.

Conditions requises pour les compartiments avec verrouillage objet S3 activé

- Si le paramètre global de verrouillage objet S3 est activé pour le système StorageGRID, vous pouvez utiliser le gestionnaire de locataires, l'API de gestion des locataires ou l'API REST S3 pour créer des compartiments avec le verrouillage objet S3 activé.
- Si vous prévoyez d'utiliser le verrouillage d'objet S3, vous devez activer le verrouillage d'objet S3 lors de la création du compartiment. Vous ne pouvez pas activer le verrouillage objet S3 pour un compartiment existant.
- Lorsque le verrouillage d'objet S3 est activé pour un compartiment, StorageGRID active automatiquement le contrôle de version pour ce compartiment. Vous ne pouvez pas désactiver le verrouillage objet S3 ou suspendre la gestion des versions pour le compartiment.
- Vous pouvez également spécifier un mode de conservation et une période de conservation par défaut pour chaque compartiment à l'aide du gestionnaire des locataires, de l'API de gestion des locataires ou de l'API REST S3. Les paramètres de conservation par défaut du compartiment s'appliquent uniquement aux nouveaux objets ajoutés au compartiment qui ne disposent pas de leurs propres paramètres de conservation. Vous pouvez remplacer ces paramètres par défaut en spécifiant un mode de conservation et une date de conservation jusqu'à pour chaque version d'objet lors du téléchargement.
- La configuration du cycle de vie des compartiments est prise en charge pour les compartiments avec le verrouillage objet S3 activé.
- La réplication CloudMirror n'est pas prise en charge pour les compartiments avec le verrouillage objet S3 activé.

Exigences relatives aux objets dans les compartiments avec le verrouillage d'objet S3 activé

- Pour protéger une version d'objet, vous pouvez spécifier les paramètres de conservation par défaut du compartiment ou les paramètres de conservation pour chaque version d'objet. Les paramètres de conservation au niveau objet peuvent être spécifiés à l'aide de l'application client S3 ou de l'API REST S3.
- Les paramètres de conservation s'appliquent aux versions d'objet individuelles. Une version d'objet peut avoir à la fois un paramètre de conservation à la date et un paramètre de conservation légal, l'un mais pas l'autre, ou l'autre. La spécification d'un paramètre de conservation à la date ou d'un paramètre de conservation légal pour un objet protège uniquement la version spécifiée dans la demande. Vous pouvez créer de nouvelles versions de l'objet, tandis que la version précédente de l'objet reste verrouillée.

Cycle de vie des objets dans des compartiments avec verrouillage objet S3 activé

Chaque objet enregistré dans un compartiment lorsque le verrouillage objet S3 est activé passe par les étapes suivantes :

1. **Entrée d'objet**

   Lors de l'ajout d'une version d'objet à un compartiment pour lequel S3 Object Lock est activé, les paramètres de conservation sont appliqués comme suit :

   - Si des paramètres de rétention sont spécifiés pour l'objet, les paramètres de niveau objet sont appliqués. Tous les paramètres de compartiment par défaut sont ignorés.
   - Si aucun paramètre de conservation n'est spécifié pour l'objet, les paramètres de compartiment par défaut sont appliqués, s'ils existent.
   - Si aucun paramètre de conservation n'est spécifié pour l'objet ou le compartiment, l'objet n'est pas protégé par le verrouillage objet S3.

   Si les paramètres de conservation sont appliqués, l'objet et les métadonnées S3 définies par l'utilisateur sont protégés.

2. **Conservation et suppression d'objets**

   StorageGRID stocke plusieurs copies de chaque objet protégé pendant la période de conservation spécifiée. Le nombre et le type exacts de copies d'objet et d'emplacements de stockage sont déterminés par les règles de conformité de la politique ILM active. La possibilité de supprimer un objet protégé avant d'atteindre sa date de conservation jusqu'à dépend de son mode de conservation.

   - Si un objet fait l'objet d'une conservation légale, personne ne peut le supprimer, quel que soit son mode de conservation.

Informations associées

- "Créer un compartiment S3"
- "Mettre à jour la conservation par défaut du verrouillage d'objet S3"
- "Utilisez l'API REST S3 pour configurer le verrouillage objet S3"
- "Exemple 7 : règle ILM conforme pour le verrouillage d'objet S3"

Activez le verrouillage global des objets S3

Si un compte de locataire S3 doit respecter les exigences réglementaires lors de la sauvegarde des données d'objet, vous devez activer le verrouillage objet S3 pour l'intégralité de votre système StorageGRID. L'activation du paramètre de verrouillage

d’objet S3 global permet aux locataires S3 de créer et de gérer des compartiments et des objets avec le verrouillage d’objet S3.

Avant de commencer

- Vous disposez de l’autorisation d’accès racine.
- Vous êtes connecté au Grid Manager à l’aide d’un "navigateur web pris en charge".
- Vous avez examiné le workflow de verrouillage d’objet S3 et vous en avez pris connaissance.
- Vous avez confirmé que la règle par défaut de la politique ILM active est conforme. Voir "Créez une règle ILM par défaut" pour plus d’informations.

Description de la tâche

Un administrateur de grid doit activer le paramètre global de verrouillage d’objet S3 pour permettre aux utilisateurs locataires de créer de nouveaux compartiments pour lesquels le verrouillage d’objet S3 est activé. Une fois ce paramètre activé, il ne peut pas être désactivé.

> Le paramètre conformité globale est obsolète. Si vous avez activé ce paramètre à l’aide d’une version précédente de StorageGRID, le paramètre verrouillage objet S3 est activé automatiquement. Vous pouvez continuer à utiliser StorageGRID pour gérer les paramètres des compartiments conformes existants ; cependant, vous ne pouvez pas créer de nouveaux compartiments conformes. Pour plus de détails, voir "Base de connaissances NetApp : comment gérer des compartiments conformes aux ancienne génération dans StorageGRID 11.5".

Étapes

1. Sélectionnez **CONFIGURATION** > **système** > **verrouillage objet S3**.

   La page Paramètres de verrouillage d’objet S3 s’affiche.

2. Sélectionnez **Activer le verrouillage d’objet S3**.
3. Sélectionnez **appliquer**.

   Une boîte de dialogue de confirmation s’affiche et vous rappelle que vous ne pouvez pas désactiver le verrouillage d’objet S3 après son activation.

4. Si vous êtes sûr de vouloir activer définitivement le verrouillage d’objet S3 pour l’ensemble du système, sélectionnez **OK**.

   Lorsque vous sélectionnez **OK**:

   - Si la règle par défaut de la règle ILM active est conforme, le verrouillage d’objet S3 est désormais activé pour l’ensemble de la grille et ne peut pas être désactivé.
   - Si la règle par défaut n’est pas conforme, une erreur s’affiche. Vous devez créer et activer une nouvelle règle ILM qui inclut une règle de conformité comme règle par défaut. Sélectionnez **OK**. Créez ensuite une nouvelle règle proposée, simulez-la et activez-la. Voir "Création de la règle ILM" pour obtenir des instructions.

Une fois que vous avez terminé

Une fois que vous avez activé le paramètre de verrouillage d’objet S3 global, vous pouvez le vouloir "Création d’une règle ILM". Une fois le paramètre activé, la règle ILM peut éventuellement inclure une règle par défaut conforme et une règle par défaut non compatible. Par exemple, vous pouvez utiliser une règle non conforme qui ne possède pas de filtres pour les objets dans des compartiments pour lesquels le verrouillage d’objet S3

n’est pas activé.

Résolvez les erreurs de cohérence lors de la mise à jour de la configuration du verrouillage d’objet S3 ou de la conformité héritée

Si un site de data Center ou plusieurs nœuds de stockage sur un site deviennent indisponibles, les locataires S3 peuvent avoir à appliquer des modifications à la configuration de verrouillage d’objet S3 ou de conformité héritée.

Les locataires qui utilisent des compartiments avec le verrouillage d’objet S3 (ou la conformité héritée) peuvent modifier certains paramètres. Par exemple, un utilisateur locataire qui utilise le verrouillage objet S3 peut avoir à mettre une version d’objet en attente légale.

Lorsqu’un locataire met à jour les paramètres d’un compartiment S3 ou d’une version d’objet, StorageGRID tente immédiatement de mettre à jour les métadonnées du compartiment ou de l’objet dans la grille. Si le système ne peut pas mettre à jour les métadonnées car un site de data Center ou plusieurs nœuds de stockage ne sont pas disponibles, une erreur s’affiche :

```
503: Service Unavailable
Unable to update compliance settings because the settings can't be
consistently applied on enough storage services. Contact your grid
administrator for assistance.
```

Pour résoudre cette erreur, procédez comme suit :

1. Essayez de rendre tous les nœuds ou sites de stockage disponibles à nouveau dès que possible.
2. Si vous ne pouvez pas rendre suffisamment de nœuds de stockage disponibles sur chaque site, contactez le support technique qui peut vous aider à restaurer les nœuds et veiller à ce que les modifications soient appliquées de manière cohérente dans l’ensemble de la grille.
3. Une fois le problème sous-jacent résolu, rappelez à l’utilisateur locataire de réessayer de modifier sa configuration.

Informations associées

- "Utilisez un compte de locataire"
- "UTILISEZ L’API REST S3"
- "Récupérer et entretenir"

Exemples de règles et de règles ILM

Exemple 1 : règles et règles ILM pour le stockage objet

Vous pouvez utiliser les exemples de règles et de règle suivants comme point de départ pour définir une règle ILM afin de répondre à vos exigences de protection et de conservation des objets.

> Les règles et règles ILM suivantes ne sont que des exemples. Les règles ILM sont nombreuses. Avant d’activer une nouvelle stratégie, simulez la stratégie proposée pour confirmer qu’elle fonctionnera comme destinée à protéger le contenu contre la perte.

Règle ILM 1, exemple 1 : copie des données d'objet vers deux sites

Cet exemple de règle ILM copie les données d'objet dans des pools de stockage de deux sites.

Définition de règle	Exemple de valeur
Pools de stockage sur un site	Deux pools de stockage, chacun contenant des sites différents, nommés site 1 et site 2.
Nom de la règle	Deux copies deux sites
Heure de référence	Temps d'ingestion
Placements	Du jour 0 à l'infini, conservez une copie répliquée sur le site 1 et une copie répliquée sur le site 2.

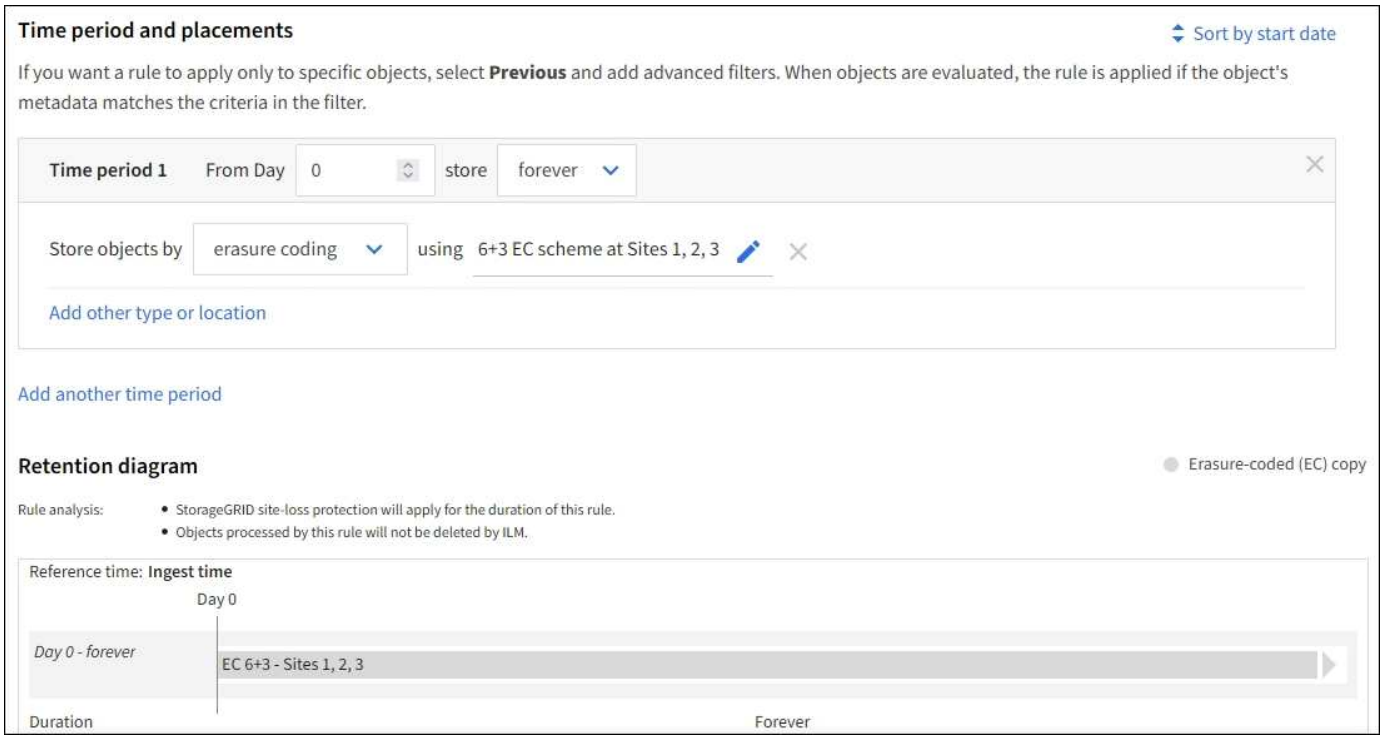
La section analyse des règles du diagramme de rétention indique :

- La protection contre la perte de site StorageGRID s'appliquera pendant toute la durée de cette règle.
- Les objets traités par cette règle ne seront pas supprimés par ILM.

Règle ILM 2, exemple 1 : profil de code d'effacement avec mise en correspondance des compartiments

Cet exemple de règle ILM utilise un profil de code d'effacement et un compartiment S3 pour déterminer l'emplacement et la durée de stockage de l'objet.

Définition de règle	Exemple de valeur
Pool de stockage avec plusieurs sites	• Un pool de stockage sur trois sites (sites 1, 2, 3) • Utilisez le schéma de code d'effacement 6+3
Nom de la règle	Dossiers financiers du compartiment S3
Heure de référence	Temps d'ingestion
Placements	Pour les objets du compartiment S3 nommés « finance-records », créez une copie avec code d'effacement dans le pool spécifié par le profil de code d'effacement. Conserver cette copie pour toujours.



Règle ILM, par exemple 1

Dans la pratique, la plupart des règles ILM sont simples, même si le système StorageGRID vous permet de concevoir des règles ILM complexes et sophistiquées.

Une règle ILM standard pour un grid multisite peut inclure des règles ILM, telles que :

- Lors de l'ingestion, stockez tous les objets appartenant au compartiment S3 nommé `finance-records` dans un pool de stockage contenant trois sites. Utilisez le code d'effacement 6+3.
- Si un objet ne correspond pas à la première règle ILM, utilisez la règle ILM par défaut de la règle, deux copies de data centers, pour stocker une copie de cet objet sur le site 1 et une copie sur le site 2.

Informations associées

- "Création d'une règle ILM : présentation"
- "Création d'une règle ILM proposée"

Exemple 2 : règles et règle ILM pour le filtrage de la taille des objets EC

Des exemples de règles et de règles ci-dessous vous permettent de définir une règle ILM qui s'applique par taille d'objet afin de répondre aux exigences EC recommandées.

> Les règles et règles ILM suivantes ne sont que des exemples. Les règles ILM sont nombreuses. Avant d'activer une nouvelle stratégie, simulez la stratégie proposée pour confirmer qu'elle fonctionnera comme destinée à protéger le contenu contre la perte.

Règle ILM 1, par exemple 2 : utilise ce pour les objets de plus de 1 Mo

Cet exemple de règle ILM code des objets dont le nombre est supérieur à 1 Mo.

Le codage d'effacement convient mieux aux objets de plus de 1 Mo. N'utilisez pas le code d'effacement pour les objets inférieurs à 200 Ko afin d'éviter la surcharge liée à la gestion de très petits fragments de code d'effacement.

Définition de règle	Exemple de valeur
Nom de la règle	Objets EC uniquement > 1 Mo
Heure de référence	Temps d'ingestion
Filtre avancé pour la taille de l'objet	Taille de l'objet supérieure à 1 Mo
Placements	Créez une copie avec code d'effacement 2+1 sur trois sites

Règle ILM 2, par exemple 2 : deux copies répliquées

Cet exemple de règle ILM crée deux copies répliquées, sans filtrer par taille d'objet. Cette règle est la règle par défaut de la règle. Étant donné que la première règle filtre tous les objets de plus de 1 Mo, cette règle s'applique uniquement aux objets de 1 Mo ou plus.

Définition de règle	Exemple de valeur
Nom de la règle	Deux copies répliquées
Heure de référence	Temps d'ingestion
Filtre avancé pour la taille de l'objet	Aucune
Placements	Du jour 0 à l'infini, conservez une copie répliquée sur le site 1 et une copie répliquée sur le site 2.

Règle ILM par exemple 2 : utilisez l'effacement pour des objets supérieurs à 1 Mo

Cet exemple de règle ILM inclut deux règles ILM :

- La première règle code tous les objets supérieurs à 1 Mo.
- La seconde règle ILM (par défaut) crée deux copies répliquées. Étant donné que les objets de plus de 1 Mo ont été filtrés par la règle 1, la règle 2 ne s'applique qu'aux objets de 1 Mo ou moins.

Exemple 3 : règles et règles ILM pour une meilleure protection des fichiers image

Vous pouvez utiliser les exemples de règles et de règles suivants pour vous assurer que les images de plus de 1 Mo sont codées par effacement et que les deux copies sont faites d'images plus petites.

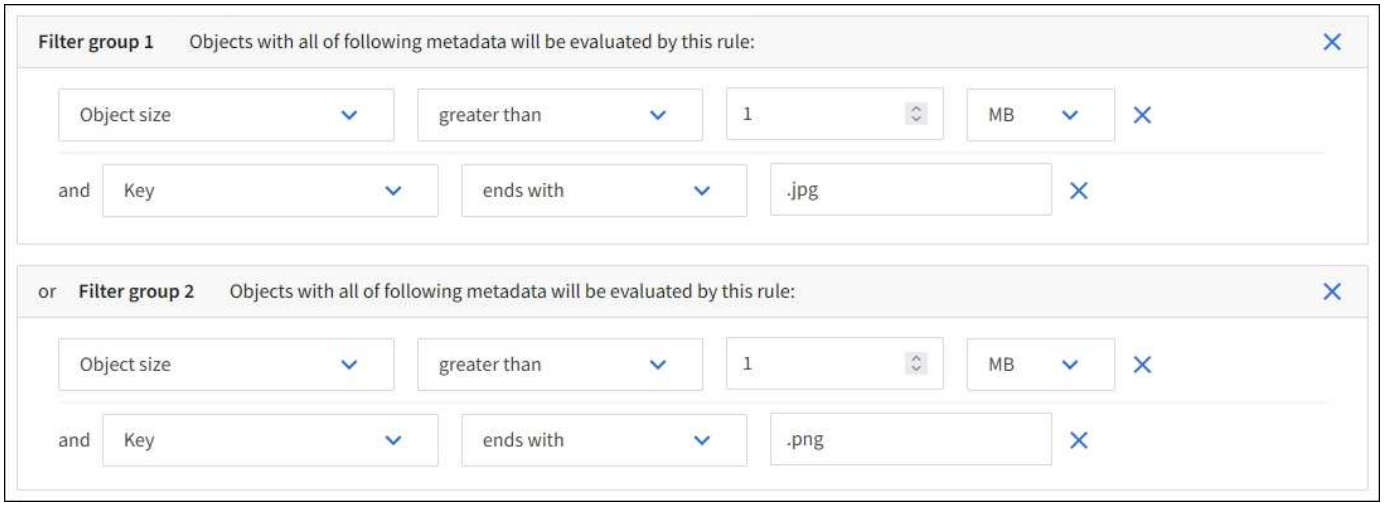
Les règles et règles ILM suivantes ne sont que des exemples. Les règles ILM sont nombreuses. Avant d'activer une nouvelle stratégie, simulez la stratégie proposée pour confirmer qu'elle fonctionnera comme destinée à protéger le contenu contre la perte.

Règle ILM 1 par exemple 3 : utilisez EC pour les fichiers image de plus de 1 Mo

Cet exemple de règle ILM utilise un filtrage avancé pour code d'effacement de tous les fichiers image de plus de 1 Mo.

Le codage d'effacement convient mieux aux objets de plus de 1 Mo. N'utilisez pas le code d'effacement pour les objets inférieurs à 200 Ko afin d'éviter la surcharge liée à la gestion de très petits fragments de code d'effacement.

Définition de règle	Exemple de valeur
Nom de la règle	Fichiers image EC > 1 Mo
Heure de référence	Temps d'ingestion
Filtre avancé pour la taille de l'objet	Taille de l'objet supérieure à 1 Mo
Filtres avancés pour la clé	• Se termine par .jpg • Se termine par .png
Placements	Créez une copie avec code d'effacement 2+1 sur trois sites



Étant donné que cette règle est configurée comme la première règle de la règle, l'instruction de placement de code d'effacement s'applique uniquement aux fichiers .jpg et .png de plus de 1 Mo.

Règle ILM 2, par exemple 3 : création de 2 copies répliquées pour tous les fichiers d'images restants

Cet exemple de règle ILM utilise un filtrage avancé pour spécifier la réplication de fichiers d'images plus petits. Comme la première règle de la stratégie a déjà mis en correspondance des fichiers d'image de plus de 1 Mo, cette règle s'applique aux fichiers d'image de 1 Mo ou moins.

Définition de règle	Exemple de valeur
Nom de la règle	2 copies pour les fichiers image
Heure de référence	Temps d'ingestion
Filtres avancés pour la clé	• Se termine par .jpg • Se termine par .png
Placements	Créez 2 copies répliquées dans deux pools de stockage

Règle ILM, par exemple 3 : meilleure protection des fichiers image

Cet exemple de règle ILM comprend trois règles :

- La première règle code tous les fichiers image de plus de 1 Mo.
- La deuxième règle crée deux copies de tous les fichiers d'image restants (c'est-à-dire les images de 1 Mo ou plus).
- La règle par défaut s'applique à tous les objets restants (c'est-à-dire tous les fichiers non images).

Exemple 4 : règles et règles ILM pour les objets avec version S3

Si la gestion des versions est activée dans un compartiment S3, vous pouvez gérer les versions d'objet non actuelles en incluant des règles dans votre règle ILM qui utilisent « Noncurrent Time » comme heure de référence.

> Si vous spécifiez une durée de conservation limitée pour les objets, ces objets seront supprimés définitivement après la période de temps atteinte. Assurez-vous de bien comprendre la durée pendant laquelle les objets seront conservés.

Comme le montre cet exemple, vous pouvez contrôler la quantité de stockage utilisée par les objets avec version à l'aide d'instructions de placement différentes pour les versions d'objets non actuelles.

> Les règles et règles ILM suivantes ne sont que des exemples. Les règles ILM sont nombreuses. Avant d'activer une nouvelle stratégie, simulez la stratégie proposée pour confirmer qu'elle fonctionnera comme destinée à protéger le contenu contre la perte.

> Pour effectuer une simulation de règle ILM sur une version non actuelle d'un objet, vous devez connaître l'UUID ou CBID de la version de l'objet. Pour rechercher l'UUID et le CBID, utilisez "recherche de métadonnées d'objet" alors que l'objet est toujours actif.

Informations associées

- "Comment supprimer les objets"

Règle ILM 1, par exemple 4 : trois copies économisées sur 10 ans

Cet exemple de règle ILM stocke une copie de chaque objet sur trois sites pendant 10 ans.

Cette règle s’applique à tous les objets, qu’ils soient versionnés ou non.

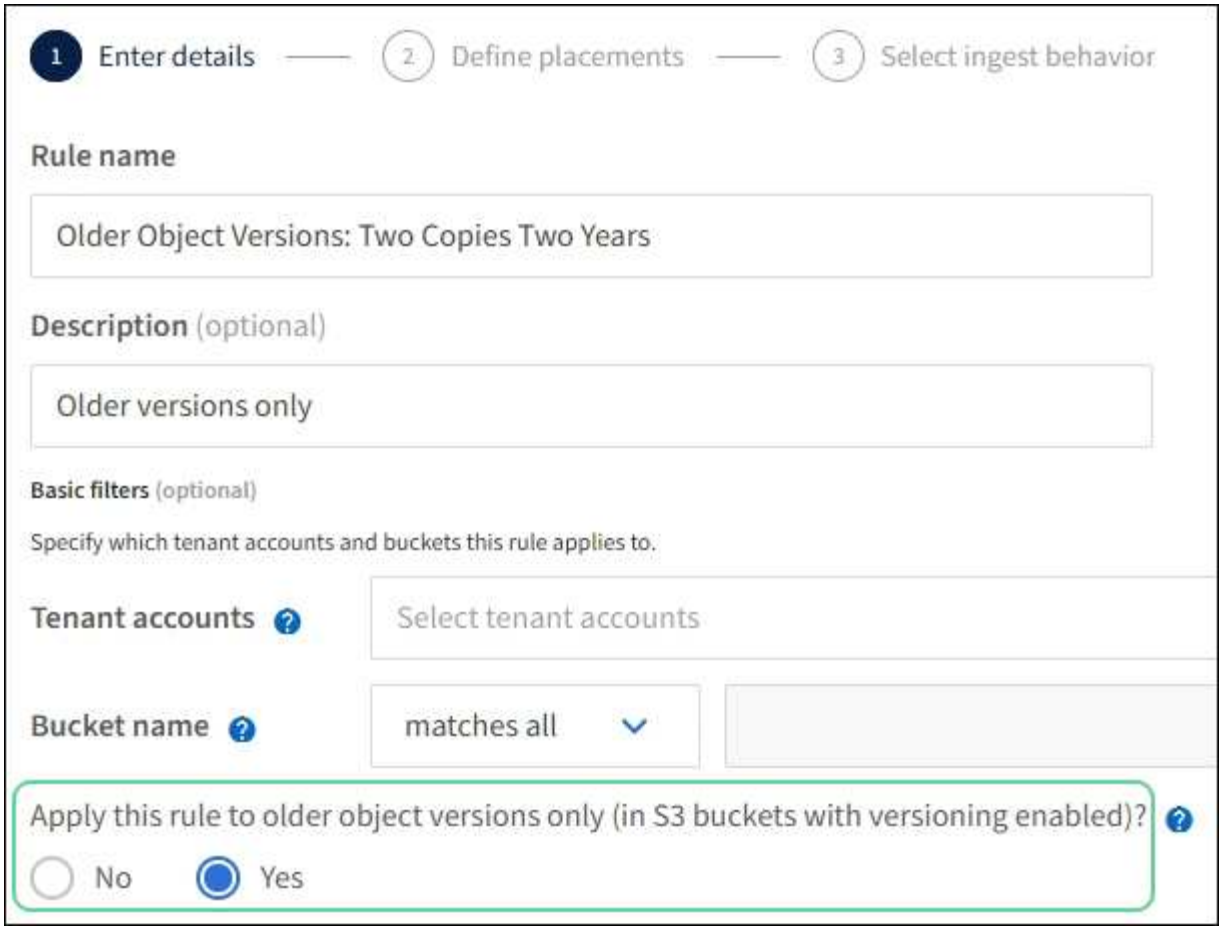
Définition de règle	Exemple de valeur
Pools de stockage	Trois pools de stockage, chacun étant constitué de data centers différents : site 1, site 2 et site 3.
Nom de la règle	Trois copies dix ans
Heure de référence	Temps d’ingestion
Placements	Au jour 0, conservez trois copies répliquées pendant 10 ans (3,652 jours), une dans le site 1, une dans le site 2 et une dans le site 3. Au bout de 10 ans, supprimez toutes les copies de l’objet.

Règle ILM 2, par exemple 4 : enregistrez deux copies de versions non actuelles pendant 2 ans

Cet exemple de règle ILM stocke deux copies des versions non actuelles d’un objet avec version S3 pendant 2 ans.

La règle ILM 1 s’applique à toutes les versions de l’objet, c’est pourquoi vous devez créer une autre règle pour filtrer toutes les versions non actuelles.

Pour créer une règle qui utilise « Noncurrent Time » comme heure de référence, sélectionnez **Oui** pour la question, « appliquer cette règle aux anciennes versions d’objet uniquement (dans les compartiments S3 avec la gestion des versions activée) ? » À l’étape 1 (entrer les détails) de l’assistant de création de règles ILM. Lorsque vous sélectionnez **Oui**, *Noncurrent Time* est automatiquement sélectionné pour l’heure de référence et vous ne pouvez pas sélectionner une autre heure de référence.



Dans cet exemple, seules deux copies des versions non actuelles sont stockées, et ces copies seront stockées pendant deux ans.

Définition de règle	Exemple de valeur
Pools de stockage	Deux pools de stockage, situés chacun au niveau de data centers différents : site 1 et site 2.
Nom de la règle	Versions non actuelles : deux copies deux ans
Heure de référence	Heure non actuelle Sélection automatique lorsque vous sélectionnez **Oui** pour la question, ""appliquer cette règle aux anciennes versions d'objet uniquement (dans les compartiments S3 avec gestion des versions activée)?" Dans l'assistant de création d'une règle ILM.
Placements	Le jour 0 par rapport à l'heure non courante (c'est-à-dire, à partir du jour où la version de l'objet devient la version non actuelle), conserver deux copies répliquées des versions de l'objet non actuel pendant 2 ans (730 jours), une dans le site 1 et une dans le site 2. À la fin de 2 ans, supprimer les versions non actuelles.

Règle ILM, par exemple 4 : objets avec version S3

Si vous souhaitez gérer des versions plus anciennes d'un objet différemment de la version actuelle, les règles qui utilisent « Noncurrent Time » comme heure de référence doivent apparaître dans la politique ILM avant les règles qui s'appliquent à la version d'objet actuelle.

Une règle ILM pour les objets avec version S3 peut inclure des règles ILM :

- Conservez les versions plus anciennes (non actuelles) de chaque objet pendant 2 ans, à partir du jour où la version n'est plus à jour.

> Les règles « Noncurrent Time » doivent apparaître dans la stratégie avant les règles qui s'appliquent à la version d'objet actuelle. Sinon, les versions d'objet non actuelles ne seront jamais mises en correspondance avec la règle « Noncurrent Time ».

- Lors de l'ingestion, créez trois copies répliquées et stockez une copie sur chacun des trois sites. Conservez les copies de la version actuelle de l'objet pendant 10 ans.

Lorsque vous simulez l'exemple de stratégie, vous vous attendez à ce que les objets test soient évalués comme suit :

- Toutes les versions d'objet non courantes seront mises en correspondance par la première règle. Si une version d'objet non actuelle a plus de 2 ans, elle est supprimée définitivement par ILM (toutes les copies de la version non actuelle sont supprimées de la grille).

> Pour simuler des versions d'objet non actuelles, vous devez utiliser l'UUID ou le CBID de cette version. Bien que l'objet soit toujours actif, vous pouvez l'utiliser "recherche de métadonnées d'objet" Pour trouver son UUID et son CBID.

- La version actuelle de l'objet sera comparée à la seconde règle. Lorsque la version d'objet actuelle est stockée pendant 10 ans, le processus ILM ajoute un marqueur de suppression comme version actuelle de l'objet et rend la version d'objet précédente « non actuelle ». Lors de la prochaine évaluation ILM, cette version non actuelle est mise en correspondance avec la première règle. Par conséquent, la copie sur le site 3 est purgée et les deux copies sur le site 1 et le site 2 sont conservées pendant 2 ans supplémentaires.

Exemple 5 : règles et règles ILM pour un comportement d'ingestion strict

Vous pouvez utiliser un filtre d'emplacement et un comportement d'ingestion strict dans une règle pour empêcher la sauvegarde des objets dans un emplacement de data Center spécifique.

Dans cet exemple, un locataire basé à Paris ne veut pas stocker certains objets en dehors de l'UE en raison de préoccupations réglementaires. Les autres objets, et notamment tous les objets des autres comptes locataires, peuvent être stockés dans le data Center de Paris ou dans le data Center des États-Unis.

> Les règles et règles ILM suivantes ne sont que des exemples. Les règles ILM sont nombreuses. Avant d'activer une nouvelle stratégie, simulez la stratégie proposée pour confirmer qu'elle fonctionnera comme destinée à protéger le contenu contre la perte.

Informations associées

- "Options d'ingestion"

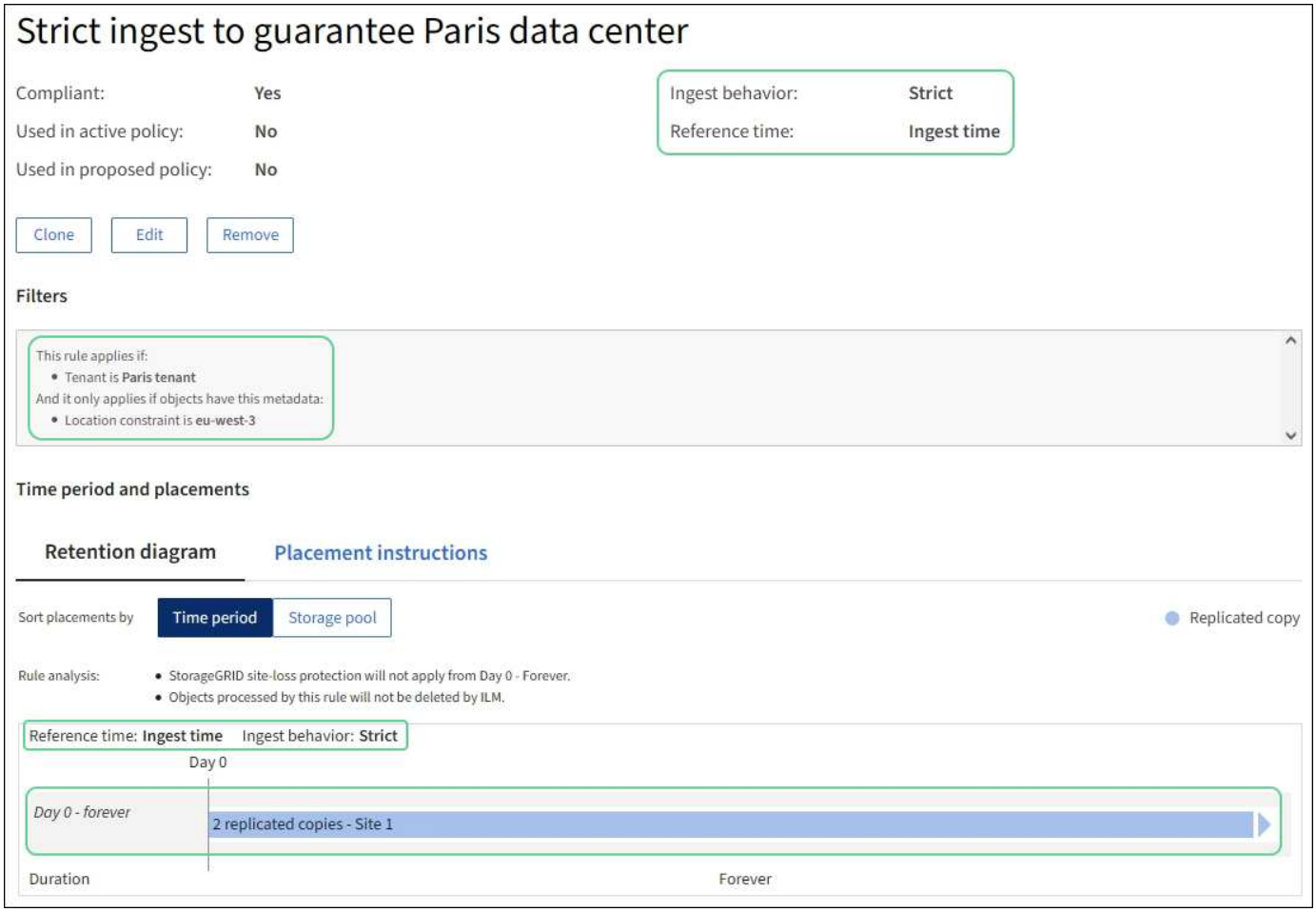
- "Créer une règle ILM : sélectionnez le comportement d'ingestion"

La règle ILM 1, par exemple 5 : une ingestion stricte pour la garantie du data Center Paris

Cet exemple de règle ILM utilise un comportement d'ingestion strict afin de garantir que les objets enregistrés par un locataire Paris dans des compartiments S3 avec la région UE-West-3 (Paris) ne sont jamais stockés dans le data Center des États-Unis.

Cette règle s'applique aux objets appartenant au locataire Paris et dont la région du compartiment S3 est définie sur eu-West-3 (Paris).

Définition de règle	Exemple de valeur
Compte locataire	Locataire Paris
Filtre avancé	Contrainte de localisation égale à eu-West-3
Pools de stockage	Site 1 (Paris)
Nom de la règle	Ingestion stricte pour le data Center de Paris
Heure de référence	Temps d'ingestion
Placements	Au jour 0, conservation de deux copies répliquées pour toujours dans le site 1 (Paris)
Comportement d'ingestion	Stricte. Utilisez toujours les placements de cette règle lors de l'entrée. L'ingestion échoue s'il est impossible de stocker deux copies de l'objet dans le data Center de Paris.



La règle ILM 2, par exemple 5, « ingestion équilibrée » pour d'autres objets

Cet exemple de règle ILM utilise le comportement d'ingestion équilibré pour offrir une efficacité ILM optimale pour tous les objets qui ne sont pas mis en correspondance avec la première règle. Deux copies de tous les objets correspondant à cette règle seront stockées : une dans le data Center des États-Unis et une dans le data Center de Paris. Si la règle ne peut pas être satisfaite immédiatement, les copies provisoires sont stockées à n'importe quel emplacement disponible.

Cette règle s'applique aux objets appartenant à n'importe quel locataire et à n'importe quelle région.

Définition de règle	Exemple de valeur
Compte locataire	Ignorer
Filtre avancé	*Non spécifié*
Pools de stockage	Site 1 (Paris) et site 2 (US)
Nom de la règle	2 copies 2 data centers
Heure de référence	Temps d'ingestion

Définition de règle	Exemple de valeur
Placements	Au premier jour, conservez deux copies répliquées à jamais dans deux data centers
Comportement d'ingestion	Équilibré. Si possible, les objets qui correspondent à cette règle sont placés conformément aux instructions de positionnement de la règle. Dans le cas contraire, des copies provisoires sont effectuées à tout emplacement disponible.

Règle ILM, par exemple 5 : combinaison de comportements d'ingestion

L'exemple de règle ILM comprend deux règles ayant des comportements d'entrée différents.

Deux règles ILM sont appliquées à deux comportements d'ingestion, notamment :

- Stockez des objets qui appartiennent au locataire Paris et qui disposent de la région du compartiment S3 définie sur eu-West-3 (Paris) uniquement dans le data Center de Paris. Echec de l'ingestion si le centre de données Paris n'est pas disponible.
- Stockez tous les autres objets (y compris ceux qui appartiennent à un locataire Paris mais qui disposent d'une région de compartiment différente) dans le data Center américain et dans le data Center de Paris. Faites des copies intermédiaires à n'importe quel emplacement disponible si l'instruction de placement ne peut pas être satisfaite.

Lorsque vous simulez l'exemple de stratégie, vous vous attendez à ce que les objets test soient évalués comme suit :

- Tous les objets qui appartiennent au locataire Paris et qui disposent de la région du compartiment S3 définie sur eu-West-3 sont mis en correspondance par la première règle et stockés dans le data Center de Paris. La première règle utilise une ingestion stricte. Ces objets ne sont donc jamais stockés dans le data Center des États-Unis. Si les nœuds de stockage du data Center de Paris ne sont pas disponibles, l'ingestion échoue.
- Tous les autres objets sont comparés à la seconde règle, y compris les objets appartenant au locataire Paris et dont la région de compartiment S3 n'est pas définie sur eu-West-3. Une copie de chaque objet est enregistrée dans chaque data Center. Cependant, la seconde règle utilise une ingestion équilibrée, si un data Center n'est plus disponible, deux copies intermédiaires sont enregistrées à tout emplacement disponible.

Exemple 6 : modification d'une règle ILM

Si vous devez modifier la protection de vos données ou ajouter de nouveaux sites, vous pouvez créer et activer une nouvelle règle ILM.

Avant de modifier une règle, vous devez savoir comment les modifications apportées aux règles ILM peuvent affecter temporairement les performances globales d'un système StorageGRID.

Dans cet exemple, un nouveau site StorageGRID a été ajouté dans une extension et une nouvelle règle ILM active doit être implémentée pour stocker les données sur le nouveau site. Pour mettre en œuvre une nouvelle politique active, commencez par créer une politique proposée par l'une ou l'autre "clonage d'une règle existante *ou* à partir de zéro". Ensuite, vous devez "simuler" puis "activer" la nouvelle politique.

Les règles et règles ILM suivantes ne sont que des exemples. Les règles ILM sont nombreuses. Avant d'activer une nouvelle stratégie, simulez la stratégie proposée pour confirmer qu'elle fonctionnera comme destinée à protéger le contenu contre la perte.

Impact de la modification d'une règle ILM sur les performances

Lorsque vous activez une nouvelle règle ILM, les performances de votre système StorageGRID peuvent être temporairement affectées, en particulier si les instructions de placement dans la nouvelle règle requièrent le déplacement d'un grand nombre d'objets existants vers de nouveaux emplacements.

Lorsque vous activez une nouvelle règle ILM, StorageGRID l'utilise pour gérer tous les objets, y compris les objets existants et les objets récemment ingérées. Avant d'activer une nouvelle règle ILM, vérifiez toutes les modifications du placement des objets répliqués et soumis au code d'effacement. La modification de l'emplacement d'un objet existant peut entraîner des problèmes de ressources temporaires lorsque les nouveaux placements sont évalués et implémentés.

Vous pouvez vérifier qu'une nouvelle règle ILM n'affecte pas le placement des objets répliqués et soumis au code d'effacement "Créez une règle ILM avec un filtre de temps d'ingestion". Par exemple, **heure d'ingestion *est on ou after <date and time>***, de sorte que la nouvelle règle s'applique uniquement aux objets ingérés à la date et à l'heure spécifiées ou après.

Les types de modifications de règles ILM susceptibles d'affecter temporairement les performances de StorageGRID sont les suivants :

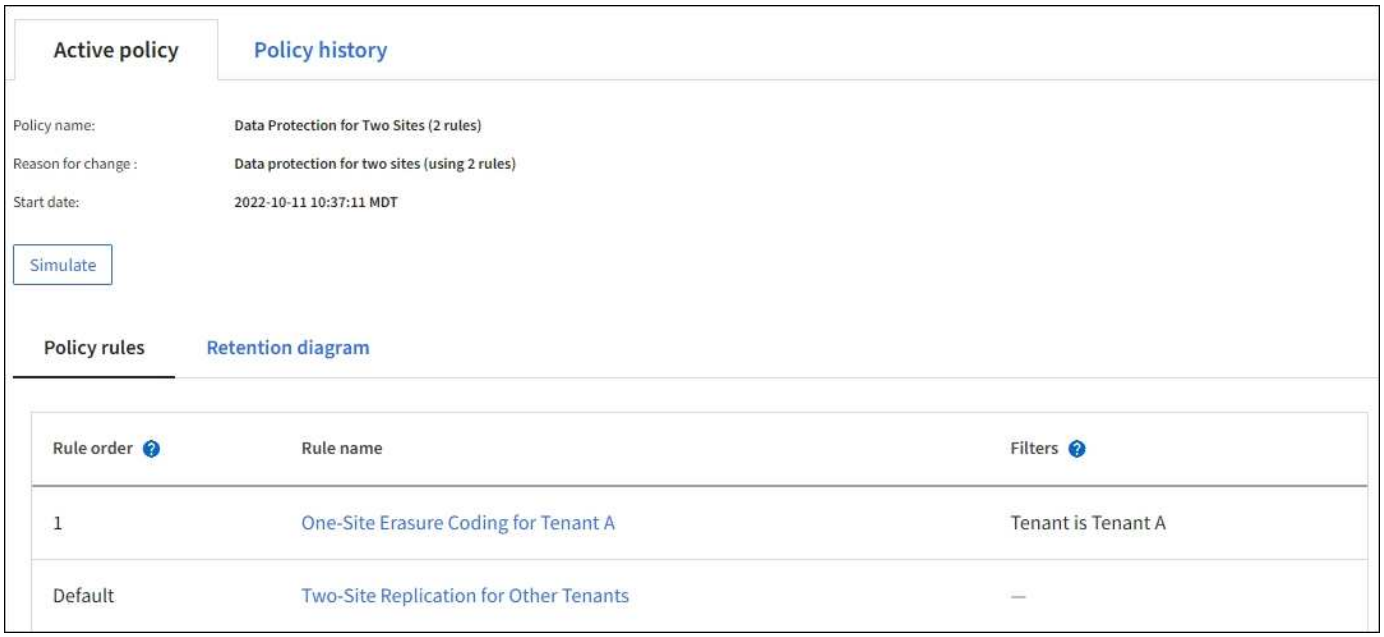
- Appliquer un profil de code d'effacement différent aux objets avec code d'effacement existants.

  StorageGRID considère chaque profil de code d'effacement comme unique et ne réutilise pas les fragments de code d'effacement lorsqu'un nouveau profil est utilisé.

- Modification du type de copies requis pour les objets existants (par exemple, conversion d'un grand pourcentage d'objets répliqués en objets avec code d'effacement).
- Déplacement des copies d'objets existants vers un emplacement totalement différent (par exemple, déplacement d'un grand nombre d'objets vers ou depuis un pool de stockage cloud, vers ou depuis un site distant).

Règle ILM active, par exemple 6 : protection des données sur deux sites

Dans cet exemple, la politique ILM active a été initialement conçue pour un système StorageGRID à deux sites et utilise deux règles ILM.



Dans cette politique ILM, les objets appartenant au locataire A sont protégés par un code d'effacement 2+1 sur un seul site, tandis que les objets de tous les autres locataires sont protégés sur deux sites à l'aide de la réplication à 2 copies.

> La première règle de cet exemple utilise un filtre avancé pour s'assurer que le codage d'effacement n'est pas utilisé pour les petits objets. Tous les objets du tenant A qui sont inférieurs à 1 Mo seront protégés par la règle par défaut, qui utilise la réplication.

Règle 1 : code d'effacement sur un site pour le locataire A

Définition de règle	Exemple de valeur
Nom de la règle	Code d'effacement sur un site pour le locataire A
Compte de locataire	Locataire A
Pool de stockage	Site 1
Placements	Code d'effacement 2+1 sur le site 1, du jour 0 à l'infini

Règle 2 : réplication sur deux sites pour d'autres locataires

Définition de règle	Exemple de valeur
Nom de la règle	Réplication sur deux sites pour d'autres locataires
Compte de locataire	Ignorer
Pools de stockage	Site 1 et site 2

Définition de règle	Exemple de valeur
Placements	Deux copies répliquées du jour 0 au jour toujours : une copie sur le site 1 et une copie sur le site 2.

Politique ILM proposée, par exemple 6 : protection des données sur trois sites

Dans cet exemple, la politique ILM est remplacée par une nouvelle règle pour un système StorageGRID à trois sites.

Après avoir effectué une extension pour ajouter le nouveau site, l'administrateur de la grille a créé deux nouveaux pools de stockage : un pool de stockage pour le site 3 et un pool de stockage contenant les trois sites (différent du pool de stockage par défaut de tous les nœuds de stockage). L'administrateur a ensuite créé deux nouvelles règles ILM et une nouvelle règle ILM, conçue pour protéger les données des trois sites.

Lors de l'activation de cette nouvelle politique ILM, les objets appartenant au locataire A seront protégés par un code d'effacement 2+1 sur trois sites, tandis que les objets appartenant à d'autres locataires (et les objets de plus petite taille appartenant au locataire A) sont protégés sur trois sites à l'aide de la réplication à 3 copies.

Règle 1 : code d'effacement à trois sites pour le locataire A

Définition de règle	Exemple de valeur
Nom de la règle	Code d'effacement à trois sites pour le locataire A
Compte de locataire	Locataire A
Pool de stockage	Tous les sites 3 (y compris le site 1, le site 2 et le site 3)
Placements	Code d'effacement 2+1 sur les 3 sites, du jour 0 à l'infini

Règle 2 : réplication sur trois sites pour d'autres locataires

Définition de règle	Exemple de valeur
Nom de la règle	Réplication sur trois sites pour les autres locataires
Compte de locataire	Ignorer
Pools de stockage	Site 1, site 2 et site 3
Placements	Trois copies répliquées du jour 0 au jour toujours : une copie sur le site 1, une copie sur le site 2 et une copie sur le site 3.

Activation de la politique ILM proposée, par exemple 6

Lorsque vous activez une nouvelle règle ILM, les objets existants peuvent être déplacés vers de nouveaux emplacements ou de nouvelles copies d'objet peuvent être créées pour des objets existants, en fonction des instructions de placement fournies dans toutes les règles mises à jour ou nouvelles.

Les erreurs de la règle ILM peuvent entraîner des pertes de données irrécupérables. Examinez attentivement et simulez la stratégie avant de l'activer pour confirmer qu'elle fonctionnera comme prévu.

Lorsque vous activez une nouvelle règle ILM, StorageGRID l'utilise pour gérer tous les objets, y compris les objets existants et les objets récemment ingérées. Avant d'activer une nouvelle règle ILM, vérifiez toutes les modifications du placement des objets répliqués et soumis au code d'effacement. La modification de l'emplacement d'un objet existant peut entraîner des problèmes de ressources temporaires lorsque les nouveaux placements sont évalués et implémentés.

Que se passe-t-il en cas de modification des instructions de code d'effacement

Dans cet exemple de règle ILM active, les objets appartenant au locataire A sont protégés par un code d'effacement 2+1 sur le site 1. Dans la nouvelle politique ILM proposée, les objets appartenant au locataire A seront protégés par un code d'effacement 2+1 sur les sites 1, 2 et 3.

Lorsque la nouvelle règle ILM est activée, les opérations ILM suivantes se produisent :

- Les nouveaux objets ingérés par le locataire A sont divisés en deux fragments de données et un fragment de parité est ajouté. Ensuite, chacun des trois fragments est stocké sur un site différent.
- Les objets existants appartenant au locataire A sont réévalués au cours du processus d'analyse ILM en cours. Les instructions de placement ILM utilisent un nouveau profil de code d'effacement, c'est pourquoi de nouveaux fragments avec code d'effacement sont créés et distribués sur les trois sites.

Les fragments 2+1 existants au site 1 ne sont pas réutilisés. StorageGRID considère chaque profil de code d'effacement comme unique et ne réutilise pas les fragments de code d'effacement lorsqu'un nouveau profil est utilisé.

Ce qui se passe lorsque les instructions de réplication changent

Dans cet exemple de règle ILM active, les objets appartenant à d'autres locataires sont protégés par deux copies répliquées dans les pools de stockage des sites 1 et 2. Dans la nouvelle règle ILM proposée, les objets appartenant à d'autres locataires seront protégés par trois copies répliquées dans les pools de stockage des sites 1, 2 et 3.

Lorsque la nouvelle règle ILM est activée, les opérations ILM suivantes se produisent :

- Lorsqu'un locataire autre que le locataire A ingère un nouvel objet, StorageGRID crée trois copies et en enregistre une copie sur chaque site.
- Les objets existants appartenant à ces autres locataires sont réévalués en cours d'analyse ILM. Étant donné que les copies d'objet existantes sur le site 1 et le site 2 continuent à satisfaire les exigences de réplication de la nouvelle règle ILM, StorageGRID ne doit créer qu'une seule copie de l'objet pour le site 3.

Impact sur les performances de l'activation de cette stratégie

Lorsque la politique ILM proposée dans cet exemple est activée, les performances globales de ce système StorageGRID sont temporairement affectées. Des niveaux de ressources de grid supérieurs à la normale seront nécessaires pour créer de nouveaux fragments avec code d'effacement pour les objets existants du locataire A et pour les nouvelles copies répliquées sur le site 3 pour les objets existants des autres locataires.

Suite à une modification de la règle ILM, les demandes de lecture et d'écriture des clients peuvent présenter

temporairement des latences supérieures à la normale. Une fois que les instructions de placement sont entièrement mises en œuvre sur la grille, les latences reprennent aux niveaux normaux.

Pour éviter les problèmes de ressources lors de l'activation d'une nouvelle stratégie ILM, vous pouvez utiliser le filtre avancé heure d'ingestion dans toute règle susceptible de modifier l'emplacement d'un grand nombre d'objets existants. Définissez le temps d'ingestion sur une valeur supérieure ou égale à la durée approximative de l'entrée en vigueur de la nouvelle règle pour vous assurer que les objets existants ne sont pas déplacés inutilement.

> Contactez le support technique si vous avez besoin de ralentir ou d'augmenter le taux de traitement des objets après une modification de la règle ILM.

Exemple 7 : règle ILM conforme pour le verrouillage d'objet S3

Vous pouvez utiliser le compartiment S3, les règles ILM et la règle ILM dans cet exemple à partir d'un point de départ lors de la définition d'une règle ILM afin de répondre aux exigences de protection et de conservation des objets dans des compartiments où le verrouillage d'objet S3 est activé.

> Si vous avez utilisé la fonctionnalité de conformité héritée dans les versions précédentes de StorageGRID, vous pouvez également utiliser cet exemple pour gérer les compartiments existants pour lesquels la fonctionnalité de conformité héritée est activée.

> Les règles et règles ILM suivantes ne sont que des exemples. Les règles ILM sont nombreuses. Avant d'activer une nouvelle stratégie, simulez la stratégie proposée pour confirmer qu'elle fonctionnera comme destinée à protéger le contenu contre la perte.

Informations associées

- "Gestion des objets avec le verrouillage d'objets S3"
- "Création d'une règle ILM"

Exemple de compartiment et d'objets pour le verrouillage d'objet S3

Dans cet exemple, un compte de locataire S3 nommé Bank of ABC a utilisé le gestionnaire de locataires pour créer un compartiment avec le verrouillage objet S3 activé pour stocker les enregistrements bancaires stratégiques.

Définition du compartiment	Exemple de valeur
Nom du compte du locataire	Banque d'ABC
Nom du compartiment	les registres bancaires
Région du godet	us-east-1 (par défaut)

Chaque objet et version d'objet ajoutés au compartiment des enregistrements bancaires utilise les valeurs suivantes pour `retain-until-date` et `legal hold` paramètres.

Paramètre pour chaque objet	Exemple de valeur
`retain-until-date`	`"2030-12-30T23:59:59Z"` (30 décembre 2030) Chaque version d'objet a sa propre version `retain-until-date` réglage. Ce réglage peut être augmenté, mais pas diminué.
`legal hold`	`"OFF"` (Pas en vigueur) Une mise en garde légale peut être placée ou levée sur n'importe quelle version d'objet à tout moment pendant la période de conservation. Si un objet fait l'objet d'une conservation légale, il ne peut pas être supprimé, même si l' `retain-until-date` a été atteint.

Règle ILM 1 pour S3 Object Lock exemple : profil de code d'effacement avec mise en correspondance des compartiments

Cet exemple de règle ILM s'applique uniquement au compte de locataire S3 nommé Bank of ABC. Il correspond à n'importe quel objet du `bank-records` Et utilise le code d'effacement pour stocker l'objet sur des nœuds de stockage sur trois sites de data Center en utilisant un profil de code d'effacement 6+3. Cette règle satisfait aux exigences des compartiments avec S3 Object Lock activé : une copie est conservée sur les nœuds de stockage du jour 0 à l'infini, en utilisant l'heure d'ingestion comme heure de référence.

Définition de règle	Exemple de valeur
Nom de la règle	Règle de conformité : objets EC dans le compartiment des enregistrements bancaires - Banque d'ABC
Compte de locataire	Banque d'ABC
Nom du compartiment	`bank-records`
Filtre avancé	Taille de l'objet (Mo) supérieure à 1 **Remarque :** ce filtre garantit que le codage d'effacement n'est pas utilisé pour les objets de 1 Mo ou plus.

Définition de règle	Exemple de valeur
Heure de référence	Temps d'ingestion
Placements	À partir du jour 0 magasin pour toujours
Profil de codage d'effacement	• Créez une copie avec code d'effacement sur les nœuds de stockage de trois sites de data Center • Utilise le schéma de code d'effacement 6+3

Règle ILM 2 pour exemple de verrouillage d'objet S3 : règle non compatible

Cet exemple de règle ILM stocke au départ deux copies d'objet répliquées sur les nœuds de stockage. Après un an, il stocke une copie sur un pool de stockage cloud pour toujours. Cette règle utilise un pool de stockage cloud. Elle n'est pas conforme et ne s'applique pas aux objets des compartiments où le verrouillage des objets S3 est activé.

Définition de règle	Exemple de valeur
Nom de la règle	Règle non conforme : utilisez le pool de stockage cloud
Comptes de locataires	Non spécifié
Nom du compartiment	Non spécifié, mais s'appliquera uniquement aux compartiments pour lesquels le verrouillage d'objet S3 (ou la fonction conformité héritée) n'est pas activé.
Filtre avancé	Non spécifié

Définition de règle	Exemple de valeur
Heure de référence	Temps d'ingestion
Placements	• Le premier jour, conservez deux copies répliquées sur les nœuds de stockage dans le data Center 1 et dans le data Center 2 pendant 365 jours • Après 1 an, conservez une copie répliquée dans un pool de stockage cloud à jamais

Règle ILM 3 pour l'exemple de verrouillage d'objet S3 : règle par défaut

Cet exemple de règle ILM copie les données d'objet vers les pools de stockage dans deux data centers. Cette règle conforme est conçue pour être la règle par défaut dans la politique ILM. Elle n'inclut aucun filtre, n'utilise pas l'heure de référence non actuelle et répond aux exigences des compartiments avec le verrouillage objet S3 activé : deux copies d'objet sont conservées sur les nœuds de stockage du jour 0 à l'infini, et l'ingestion comme heure de référence.

Définition de règle	Exemple de valeur
Nom de la règle	Règle de conformité par défaut : deux copies de deux data centers
Compte locataire	Non spécifié
Nom du compartiment	Non spécifié
Filtre avancé	Non spécifié

Définition de règle	Exemple de valeur
Heure de référence	Temps d'ingestion
Placements	Dès le premier jour, conservez deux copies répliquées : une sur des nœuds de stockage dans le data Center 1 et une sur des nœuds de stockage dans le data Center 2.

Exemple de règle ILM conforme pour l'exemple de verrouillage d'objet S3

Pour créer une règle ILM protégeant efficacement tous les objets de votre système, y compris ceux des compartiments avec le verrouillage objet S3 activé, vous devez sélectionner des règles ILM qui répondent aux besoins de stockage de tous les objets. Vous devez ensuite simuler et activer la règle proposée.

Ajouter des règles à la règle

Dans cet exemple, la politique ILM inclut trois règles ILM, dans l'ordre suivant :

1. Règle conforme qui utilise le code d'effacement pour protéger les objets de plus de 1 Mo dans un compartiment spécifique avec le verrouillage objet S3 activé. Les objets sont stockés sur les nœuds de stockage du premier jour vers toujours.
2. Une règle non conforme qui crée deux copies d'objets répliquées sur les nœuds de stockage pendant un an, puis déplace une copie d'objet vers un pool de stockage cloud à tout moment. Cette règle ne s'applique pas aux compartiments avec le verrouillage d'objet S3 activé car elle utilise un pool de stockage cloud.
3. La règle de conformité par défaut qui crée deux copies d'objets répliquées sur les nœuds de stockage du jour 0 à l'infini.

Simuler la règle proposée

Une fois que vous avez ajouté des règles dans la stratégie proposée, choisi une règle conforme par défaut et arrangé les autres règles, vous devez simuler la règle en testant les objets à partir du compartiment avec le verrouillage d'objet S3 activé et à partir d'autres compartiments. Par exemple, lorsque vous simulez l'exemple de règle, vous attendez à ce que les objets test soient évalués comme suit :

- La première règle correspond uniquement aux objets de test supérieurs à 1 Mo dans les banques d'enregistrements du compartiment pour le locataire Bank of ABC.
- La deuxième règle fait correspondre tous les objets de tous les compartiments non conformes pour tous les autres comptes de tenant.
- La règle par défaut correspond à ces objets :
  - Objets de 1 Mo ou plus petits dans les banques d'enregistrements du compartiment pour le locataire Banque d'ABC.
  - Objets dans tout autre compartiment pour lequel le verrouillage objet S3 est activé pour tous les autres comptes locataires.

Activer la règle

Si vous êtes pleinement satisfait de la nouvelle règle assurant la protection des données d'objet comme prévu, vous pouvez l'activer.

Durcissement du système

Durcissement du système : vue d'ensemble

Le renforcement des systèmes consiste à éliminer autant de risques que possible pour la sécurité d'un système StorageGRID.

Ce document présente les directives de renforcement propres à StorageGRID. Ces directives constituent un complément aux meilleures pratiques standard du secteur en matière de renforcement des systèmes. Par exemple, ces instructions partent du principe que vous utilisez des mots de passe forts pour StorageGRID, utilisez HTTPS au lieu de HTTP et activez l'authentification basée sur les certificats, le cas échéant.

Lors de l'installation et de la configuration de StorageGRID, ces instructions vous aideront à répondre aux objectifs de sécurité que vous avez définis pour la confidentialité, l'intégrité et la disponibilité des systèmes d'information.

StorageGRID suit le "Politique de gestion des vulnérabilités de NetApp". Toutes les vulnérabilités signalées sont vérifiées et traitées selon le processus de réponse aux incidents de sécurité.

Considérations générales relatives au renforcement des systèmes StorageGRID

Lors du renforcement d'un système StorageGRID, vous devez prendre en compte les éléments suivants :

- Parmi les trois réseaux StorageGRID que vous avez mis en place, lesquels ? Tous les systèmes StorageGRID doivent utiliser le réseau Grid, mais vous pouvez également utiliser le réseau Admin, le réseau client ou les deux. Chaque réseau a des considérations de sécurité différentes.
- Type de plateforme utilisé pour les nœuds individuels du système StorageGRID. Les nœuds StorageGRID peuvent être déployés sur des machines virtuelles VMware, au sein d'un moteur de conteneurs sur des hôtes Linux, ou en tant qu'appliances matérielles dédiées. Chaque type de plateforme dispose de son propre ensemble de meilleures pratiques en matière de renforcement.
- Fiabilité des comptes locataires. Si vous êtes un fournisseur de services avec des comptes de locataires non fiables, vous vous interrogez différemment que si vous utilisez uniquement des locataires internes fiables.
- Les exigences et conventions de sécurité sont respectées par votre entreprise. Vous devrez peut-être vous conformer à des exigences réglementaires ou d'entreprise spécifiques.

Directives de renforcement des mises à niveau logicielles

Vous devez maintenir votre système StorageGRID et les services associés à jour pour vous protéger contre les attaques.

Mises à niveau du logiciel StorageGRID

Dans la mesure du possible, vous devez mettre à niveau le logiciel StorageGRID vers la version principale la plus récente ou vers la version majeure précédente. Maintenir StorageGRID à jour permet de réduire le temps d'activation des vulnérabilités connues et de réduire la surface d'attaque globale. En outre, les versions les plus récentes de StorageGRID comprennent souvent des fonctionnalités de renforcement de la sécurité qui ne sont pas incluses dans les versions précédentes.

Consulter le "Matrice d'interopérabilité NetApp" (IMT) pour déterminer quelle version du logiciel StorageGRID vous devez utiliser. Lorsqu'un correctif est requis, NetApp privilégie la création de mises à jour pour les

dernières versions. Certains correctifs peuvent ne pas être compatibles avec les versions antérieures.

- Pour télécharger les versions et correctifs StorageGRID les plus récents, rendez-vous sur le site "Téléchargement NetApp : StorageGRID".
- Pour mettre à niveau le logiciel StorageGRID, reportez-vous au "instructions de mise à niveau".
- Pour appliquer un correctif, reportez-vous au "Procédure de correctif StorageGRID".

Mises à niveau vers des services externes

Les services externes peuvent comporter des vulnérabilités qui affectent indirectement StorageGRID. Vous devez vous assurer que les services dont dépend StorageGRID sont tenus à jour. Ces services incluent : LDAP, KMS (ou serveur KMIP), DNS et NTP.

Utilisez le "Matrice d'interopérabilité NetApp" pour obtenir une liste des versions prises en charge.

Mises à niveau vers les hyperviseurs

Si vos nœuds StorageGRID s'exécutent sur VMware ou sur un autre hyperviseur, vous devez vous assurer que le logiciel et le firmware de l'hyperviseur sont à jour.

Utilisez le "Matrice d'interopérabilité NetApp" pour obtenir une liste des versions prises en charge.

Mises à niveau vers les nœuds Linux

Si vos nœuds StorageGRID utilisent des plates-formes hôtes Linux, vous devez vous assurer que les mises à jour de sécurité et de noyau sont appliquées au système d'exploitation hôte. En outre, vous devez appliquer des mises à jour de micrologiciel au matériel vulnérable lorsque ces mises à jour sont disponibles.

Utilisez le "Matrice d'interopérabilité NetApp" pour obtenir une liste des versions prises en charge.

Instructions de renforcement des réseaux StorageGRID

Le système StorageGRID prend en charge jusqu'à trois interfaces réseau par nœud grid, ce qui vous permet de configurer le réseau pour chaque nœud grid en fonction de vos besoins de sécurité et d'accès.

Pour plus d'informations sur les réseaux StorageGRID, reportez-vous au "Types de réseau StorageGRID".

Instructions relatives au réseau Grid

Vous devez configurer un réseau Grid pour tout le trafic StorageGRID interne. Tous les nœuds de la grille se trouvent sur le réseau Grid et ils doivent pouvoir communiquer avec tous les autres nœuds.

Lors de la configuration du réseau Grid, suivez les instructions suivantes :

- Assurez-vous que le réseau est sécurisé par des clients non approuvés, tels que ceux qui se trouvent sur Internet ouvert.
- Si possible, utilisez le réseau Grid exclusivement pour le trafic interne. Le réseau d'administration et le réseau client disposent d'autres restrictions de pare-feu qui bloquent le trafic externe vers les services internes. L'utilisation du réseau Grid pour le trafic client externe est prise en charge, mais cette utilisation offre moins de couches de protection.
- Si le déploiement StorageGRID s'étend sur plusieurs data centers, utilisez un réseau privé virtuel (VPN) ou

un équivalent sur le réseau Grid afin de protéger le trafic interne.

- Certaines procédures de maintenance exigent un accès SSH (Secure Shell) sur le port 22 entre le nœud d'administration principal et tous les autres nœuds de la grille. Utilisez un pare-feu externe pour restreindre l'accès SSH aux clients approuvés.

Instructions pour le réseau d'administration

Le réseau Admin est généralement utilisé pour les tâches d'administration (employés de confiance utilisant Grid Manager ou SSH) et pour la communication avec d'autres services de confiance tels que LDAP, DNS, NTP, KMS (ou serveur KMIP). Cependant, StorageGRID n'applique pas cette utilisation en interne.

Si vous utilisez le réseau Admin, suivez les instructions suivantes :

- Bloquez tous les ports de trafic internes sur le réseau d'administration. Voir la "liste des ports internes".
- Si des clients non approuvés peuvent accéder au réseau d'administration, bloquez l'accès à StorageGRID sur le réseau d'administration avec un pare-feu externe.

Directives pour le réseau client

Le réseau client est généralement utilisé pour les locataires et pour communiquer avec des services externes, tels que le service de réplication CloudMirror ou un autre service de plate-forme. Cependant, StorageGRID n'applique pas cette utilisation en interne.

Si vous utilisez le réseau client, suivez les instructions suivantes :

- Bloquer tous les ports de trafic interne sur le réseau client. Voir la "liste des ports internes".
- Acceptez le trafic client entrant uniquement sur les terminaux configurés explicitement. Voir les informations sur "gestion des contrôles de pare-feu".

Instructions de renforcement pour les nœuds StorageGRID

Les nœuds StorageGRID peuvent être déployés sur des machines virtuelles VMware, au sein d'un moteur de conteneurs sur des hôtes Linux, ou en tant qu'appliances matérielles dédiées. Chaque type de plateforme et chaque type de nœud dispose de ses propres pratiques de renforcement.

Configuration du pare-feu

Dans le cadre du processus de renforcement du système, vous devez examiner les configurations de pare-feu externes et les modifier afin que le trafic soit accepté uniquement à partir des adresses IP et sur les ports à partir desquels il est strictement nécessaire.

StorageGRID comprend un pare-feu interne sur chaque nœud qui améliore la sécurité de votre grille en vous permettant de contrôler l'accès réseau au nœud. Vous devriez "gérer les contrôles de pare-feu internes" pour empêcher l'accès au réseau sur tous les ports, à l'exception de ceux nécessaires à votre déploiement de grid spécifique. Les modifications de configuration effectuées sur la page de contrôle du pare-feu sont déployées sur chaque nœud.

Plus précisément, vous pouvez gérer les domaines suivants :

- **Adresses privilégiées** : vous pouvez autoriser certaines adresses IP ou sous-réseaux à accéder aux ports fermés par les paramètres de l'onglet gérer l'accès externe.

- **Gérer l'accès externe** : vous pouvez fermer les ports ouverts par défaut ou rouvrir les ports précédemment fermés.
- **Réseau client non approuvé** : vous pouvez spécifier si un nœud approuve le trafic entrant provenant du réseau client ainsi que les ports supplémentaires que vous souhaitez ouvrir lorsque le réseau client non approuvé est configuré.

Bien que ce pare-feu interne offre une couche supplémentaire de protection contre certaines menaces courantes, il ne supprime pas la nécessité d'un pare-feu externe.

Pour obtenir la liste de tous les ports internes et externes utilisés par StorageGRID, reportez-vous à la section "Référence du port réseau".

Désactiver les services inutilisés

Pour tous les nœuds StorageGRID, désactivez ou bloquez l'accès aux services non utilisés. Par exemple, si vous n'envisagez pas de configurer l'accès client aux partages d'audit pour NFS, bloquez ou désactivez l'accès à ces services.

Virtualisation, conteneurs et matériel partagé

Pour tous les nœuds StorageGRID, évitez d'exécuter StorageGRID sur le même matériel physique que les logiciels non fiables. Ne supposez pas que les protections de l'hyperviseur empêchent les logiciels malveillants d'accéder aux données protégées par StorageGRID si StorageGRID et le logiciel malveillant existent sur le même matériel physique. Par exemple, les attaques Meltdown et Specter exploitent des vulnérabilités critiques dans les processeurs modernes et permettent aux programmes de voler des données en mémoire sur le même ordinateur.

Protéger les nœuds pendant l'installation

N'autorisez pas les utilisateurs non approuvés à accéder aux nœuds StorageGRID sur le réseau lors de l'installation des nœuds. Les nœuds ne sont pas entièrement sécurisés tant qu'ils n'ont pas rejoint la grille.

Instructions pour les nœuds d'administration

Des nœuds d'administration qui assurent les services de gestion tels que la configuration du système, la surveillance et la journalisation. Lorsque vous vous connectez à Grid Manager ou au Gestionnaire de locataires, vous vous connectez à un noeud d'administration.

Suivez les instructions suivantes pour sécuriser les nœuds d'administration dans votre système StorageGRID :

- Sécurisez tous les nœuds d'administration des clients non fiables, tels que ceux qui sont sur Internet ouvert. Assurez-vous qu'aucun client non approuvé ne peut accéder à un nœud d'administration sur le réseau Grid, le réseau d'administration ou le réseau client.
- Les groupes StorageGRID contrôlent l'accès aux fonctionnalités de Grid Manager et de tenant Manager. Accordez à chaque groupe d'utilisateurs les autorisations minimales requises pour leur rôle et utilisez le mode d'accès en lecture seule pour empêcher les utilisateurs de modifier la configuration.
- Lorsque vous utilisez des terminaux d'équilibrage de charge StorageGRID, utilisez des nœuds de passerelle au lieu des nœuds d'administration pour le trafic client non fiable.
- Si vous avez des locataires non approuvés, ne les autorisez pas à avoir un accès direct au gestionnaire de locataires ou à l'API de gestion des locataires. Certains locataires non fiables utilisent un portail de locataires ou un système de gestion externe des locataires qui interagit avec l'API de gestion des locataires.

- Vous pouvez également utiliser un proxy d'administration pour mieux contrôler la communication AutoSupport entre les nœuds d'administration et le support NetApp. Voir les étapes pour "Création d'un proxy Admin".
- Utilisez éventuellement les ports 8443 et 9443 restreints pour séparer les communications Grid Manager et tenant Manager. Bloquez le port partagé 443 et limitez les demandes des locataires au port 9443 pour une protection supplémentaire.
- La possibilité d'utiliser des nœuds d'administration distincts pour les administrateurs du grid et les utilisateurs des locataires.

Pour plus d'informations, reportez-vous aux instructions de "Administration d'StorageGRID".

Consignes relatives aux nœuds de stockage

Des nœuds de stockage gèrent et stockent les données et les métadonnées d'objets. Suivez ces instructions pour sécuriser les nœuds de stockage dans votre système StorageGRID.

- Ne permettez pas aux clients non approuvés de se connecter directement aux nœuds de stockage. Utilisez un terminal d'équilibrage de charge desservi par un nœud de passerelle ou un équilibreur de charge tiers.
- N'activez pas les services sortants pour les locataires non approuvés. Par exemple, lors de la création du compte pour un locataire non approuvé, n'autorisez pas le locataire à utiliser son propre référentiel d'identité et n'autorisez pas l'utilisation des services de plate-forme. Voir les étapes pour "création d'un compte de locataire".
- Utilisez un équilibreur de charge tiers pour le trafic client non fiable. L'équilibrage de la charge fourni par des tiers offre un meilleur contrôle et des couches de protection supplémentaires contre les attaques.
- Vous pouvez également utiliser un proxy de stockage pour plus de contrôle sur les pools de stockage cloud et les communications des services de plateforme depuis les nœuds de stockage vers les services externes. Voir les étapes pour "Création d'un proxy de stockage".
- Vous pouvez également vous connecter à des services externes à l'aide du réseau client. Sélectionnez ensuite **CONFIGURATION** > **sécurité** > **contrôle du pare-feu** > **réseaux clients non approuvés** et indiquez que le réseau client sur le noeud de stockage n'est pas fiable. Le nœud de stockage n'accepte plus de trafic entrant sur le réseau client, mais il continue à autoriser les requêtes sortantes pour les services de plate-forme.

Instructions pour les nœuds de passerelle

Les nœuds de passerelle fournissent une interface d'équilibrage de la charge facultative que les applications client peuvent utiliser pour se connecter à StorageGRID. Pour sécuriser tous les nœuds de passerelle de votre système StorageGRID, procédez comme suit :

- Configurez et utilisez des terminaux d'équilibrage de charge. Voir "Considérations relatives à l'équilibrage de charge".
- Utilisez un équilibreur de charge tiers entre le client et le nœud de passerelle ou les nœuds de stockage pour le trafic client non fiable. L'équilibrage de la charge fourni par des tiers offre un meilleur contrôle et des couches de protection supplémentaires contre les attaques. Si vous utilisez un équilibreur de charge tiers, le trafic réseau peut, éventuellement, être configuré de manière à passer par un terminal interne d'équilibrage de la charge ou être directement envoyé aux nœuds de stockage.
- Si vous utilisez des points de terminaison d'équilibrage de charge, les clients peuvent éventuellement se connecter via le réseau client. Sélectionnez ensuite **CONFIGURATION** > **sécurité** > **contrôle du pare-feu** > **réseaux clients non approuvés** et indiquez que le réseau client sur le nœud passerelle n'est pas fiable. Le nœud passerelle accepte uniquement le trafic entrant sur les ports explicitement configurés en tant que

points finaux d'équilibreur de charge.

Consignes pour les nœuds d'appliances matérielles

Les appliances matérielles StorageGRID sont spécialement conçues pour une utilisation dans un système StorageGRID. Certaines appliances peuvent être utilisées comme nœuds de stockage. Les autres appliances peuvent être utilisées comme nœuds d'administration ou nœuds de passerelle. Vous pouvez associer des nœuds d'appliance à des nœuds basés sur logiciel ou déployer des grilles 100 % appliance entièrement conçues.

Pour sécuriser les nœuds d'appliance matérielle de votre système StorageGRID, procédez comme suit :

- Si l'appliance utilise SANtricity System Manager pour la gestion du contrôleur de stockage, empêchez les clients non fiables d'accéder à SANtricity System Manager sur le réseau.
- Si l'appliance est équipée d'un contrôleur de gestion de la carte mère (BMC), notez que le port de gestion du BMC permet un accès matériel de faible niveau. Connectez le port de gestion BMC uniquement à un réseau de gestion interne sécurisé, fiable et. Si aucun réseau de ce type n'est disponible, laissez le port de gestion BMC déconnecté ou bloqué, à moins qu'une connexion BMC ne soit demandée par le support technique.
- Si l'appliance prend en charge la gestion à distance du matériel du contrôleur via Ethernet à l'aide de la norme IPMI (Intelligent Platform Management interface), bloquez le trafic non fiable sur le port 623.

> Vous pouvez activer ou désactiver l'accès IPMI à distance pour tous les dispositifs contenant un contrôleur BMC en utilisant le point de terminaison privé de l'API de gestion, PUT /private/bmc.

- Si le contrôleur de stockage de l'appliance inclut des disques FDE ou FIPS et que la fonction de sécurité des disques est activée, utilisez SANtricity pour configurer les clés de sécurité des disques. Voir "Configuration de SANtricity System Manager (SG6000 et SG5700)".
- Pour les appliances sans disques FDE ou FIPS, activez le chiffrement de nœud à l'aide d'un serveur de gestion des clés (KMS). Voir "Facultatif : activez le chiffrement de nœud".

Instructions de renforcement pour TLS et SSH

Vous devez remplacer les certificats par défaut créés lors de l'installation et sélectionner la stratégie de sécurité appropriée pour les connexions TLS et SSH.

Directives de renforcement des certificats

Vous devez remplacer les certificats par défaut créés lors de l'installation par vos propres certificats personnalisés.

Pour de nombreuses organisations, le certificat numérique auto-signé pour l'accès au Web StorageGRID n'est pas conforme à leurs politiques de sécurité de l'information. Sur les systèmes de production, vous devez installer un certificat numérique signé par une autorité de certification pour l'authentification de StorageGRID.

Plus précisément, vous devez utiliser des certificats de serveur personnalisés au lieu de ces certificats par défaut :

- **Certificat d'interface de gestion** : utilisé pour sécuriser l'accès au Grid Manager, au tenant Manager, à l'API Grid Management et à l'API tenant Management.
- **Certificat API S3 et Swift** : utilisé pour sécuriser l'accès aux nœuds de stockage et aux nœuds de passerelle, que les applications client S3 et Swift utilisent pour charger et télécharger des données d'objet.

Voir "Gérer les certificats de sécurité" pour plus de détails et d'instructions.

> StorageGRID gère séparément les certificats utilisés pour les terminaux de l'équilibreur de charge. Pour configurer les certificats d'équilibreur de charge, reportez-vous à la section "Configurer les terminaux de l'équilibreur de charge".

Lorsque vous utilisez des certificats de serveur personnalisés, suivez les instructions suivantes :

- Les certificats doivent avoir un *`subjectAltName`* Correspondant aux entrées DNS de StorageGRID. Pour plus de détails, reportez-vous à la section 4.2.1.6, «sous-objet autre nom», dans "RFC 5280 : certificat PKIX et profil CRL".
- Si possible, évitez d'utiliser des certificats génériques. À l'exception de cette règle, le certificat d'un terminal de type hébergement virtuel S3 nécessite l'utilisation d'un caractère générique si les noms de compartiment ne sont pas connus à l'avance.
- Lorsque vous devez utiliser des caractères génériques dans les certificats, vous devez prendre des mesures supplémentaires pour réduire les risques. Utilisez un motif générique comme `*.s3.example.com`, et n'utilisez pas le `s3.example.com` suffixe pour les autres applications. Ce modèle fonctionne également avec l'accès S3 de type chemin d'accès, comme `dc1-s1.s3.example.com/mybucket`.
- Définissez les délais d'expiration du certificat sur court (par exemple, 2 mois) et utilisez l'API Grid Management pour automatiser la rotation des certificats. Ceci est particulièrement important pour les certificats génériques.

En outre, les clients doivent utiliser un contrôle strict du nom d'hôte lors de la communication avec StorageGRID.

Directives de renforcement pour les règles TLS et SSH

Vous pouvez sélectionner une stratégie de sécurité pour déterminer quels protocoles et chiffrements sont utilisés pour établir des connexions TLS sécurisées avec les applications client et des connexions SSH sécurisées avec les services StorageGRID internes.

La règle de sécurité contrôle la façon dont TLS et SSH chiffrent les données en mouvement. Il est recommandé de désactiver les options de cryptage qui ne sont pas nécessaires pour assurer la compatibilité des applications. Utilisez la stratégie moderne par défaut, sauf si votre système doit être conforme aux critères communs ou si vous devez utiliser d'autres chiffrements.

Voir "Gestion des règles TLS et SSH" pour plus de détails et d'instructions.

Autres directives de durcissement

Outre les directives de renforcement des réseaux et nœuds StorageGRID, vous devez suivre les instructions de renforcement correspondant à d'autres domaines du système StorageGRID.

Journaux et messages d'audit

Protégez toujours les journaux StorageGRID et la sortie des messages d'audit de manière sécurisée. Les journaux et les messages d'audit StorageGRID fournissent des informations précieuses du point de vue du support et de la disponibilité du système. En outre, les informations figurant dans les journaux StorageGRID et dans les résultats des messages d'audit sont généralement sensibles.

Configurez StorageGRID pour envoyer des événements de sécurité à un serveur syslog externe. Si vous utilisez syslog export, sélectionnez TLS et RELP/TLS pour les protocoles de transport.

Voir la "Référence des fichiers journaux" Pour plus d'informations sur les journaux StorageGRID. Voir "Messages d'audit" Pour plus d'informations sur les messages d'audit StorageGRID.

NetApp AutoSupport

La fonction AutoSupport de StorageGRID vous permet de contrôler de manière proactive l'état de votre système et d'envoyer automatiquement des messages et des détails au support technique NetApp, à l'équipe de support interne de votre entreprise ou à un partenaire de support. Par défaut, les messages AutoSupport envoyés au support technique NetApp sont activés lorsque StorageGRID est configuré pour la première fois.

La fonction AutoSupport peut être désactivée. Cependant, NetApp recommande de l'activer, car AutoSupport accélère l'identification et la résolution des problèmes sur le système StorageGRID.

AutoSupport prend en charge les protocoles de transport HTTPS, HTTP et SMTP. En raison du caractère sensible des messages AutoSupport, NetApp recommande vivement d'utiliser le protocole de transport par défaut HTTPS pour l'envoi des messages AutoSupport au support NetApp.

Partage des ressources d'origine croisée (CORS)

Vous pouvez configurer le partage de ressources entre sources (CORS) pour un compartiment S3 si vous souhaitez que ce compartiment et ces objets soient accessibles aux applications web d'autres domaines. En général, n'activez pas les codes de commande à moins qu'ils ne soient requis. Si CORS est requis, limitez-le aux origines de confiance.

Voir les étapes pour "Configuration du partage des ressources d'origine croisée (CORS)".

Dispositifs de sécurité externes

Une solution de renforcement complète doit traiter des mécanismes de sécurité en dehors de StorageGRID. L'utilisation de dispositifs d'infrastructure supplémentaires pour filtrer et limiter l'accès à StorageGRID constitue un moyen efficace d'établir et de maintenir un niveau de sécurité strict. Ces systèmes de sécurité externes comprennent des pare-feu, des systèmes de prévention des intrusions (IDS) et d'autres dispositifs de sécurité.

Un équilibreur de charge tiers est recommandé pour le trafic client non fiable. L'équilibrage de la charge fourni par des tiers offre un meilleur contrôle et des couches de protection supplémentaires contre les attaques.

Réduction des ransomwares

Protégez vos données d'objet contre les attaques par ransomware en suivant les recommandations du "Protégez vos données contre les ransomwares avec StorageGRID".

Configuration de StorageGRID pour FabricPool

Configurer StorageGRID pour FabricPool : présentation

Si vous utilisez le logiciel NetApp ONTAP, vous pouvez utiliser NetApp FabricPool pour effectuer le Tiering des données inactives vers un système de stockage objet NetApp StorageGRID.

Suivez ces instructions pour :

- Découvrez les points à prendre en compte et les bonnes pratiques pour configurer StorageGRID pour une charge de travail FabricPool.
- Découvrez comment configurer un système de stockage objet StorageGRID à utiliser avec FabricPool.
- Découvrez comment fournir les valeurs requises à ONTAP lorsque StorageGRID est attaché à un Tier cloud FabricPool.

Démarrage rapide de la configuration de StorageGRID pour FabricPool

Planification de la configuration

- Déterminez quelle règle de Tiering des volumes FabricPool vous utiliserez pour effectuer le Tiering des données ONTAP inactives vers StorageGRID.
- Planifiez et installez un système StorageGRID pour répondre à vos besoins en capacité de stockage et en performances.
- Familiarisez-vous avec les logiciels système StorageGRID, y compris avec le "Gestionnaire de grille" et le "Gestionnaire de locataires".
- Consultez les bonnes pratiques FabricPool pour la section "Groupes HAUTE DISPONIBILITÉ", "équilibrage de la charge", "ILM", et "plus encore".
- Consultez les ressources supplémentaires suivantes, qui contiennent des informations détaillées sur l'utilisation et la configuration de ONTAP et FabricPool :

  "Tr-4598 : meilleures pratiques FabricPool dans ONTAP"

  "ONTAP 9 : présentation de la gestion des niveaux FabricPool avec System Manager"

Effectuer des tâches préalables

Se procurer le "Informations requises pour associer StorageGRID en tant que Tier cloud", y compris :

- Adresses IP
- Noms de domaine
- Certificat SSL

Éventuellement, configurer "fédération des identités" et "authentification unique".

Configurer les paramètres StorageGRID

Utilisez StorageGRID pour obtenir les valeurs dont ONTAP a besoin pour se connecter à la grille.

À l'aide du "Assistant d'installation FabricPool" est le moyen recommandé et le plus rapide de configurer tous les éléments, mais vous pouvez également configurer chaque entité manuellement, si nécessaire.

Configurer ONTAP et DNS

Utilisez ONTAP pour "ajoutez un tier de cloud" Qui utilise les valeurs StorageGRID. Puis, "Configurer les entrées DNS" Pour associer des adresses IP à tous les noms de domaine que vous prévoyez d'utiliser.

5 Contrôler et gérer

Une fois votre système opérationnel, vous pouvez effectuer des tâches continues dans ONTAP et StorageGRID afin de gérer et de surveiller le Tiering des données FabricPool au fil du temps.

Qu'est-ce que FabricPool ?

FabricPool est une solution de stockage hybride ONTAP qui utilise un agrégat Flash haute performance comme Tier de performance et un magasin d'objets comme Tier cloud. Les agrégats compatibles FabricPool vous permettent de réduire les coûts de stockage sans nuire aux performances, à l'efficacité ou à la protection.

FabricPool associe un niveau cloud (un magasin d'objets externe tel que StorageGRID) à un niveau local (un agrégat de stockage ONTAP) pour créer une collection composite de disques. Les volumes dans FabricPool peuvent ensuite exploiter le Tiering en conservant les données actives dans un stockage haute performance (Tier local) et en inactivant les données inactives vers le magasin d'objets externe (Tier cloud).

Aucune modification de l'architecture n'est requise. Vous pouvez continuer à gérer vos données et votre environnement applicatif à partir du système de stockage ONTAP central.

Qu'est-ce que StorageGRID ?

NetApp StorageGRID est une architecture de stockage qui gère les données en tant qu'objets, contrairement aux autres architectures de stockage telles que le stockage en mode bloc ou fichier. Les objets sont conservés dans un seul conteneur (tel qu'un compartiment) et ne sont pas imbriqués en tant que fichiers dans un répertoire à l'intérieur d'autres répertoires. Le stockage objet offre généralement des performances moins élevées que le stockage en mode bloc ou fichier, mais il présente aussi l'évolutivité la plus remarquable. Les compartiments StorageGRID peuvent contenir des pétaoctets de données et des milliards d'objets.

Pourquoi utiliser StorageGRID comme Tier cloud FabricPool ?

FabricPool peut hiérarchiser les données ONTAP avec plusieurs fournisseurs de stockage objet, y compris StorageGRID. Contrairement aux clouds publics qui peuvent fixer un nombre maximal d'opérations d'entrée/sortie par seconde (IOPS) pris en charge au niveau du compartiment ou du conteneur, les performances StorageGRID évoluent en fonction du nombre de nœuds qu'un système permet. En utilisant StorageGRID comme Tier cloud FabricPool, vous pouvez conserver vos données inactives dans votre propre cloud privé et bénéficier d'une performance optimale et d'un contrôle total sur vos données.

En outre, vous n'avez pas besoin d'une licence FabricPool lorsque vous utilisez StorageGRID en tant que Tier cloud.

Informations nécessaires pour rattacher StorageGRID à un niveau cloud

Avant de connecter StorageGRID en tant que niveau cloud pour FabricPool, vous devez effectuer les étapes de configuration dans StorageGRID et obtenir certaines valeurs à utiliser dans ONTAP.

Quelles valeurs ai-je besoin ?

Le tableau suivant indique les valeurs que vous devez configurer dans StorageGRID et la manière dont ces valeurs sont utilisées par ONTAP et le serveur DNS.

Valeur	Où la valeur est configurée	Où la valeur est utilisée
Adresses IP virtuelles (VIP)	Groupe StorageGRID > HA	Entrée DNS
Port	StorageGRID > terminal de l'équilibreur de charge	ONTAP System Manager > Ajouter un Tier cloud
Certificat SSL	StorageGRID > terminal de l'équilibreur de charge	ONTAP System Manager > Ajouter un Tier cloud
Nom du serveur (FQDN)	StorageGRID > terminal de l'équilibreur de charge	Entrée DNS
ID de clé d'accès et clé d'accès secrète	StorageGRID > locataire et compartiment	ONTAP System Manager > Ajouter un Tier cloud
Nom du compartiment/conteneur	StorageGRID > locataire et compartiment	ONTAP System Manager > Ajouter un Tier cloud

Comment obtenir ces valeurs ?

Selon vos besoins, vous pouvez effectuer l'une des opérations suivantes pour obtenir les informations dont vous avez besoin :

- Utilisez le "Assistant d'installation FabricPool". L'assistant d'installation FabricPool vous aide à configurer rapidement les valeurs requises dans StorageGRID et génère un fichier que vous pouvez utiliser pour configurer ONTAP System Manager. Cet assistant vous guide tout au long des étapes requises et vous aide à vous assurer que vos paramètres sont conformes aux meilleures pratiques StorageGRID et FabricPool.
- Configurez chaque élément manuellement. Entrez ensuite les valeurs dans ONTAP System Manager ou dans l'interface de ligne de commandes ONTAP. Voici la procédure à suivre :
  a. "Configurez un groupe haute disponibilité pour FabricPool".
  b. "Créez un noeud final d'équilibrage de charge pour FabricPool".
  c. "Créez un compte de locataire pour FabricPool".
  d. Connectez-vous au compte du locataire, et "créez le compartiment et les clés d'accès pour l'utilisateur root".
  e. Créez une règle ILM pour les données FabricPool et ajoutez-la à votre règle ILM active. Voir "Configurez la solution ILM pour les données FabricPool".
  f. En option, "Créez une stratégie de classification du trafic pour FabricPool".

Utilisez l'assistant d'installation FabricPool

Utilisez l'assistant de configuration FabricPool : considérations et configuration requise

Vous pouvez utiliser l'assistant d'installation de FabricPool pour configurer StorageGRID en tant que système de stockage objet pour un Tier cloud FabricPool. Une fois l'assistant d'installation terminé, vous pouvez entrer les informations requises dans ONTAP System

Manager.

Quand utiliser l'assistant de configuration FabricPool

L'assistant d'installation FabricPool vous guide à chaque étape de la configuration de StorageGRID pour une utilisation avec FabricPool et configure automatiquement certaines entités pour vous, telles que les règles ILM et de classification du trafic. Dans le cadre de l'assistant, vous téléchargez un fichier que vous pouvez utiliser pour saisir des valeurs dans ONTAP System Manager. Utilisez l'assistant pour configurer votre système plus rapidement et pour vous assurer que vos paramètres sont conformes aux meilleures pratiques StorageGRID et FabricPool.

En supposant que vous disposez de l'autorisation d'accès racine, vous pouvez exécuter l'assistant de configuration FabricPool lorsque vous commencez à utiliser le Gestionnaire de grille StorageGRID, ou vous pouvez accéder à l'assistant et l'exécuter ultérieurement. En fonction de vos besoins, vous pouvez également configurer manuellement une partie ou la totalité des éléments requis, puis utiliser l'assistant pour assembler les valeurs dont ONTAP a besoin dans un seul fichier.

Utilisez l'assistant d'installation de FabricPool, sauf si vous savez que vous avez des exigences spéciales, sinon votre implémentation nécessitera une personnalisation importante.

Avant d'utiliser l'assistant

Confirmez que vous avez effectué ces étapes préalables.

Passez en revue les bonnes pratiques

- Vous avez une compréhension générale du "Informations requises pour associer StorageGRID en tant que Tier cloud".
- Vous avez examiné les bonnes pratiques de FabricPool pour :
  - "Groupes haute disponibilité (HA)"
  - "Équilibrage de la charge"
  - "Règles et règles ILM"

Obtenir des adresses IP et configurer des interfaces VLAN

Si vous configurez un groupe haute disponibilité, vous savez à quels nœuds ONTAP se connectera et à quel réseau StorageGRID sera utilisé. Vous savez également quelles valeurs entrer pour le CIDR de sous-réseau, l'adresse IP de la passerelle et les adresses IP virtuelles (VIP).

Si vous prévoyez d'utiliser un réseau local virtuel pour isoler le trafic FabricPool, vous avez déjà configuré l'interface VLAN. Voir "Configurez les interfaces VLAN".

Configurer la fédération des identités et SSO

Si vous prévoyez d'utiliser la fédération des identités ou l'authentification unique (SSO) pour votre système StorageGRID, vous avez activé ces fonctionnalités. Vous savez également quel groupe fédéré doit disposer d'un accès racine pour le compte de locataire que ONTAP utilisera. Voir "Utiliser la fédération des identités" et "Configurer l'authentification unique".

Obtenir et configurer des noms de domaine

- Vous savez quel nom de domaine complet (FQDN) utiliser pour StorageGRID. Les entrées de serveur de

noms de domaine (DNS) mapperont ce FQDN aux adresses IP virtuelles (VIP) du groupe haute disponibilité que vous créez à l'aide de l'assistant. Voir "Configurez le serveur DNS".

- Si vous prévoyez d'utiliser des requêtes de type hébergement virtuel S3, c'est le cas "Noms de domaine de terminaux S3 configurés". ONTAP utilise par défaut des URL de type chemin d'accès, mais il est recommandé d'utiliser des requêtes de type hébergement virtuel.

Examinez les exigences en matière d'équilibreur de charge et de certificat de sécurité

Si vous envisagez d'utiliser l'équilibreur de charge StorageGRID, vous avez consulté la page générale "considérations relatives à l'équilibrage de charge". Vous disposez des certificats que vous allez télécharger ou des valeurs dont vous avez besoin pour générer un certificat.

Si vous prévoyez d'utiliser un noeud final externe (tiers) d'équilibreur de charge, vous disposez du nom de domaine complet (FQDN), du port et du certificat pour cet équilibreur de charge.

Confirmation de la configuration du pool de stockage ILM

Si vous avez mis à niveau vers StorageGRID 11.7 à partir d'une version précédente de StorageGRID, vous avez configuré le pool de stockage que vous utiliserez. En général, vous devez créer un pool de stockage pour chaque site StorageGRID que vous utiliserez pour stocker des données ONTAP.

> Cette condition préalable ne s'applique pas aux nouvelles installations de StorageGRID 11.7. Lorsque vous installez StorageGRID 11.7 sur une nouvelle grille, les pools de stockage sont automatiquement créés pour chaque site.

Relation entre ONTAP et le niveau cloud StorageGRID

L'assistant FabricPool vous guide tout au long du processus de création d'un niveau cloud StorageGRID unique, qui inclut un locataire StorageGRID, un ensemble de clés d'accès et un compartiment StorageGRID. Vous pouvez associer ce niveau cloud StorageGRID à un ou plusieurs niveaux locaux ONTAP.

L'association d'un seul niveau de cloud à plusieurs niveaux locaux dans un cluster est la meilleure pratique générale. Cependant, selon vos besoins, vous pouvez utiliser plusieurs compartiments, voire plus d'un locataire StorageGRID pour les niveaux locaux dans un seul cluster. L'utilisation de différents compartiments et locataires vous permet d'isoler les données et l'accès aux données entre les tiers locaux ONTAP, mais sa configuration et sa gestion sont un peu plus complexes.

NetApp déconseille d'associer un seul Tier cloud à des tiers locaux dans plusieurs clusters.

> Pour connaître les bonnes pratiques d'utilisation de StorageGRID avec NetApp MetroCluster™ et FabricPool Mirror, consultez le site "Tr-4598 : meilleures pratiques FabricPool dans ONTAP".

Facultatif : utilisez un compartiment différent pour chaque niveau local

Pour utiliser plusieurs compartiments pour les tiers locaux d'un cluster ONTAP, ajoutez plusieurs niveaux cloud StorageGRID dans ONTAP. Chaque Tier cloud partage le même groupe haute disponibilité, mais il utilise un conteneur différent (compartiment StorageGRID) pour le terminal de l'équilibreur de charge, le locataire et les clés d'accès. Procédez comme suit :

1. Dans StorageGRID Grid Manager, suivez les instructions de l'assistant d'installation FabricPool pour le premier niveau cloud.
2. Dans ONTAP System Manager, ajoutez un Tier cloud et utilisez le fichier téléchargé depuis StorageGRID pour fournir les valeurs requises.

3. Dans le gestionnaire de locataires StorageGRID, connectez-vous au locataire créé par l'assistant, puis créez un second compartiment.
4. Terminez à nouveau l'assistant FabricPool. Sélectionnez le groupe haute disponibilité, le terminal de l'équilibreur de charge et le locataire existants. Sélectionnez ensuite le nouveau compartiment que vous avez créé manuellement. Créez une règle ILM pour le nouveau compartiment et activez une règle ILM pour inclure cette règle.
5. Depuis ONTAP, ajoutez un second Tier cloud, mais indiquez le nouveau nom de compartiment.

Facultatif : utilisez un locataire et un compartiment différents pour chaque niveau local

Pour utiliser plusieurs locataires et jeux de clés d'accès différents pour les tiers locaux d'un cluster ONTAP, ajoutez plusieurs niveaux cloud StorageGRID dans ONTAP. Chaque Tier cloud partage le même groupe haute disponibilité et le même terminal d'équilibrage de la charge, mais utilise un locataire, des clés d'accès et un conteneur différents (compartiment StorageGRID). Procédez comme suit :

1. Dans StorageGRID Grid Manager, suivez les instructions de l'assistant d'installation FabricPool pour le premier niveau cloud.
2. Dans ONTAP System Manager, ajoutez un Tier cloud et utilisez le fichier téléchargé depuis StorageGRID pour fournir les valeurs requises.
3. Terminez à nouveau l'assistant FabricPool. Sélectionnez le groupe haute disponibilité et le terminal d'équilibrage de la charge existants. Créez un locataire et un compartiment. Créez une règle ILM pour le nouveau compartiment et activez une règle ILM pour inclure cette règle.
4. Depuis ONTAP, ajoutez un second Tier cloud, mais fournissez la nouvelle clé d'accès, la clé secrète et le nom du compartiment.

Accédez à l'assistant d'installation FabricPool et terminez-le

Vous pouvez utiliser l'assistant d'installation de FabricPool pour configurer StorageGRID en tant que système de stockage objet pour un Tier cloud FabricPool.

Avant de commencer

- Vous avez passé en revue le "considérations et exigences" Pour utiliser l'assistant de configuration FabricPool.

> Si vous souhaitez configurer StorageGRID pour une utilisation avec une autre application client S3, rendez-vous sur "Utilisation de l'assistant d'installation S3".

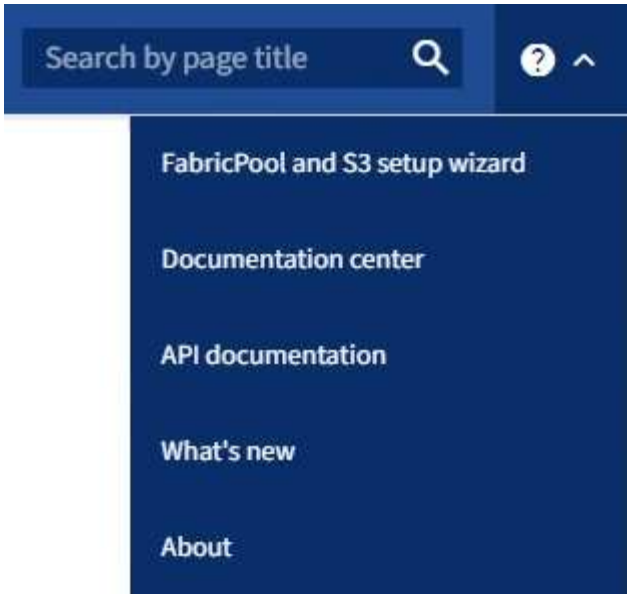
- Vous disposez de l'autorisation d'accès racine.

Accéder à l'assistant

Vous pouvez exécuter l'assistant d'installation FabricPool lorsque vous commencez à utiliser le Gestionnaire de grille StorageGRID, ou vous pouvez accéder à l'assistant et l'exécuter ultérieurement.

Étapes

1. Connectez-vous au Grid Manager à l'aide d'un "navigateur web pris en charge".
2. Si la bannière **FabricPool and S3 setup Wizard** apparaît sur le tableau de bord, sélectionnez le lien dans la bannière. Si la bannière ne s'affiche plus, sélectionnez l'icône d'aide dans la barre d'en-tête du Gestionnaire de grille et sélectionnez **Assistant d'installation FabricPool et S3**.



3. Dans la section FabricPool de la page de l'assistant d'installation de FabricPool et S3, sélectionnez **configurer maintenant**.

   L'étape 1 sur 9 : configurer le groupe HA s'affiche.

Étape 1 sur 9 : configuration du groupe haute disponibilité

Un groupe haute disponibilité (HA) est un ensemble de nœuds qui contiennent chacun le service StorageGRID Load Balancer. Un groupe haute disponibilité peut contenir des nœuds de passerelle, des nœuds d'administration, ou les deux.

Vous pouvez utiliser un groupe haute disponibilité pour maintenir les connexions de données FabricPool disponibles. Un groupe haute disponibilité utilise des adresses IP virtuelles (VIP) pour fournir un accès haute disponibilité au service Load Balancer. En cas de défaillance de l'interface active du groupe haute disponibilité, une interface de sauvegarde peut gérer la charge de travail avec un faible impact sur les opérations FabricPool

Pour plus d'informations sur cette tâche, reportez-vous à la section "Gérez les groupes haute disponibilité" et "Meilleures pratiques pour les groupes à haute disponibilité".

Étapes

1. Si vous prévoyez d'utiliser un équilibreur de charge externe, il n'est pas nécessaire de créer un groupe haute disponibilité. Sélectionnez **Ignorer cette étape** et passez à l' Étape 2 sur 9 : configuration du terminal de l'équilibreur de charge.
2. Pour utiliser l'équilibreur de charge StorageGRID, créez un nouveau groupe haute disponibilité ou utilisez un groupe haute disponibilité existant.

Création du groupe haute disponibilité

a. Pour créer un nouveau groupe HA, sélectionnez **Create HA group**.

b. Pour l'étape **entrer les détails**, remplissez les champs suivants.

Champ	Description
Nom du groupe HAUTE DISPONIBILITÉ	Un nom d'affichage unique pour ce groupe haute disponibilité.
Description (facultatif)	La description de ce groupe HA.

c. Pour l'étape **Ajouter des interfaces**, sélectionnez les interfaces de nœud que vous souhaitez utiliser dans ce groupe haute disponibilité.

Utilisez les en-têtes de colonne pour trier les lignes ou entrez un terme de recherche pour localiser les interfaces plus rapidement.

Vous pouvez sélectionner un ou plusieurs nœuds, mais vous ne pouvez sélectionner qu'une seule interface pour chaque nœud.

d. Pour l'étape **hiérarchiser les interfaces**, déterminez l'interface principale et les interfaces de sauvegarde pour ce groupe haute disponibilité.

Faites glisser des lignes pour modifier les valeurs de la colonne **ordre de priorité**.

La première interface de la liste est l'interface principale. L'interface principale est l'interface active, sauf en cas de défaillance.

Si le groupe haute disponibilité comprend plusieurs interfaces et que l'interface active est défaillante, les adresses IP virtuelles (VIP) sont déplacées vers la première interface de sauvegarde, dans l'ordre de priorité. Si cette interface échoue, les adresses VIP passent à l'interface de sauvegarde suivante, etc. Lorsque les pannes sont résolues, les adresses VIP repassent à l'interface de priorité la plus élevée disponible.

e. Pour l'étape **entrer les adresses IP**, renseignez les champs suivants.

Champ	Description
Sous-réseau CIDR	Adresse du sous-réseau VIP en notation CIDR—adresse IPv4 suivie d'une barre oblique et de la longueur du sous-réseau (0-32). Aucun bit d'hôte ne doit être défini pour l'adresse réseau. Par exemple : `192.16.0.0/22`.
Adresse IP de la passerelle (facultative)	Facultatif. Si les adresses IP ONTAP utilisées pour accéder à StorageGRID ne se trouvent pas sur le même sous-réseau que les adresses VIP StorageGRID, entrez l'adresse IP de la passerelle locale VIP StorageGRID. L'adresse IP de la passerelle locale doit se trouver dans le sous-réseau VIP.

Champ	Description
Adresse IP virtuelle	Entrez au moins une et dix adresses VIP pour l'interface active du groupe HA. Toutes les adresses VIP doivent se trouver dans le sous-réseau VIP et toutes seront actives en même temps sur l'interface active. Au moins une adresse doit être IPv4. Vous pouvez éventuellement spécifier des adresses IPv4 et IPv6 supplémentaires.

f. Sélectionnez **Créer un groupe HA**, puis sélectionnez **Terminer** pour revenir à l'assistant de configuration FabricPool.

g. Sélectionnez **Continuer** pour passer à l'étape d'équilibrage de charge.

Utilisez un groupe haute disponibilité existant

a. Pour utiliser un groupe HA existant, sélectionnez le nom du groupe HA dans la liste déroulante **Sélectionner un groupe HA**.

b. Sélectionnez **Continuer** pour passer à l'étape d'équilibrage de charge.

Étape 2 sur 9 : configuration du terminal de l'équilibreur de charge

StorageGRID utilise un équilibreur de charge pour gérer la charge de travail à partir d'applications client, telles qu'FabricPool. L'équilibrage de la charge optimise la vitesse et la capacité de connexion sur plusieurs nœuds de stockage.

Vous pouvez utiliser le service StorageGRID Load Balancer, qui existe sur tous les nœuds de passerelle et d'administration, ou vous pouvez vous connecter à un équilibreur de charge externe (tiers). L'utilisation de l'équilibreur de charge StorageGRID est recommandée.

Pour plus d'informations sur cette tâche, reportez-vous à la section général "considérations relatives à l'équilibrage de charge" et le "Bonnes pratiques en matière d'équilibrage de charge pour FabricPool".

Étapes

1. Sélectionnez ou créez un point d'extrémité de l'équilibreur de charge StorageGRID ou utilisez un équilibreur de charge externe.

Créer un point final

a. Sélectionnez **Créer un noeud final**.

b. Pour l'étape **entrer les détails du noeud final**, renseignez les champs suivants.

Champ	Description
Nom	Nom descriptif du noeud final.
Port	Port StorageGRID que vous souhaitez utiliser pour l'équilibrage de charge. Ce champ est défini par défaut sur 10433 pour le premier noeud final que vous créez, mais vous pouvez entrer n'importe quel port externe inutilisé. Si vous entrez 80 ou 443, le noeud final est configuré uniquement sur les noeuds de passerelle, car ces ports sont réservés sur les noeuds d'administration. **Remarque :** les ports utilisés par d'autres services de grille ne sont pas autorisés. Voir la"Référence du port réseau".
Type de client	Doit être **S3**.
Protocole réseau	Sélectionnez **HTTPS**. **Remarque** : la communication avec StorageGRID sans chiffrement TLS est prise en charge, mais elle n'est pas recommandée.

c. Pour l'étape **Sélectionner le mode de liaison**, spécifiez le mode de liaison. Le mode de liaison contrôle la façon dont le noeud final est accédé—en utilisant une adresse IP ou des adresses IP et des interfaces réseau spécifiques.

Option	Description
Global (par défaut)	Les clients peuvent accéder au point final en utilisant l'adresse IP de n'importe quel nœud de passerelle ou nœud d'administration, l'adresse IP virtuelle (VIP) de n'importe quel groupe haute disponibilité sur n'importe quel réseau, ou un FQDN correspondant. Utilisez le paramètre **Global** (valeur par défaut) sauf si vous devez restreindre l'accessibilité de ce point final.
Adresses IP virtuelles de groupes haute disponibilité	Les clients doivent utiliser une adresse IP virtuelle (ou le nom de domaine complet correspondant) d'un groupe haute disponibilité pour accéder à ce point final. Les terminaux associés à ce mode de liaison peuvent tous utiliser le même numéro de port, tant que les groupes haute disponibilité que vous sélectionnez pour les terminaux ne se chevauchent pas.

Option	Description
Interfaces de nœuds	Les clients doivent utiliser les adresses IP (ou les FQDN correspondants) des interfaces de nœud sélectionnées pour accéder à ce noeud final.
Type de nœud	En fonction du type de nœud que vous sélectionnez, les clients doivent utiliser l'adresse IP (ou le nom de domaine complet correspondant) de tout nœud d'administration ou l'adresse IP (ou le nom de domaine complet correspondant) de tout nœud de passerelle pour accéder à ce point final.

d. Pour l'étape **tenant Access**, sélectionnez l'une des options suivantes :

Champ	Description
Autoriser tous les locataires (par défaut)	Tous les comptes de locataires peuvent utiliser ce terminal pour accéder à leurs compartiments. **Autoriser tous les locataires** est presque toujours l'option appropriée pour le noeud final de l'équilibreur de charge utilisé pour FabricPool. Vous devez sélectionner cette option si vous utilisez l'assistant d'installation FabricPool pour un nouveau système StorageGRID et que vous n'avez pas encore créé de compte de locataire.
Autoriser les locataires sélectionnés	Seuls les comptes de locataire sélectionnés peuvent utiliser ce terminal pour accéder à leurs compartiments.
Bloquez les locataires sélectionnés	Les comptes de locataire sélectionnés ne peuvent pas utiliser ce terminal pour accéder à leurs compartiments. Tous les autres locataires peuvent utiliser ce noeud final.

e. Pour l'étape **joindre un certificat**, sélectionnez l'une des options suivantes :

Champ	Description
Télécharger le certificat (recommandé)	Utilisez cette option pour télécharger un certificat de serveur signé par une autorité de certification, une clé privée de certificat et un ensemble d'autorité de certification facultatif.
Générez un certificat	Utilisez cette option pour générer un certificat auto-signé. Voir "Configurer les terminaux de l'équilibreur de charge" pour plus de détails sur ce que vous devez saisir.
Utilisez les certificats StorageGRID S3 et Swift	Cette option n'est disponible que si vous avez déjà téléchargé ou généré une version personnalisée du certificat global StorageGRID. Voir "Configurez les certificats API S3 et Swift" pour plus d'informations.

f. Sélectionnez **Terminer** pour revenir à l'assistant de configuration FabricPool.

g. Sélectionnez **Continuer** pour accéder à l'étape tenant et bucket.

> Les modifications apportées à un certificat de point final peuvent prendre jusqu'à 15 minutes pour être appliquées à tous les nœuds.

Utilisez le terminal d'équilibrage de charge existant

a. Sélectionnez le nom d'un noeud final existant dans la liste déroulante **Sélectionner un noeud final d'équilibrage de charge**.

b. Sélectionnez **Continuer** pour accéder à l'étape tenant et bucket.

Utiliser un équilibreur de charge externe

a. Renseignez les champs suivants pour l'équilibreur de charge externe.

Champ	Description
FQDN	Nom de domaine complet (FQDN) de l'équilibreur de charge externe.
Port	Le numéro de port que FabricPool utilisera pour se connecter à l'équilibreur de charge externe.
Certificat	Copiez le certificat du serveur pour l'équilibreur de charge externe et collez-le dans ce champ.

b. Sélectionnez **Continuer** pour accéder à l'étape tenant et bucket.

Étape 3 sur 9 : locataire et compartiment

Un locataire est une entité qui peut utiliser les applications S3 pour stocker et récupérer des objets dans StorageGRID. Chaque locataire dispose de ses propres utilisateurs, clés d'accès, compartiments, objets et un ensemble spécifique de fonctionnalités. Vous devez créer un locataire StorageGRID avant de pouvoir créer le compartiment que FabricPool utilisera.

Un compartiment est un conteneur utilisé pour stocker les objets d'un locataire et ses métadonnées d'objet. Même si certains locataires peuvent avoir plusieurs compartiments, l'assistant vous permet de créer ou de sélectionner un seul locataire et un compartiment à la fois. Vous pouvez utiliser le gestionnaire de locataires ultérieurement pour ajouter des compartiments supplémentaires dont vous avez besoin.

Vous pouvez créer un locataire et un compartiment pour FabricPool ou sélectionner un locataire et un compartiment existants. Si vous créez un nouveau locataire, le système crée automatiquement l'ID de clé d'accès et la clé d'accès secrète pour l'utilisateur root du locataire.

Pour plus d'informations sur cette tâche, reportez-vous à la section "Créez un compte de locataire pour FabricPool" et "Créez un compartiment S3 et obtenez une clé d'accès".

Étapes

Créez un locataire et un compartiment ou sélectionnez un locataire existant.

Nouveaux locataires et compartiments

1. Pour créer un nouveau tenant et un compartiment, entrez un **tenant name**. Par exemple : `FabricPool tenant`.
2. Définissez l'accès racine pour le compte de locataire, selon que votre système StorageGRID utilise ou non "fédération des identités", "Authentification unique (SSO)", ou les deux.

Option	Faites ça
Si la fédération des identités n'est pas activée	Spécifiez le mot de passe à utiliser lors de la connexion au tenant en tant qu'utilisateur root local.
Si la fédération des identités est activée	a. Sélectionnez un groupe fédéré existant pour obtenir l'autorisation d'accès racine pour le tenant. b. Vous pouvez également spécifier le mot de passe à utiliser lors de la connexion au tenant en tant qu'utilisateur root local.
Si la fédération des identités et l'authentification unique (SSO) sont toutes deux activées	Sélectionnez un groupe fédéré existant pour obtenir l'autorisation d'accès racine pour le tenant. Aucun utilisateur local ne peut se connecter.

3. Pour **nom de compartiment**, entrez le nom du compartiment que FabricPool utilisera pour stocker les données ONTAP. Par exemple : `fabricpool-bucket`.

   Vous ne pouvez pas modifier le nom du compartiment après la création du compartiment.

4. Sélectionnez la **région** pour ce compartiment.

   Utilisez la région par défaut (US-East-1), sauf si vous prévoyez d'utiliser ILM pour filtrer des objets en fonction de la région du compartiment.

5. Sélectionnez **Créer et continuer** pour créer le tenant et le compartiment et pour accéder à l'étape de téléchargement des données

Sélectionnez locataire et compartiment

La gestion des versions du compte de locataire existant doit comporter au moins un compartiment pour lequel la gestion des versions n'est pas activée. Vous ne pouvez pas sélectionner un compte de locataire existant s'il n'existe aucun compartiment pour ce locataire.

1. Sélectionnez le locataire existant dans la liste déroulante **tenant name**.
2. Sélectionnez le compartiment existant dans la liste déroulante **Nom du compartiment**.

   FabricPool ne prend pas en charge la gestion des versions d'objet, de sorte que les compartiments pour lesquels la gestion des versions est activée ne sont pas affichés.

Ne sélectionnez pas un compartiment dans lequel le verrouillage d'objet S3 est activé pour FabricPool.

3. Sélectionnez **Continuer** pour accéder à l'étape de téléchargement des données.

Étape 4 sur 9 : télécharger les paramètres ONTAP

Au cours de cette étape, vous téléchargez un fichier que vous pouvez utiliser pour saisir des valeurs dans ONTAP System Manager.

Étapes

1. Si vous le souhaitez, sélectionnez l'icône de copie ( ) Pour copier l'ID de la clé d'accès et la clé d'accès secrète dans le presse-papiers.

   Ces valeurs sont incluses dans le fichier de téléchargement, mais vous pouvez les enregistrer séparément.

2. Sélectionnez **Télécharger les paramètres ONTAP** pour télécharger un fichier texte contenant les valeurs que vous avez saisies jusqu'à présent.

   Le `ONTAP_FabricPool_settings_bucketname.txt` Ce fichier contient les informations dont vous avez besoin pour configurer StorageGRID en tant que système de stockage objet pour un Tier cloud FabricPool, notamment :

   - Détails de la connexion de l'équilibreur de charge, y compris le nom du serveur (FQDN), le port et le certificat
   - Nom du compartiment
   - ID de clé d'accès et clé d'accès secrète pour l'utilisateur root du compte de locataire

3. Enregistrez les clés copiées et le fichier téléchargé dans un emplacement sécurisé.

   Ne fermez pas cette page tant que vous n'avez pas copié les deux clés d'accès, téléchargé les paramètres ONTAP ou les deux. Les touches ne seront pas disponibles après la fermeture de cette page. Veillez à enregistrer ces informations dans un emplacement sécurisé car elles peuvent être utilisées pour obtenir des données de votre système StorageGRID.

4. Cochez la case pour confirmer que vous avez téléchargé ou copié l'ID de clé d'accès et la clé d'accès secrète.
5. Sélectionnez **Continuer** pour accéder à l'étape du pool de stockage ILM.

Étape 5 sur 9 : sélectionnez un pool de stockage

Un pool de stockage est un groupe de nœuds de stockage. Lorsque vous sélectionnez un pool de stockage, vous déterminez les nœuds que StorageGRID utilisera pour stocker les données hiérarchisées depuis ONTAP.

Pour plus de détails sur cette étape, voir "Créer un pool de stockage".

Étapes

1. Dans la liste déroulante **site**, sélectionnez le site StorageGRID que vous souhaitez utiliser pour les données hiérarchisées à partir de ONTAP.
2. Dans la liste déroulante **Storage pool**, sélectionnez le pool de stockage pour ce site.

Le pool de stockage d'un site inclut tous les nœuds de stockage de ce site.

3. Sélectionnez **Continuer** pour accéder à l'étape de la règle ILM.

Étape 6 sur 9 : révision de la règle ILM pour FabricPool

Les règles de gestion du cycle de vie des informations (ILM) contrôlent le placement, la durée et le comportement d'ingestion de tous les objets de votre système StorageGRID.

L'assistant d'installation de FabricPool crée automatiquement la règle ILM recommandée pour l'utilisation de FabricPool. Cette règle s'applique uniquement au compartiment spécifié. Elle stocke les données hiérarchisées depuis ONTAP en utilisant un code d'effacement 2+1 sur un même site.

Pour plus de détails sur cette étape, voir "Création d'une règle ILM" et "Bonnes pratiques d'utilisation d'ILM avec des données FabricPool".

Étapes

1. Vérifiez les détails de la règle.

Champ	Description
Nom de la règle	Généré automatiquement et ne pouvant pas être modifié
Description	Généré automatiquement et ne pouvant pas être modifié
Filtre	Nom du compartiment Cette règle s'applique uniquement aux objets enregistrés dans le compartiment spécifié.
Heure de référence	Temps d'ingestion L'instruction de placement démarre lorsque les objets sont initialement enregistrés dans le compartiment.
Instruction de placement	Utilisez le code d'effacement 2+1 du jour 0 à l'infini

2. Triez le diagramme de rétention par **période** et **pool de stockage** pour confirmer l'instruction de placement.
   - La **période** pour la règle est **jour 0 - pour toujours**. **Jour 0** signifie que la règle est appliquée lorsque les données sont hiérarchisées depuis ONTAP. **Forever** signifie que l'ILM de StorageGRID ne supprimera pas les données qui ont été hiérarchisées depuis ONTAP.
   - Le **pool de stockage** de la règle est le pool de stockage que vous avez sélectionné. **EC 2+1** signifie que les données seront stockées à l'aide du code d'effacement 2+1. Chaque objet sera enregistré sous forme de deux fragments de données et d'un fragment de parité. Les trois fragments de chaque objet seront enregistrés sur différents nœuds de stockage sur un seul site.
3. Sélectionnez **Créer et continuer** pour créer cette règle et accéder à l'étape de la stratégie ILM.

Étape 7 sur 9 : vérification et activation de la règle ILM

Une fois que l'assistant d'installation de FabricPool a créé la règle ILM pour FabricPool, il crée une règle ILM proposée. Vous devez examiner attentivement cette stratégie avant de l'activer.

Pour plus de détails sur cette étape, voir "Création de la règle ILM" et "Bonnes pratiques d'utilisation d'ILM avec des données FabricPool".

> Lorsque vous activez une nouvelle règle ILM, StorageGRID utilise cette règle pour gérer le placement, la durée et la protection des données de tous les objets de la grille, y compris les objets existants et les objets nouvellement ingérés. Dans certains cas, l'activation d'une nouvelle stratégie peut entraîner le déplacement d'objets existants vers de nouveaux emplacements.

> Pour éviter toute perte de données, n'utilisez pas de règle ILM qui expirera ou supprimera les données de Tier cloud FabricPool. Définissez la période de conservation sur **Forever** pour vous assurer que les objets FabricPool ne sont pas supprimés par la ILM de StorageGRID.

Étapes

1. Si vous le souhaitez, mettez à jour le **Nom de la stratégie** généré par le système. Par défaut, le système ajoute "+ FabricPool" au nom de votre police active ou proposée, mais vous pouvez fournir votre propre nom.
2. Examiner la liste des règles de la politique proposée.
   - Si aucune règle ILM n'est proposée pour votre grid, l'assistant crée une règle proposée en clonant la règle active, puis en ajoutant la nouvelle règle en haut de la page.
   - Si une règle ILM est déjà proposée dans votre grid et que cette règle utilise le même ordre et les mêmes règles que la règle ILM active, l'assistant ajoute la nouvelle règle en haut de la règle proposée.
   - Si votre stratégie proposée contient des règles différentes ou un ordre différent de celui de la stratégie active, un message s'affiche. Vous devez ajouter manuellement la nouvelle règle FabricPool à la règle ILM. Suivez ces étapes, en fonction de votre choix entre la stratégie active ou la stratégie proposée.

Stratégie à partir de	Étapes
Règle active	i. Sélectionnez **ILM** > **Policies** dans le menu de gauche de Grid Manager. ii. Sélectionnez l'onglet Stratégie proposée. iii. Sélectionnez **actions** > **Supprimer** pour supprimer la stratégie proposée existante. iv. Retournez à l'assistant d'installation de FabricPool. L'assistant peut à présent cloner votre stratégie active pour créer une nouvelle stratégie proposée. La nouvelle règle FabricPool sera ajoutée en haut.

Stratégie à partir de	Étapes
Politique proposée	i. Sélectionnez **ILM** > **Policies** dans le menu de gauche de Grid Manager. ii. Sélectionnez l'onglet Stratégie proposée. iii. Sélectionnez **actions** > **Modifier** pour modifier la stratégie proposée existante. iv. Ajoutez la nouvelle règle FabricPool en haut. v. Activez la stratégie mise à jour. vi. Accédez au classification du trafic étape.

Voir "Création de la règle ILM proposée" si vous avez besoin d'instructions plus détaillées.

3. Passez en revue l'ordre des règles de la nouvelle politique.

   Étant donné que la règle FabricPool est la première règle, tous les objets du compartiment FabricPool sont placés avant que les autres règles de la règle ne soient évaluées. Les objets d'autres compartiments sont placés selon les règles suivantes de la règle.

4. Consultez le diagramme de rétention pour savoir comment les différents objets seront conservés.
   a. Sélectionnez **développer tout** pour afficher un diagramme de rétention pour chaque règle de la stratégie proposée.
   b. Sélectionnez **Time Period** et **Storage Pool** pour consulter le diagramme de rétention. Vérifiez que toutes les règles qui s'appliquent au compartiment FabricPool ou au locataire conservent les objets **Forever**.
5. Une fois que vous avez examiné la politique proposée, sélectionnez **Activer et continuer** pour activer la stratégie et passer à l'étape de classification du trafic.

> Les erreurs d'une règle ILM peuvent entraîner des pertes de données irréparables. Examinez attentivement la stratégie avant de l'activer.

Étape 8 de 9 : création d'une politique de classification du trafic

L'assistant d'installation FabricPool peut également créer une règle de classification du trafic que vous pouvez utiliser pour contrôler la charge de travail FabricPool. La stratégie créée par le système utilise une règle de correspondance pour identifier tout le trafic réseau lié au compartiment que vous avez créé. Cette règle surveille uniquement le trafic ; elle ne limite pas le trafic pour FabricPool ou tout autre client.

Pour plus de détails sur cette étape, voir "Créer une règle de classification du trafic pour FabricPool".

Étapes

1. Consultez la politique.
2. Si vous souhaitez créer cette stratégie de classification de trafic, sélectionnez **Créer et continuer**.

   Dès que FabricPool commence à hiérarchiser les données vers StorageGRID, vous pouvez accéder à la page règles de classification du trafic pour afficher les mesures du trafic réseau correspondant à cette règle. Par la suite, vous pouvez également ajouter des règles pour limiter d'autres charges de travail et vous assurer que la charge de travail FabricPool dispose de la plus grande partie de la bande passante.

3. Sinon, sélectionnez **Ignorer cette étape**.

Étape 9 sur 9 : passez en revue le résumé

Ce récapitulatif fournit des informations détaillées sur les éléments que vous avez configurés, notamment le nom de l'équilibreur de charge, le locataire et le compartiment, la règle de classification du trafic et la règle ILM active.

Étapes

1. Passez en revue le résumé.
2. Sélectionnez **Terminer**.

Étapes suivantes

Une fois l'assistant FabricPool terminé, effectuez les étapes suivantes.

Étapes

1. Accédez à "Configuration de ONTAP System Manager" Pour saisir les valeurs enregistrées et terminer le côté ONTAP de la connexion. Vous devez ajouter StorageGRID en tant que Tier cloud, relier le Tier cloud à un Tier local pour créer une FabricPool et définir des règles de Tiering des volumes.
2. Accédez à "Configurer le serveur DNS" Et assurez-vous que le DNS inclut un enregistrement permettant d'associer le nom du serveur StorageGRID (nom de domaine complet) à chaque adresse IP StorageGRID que vous utiliserez.
3. Accédez à "Autres meilleures pratiques pour StorageGRID et FabricPool" Découvrez les bonnes pratiques pour les journaux d'audit StorageGRID et d'autres options de configuration globale.

Configurez StorageGRID manuellement

Créez un groupe haute disponibilité pour FabricPool

Lorsque vous configurez StorageGRID pour une utilisation avec FabricPool, vous pouvez éventuellement créer un ou plusieurs groupes haute disponibilité (HA). Un groupe haute disponibilité est un ensemble de nœuds qui contiennent chacun le service StorageGRID Load Balancer. Un groupe haute disponibilité peut contenir des nœuds de passerelle, des nœuds d'administration, ou les deux.

Vous pouvez utiliser un groupe haute disponibilité pour maintenir les connexions de données FabricPool disponibles. Un groupe haute disponibilité utilise des adresses IP virtuelles (VIP) pour fournir un accès haute disponibilité au service Load Balancer. En cas de défaillance de l'interface active du groupe haute disponibilité, une interface de sauvegarde peut gérer la charge de travail avec un faible impact sur les opérations FabricPool.

Pour plus d'informations sur cette tâche, reportez-vous à la section "Gérez les groupes haute disponibilité". Pour exécuter cette tâche à l'aide de l'assistant de configuration FabricPool, accédez à "Accédez à l'assistant d'installation FabricPool et terminez-le".

Avant de commencer

- Vous avez passé en revue le "meilleures pratiques pour les groupes haute disponibilité".
- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous disposez de l'autorisation d'accès racine.
- Si vous prévoyez d'utiliser un VLAN, vous avez créé l'interface VLAN. Voir "Configurez les interfaces VLAN".

Étapes

1. Sélectionnez **CONFIGURATION** > **réseau** > **groupes haute disponibilité**.
2. Sélectionnez **Créer**.
3. Pour l'étape **entrer les détails**, remplissez les champs suivants.

Champ	Description
Nom du groupe HAUTE DISPONIBILITÉ	Un nom d'affichage unique pour ce groupe haute disponibilité.
Description (facultatif)	La description de ce groupe HA.

4. Pour l'étape **Ajouter des interfaces**, sélectionnez les interfaces de nœud que vous souhaitez utiliser dans ce groupe haute disponibilité.

   Utilisez les en-têtes de colonne pour trier les lignes ou entrez un terme de recherche pour localiser les interfaces plus rapidement.

   Vous pouvez sélectionner un ou plusieurs nœuds, mais vous ne pouvez sélectionner qu'une seule interface pour chaque nœud.

5. Pour l'étape **hiérarchiser les interfaces**, déterminez l'interface principale et les interfaces de sauvegarde pour ce groupe haute disponibilité.

   Faites glisser des lignes pour modifier les valeurs de la colonne **ordre de priorité**.

   La première interface de la liste est l'interface principale. L'interface principale est l'interface active, sauf en cas de défaillance.

   Si le groupe haute disponibilité comprend plusieurs interfaces et que l'interface active est défaillante, les adresses IP virtuelles (VIP) sont déplacées vers la première interface de sauvegarde, dans l'ordre de priorité. Si cette interface échoue, les adresses VIP passent à l'interface de sauvegarde suivante, etc. Lorsque les pannes sont résolues, les adresses VIP repassent à l'interface de priorité la plus élevée disponible.

6. Pour l'étape **entrer les adresses IP**, renseignez les champs suivants.

Champ	Description
Sous-réseau CIDR	Adresse du sous-réseau VIP en notation CIDR—adresse IPv4 suivie d'une barre oblique et de la longueur du sous-réseau (0-32). Aucun bit d'hôte ne doit être défini pour l'adresse réseau. Par exemple : `192.16.0.0/22`.
Adresse IP de la passerelle (facultative)	Facultatif. Si les adresses IP ONTAP utilisées pour accéder à StorageGRID ne se trouvent pas sur le même sous-réseau que les adresses VIP StorageGRID, entrez l'adresse IP de la passerelle locale VIP StorageGRID. L'adresse IP de la passerelle locale doit se trouver dans le sous-réseau VIP.

Champ	Description
Adresse IP virtuelle	Entrez au moins une et dix adresses VIP pour l'interface active du groupe HA. Toutes les adresses VIP doivent se trouver dans le sous-réseau VIP. Au moins une adresse doit être IPv4. Vous pouvez éventuellement spécifier des adresses IPv4 et IPv6 supplémentaires.

7. Sélectionnez **Créer groupe HA**, puis **Terminer**.

Créez un noeud final d'équilibrage de charge pour FabricPool

StorageGRID utilise un équilibreur de charge pour gérer la charge de travail à partir d'applications client, telles qu'FabricPool. L'équilibrage de la charge optimise la vitesse et la capacité de connexion sur plusieurs nœuds de stockage.

Lors de la configuration de StorageGRID pour une utilisation avec FabricPool, vous devez configurer un point d'extrémité d'équilibreur de charge et télécharger ou générer un certificat de point d'extrémité d'équilibreur de charge, utilisé pour sécuriser la connexion entre ONTAP et StorageGRID.

Pour exécuter cette tâche à l'aide de l'assistant de configuration FabricPool, accédez à "Accédez à l'assistant d'installation FabricPool et terminez-le".

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous disposez de l'autorisation d'accès racine.
- Vous avez examiné le général "considérations relatives à l'équilibrage de charge" ainsi que le "Bonnes pratiques en matière d'équilibrage de charge pour FabricPool".

Étapes

1. Sélectionnez **CONFIGURATION** > **réseau** > **noeuds finaux de l'équilibreur de charge**.
2. Sélectionnez **Créer**.
3. Pour l'étape **entrer les détails du noeud final**, renseignez les champs suivants.

Champ	Description
Nom	Nom descriptif du noeud final.

Champ	Description
Port	Port StorageGRID que vous souhaitez utiliser pour l'équilibrage de charge. Ce champ est défini par défaut sur 10433 pour le premier noeud final que vous créez, mais vous pouvez entrer n'importe quel port externe inutilisé. Si vous entrez 80 ou 443, le noeud final est configuré uniquement sur les noeuds de passerelle. Ces ports sont réservés sur des nœuds d'administration. **Remarque :** les ports utilisés par d'autres services de grille ne sont pas autorisés. Voir la"Référence du port réseau". Vous fournissez ce numéro à ONTAP lorsque vous associez StorageGRID à un niveau cloud FabricPool.
Type de client	Sélectionnez **S3**.
Protocole réseau	Sélectionnez **HTTPS**. **Remarque** : la communication avec StorageGRID sans chiffrement TLS est prise en charge, mais elle n'est pas recommandée.

4. Pour l'étape **Sélectionner le mode de liaison**, spécifiez le mode de liaison. Le mode de liaison contrôle la façon dont le noeud final est accédé—en utilisant une adresse IP ou des adresses IP et des interfaces réseau spécifiques.

Option	Description
Global (par défaut)	Les clients peuvent accéder au point final en utilisant l'adresse IP de n'importe quel nœud de passerelle ou nœud d'administration, l'adresse IP virtuelle (VIP) de n'importe quel groupe haute disponibilité sur n'importe quel réseau, ou un FQDN correspondant. Utilisez le paramètre **Global** (valeur par défaut) sauf si vous devez restreindre l'accessibilité de ce point final.
Adresses IP virtuelles de groupes haute disponibilité	Les clients doivent utiliser une adresse IP virtuelle (ou le nom de domaine complet correspondant) d'un groupe haute disponibilité pour accéder à ce point final. Les terminaux associés à ce mode de liaison peuvent tous utiliser le même numéro de port, tant que les groupes haute disponibilité que vous sélectionnez pour les terminaux ne se chevauchent pas.
Interfaces de nœuds	Les clients doivent utiliser les adresses IP (ou les FQDN correspondants) des interfaces de nœud sélectionnées pour accéder à ce noeud final.
Type de nœud	En fonction du type de nœud que vous sélectionnez, les clients doivent utiliser l'adresse IP (ou le nom de domaine complet correspondant) de tout nœud d'administration ou l'adresse IP (ou le nom de domaine complet correspondant) de tout nœud de passerelle pour accéder à ce point final.

5. Pour l'étape **tenant Access**, sélectionnez l'une des options suivantes :

Champ	Description
Autoriser tous les locataires (par défaut)	Tous les comptes de locataires peuvent utiliser ce terminal pour accéder à leurs compartiments. **Autoriser tous les locataires** est presque toujours l'option appropriée pour le noeud final de l'équilibreur de charge utilisé pour FabricPool. Vous devez sélectionner cette option si vous n'avez pas encore créé de compte de locataire.
Autoriser les locataires sélectionnés	Seuls les comptes de locataire sélectionnés peuvent utiliser ce terminal pour accéder à leurs compartiments.
Bloquez les locataires sélectionnés	Les comptes de locataire sélectionnés ne peuvent pas utiliser ce terminal pour accéder à leurs compartiments. Tous les autres locataires peuvent utiliser ce noeud final.

6. Pour l'étape **joindre un certificat**, sélectionnez l'une des options suivantes :

Champ	Description
Télécharger le certificat (recommandé)	Utilisez cette option pour télécharger un certificat de serveur signé par une autorité de certification, une clé privée de certificat et un ensemble d'autorité de certification facultatif.
Générez un certificat	Utilisez cette option pour générer un certificat auto-signé. Voir "Configurer les terminaux de l'équilibreur de charge" pour plus de détails sur ce que vous devez saisir.
Utilisez les certificats StorageGRID S3 et Swift	Cette option n'est disponible que si vous avez déjà téléchargé ou généré une version personnalisée du certificat global StorageGRID. Voir "Configurez les certificats API S3 et Swift" pour plus d'informations.

7. Sélectionnez **Créer**.

> Les modifications apportées à un certificat de point final peuvent prendre jusqu'à 15 minutes pour être appliquées à tous les nœuds.

Créez un compte de locataire pour FabricPool

Vous devez créer un compte de tenant dans le Grid Manager pour utilisation FabricPool.

Les comptes de locataire permettent aux applications client de stocker et de récupérer des objets sur StorageGRID. Chaque compte locataire possède son propre ID de compte, groupes et utilisateurs autorisés, compartiments et objets.

Pour plus d'informations sur cette tâche, reportez-vous à la section "Créer un compte de locataire". Pour exécuter cette tâche à l'aide de l'assistant de configuration FabricPool, accédez à "Accédez à l'assistant d'installation FabricPool et terminez-le".

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous disposez d'autorisations d'accès spécifiques.

Étapes

1. Sélectionnez **LOCATAIRES**.
2. Sélectionnez **Créer**.
3. Pour les étapes entrer les détails, entrez les informations suivantes.

Champ	Description
Nom	Nom du compte de locataire. Les noms de locataires n'ont pas besoin d'être uniques. Lors de la création du compte locataire, il reçoit un ID de compte numérique unique.
Description (facultatif)	Une description pour aider à identifier le locataire.
Type de client	Doit être **S3** pour FabricPool.
Quota de stockage (facultatif)	Laissez ce champ vide pour FabricPool.

4. Pour l'étape Sélectionner les autorisations :
   a. Ne sélectionnez pas **Autoriser les services de plate-forme**.

      Les locataires FabricPool n'ont généralement pas besoin d'utiliser des services de plateforme, tels que la réplication CloudMirror.

   b. Si vous le souhaitez, sélectionnez **utiliser le propre référentiel d'identité**.
   c. Ne sélectionnez pas **Autoriser la sélection S3**.

      Les locataires FabricPool n'ont généralement pas besoin d'utiliser S3 Select.

   d. Si vous le souhaitez, sélectionnez **utiliser la connexion de fédération de grille** pour permettre au locataire d'utiliser un "connexion de fédération de grille" pour le clone de compte et la réplication entre grille. Sélectionnez ensuite la connexion de fédération de grille à utiliser.
5. Pour l'étape définir l'accès racine, spécifiez l'utilisateur qui aura l'autorisation d'accès racine initiale pour le compte de locataire, selon que votre système StorageGRID utilise ou non "fédération des identités", "Authentification unique (SSO)", ou les deux.

Option	Faites ça
Si la fédération des identités n'est pas activée	Spécifiez le mot de passe à utiliser lors de la connexion au tenant en tant qu'utilisateur root local.

Option	Faites ça
Si la fédération des identités est activée	a. Sélectionnez un groupe fédéré existant pour obtenir l'autorisation d'accès racine pour le tenant. b. Vous pouvez également spécifier le mot de passe à utiliser lors de la connexion au tenant en tant qu'utilisateur root local.
Si la fédération des identités et l'authentification unique (SSO) sont toutes deux activées	Sélectionnez un groupe fédéré existant pour obtenir l'autorisation d'accès racine pour le tenant. Aucun utilisateur local ne peut se connecter.

6. Sélectionnez **Créer locataire**.

Création d'un compartiment S3 et obtention des clés d'accès

Avant d'utiliser StorageGRID avec un workload FabricPool, vous devez créer un compartiment S3 pour vos données FabricPool. Vous devez également obtenir une clé d'accès et une clé secrète pour le compte de locataire que vous utiliserez pour FabricPool.

Pour plus d'informations sur cette tâche, reportez-vous à la section "Créer un compartiment S3" et "Créez vos propres clés d'accès S3". Pour exécuter cette tâche à l'aide de l'assistant de configuration FabricPool, accédez à "Accédez à l'assistant d'installation FabricPool et terminez-le".

Avant de commencer

- Vous avez créé un compte de locataire pour l'utilisation de FabricPool.
- Vous disposez d'un accès racine au compte de locataire.

Étapes

1. Connectez-vous au Gestionnaire de locataires.

   Vous pouvez effectuer l'une des opérations suivantes :

   - Dans la page comptes de tenant du Gestionnaire de grille, sélectionnez le lien **se connecter** pour le tenant et entrez vos informations d'identification.
   - Saisissez l'URL du compte de tenant dans un navigateur Web et saisissez vos informations d'identification.

2. Créez un compartiment S3 pour les données FabricPool.

   Vous devez créer un compartiment unique pour chaque cluster ONTAP que vous prévoyez d'utiliser.

   a. Sélectionnez **Afficher les compartiments** dans le tableau de bord ou sélectionnez **STOCKAGE (S3) > compartiments**.

   b. Sélectionnez **Créer un compartiment**.

   c. Entrez le nom du compartiment StorageGRID à utiliser avec FabricPool. Par exemple : `fabricpool-bucket`.

Vous ne pouvez pas modifier le nom du compartiment après la création du compartiment.

d. Sélectionnez la région de ce compartiment.

   Par défaut, tous les compartiments sont créés dans le `us-east-1` région.

e. Sélectionnez **Continuer**.

f. Sélectionnez **Créer un compartiment**.

Ne sélectionnez pas **Activer la gestion des versions d'objet** pour le compartiment FabricPool. De même, ne modifiez pas un compartiment FabricPool pour utiliser **disponible** ou un niveau de cohérence non par défaut. Le niveau de cohérence de compartiment recommandé pour les compartiments FabricPool est **Read-after-New-write**, qui est le paramètre par défaut pour un nouveau compartiment.

3. Créez une clé d'accès et une clé d'accès secrète.

   a. Sélectionnez **STORAGE (S3)** > **Mes clés d'accès**.

   b. Sélectionnez **Créer clé**.

   c. Sélectionnez **Créer une clé d'accès**.

   d. Copiez l'ID de la clé d'accès et la clé secrète dans un emplacement sûr, ou sélectionnez **Download .csv** pour enregistrer un fichier de feuille de calcul contenant l'ID de la clé d'accès et la clé secrète d'accès.

      Ces valeurs seront saisies dans ONTAP lorsque vous configurez StorageGRID en tant que Tier cloud FabricPool.

Si vous générez une nouvelle clé d'accès et une nouvelle clé d'accès secrète dans StorageGRID à l'avenir, entrez les nouvelles clés dans ONTAP avant de supprimer les anciennes valeurs de StorageGRID. Sinon, ONTAP risque de perdre temporairement son accès à StorageGRID.

Configurez la solution ILM pour les données FabricPool

Cet exemple de règle simple vous permet de commencer par vos propres règles et règles ILM.

Nous partons du principe que vous concevez les règles ILM et une règle ILM pour un système StorageGRID qui possède quatre nœuds de stockage dans un data Center unique à Denver, Colorado. Les données FabricPool dans cet exemple utilisent un compartiment nommé `fabricpool-bucket`.

Les règles et règles ILM suivantes ne sont que des exemples. Les règles ILM sont nombreuses. Avant d'activer une nouvelle stratégie, simulez la stratégie proposée pour confirmer qu'elle fonctionnera comme destinée à protéger le contenu contre la perte. Pour en savoir plus, voir "Gestion des objets avec ILM".

Pour éviter toute perte de données, n'utilisez pas de règle ILM qui expirera ou supprimera les données de Tier cloud FabricPool. Définissez la période de conservation sur **Forever** pour vous assurer que les objets FabricPool ne sont pas supprimés par la ILM de StorageGRID.

Avant de commencer

- Vous avez passé en revue le "Bonnes pratiques d'utilisation d'ILM avec des données FabricPool".
- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous disposez de l'autorisation ILM ou Root Access.
- Si vous avez mis à niveau vers StorageGRID 11.7 à partir d'une version précédente de StorageGRID, vous avez configuré le pool de stockage que vous utiliserez. En général, vous devez créer un pool de stockage pour chaque site StorageGRID.

Cette condition préalable ne s'applique pas aux nouvelles installations de StorageGRID 11.7. Lorsque vous installez StorageGRID 11.7 sur une nouvelle grille, les pools de stockage sont automatiquement créés pour chaque site.

Étapes

1. Créez une règle ILM qui s'applique uniquement aux données dans `fabricpool-bucket`. Dans cet exemple de règle, des copies avec code d'effacement sont créées.

Définition de règle	Exemple de valeur
Nom de la règle	2 + 1 code d'effacement pour données FabricPool
Nom du compartiment	`fabricpool-bucket` Vous pouvez également filtrer le compte de tenant FabricPool.
Filtres avancés	Taille de l'objet supérieure à 0.2 Mo. **Remarque :** FabricPool écrit uniquement des objets de 4 Mo, mais vous devez ajouter un filtre de taille d'objet car cette règle utilise le code d'effacement.
Heure de référence	Temps d'ingestion
Période de temps et placements	Magasin du jour 0 pour toujours Stockez les objets par code d'effacement à l'aide d'un schéma EC 2+1 à Denver et conservez-les indéfiniment dans StorageGRID. Pour éviter toute perte de données, n'utilisez pas de règle ILM qui expirera ou supprimera les données de Tier cloud FabricPool.
Comportement d'ingestion	Équilibré

2. Créez une règle ILM par défaut qui crée deux copies répliquées de tout objet non associé à la première règle. Ne sélectionnez pas de filtre de base (compte de locataire ou nom de compartiment) ni de filtre avancé.

Définition de règle	Exemple de valeur
Nom de la règle	Deux copies répliquées
Nom du compartiment	*aucun*
Filtres avancés	*aucun*
Heure de référence	Temps d'ingestion
Période de temps et placements	Magasin du jour 0 pour toujours Stockage d'objets en répliquant 2 copies à Denver.
Comportement d'ingestion	Équilibré

3. Création d'une règle ILM proposée et sélection des deux règles Comme la règle de réplication n'utilise aucun filtre, elle peut être la règle par défaut (dernière) de la règle.
4. Ingestion des objets de test dans la grille.
5. Simuler la règle avec les objets de test pour vérifier le comportement.
6. Activer la règle.

Lorsque cette règle est activée, StorageGRID place les données d'objet comme suit :

- Les données sont hiérarchisées à partir du système FabricPool In `fabricpool-bucket` le code d'effacement sera appliqué à l'aide du schéma de code d'effacement 2+1. Deux fragments de données et un fragment de parité seront placés sur trois nœuds de stockage différents.
- Tous les objets dans tous les autres compartiments sont répliqués. Deux copies sont créées et placées sur deux nœuds de stockage différents.
- Les copies seront conservées dans StorageGRID indéfiniment. La solution ILM de StorageGRID ne supprime pas ces objets.

Créer une règle de classification du trafic pour FabricPool

Vous pouvez éventuellement concevoir une règle de classification du trafic StorageGRID afin d'optimiser la qualité de service pour la charge de travail FabricPool.

Pour plus d'informations sur cette tâche, reportez-vous à la section "Gérer les stratégies de classification du trafic". Pour exécuter cette tâche à l'aide de l'assistant de configuration FabricPool, accédez à "Accédez à l'assistant d'installation FabricPool et terminez-le".

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous disposez de l'autorisation d'accès racine.

Description de la tâche

Les meilleures pratiques de création d'une stratégie de classification du trafic pour FabricPool dépendent de la charge de travail :

- Si vous prévoyez de transférer les données de la charge de travail principale FabricPool vers StorageGRID, vous devez vous assurer que la charge de travail FabricPool dispose de la plus grande partie de la bande passante. Vous pouvez créer une règle de classification du trafic pour limiter tous les autres workloads.

  > En général, les opérations de lecture FabricPool sont plus importantes que les opérations d'écriture.

  Par exemple, si d'autres clients S3 utilisent ce système StorageGRID, vous devez créer une règle de classification du trafic. Vous pouvez limiter le trafic réseau pour les autres compartiments, locataires, sous-réseaux IP ou terminaux d'équilibrage de charge.

*En général, vous ne devez pas imposer de limites de qualité de service à une charge de travail FabricPool ; vous devez uniquement limiter les autres charges de travail.

- Les limites placées sur d'autres charges de travail doivent tenir compte du comportement de ces dernières. Les limites imposées varient également en fonction du dimensionnement et des capacités de votre réseau et du taux d'utilisation attendu.

Étapes

1. Sélectionnez **CONFIGURATION** > **réseau** > **classification du trafic**.
2. Sélectionnez **Créer**.
3. Entrez un nom et une description (facultatif) pour la stratégie et sélectionnez **Continuer**.
4. Pour l'étape Ajouter des règles de correspondance, ajoutez au moins une règle.
   a. Sélectionnez **Ajouter une règle**
   b. Sous Type, sélectionnez **noeud final de l'équilibreur de charge**, puis sélectionnez le noeud final de l'équilibreur de charge que vous avez créé pour FabricPool.

      Vous pouvez également sélectionner le compartiment ou le compte de locataire FabricPool.

   c. Si vous souhaitez que cette stratégie de trafic limite le trafic pour les autres noeuds finaux, sélectionnez **comparaison inverse**.
5. Vous pouvez également ajouter une ou plusieurs limites pour contrôler le trafic réseau correspondant à la règle.

   > StorageGRID collecte des mesures, même si vous n'ajoutez aucune limite, pour vous permettre de comprendre les tendances du trafic.

   a. Sélectionnez **Ajouter une limite**.
   b. Sélectionnez le type de trafic que vous souhaitez limiter et la limite à appliquer.
6. Sélectionnez **Continuer**.
7. Lisez et passez en revue la politique de classification du trafic. Utilisez le bouton **Précédent** pour revenir en arrière et apporter les modifications nécessaires. Lorsque vous êtes satisfait de la stratégie, sélectionnez **Enregistrer et continuer**.

Une fois que vous avez terminé

"Afficher les données de trafic réseau" pour vérifier que les stratégies appliquent les limites de trafic que vous attendez.

Configuration de ONTAP System Manager

Une fois que vous avez obtenu les informations StorageGRID requises, vous pouvez accéder à ONTAP pour ajouter StorageGRID en tant que Tier cloud.

Avant de commencer

- Si vous avez terminé l'assistant d'installation de FabricPool, vous avez le `ONTAP_FabricPool_settings_bucketname.txt` fichier que vous avez téléchargé.
- Si vous avez configuré StorageGRID manuellement, vous disposez du nom de domaine complet (FQDN) que vous utilisez pour StorageGRID ou de l'adresse IP virtuelle (VIP) pour le groupe haute disponibilité StorageGRID, du numéro de port du point final de l'équilibreur de charge, du certificat d'équilibrage de charge, L'ID de clé d'accès et la clé secrète de l'utilisateur root du compte de locataire, ainsi que le nom du compartiment ONTAP seront utilisés dans ce locataire.

Accédez à ONTAP System Manager

Ces instructions expliquent comment utiliser ONTAP System Manager pour ajouter StorageGRID en tant que niveau cloud. Vous pouvez effectuer la même configuration via l'interface de ligne de commandes de ONTAP. Pour obtenir des instructions, reportez-vous à la section "ONTAP 9 : gestion des tiers FabricPool avec l'interface de ligne de commandes".

Étapes

1. Accédez à System Manager pour le cluster ONTAP que vous souhaitez mettre au niveau vers StorageGRID.
2. Connectez-vous en tant qu'administrateur du cluster.
3. Naviguez jusqu'à **STORAGE** > **tiers** > **Add Cloud Tier**.
4. Sélectionnez **StorageGRID** dans la liste des fournisseurs de magasins d'objets.

Entrez les valeurs StorageGRID

Voir "ONTAP 9 : présentation de la gestion des niveaux FabricPool avec System Manager" pour en savoir plus.

Étapes

1. Remplissez le formulaire Add Cloud Tier, à l'aide du `ONTAP_FabricPool_settings_bucketname.txt` ou les valeurs que vous avez obtenues manuellement.

Champ	Description
Nom	Entrez un nom unique pour ce niveau de cloud. Vous pouvez accepter la valeur par défaut.

Champ	Description
Style d'URL	Si vous "Noms de domaine de terminaux S3 configurés", Sélectionnez **URL de style hébergé virtuel**. **URL de style de chemin** est la valeur par défaut pour ONTAP, mais l'utilisation de requêtes de type hébergement virtuel est recommandée pour StorageGRID. Vous devez utiliser **Path-style URL** si vous indiquez une adresse IP au lieu d'un nom de domaine pour le champ **Server name (FQDN)**.
Nom du serveur (FQDN)	Entrez le nom de domaine complet (FQDN) que vous utilisez pour StorageGRID ou l'adresse IP virtuelle (VIP) du groupe StorageGRID HA. Par exemple : `s3.storagegrid.company.com`. Notez ce qui suit : • L'adresse IP ou le nom de domaine que vous spécifiez ici doit correspondre au certificat que vous avez téléchargé ou généré pour le noeud final de l'équilibreur de charge StorageGRID. • Si vous fournissez un nom de domaine, l'enregistrement DNS doit correspondre à chaque adresse IP que vous utiliserez pour vous connecter à StorageGRID. Voir "Configurer le serveur DNS".
SSL	Activé (par défaut).
Certificat de magasin d'objets	Collez le certificat PEM que vous utilisez pour le noeud final de l'équilibreur de charge StorageGRID, notamment : `-----BEGIN CERTIFICATE-----` et `-----END CERTIFICATE-----`. **Remarque :** si une autorité de certification intermédiaire a émis le certificat StorageGRID, vous devez fournir le certificat CA intermédiaire. Si le certificat StorageGRID a été émis directement par l'autorité de certification racine, vous devez fournir le certificat d'autorité de certification racine.
Port	Indiquez le port utilisé par le noeud final de l'équilibreur de charge StorageGRID. ONTAP utilise ce port lorsqu'il se connecte à StorageGRID. Par exemple, 10433.
Clé d'accès et clé secrète	Entrez l'ID de clé d'accès et la clé d'accès secrète pour l'utilisateur root du compte de locataire StorageGRID. **Conseil** : si vous générez une nouvelle clé d'accès et une nouvelle clé d'accès secrète dans StorageGRID à l'avenir, entrez les nouvelles clés dans ONTAP avant de supprimer les anciennes valeurs de StorageGRID. Sinon, ONTAP risque de perdre temporairement son accès à StorageGRID.
Nom du conteneur	Indiquez le nom du compartiment StorageGRID que vous avez créé pour être utilisé avec ce niveau ONTAP.

2. Terminez la configuration finale de FabricPool dans ONTAP.

a. Reliez un ou plusieurs agrégats au Tier cloud.

b. Si vous le souhaitez, créez une règle de Tiering de volume.

Configurer le serveur DNS

Après avoir configuré des groupes haute disponibilité, des terminaux d'équilibrage de la charge et des noms de domaine de terminaux S3, vous devez vous assurer que le DNS inclut les entrées nécessaires à StorageGRID. Vous devez inclure une entrée DNS pour chaque nom du certificat de sécurité et pour chaque adresse IP que vous pourriez utiliser.

Voir "Considérations relatives à l'équilibrage de charge".

Entrées DNS pour le nom du serveur StorageGRID

Ajoutez des entrées DNS pour associer le nom du serveur StorageGRID (nom de domaine complet) à chaque adresse IP StorageGRID que vous utiliserez. Les adresses IP que vous entrez dans le DNS dépendent de l'utilisation ou non d'un groupe haute disponibilité de nœuds d'équilibrage de charge :

- Si vous avez configuré un groupe haute disponibilité, ONTAP se connecte aux adresses IP virtuelles de ce groupe haute disponibilité.
- Si vous n'utilisez pas de groupe haute disponibilité, ONTAP peut se connecter au service StorageGRID Load Balancer en utilisant l'adresse IP d'un nœud de passerelle ou d'un nœud d'administration.
- Si le nom du serveur résout plusieurs adresses IP, ONTAP établit des connexions client avec toutes les adresses IP (jusqu'à 16 adresses IP). Les adresses IP sont récupérées dans une méthode de séquence périodique lors de l'établissement des connexions.

Entrées DNS pour les demandes de type hébergement virtuel

Si vous avez défini "Noms de domaine de terminaux S3" Et vous utiliserez des requêtes de type hébergement virtuel, ajouterez des entrées DNS pour tous les noms de domaine de point final S3 requis, y compris les noms génériques.

Meilleures pratiques StorageGRID pour FabricPool

Bonnes pratiques pour les groupes à haute disponibilité (HA)

Avant de connecter StorageGRID en tant que Tier cloud FabricPool, découvrez les groupes haute disponibilité StorageGRID et consultez les bonnes pratiques d'utilisation des groupes haute disponibilité avec FabricPool.

Qu'est-ce qu'un groupe haute disponibilité ?

Un groupe haute disponibilité est un ensemble d'interfaces issues de plusieurs nœuds de passerelle StorageGRID, nœuds d'administration ou les deux. Un groupe haute disponibilité contribue à maintenir les connexions de données des clients disponibles. En cas de défaillance de l'interface active du groupe haute disponibilité, une interface de sauvegarde peut gérer la charge de travail avec un faible impact sur les opérations FabricPool.

Chaque groupe haute disponibilité fournit un accès hautement disponible aux services partagés sur les nœuds associés. Par exemple, un groupe haute disponibilité qui se compose d'interfaces uniquement sur les nœuds

de passerelle ou sur les deux nœuds d'administration et de passerelle fournit un accès hautement disponible au service Load Balancer partagé.

Pour en savoir plus sur les groupes haute disponibilité, reportez-vous à la section "Gestion des groupes haute disponibilité".

À l'aide de groupes haute disponibilité

Les bonnes pratiques de création de groupe haute disponibilité StorageGRID pour FabricPool dépendent de la charge de travail.

- Si vous prévoyez d'utiliser FabricPool avec les données des principaux workloads, vous devez créer un groupe haute disponibilité incluant au moins deux nœuds d'équilibrage de la charge pour éviter toute interruption de la récupération des données.
- Si vous prévoyez d'utiliser la règle de Tiering de volume FabricPool snapshot uniquement ou des tiers de performance locaux non principaux (par exemple, emplacements de reprise après incident ou destinations NetApp SnapMirror®), vous pouvez configurer un groupe haute disponibilité avec un seul nœud.

Ces instructions décrivent la configuration d'un groupe haute disponibilité pour Active-Backup HA (un nœud est actif et un nœud est une sauvegarde). Cependant, vous préférez peut-être utiliser DNS Round Robin ou Active-Active HA. Pour découvrir les avantages de ces autres configurations haute disponibilité, consultez "Options de configuration pour les groupes haute disponibilité".

Bonnes pratiques en matière d'équilibrage de charge pour FabricPool

Avant de rattacher StorageGRID en tant que Tier cloud FabricPool, consultez les bonnes pratiques pour l'utilisation d'équilibreurs de charge avec FabricPool.

Pour plus d'informations générales sur l'équilibreur de charge StorageGRID et le certificat d'équilibreur de charge, reportez-vous à la section "Considérations relatives à l'équilibrage de charge".

Bonnes pratiques pour l'accès du locataire au terminal d'équilibrage de la charge utilisé pour FabricPool

Vous pouvez contrôler les locataires qui peuvent utiliser un terminal d'équilibrage de la charge spécifique pour accéder à leurs compartiments. Vous pouvez autoriser tous les locataires, autoriser certains locataires ou bloquer certains locataires. Lors de la création d'un noeud final d'équilibrage de charge pour l'utilisation de FabricPool, sélectionnez **Autoriser tous les locataires**. ONTAP chiffre les données qui sont placées dans des compartiments StorageGRID. Cette couche de sécurité supplémentaire ne fournit donc que peu de sécurité supplémentaire.

Meilleures pratiques pour le certificat de sécurité

Lorsque vous créez un terminal d'équilibrage de charge StorageGRID pour une utilisation avec FabricPool, vous fournissez le certificat de sécurité qui permettra à ONTAP de s'authentifier auprès de StorageGRID.

Dans la plupart des cas, la connexion entre ONTAP et StorageGRID doit utiliser le chiffrement TLS (transport Layer Security). L'utilisation de FabricPool sans chiffrement TLS est prise en charge, mais elle n'est pas recommandée. Lorsque vous sélectionnez le protocole réseau pour le noeud final de l'équilibreur de charge StorageGRID, sélectionnez **HTTPS**. Fournissez ensuite le certificat de sécurité qui permettra à ONTAP de s'authentifier auprès de StorageGRID.

Pour en savoir plus sur le certificat de serveur pour un point final d'équilibrage de charge :

- "Gérer les certificats de sécurité"

- "Considérations relatives à l'équilibrage de charge"
- "Consignes de renforcement des certificats de serveur"

Ajouter le certificat à ONTAP

Lorsque vous ajoutez StorageGRID en tant que niveau de cloud FabricPool, vous devez installer le même certificat sur le cluster ONTAP, y compris le certificat racine et tout certificat d'autorité de certification subordonnée.

Gérer l'expiration des certificats

> Si le certificat utilisé pour sécuriser la connexion entre ONTAP et StorageGRID expire, FabricPool cesse temporairement de fonctionner et ONTAP perd temporairement l'accès aux données hiérarchisées vers StorageGRID.

Pour éviter les problèmes d'expiration des certificats, suivez les bonnes pratiques suivantes :

- Surveillez attentivement toutes les alertes qui vous avertissent d'une date d'expiration de certificat proche, telles que les alertes **expiration du certificat de noeud final de l'équilibreur de charge** et **expiration du certificat de serveur global pour les alertes S3 et Swift API**.
- Gardez toujours les versions StorageGRID et ONTAP du certificat synchronisées. Si vous remplacez ou renouvelez le certificat utilisé pour un terminal d'équilibrage de charge, vous devez remplacer ou renouveler le certificat équivalent utilisé par ONTAP pour le Tier cloud.
- Utiliser un certificat d'autorité de certification signé publiquement. Si vous utilisez un certificat signé par une autorité de certification, vous pouvez utiliser l'API de gestion de grille pour automatiser la rotation des certificats. Vous pouvez ainsi remplacer les certificats dont la date d'expiration arrive à expiration sans interrompre l'activité.
- Si vous avez généré un certificat StorageGRID auto-signé et que ce certificat est sur le point d'expirer, vous devez le remplacer manuellement dans StorageGRID et dans ONTAP avant que le certificat existant n'expire. Si un certificat auto-signé a déjà expiré, désactivez la validation du certificat dans ONTAP pour éviter toute perte d'accès.

  Voir "Base de connaissances NetApp : comment configurer un nouveau certificat de serveur autosigné StorageGRID sur un déploiement ONTAP FabricPool existant" pour obtenir des instructions.

Bonnes pratiques d'utilisation d'ILM avec des données FabricPool

Si vous utilisez FabricPool pour hiérarchiser les données vers StorageGRID, vous devez connaître les exigences d'utilisation de la gestion du cycle de vie des informations (ILM) StorageGRID avec les données FabricPool.

> FabricPool ne connaît pas les règles ou les règles ILM de StorageGRID. La perte des données peut se produire si la règle ILM de StorageGRID est mal configurée. Pour plus d'informations, reportez-vous à la section "Création d'une règle ILM : présentation" et "Création d'une règle ILM : présentation".

Règles d'utilisation d'ILM avec FabricPool

Lorsque vous utilisez l'assistant d'installation FabricPool, il crée automatiquement une règle ILM pour chaque compartiment S3 que vous créez, ajoute cette règle à une règle proposée et vous invite à activer la nouvelle

règle dans le cadre de l'assistant. La règle automatiquement créée respecte les bonnes pratiques recommandées : elle utilise un code d'effacement 2+1 sur un seul site.

Si vous configurez StorageGRID manuellement au lieu d'utiliser l'assistant d'installation FabricPool, lisez ces instructions pour vous assurer que les règles ILM et la politique ILM sont adaptées aux données FabricPool et aux exigences de votre entreprise. Vous devrez peut-être créer de nouvelles règles et mettre à jour votre politique ILM active pour répondre à ces instructions.

- Vous pouvez utiliser toutes les combinaisons de réplication et de règles de code d'effacement pour protéger les données de Tier cloud.

  Il est recommandé d'utiliser un code d'effacement 2+1 sur un site pour une protection des données économique. Le code d'effacement consomme plus de ressources de processeur, mais sa capacité de stockage est bien inférieure à la réplication. Les schémas 4+1 et 6+1 utilisent moins de capacité que le schéma 2+1. Toutefois, les schémas 4+1 et 6+1 sont moins flexibles si vous avez besoin d'ajouter des nœuds de stockage lors de l'extension de grid. Pour plus de détails, voir "Ajoutez de la capacité de stockage pour les objets avec code d'effacement".

- Chaque règle appliquée aux données FabricPool doit au moins deux copies répliquées grâce au code d'effacement.

  > La règle ILM de création d'une seule copie répliquée pendant toute période met les données à risque de perte permanente. Si une seule copie répliquée d'un objet existe, cet objet est perdu en cas de défaillance ou d'erreur importante d'un noeud de stockage. De plus, lors des procédures de maintenance telles que les mises à niveau, l'accès à l'objet est temporairement perdu.

- À vos besoins "Supprimez les données FabricPool de StorageGRID", Utilisez ONTAP pour récupérer toutes les données du volume FabricPool et les promouvoir dans le Tier de performance.

  > Pour éviter toute perte de données, n'utilisez pas de règle ILM qui expirera ou supprimera les données de Tier cloud FabricPool. Définissez la période de conservation de chaque règle ILM sur **Forever** pour vous assurer que les objets FabricPool ne sont pas supprimés par la ILM de StorageGRID.

- Ne créez pas de règles qui déplacera les données de Tier cloud FabricPool hors du compartiment vers un autre emplacement. Vous ne pouvez pas utiliser un pool de stockage cloud pour déplacer des données FabricPool vers un autre magasin d'objets. De même, vous ne pouvez pas archiver de données FabricPool sur bande à l'aide d'un nœud d'archivage.

  > L'utilisation de pools de stockage cloud avec FabricPool n'est pas prise en charge en raison de la latence ajoutée pour extraire un objet de la cible du pool de stockage cloud.

- Depuis ONTAP 9.8, vous pouvez créer des balises d'objet pour classer et trier les données hiérarchisées pour simplifier la gestion. Par exemple, vous pouvez définir des balises uniquement sur les volumes FabricPool reliés à StorageGRID. Ensuite, lorsque vous créez des règles ILM dans StorageGRID, vous pouvez utiliser le filtre avancé balise d'objet pour sélectionner et placer ces données.

Autres meilleures pratiques pour StorageGRID et FabricPool

Lors de la configuration d'un système StorageGRID pour une utilisation avec FabricPool, vous devrez peut-être modifier d'autres options StorageGRID. Avant de modifier un paramètre global, réfléchissez à l'impact de cette modification sur les autres applications

S3.

Vérifiez les destinations des messages et des journaux

Les charges de travail FabricPool disposent souvent d'un taux élevé d'opérations de lecture, ce qui peut générer un grand nombre de messages d'audit.

- Si vous n'avez pas besoin d'enregistrer les opérations de lecture du client pour FabricPool ou toute autre application S3, vous pouvez également accéder à **CONFIGURATION** > **surveillance** > **serveur d'audit et syslog**. Définissez le paramètre **lecture client** sur **erreur** pour diminuer le nombre de messages d'audit enregistrés dans le journal d'audit. Voir "Configurez les messages d'audit et les destinations des journaux" pour plus d'informations.
- Si vous disposez d'une grande grille, utilisez plusieurs types d'applications S3 ou souhaitez conserver toutes les données d'audit, configurez un serveur syslog externe et enregistrez les informations d'audit à distance. L'utilisation d'un serveur externe réduit l'impact sur les performances de la journalisation des messages d'audit sans réduire l'exhaustivité des données d'audit. Voir "Considérations relatives au serveur syslog externe" pour plus d'informations.

Chiffrement d'objet

Lors de la configuration de StorageGRID, vous pouvez éventuellement activer le "option globale de chiffrement des objets stockés" Si un chiffrement des données est nécessaire pour les autres clients StorageGRID. Les données envoyées depuis FabricPool vers StorageGRID sont déjà chiffrées, ce qui signifie qu'il n'est pas nécessaire d'activer le paramètre StorageGRID. Les clés de chiffrement côté client sont la propriété de ONTAP.

Compression d'objet

Lors de la configuration de StorageGRID, n'activez pas le "option globale pour compresser les objets stockés". Les données envoyées depuis FabricPool vers StorageGRID sont déjà compressées. L'utilisation de l'option StorageGRID ne réduira pas davantage la taille d'un objet.

Niveau de cohérence du compartiment

Pour les compartiments FabricPool, le niveau de cohérence de compartiment recommandé est **Read-After-New-write**, qui est le paramètre par défaut d'un nouveau compartiment. Ne modifiez pas les compartiments FabricPool pour utiliser **disponible** ou tout autre niveau de cohérence.

Hiérarchisation FabricPool

Si un nœud StorageGRID utilise du stockage attribué à un système NetApp ONTAP, vérifiez qu'aucune règle de hiérarchisation FabricPool n'est activée sur le volume. Par exemple, si un nœud StorageGRID s'exécute sur un hôte VMware, assurez-vous que la règle de hiérarchisation FabricPool n'est pas activée sur le volume qui sauvegarde le datastore pour le nœud StorageGRID. La désactivation du Tiering FabricPool pour les volumes utilisés avec des nœuds StorageGRID simplifie la résolution des problèmes et les opérations de stockage.

N'utilisez jamais FabricPool pour transférer automatiquement toutes les données liées à StorageGRID vers StorageGRID. Le Tiering des données StorageGRID vers StorageGRID augmente la complexité opérationnelle et la résolution des problèmes.

Supprimez les données FabricPool de StorageGRID

Si vous devez supprimer les données FabricPool qui sont actuellement stockées dans StorageGRID, vous devez utiliser ONTAP pour récupérer toutes les données du volume FabricPool et les promouvoir dans le Tier de performance.

Avant de commencer

- Vous avez examiné les instructions et les considérations de la section "Promouvoir les données vers le Tier de performance".
- Vous utilisez ONTAP 9.8 ou une version ultérieure.
- Vous utilisez un "navigateur web pris en charge".
- Vous appartenez à un groupe d'utilisateurs StorageGRID pour le compte de tenant FabricPool qui possède "Gérez tous les compartiments ou l'autorisation d'accès racine".

Description de la tâche

Ces instructions expliquent comment transférer des données de StorageGRID vers FabricPool. Cette procédure s'effectue à l'aide de ONTAP et du Gestionnaire de locataires StorageGRID.

Étapes

1. Dans ONTAP, exécutez le `volume modify` commande.

   Réglez `tiering-policy` à `none` pour arrêter et définir un nouveau tiering `cloud-retrieval-policy` à `promote` Pour renvoyer toutes les données qui étaient auparavant hiérarchisées vers StorageGRID.

   Voir "Promotion de toutes les données d'un volume FabricPool vers le Tier de performance".

2. Attendez la fin de l'opération.

   Vous pouvez utiliser le `volume object-store` commande avec `tiering` option à "vérifier le statut de la promotion du niveau de performances".

3. Une fois l'opération de promotion terminée, connectez-vous au gestionnaire de locataires StorageGRID pour le compte de locataire FabricPool.
4. Sélectionnez **Afficher les compartiments** dans le tableau de bord ou sélectionnez **STOCKAGE (S3)** > **compartiments**.
5. Vérifiez que le compartiment FabricPool est vide.
6. Si le godet est vide, "supprimez le compartiment".

Une fois que vous avez terminé

Lorsque vous supprimez le compartiment, le Tiering de FabricPool vers StorageGRID ne peut plus se poursuivre. Cependant, le niveau local étant toujours attaché au niveau cloud StorageGRID, ONTAP System Manager renvoie des messages d'erreur indiquant que le compartiment est inaccessible.

Pour éviter ces messages d'erreur, effectuez l'une des opérations suivantes :

- Utilisez FabricPool Mirror pour associer un Tier cloud différent à l'agrégat.
- Déplacez les données de l'agrégat FabricPool vers un agrégat non FabricPool, puis supprimez l'agrégat non utilisé.

Voir la "Documentation ONTAP pour FabricPool" pour obtenir des instructions.

Utiliser StorageGRID

Utilisez un compte de locataire

Utilisez un compte de locataire : présentation

Un compte de locataire vous permet d'utiliser l'API REST S3 (simple Storage Service) ou l'API REST Swift pour stocker et récupérer des objets dans un système StorageGRID.

Qu'est-ce qu'un compte de locataire ?

Chaque compte de locataire possède ses propres groupes, utilisateurs, compartiments S3, conteneurs Swift et objets fédérés.

Les comptes de tenant peuvent être utilisés pour isoler les objets stockés par des entités différentes. Par exemple, vous pouvez utiliser plusieurs comptes locataires pour l'une de ces utilisations :

- **Utilisation en entreprise :** si le système StorageGRID est utilisé au sein d'une entreprise, le stockage objet de la grille peut être séparé par les différents services de l'organisation. Par exemple, il peut y avoir des comptes de tenant pour le service Marketing, le service Customer support, le service des ressources humaines, etc.

> Si vous utilisez le protocole client S3, vous pouvez également utiliser des compartiments S3 et des règles de compartiment pour isoler les objets entre les différents départements d'une entreprise. Vous n'avez pas besoin de créer des comptes de locataire distincts. Voir les instructions de mise en œuvre "Compartiments S3 et règles de compartiments" pour en savoir plus.

- **Cas d'utilisation du fournisseur de services :** si le système StorageGRID est utilisé par un fournisseur de services, le stockage objet de la grille peut être séparé par les différentes entités qui louent le stockage. Il peut s'agir, par exemple, de comptes de locataires pour la société A, la société B, la société C, etc.

Comment créer un compte de locataire

Les comptes de locataire sont créés par un "Administrateur du grid StorageGRID utilisant le gestionnaire de grille". Lors de la création d'un compte de locataire, l'administrateur de la grille spécifie ce qui suit :

- Informations de base comprenant le nom du locataire, le type de client (S3 ou Swift) et le quota de stockage facultatif.
- Autorisations pour le compte de locataire, par exemple si le compte de locataire peut utiliser les services de la plateforme S3, configurer son propre référentiel d'identité, utiliser S3 Select ou utiliser une connexion de fédération grid.
- Accès racine initial pour le locataire, selon que le système StorageGRID utilise des groupes et utilisateurs locaux, la fédération des identités ou l'authentification unique (SSO).

En outre, les administrateurs du grid peuvent activer le paramètre de verrouillage objet S3 pour le système StorageGRID si les comptes de locataires S3 doivent être conformes aux exigences réglementaires. Lorsque le verrouillage des objets S3 est activé, tous les comptes de locataires S3 peuvent créer et gérer des compartiments conformes.

Configurez les locataires S3

Après un "Le compte de locataire S3 est créé", Vous pouvez accéder au Gestionnaire de tenant pour effectuer des tâches telles que :

- Configurer la fédération des identités (sauf si le référentiel d'identité est partagé avec la grille)
- Gestion des groupes et des utilisateurs
- Utilisez la fédération grid pour le clone de compte et la réplication inter-grid
- Gestion des clés d'accès S3
- Création et gestion de compartiments S3
- Utilisez les services de plateforme S3
- Utiliser S3 Select
- Contrôle de l'utilisation du stockage

> Même si vous pouvez créer et gérer des compartiments S3 avec le gestionnaire des locataires, vous devez utiliser un client S3 pour ingérer et gérer les objets. Voir "UTILISEZ L'API REST S3" pour plus d'informations.

Configurez les locataires Swift

Après un "Le compte de locataire Swift est créé", Vous pouvez accéder au Gestionnaire de tenant pour effectuer des tâches telles que :

- Configurer la fédération des identités (sauf si le référentiel d'identité est partagé avec la grille)
- Gestion des groupes et des utilisateurs
- Contrôle de l'utilisation du stockage

> Les utilisateurs Swift doivent disposer de l'autorisation d'accès racine pour accéder au Gestionnaire de locataires. Cependant, l'autorisation d'accès racine ne permet pas aux utilisateurs de s'authentifier dans "API REST Swift" pour créer des conteneurs et ingérer des objets. Les utilisateurs doivent disposer de l'autorisation Administrateur Swift pour s'authentifier dans l'API REST de Swift.

Comment se connecter et se déconnecter

Connectez-vous au Gestionnaire de locataires

Pour accéder au Gestionnaire de locataires, entrez l'URL du locataire dans la barre d'adresse d'un "navigateur web pris en charge".

Avant de commencer

- Vous disposez de vos identifiants de connexion.
- Vous disposez d'une URL permettant d'accéder au gestionnaire de locataires, fournie par votre administrateur de grille. L'URL se présente comme l'un de ces exemples :

```
https://FQDN_or_Admin_Node_IP/

https://FQDN_or_Admin_Node_IP:port/
```

```
https://FQDN_or_Admin_Node_IP/?accountId=20-digit-account-id

https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id
```

L'URL inclut toujours un nom de domaine complet (FQDN), l'adresse IP d'un nœud d'administration ou l'adresse IP virtuelle d'un groupe haute disponibilité de nœuds d'administration. Il peut également inclure un numéro de port, l'ID de compte de locataire à 20 chiffres, ou les deux.

- Si l'URL n'inclut pas l'ID de compte à 20 chiffres du locataire, vous disposez de cet ID de compte.
- Vous utilisez un "navigateur web pris en charge".
- Les cookies sont activés dans votre navigateur Web.
- Vous appartenez à un groupe d'utilisateurs qui possède "autorisations d'accès spécifiques".

Étapes

1. Lancez un "navigateur web pris en charge".
2. Dans la barre d'adresse du navigateur, entrez l'URL d'accès au Gestionnaire de locataires.
3. Si vous êtes invité à recevoir une alerte de sécurité, installez le certificat à l'aide de l'assistant d'installation du navigateur.
4. Connectez-vous au Gestionnaire de locataires.

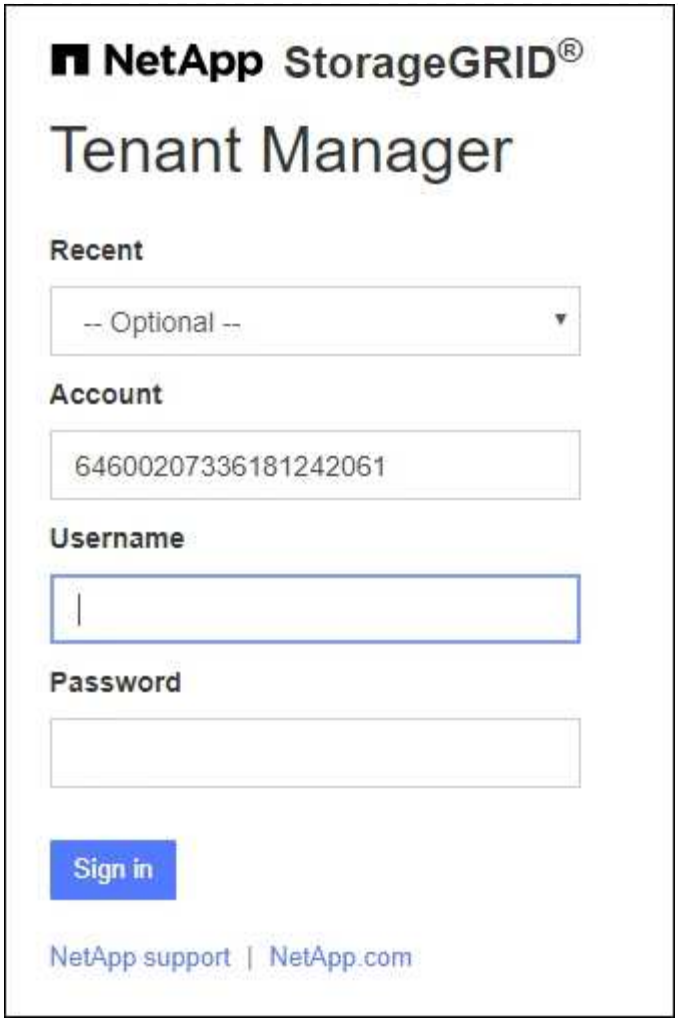
   L'écran d'ouverture de session qui s'affiche dépend de l'URL que vous avez saisie et de la configuration de l'authentification unique (SSO) pour StorageGRID.

Pas d'utilisation de SSO

Si StorageGRID n'utilise pas SSO, l'un des écrans suivants s'affiche :

- Page de connexion de Grid Manager. Sélectionnez le lien **tenant sign-in**.

- Page de connexion du Gestionnaire de locataires. Le champ **compte** est peut-être déjà renseigné, comme indiqué ci-dessous.



i. Si l'ID de compte à 20 chiffres du locataire ne s'affiche pas, sélectionnez le nom du compte du locataire s'il apparaît dans la liste des comptes récents ou saisissez l'ID du compte.

ii. Saisissez votre nom d'utilisateur et votre mot de passe.

iii. Sélectionnez **connexion**.

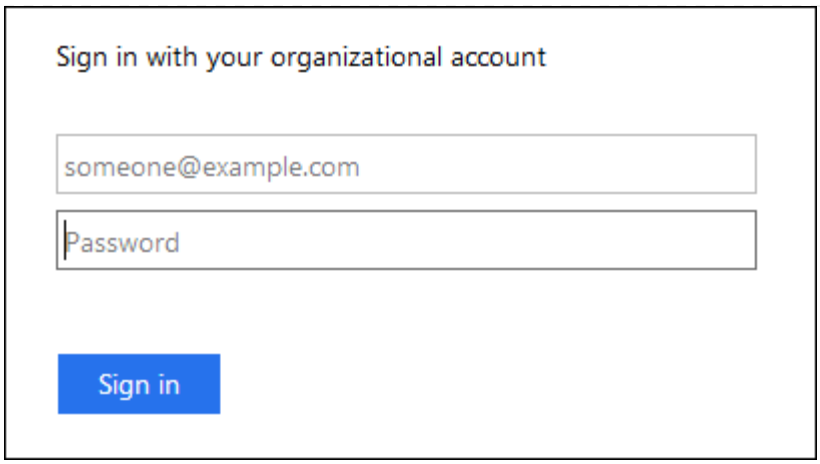
Le tableau de bord du gestionnaire de locataires s'affiche.

iv. Si vous avez reçu un mot de passe initial de la part d'une autre personne, sélectionnez ***username*** > **change password** pour sécuriser votre compte.

Utilisation de SSO

Si StorageGRID utilise SSO, l'un des écrans suivants s'affiche :

◦ La page SSO de votre organisation. Par exemple :



Entrez vos informations d'identification SSO standard et sélectionnez **se connecter**.

- Page de connexion SSO du Gestionnaire de locataires.

i. Si l'ID de compte à 20 chiffres du locataire ne s'affiche pas, sélectionnez le nom du compte du locataire s'il apparaît dans la liste des comptes récents ou saisissez l'ID du compte.

ii. Sélectionnez **connexion**.

iii. Connectez-vous à l'aide de vos identifiants SSO standard sur la page de connexion SSO de votre entreprise.

Le tableau de bord du gestionnaire de locataires s'affiche.

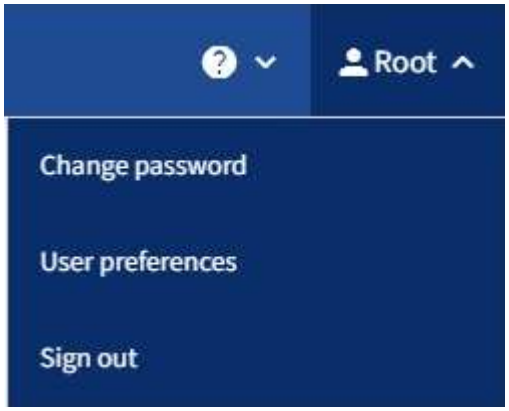
Déconnectez-vous du Gestionnaire de locataires

Lorsque vous avez terminé de travailler avec le Gestionnaire de locataires, vous devez

vous déconnecter pour vous assurer que les utilisateurs non autorisés ne peuvent pas accéder au système StorageGRID. La fermeture de votre navigateur risque de ne pas vous déconnecter du système, en fonction des paramètres des cookies du navigateur.

Étapes

1. Localisez la liste déroulante Nom d'utilisateur dans le coin supérieur droit de l'interface utilisateur.



2. Sélectionnez le nom d'utilisateur, puis sélectionnez **Déconnexion**.

   - Si SSO n'est pas utilisé :

     Vous êtes déconnecté du nœud d'administration. La page de connexion au Gestionnaire de locataires s'affiche.

     Si vous vous êtes connecté à plusieurs nœuds d'administration, vous devez vous déconnecter de chaque nœud.

   - Si SSO est activé :

     Vous êtes déconnecté de tous les nœuds d'administration auxquels vous accédiez. La page de connexion StorageGRID s'affiche. Le nom du compte de locataire que vous venez d'accéder est indiqué par défaut dans la liste déroulante **comptes récents** et le **ID de compte** du locataire s'affiche.

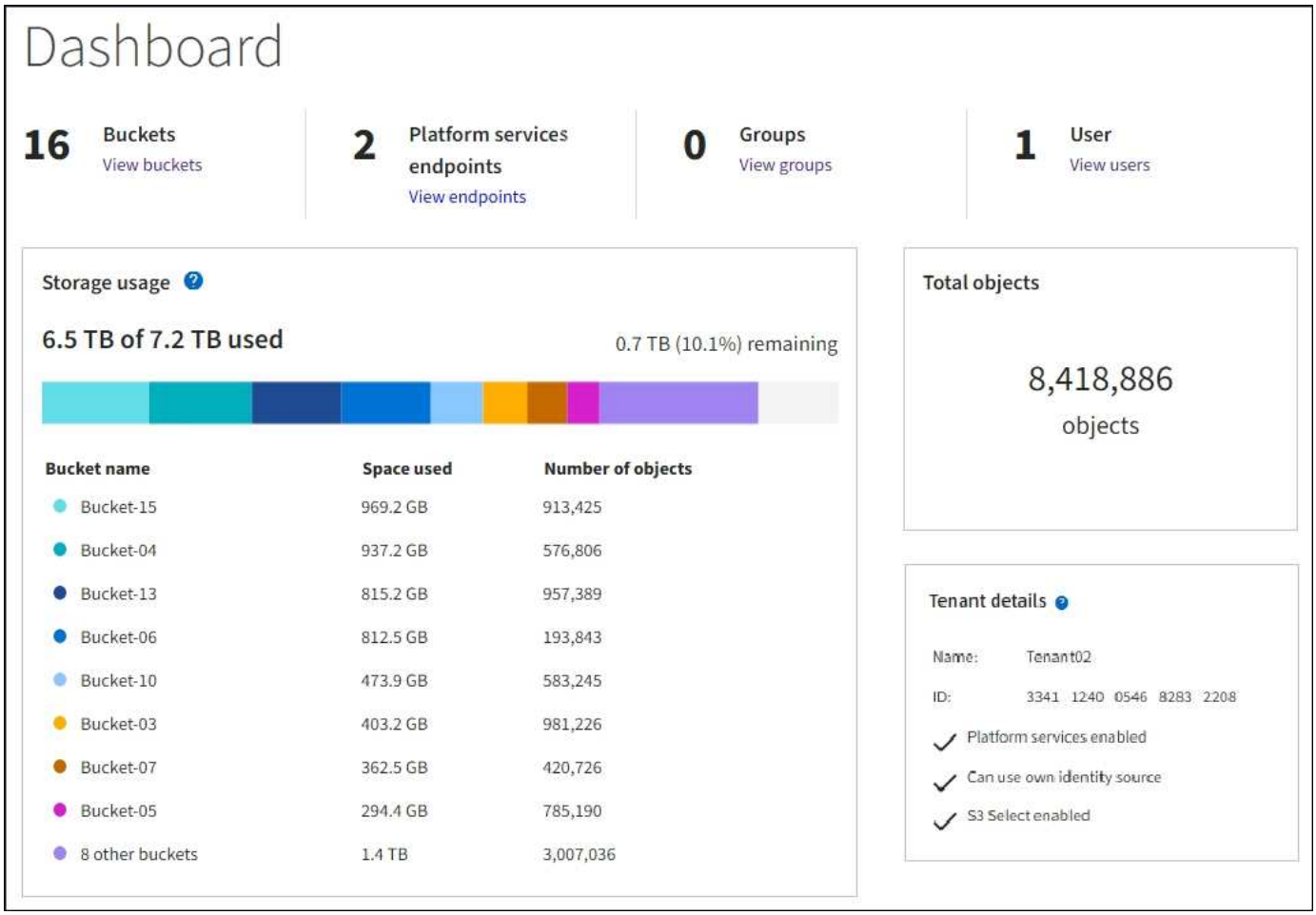
     Si SSO est activé et que vous êtes également connecté à Grid Manager, vous devez également vous déconnecter de Grid Manager pour vous déconnecter de SSO.

Présentation du tableau de bord du gestionnaire de locataires

Le tableau de bord du gestionnaire de locataires présente la configuration d'un compte de locataire et la quantité d'espace utilisée par les objets dans les compartiments du locataire (S3) ou les conteneurs (Swift). Si le locataire dispose d'un quota, le tableau de bord indique la part du quota utilisée et la quantité restante. En cas d'erreurs liées au compte de tenant, les erreurs s'affichent dans le tableau de bord.

Les valeurs espace utilisé sont des estimations. Ces estimations sont affectées par le moment de l'ingestion, la connectivité réseau et l'état des nœuds.

Une fois les objets téléchargés, le tableau de bord ressemble à l'exemple suivant :



Récapitulatif du compte de locataire

La partie supérieure du tableau de bord contient les informations suivantes :

- Le nombre de compartiments ou de conteneurs configurés, de groupes et d'utilisateurs
- Le nombre de terminaux de services de plate-forme, le cas échéant, ont été configurés

Vous pouvez sélectionner les liens pour afficher les détails.

Le côté droit du tableau de bord contient les informations suivantes :

- Nombre total d'objets pour le locataire.

  Pour un compte S3, si aucun objet n'a été ingéré et que vous disposez de l'autorisation d'accès racine, les directives de démarrage s'affichent à la place du nombre total d'objets.

- Détails du locataire, y compris le nom et l'ID du compte de locataire, et si le locataire peut l'utiliser "services de plateforme", "son propre référentiel d'identité", "fédération des grilles", ou "S3 Select" (seules les autorisations activées sont répertoriées).

Utilisation du stockage et des quotas

Le panneau utilisation du stockage contient les informations suivantes :

- Volume des données d'objet pour le locataire.

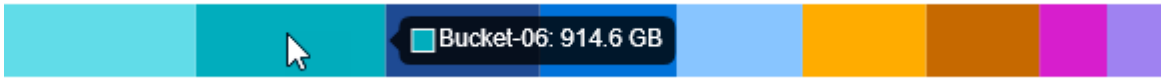
Cette valeur indique la quantité totale de données d'objet chargées et ne représente pas l'espace utilisé pour stocker les copies de ces objets et leurs métadonnées.

- Si un quota est défini, la quantité totale d'espace disponible pour les données d'objet ainsi que la quantité et le pourcentage d'espace restant. Le quota limite la quantité de données d'objet pouvant être ingérées.

L'utilisation des quotas est basée sur des estimations internes et peut être dépassée dans certains cas. Par exemple, StorageGRID vérifie le quota lorsqu'un locataire commence à charger des objets et rejette les nouvelles ingère si le locataire a dépassé le quota. Cependant, StorageGRID ne prend pas en compte la taille du téléchargement actuel lors de la détermination du dépassement du quota. Si des objets sont supprimés, un locataire peut temporairement empêcher le téléchargement de nouveaux objets jusqu'au recalcul de l'utilisation du quota. Le calcul de l'utilisation des quotas peut prendre 10 minutes ou plus.

- Un graphique à barres qui représente les tailles relatives des grands godets ou conteneurs.

  Vous pouvez placer le curseur sur n'importe quel segment de graphique pour afficher l'espace total utilisé par ce compartiment ou ce conteneur.



- Pour correspondre au graphique à barres, une liste des plus grands seaux ou conteneurs, y compris la quantité totale de données d'objet et le nombre d'objets pour chaque godet ou conteneur.

Bucket name	Space used	Number of objects
Bucket-02	944.7 GB	7,575
Bucket-09	899.6 GB	589,677
Bucket-15	889.6 GB	623,542
Bucket-06	846.4 GB	648,619
Bucket-07	730.8 GB	808,655
Bucket-04	700.8 GB	420,493
Bucket-11	663.5 GB	993,729
Bucket-03	656.9 GB	379,329
9 other buckets	2.3 TB	5,171,588

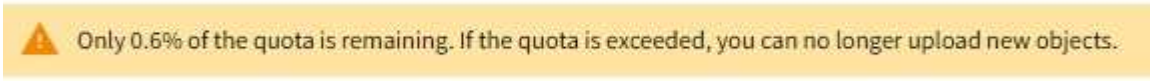
  Si le locataire possède plus de neuf compartiments ou conteneurs, tous les autres compartiments ou conteneurs sont regroupés en une seule entrée au bas de la liste.

Pour modifier les unités des valeurs de stockage affichées dans le Gestionnaire de locataires, sélectionnez la liste déroulante utilisateur dans le coin supérieur droit du Gestionnaire de locataires, puis sélectionnez **Préférences utilisateur**.

Alertes d'utilisation des quotas

Si les alertes d'utilisation des quotas ont été activées dans Grid Manager, elles s'affichent dans le Gestionnaire de locataires lorsque le quota est faible ou dépassé, comme suit :

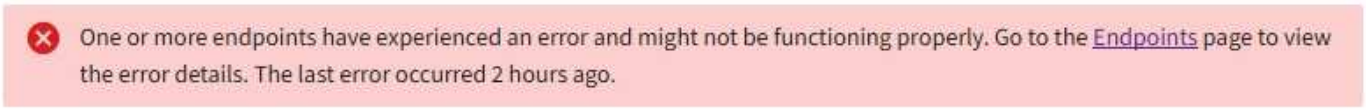
Si 90 % ou plus du quota d'un locataire a été utilisé, l'alerte **usage du quota de locataire élevé** est déclenchée. Effectuez les actions recommandées pour l'alerte.



Si vous dépassez votre quota, vous ne pouvez pas télécharger de nouveaux objets.

Erreurs de point final

Si vous avez utilisé le gestionnaire de grille pour configurer un ou plusieurs points de terminaison pour les services de plateforme, le tableau de bord du gestionnaire de locataires affiche une alerte si des erreurs de point de terminaison se sont produites au cours des sept derniers jours.



Pour afficher des détails sur "erreurs de noeud final des services de plate-forme", Sélectionnez **noeuds finaux** pour afficher la page noeuds finaux.

API de gestion des locataires

Compréhension de l'API de gestion des locataires

Vous pouvez effectuer des tâches de gestion du système via l'API REST de gestion des locataires plutôt que dans l'interface utilisateur du gestionnaire de locataires. Par exemple, vous pouvez utiliser l'API pour automatiser les opérations ou créer plusieurs entités plus rapidement (par exemple, les utilisateurs).

L'API de gestion des locataires :

- Utilise la plate-forme API open source swagger. Swagger fournit une interface utilisateur intuitive qui permet aux développeurs et aux non-développeurs d'interagir avec l'API. L'interface utilisateur swagger fournit des détails complets et de la documentation pour chaque opération API.
- Utilisations "gestion des versions pour prendre en charge les mises à niveau sans interruption".

Pour accéder à la documentation de swagger pour l'API de gestion des locataires :

1. Connectez-vous au Gestionnaire de locataires.
2. Dans le haut du Gestionnaire de locataires, sélectionnez l'icône d'aide et sélectionnez **documentation API**.

Opérations d'API

L'API de gestion des locataires organise les opérations API disponibles dans les sections suivantes :

- **Compte** : opérations sur le compte locataire actuel, y compris l'obtention d'informations sur l'utilisation du stockage.
- **Auth** : opérations pour effectuer l'authentification de session utilisateur.

  L'API de gestion des locataires prend en charge le schéma d'authentification par jeton Bearer. Pour une connexion locataire, vous fournissez un nom d'utilisateur, un mot de passe et un ID de compte dans le corps JSON de la demande d'authentification (c'est-à-dire, `POST /api/v3/authorize`). Si l'utilisateur est authentifié, un jeton de sécurité est renvoyé. Ce token doit être fourni dans l'en-tête des requêtes API suivantes (« autorisation : jeton porteur »).

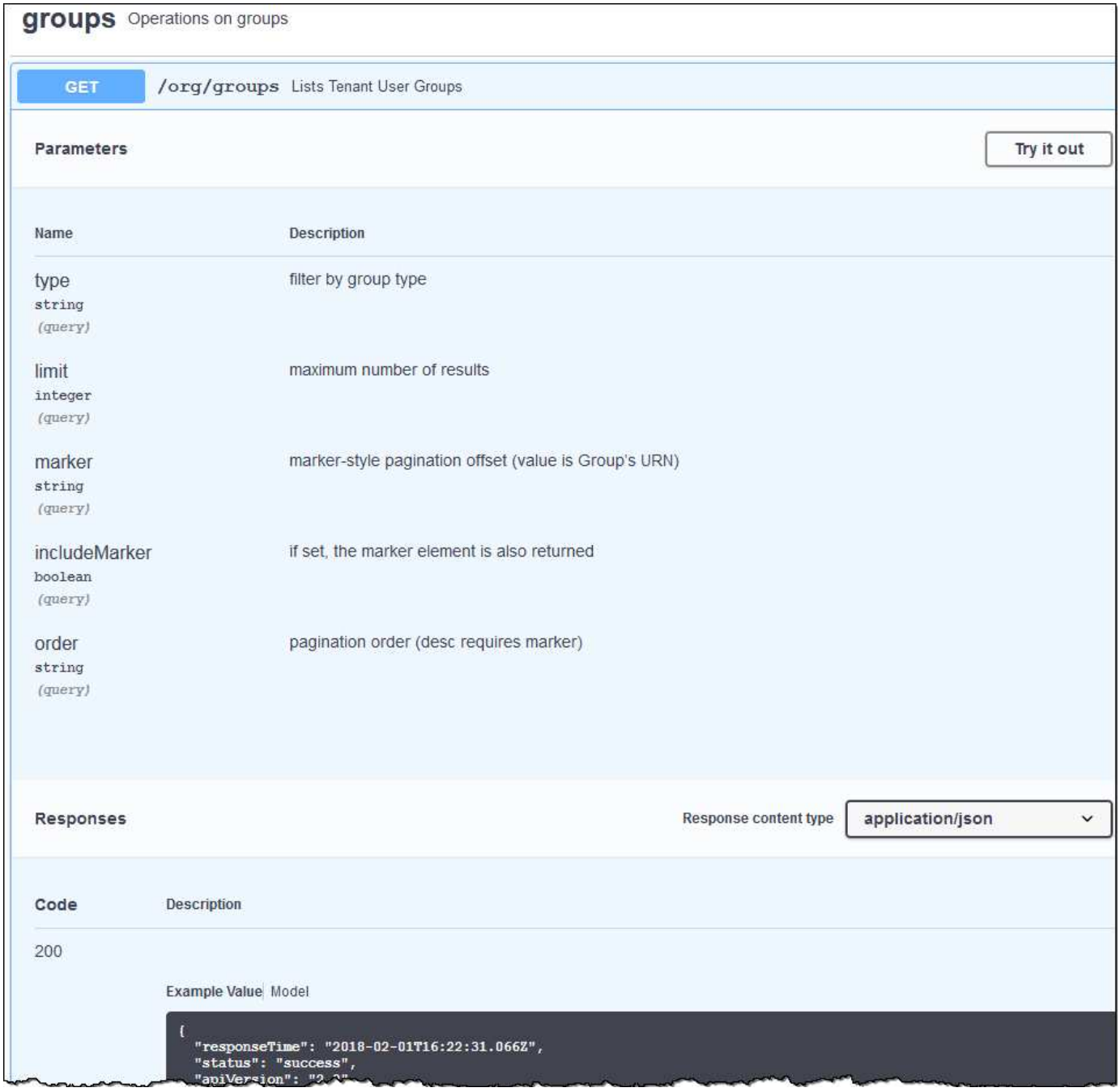
  Pour plus d'informations sur l'amélioration de la sécurité d'authentification, reportez-vous à la section "Protéger contre la contrefaçon de demandes intersites".

  > Si l'authentification unique (SSO) est activée pour le système StorageGRID, vous devez effectuer différentes étapes pour l'authentification. Voir la "Instructions d'utilisation de l'API de gestion de grille".

- **Config** : opérations liées à la version du produit et aux versions de l'API de gestion des locataires. Vous pouvez lister la version du produit ainsi que les versions principales de l'API prises en charge par cette version.
- **Conteneurs** : opérations sur les compartiments S3 ou les conteneurs Swift.
- **Désactivé-features** : opérations permettant d'afficher les fonctions qui auraient pu être désactivées.
- **Noeuds finaux** : opérations pour gérer un noeud final. Les terminaux permettent à un compartiment S3 d'utiliser un service externe pour la réplication StorageGRID CloudMirror, les notifications ou l'intégration de la recherche.
- **Grid-federation-connections** : opérations sur les connexions de fédération de grille et la réplication de grille transversale.
- **Groupes** : opérations de gestion des groupes de locataires locaux et de récupération des groupes de locataires fédérés à partir d'un référentiel d'identité externe.
- **Identity-source** : opérations permettant de configurer un référentiel d'identité externe et de synchroniser manuellement les informations relatives au groupe fédéré et à l'utilisateur.
- **Régions** : opérations permettant de déterminer quelles régions ont été configurées pour le système StorageGRID.
- **s3** : opérations de gestion des clés d'accès S3 pour les utilisateurs locataires.
- **s3-object-lock** : opérations sur les paramètres globaux de verrouillage d'objet S3, utilisées pour prendre en charge la conformité réglementaire.
- **Utilisateurs** : opérations pour afficher et gérer les utilisateurs locataires.

Détails de l'opération

Lorsque vous développez chaque opération d'API, vous pouvez voir son action HTTP, son URL de point final, une liste de tous les paramètres obligatoires ou facultatifs, un exemple du corps de la demande (si nécessaire) et les réponses possibles.



Émettre des requêtes API

> Toutes les opérations d'API que vous effectuez à l'aide de la page Web API Docs sont des opérations en direct. Veillez à ne pas créer, mettre à jour ou supprimer des données de configuration ou d'autres données par erreur.

Étapes

1. Sélectionnez l'action HTTP pour afficher les détails de la demande.

2. Déterminez si la demande nécessite des paramètres supplémentaires, tels qu'un ID de groupe ou d'utilisateur. Ensuite, obtenir ces valeurs. Vous devrez peut-être d'abord lancer une autre demande d'API pour obtenir les informations dont vous avez besoin.
3. Déterminez si vous devez modifier l'exemple de corps de la demande. Si c'est le cas, vous pouvez sélectionner **modèle** pour connaître les exigences de chaque champ.
4. Sélectionnez **essayez-le**.
5. Fournir tous les paramètres requis ou modifier le corps de la demande selon les besoins.
6. Sélectionnez **Exécuter**.
7. Vérifiez le code de réponse pour déterminer si la demande a réussi.

Gestion des versions de l'API de gestion des locataires

L'API de gestion des locataires utilise la gestion des versions pour prendre en charge les mises à niveau sans interruption.

Par exemple, cette URL de demande spécifie la version 3 de l'API.

`https://hostname_or_ip_address/api/v3/authorize`

La version principale de l'API de gestion des locataires est incrémentée lorsque des modifications sont effectuées et que *non compatibles* sont apportées aux versions antérieures. La version mineure de l'API de gestion des locataires est incrémentée lorsque des modifications qui sont *compatibles* avec les versions antérieures sont effectuées. Les modifications compatibles incluent l'ajout de nouveaux noeuds finaux ou de nouvelles propriétés. L'exemple suivant illustre comment la version de l'API est incrémentée en fonction du type de modifications apportées.

Type de modification de l'API	Ancienne version	Nouvelle version
Compatible avec les versions plus anciennes	2.1	2.2
Non compatible avec les versions plus anciennes	2.1	3.0

Lors de la première installation du logiciel StorageGRID, seule la version la plus récente de l'API de gestion des locataires est activée. Cependant, lorsque StorageGRID est mis à niveau vers une nouvelle version de fonction, vous continuez à accéder à l'ancienne version de l'API pour au moins une version de StorageGRID.

Les requêtes obsolètes sont marquées comme obsolètes de l'une des manières suivantes :

- L'en-tête de réponse est « obsolète : vrai »
- Le corps de la réponse JSON inclut « obsolète » : vrai

Identification des versions d'API prises en charge dans la version actuelle

Utilisez la requête d'API suivante pour renvoyer une liste des versions principales de l'API prises en charge :

```
GET https://{{IP-Address}}/api/versions
{
  "responseTime": "2019-01-10T20:41:00.845Z",
  "status": "success",
  "apiVersion": "3.0",
  "data": [
    2,
    3
  ]
}
```

Spécifiez la version de l'API pour la demande

Vous pouvez spécifier la version de l'API à l'aide d'un paramètre de chemin d'accès (`/api/v3`) ou un en-tête (`Api-Version: 3`). Si vous indiquez les deux valeurs, la valeur de l'en-tête remplace la valeur du chemin d'accès.

```
curl https://<IP-Address>/api/v3/grid/accounts

curl -H "Api-Version: 3" https://<IP-Address>/api/grid/accounts
```

Protection contre la contrefaçon de demandes intersites (CSRF)

Vous pouvez vous protéger contre les attaques de contrefaçon de requêtes intersites (CSRF) contre StorageGRID en utilisant des jetons CSRF pour améliorer l'authentification qui utilise des cookies. Grid Manager et tenant Manager activent automatiquement cette fonction de sécurité ; les autres clients API peuvent choisir de l'activer lorsqu'ils se connectent.

Un attaquant pouvant déclencher une requête vers un autre site (par exemple avec UN POST de formulaire HTTP) peut créer certaines requêtes à l'aide des cookies de l'utilisateur connecté.

StorageGRID contribue à la protection contre les attaques CSRF en utilisant des jetons CSRF. Lorsque cette option est activée, le contenu d'un cookie spécifique doit correspondre au contenu d'un en-tête spécifique ou d'un paramètre DE CORPS POST spécifique.

Pour activer la fonction, définissez l' `csrfToken` paramètre à `true` pendant l'authentification. La valeur par défaut est `false`.

```
curl -X POST --header "Content-Type: application/json" --header "Accept:
application/json" -d "{
  \"username\": \"MyUserName\",
  \"password\": \"MyPassword\",
  \"cookie\": true,
  \"csrfToken\": true
}" "https://example.com/api/v3/authorize"
```

Si vrai, un `GridCsrfToken` Le cookie est défini avec une valeur aléatoire pour les connexions dans Grid Manager et dans `AccountCsrfToken` Le cookie est défini avec une valeur aléatoire pour les connexions au Gestionnaire de locataires.

Si le cookie est présent, toutes les demandes pouvant modifier l'état du système (POST, PUT, PATCH, DELETE) doivent inclure l'une des options suivantes :

- Le `X-Csrf-Token` En-tête, avec la valeur de l'en-tête définie sur la valeur du cookie de jeton CSRF.
- Pour les noeuds finaux qui acceptent un corps codé par formulaire : a `csrfToken` paramètre corps de demande codé par formulaire.

Pour configurer la protection CSRF, utilisez le "API de gestion du grid" ou "API de gestion des locataires".

> Les demandes disposant d'un jeu de cookies de jeton CSRF appliquent également le `"Content-Type: application/json"` En-tête pour toute demande qui attend un corps de requête JSON comme une protection supplémentaire contre les attaques CSRF.

Utiliser les connexions de fédération de grille

Cloner des groupes de locataires et des utilisateurs

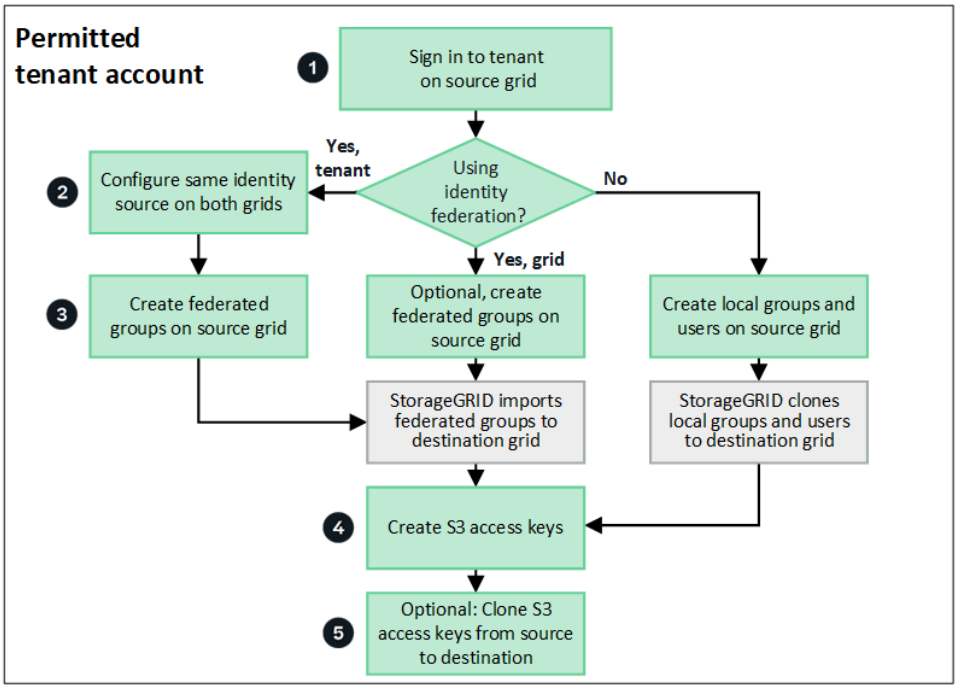
Si un nouveau locataire est autorisé à utiliser une connexion de fédération de grille, ce dernier est répliqué d'un système StorageGRID vers un autre système StorageGRID lors de sa création. Une fois le locataire répliqué, tous les groupes et utilisateurs ajoutés au locataire source sont clonés dans le locataire de destination.

Le système StorageGRID dans lequel le tenant est créé à l'origine est *source GRID* du tenant. Le système StorageGRID dans lequel le locataire est répliqué est la *grille de destination* du locataire. Les deux comptes de tenant possèdent les mêmes ID de compte, nom, description, quota de stockage et autorisations attribuées, mais le locataire de destination ne dispose pas initialement d'un mot de passe utilisateur root. Pour plus de détails, voir "Qu'est-ce que le clone de compte" et "Gérer les locataires autorisés".

Le clonage des informations de compte de locataire est requis pour "réplication entre plusieurs grilles" d'objets de compartiment. Le fait de disposer des mêmes groupes de locataires et utilisateurs sur les deux grilles vous permet d'accéder aux compartiments et objets correspondants sur l'une ou l'autre grille.

Workflow des locataires pour le clone de compte

Si votre compte de locataire dispose de l'autorisation **utiliser la connexion de fédération de grille**, consultez le diagramme de flux de travail pour voir les étapes à suivre pour cloner des groupes, des utilisateurs et des clés d'accès S3.



Voici les principales étapes du flux de travail :

1 Connectez-vous au locataire

Connectez-vous au compte de locataire sur la grille source (la grille dans laquelle le locataire a été initialement créé).

2 Vous pouvez également configurer la fédération des identités

Si votre compte de tenant dispose de l'autorisation **utiliser son propre référentiel d'identité** pour utiliser des groupes et des utilisateurs fédérés, configurez le même référentiel d'identité (avec les mêmes paramètres) pour les comptes de tenant source et de destination. Les groupes et utilisateurs fédérés ne peuvent pas être clonés à moins que les deux grilles n'utilisent le même référentiel d'identité. Pour obtenir des instructions, reportez-vous à la section "Utiliser la fédération des identités".

3 Créer des groupes et des utilisateurs

Lorsque vous créez des groupes et des utilisateurs, commencez toujours par la grille source du locataire. Lorsque vous ajoutez un nouveau groupe, StorageGRID le clone automatiquement dans la grille de destination.

- Si la fédération des identités est configurée pour l'ensemble du système StorageGRID ou pour votre compte de locataire, "créer de nouveaux groupes de locataires" en important des groupes fédérés à partir du référentiel d'identité.
- Si vous n'utilisez pas la fédération des identités, "créer de nouveaux groupes locaux" puis "créer des utilisateurs locaux".

4 Création de clés d'accès S3

C'est possible "créez vos propres clés d'accès" ou à "créez les clés d'accès d'un autre utilisateur" sur la grille source ou de destination pour accéder aux compartiments de cette grille.

5 **Vous pouvez également cloner les clés d'accès S3**

Si vous avez besoin d'accéder à des compartiments avec les mêmes clés d'accès sur les deux grilles, créez les clés d'accès sur la grille source, puis utilisez l'API du gestionnaire de locataires pour les cloner manuellement dans la grille de destination. Pour obtenir des instructions, reportez-vous à la section "Cloner les clés d'accès S3 à l'aide de l'API".

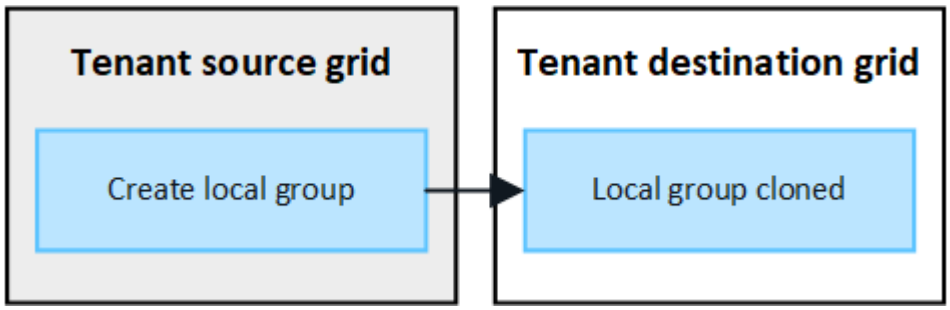
Comment les groupes, les utilisateurs et les clés d'accès S3 sont-ils clonés ?

Dans cette section, vous apprendrez comment les groupes, les utilisateurs et les clés d'accès S3 sont clonés entre la grille source des locataires et la grille de destination des locataires.

Les groupes locaux créés dans la grille source sont clonés

Une fois qu'un compte de locataire est créé et répliqué sur la grille de destination, StorageGRID clone automatiquement tous les groupes locaux que vous ajoutez à la grille source du locataire dans la grille de destination du locataire.

Le groupe d'origine et le clone disposent des mêmes mode d'accès, autorisations de groupe et règles de groupe S3. Pour obtenir des instructions, reportez-vous à la section "Créez des groupes pour les locataires S3".

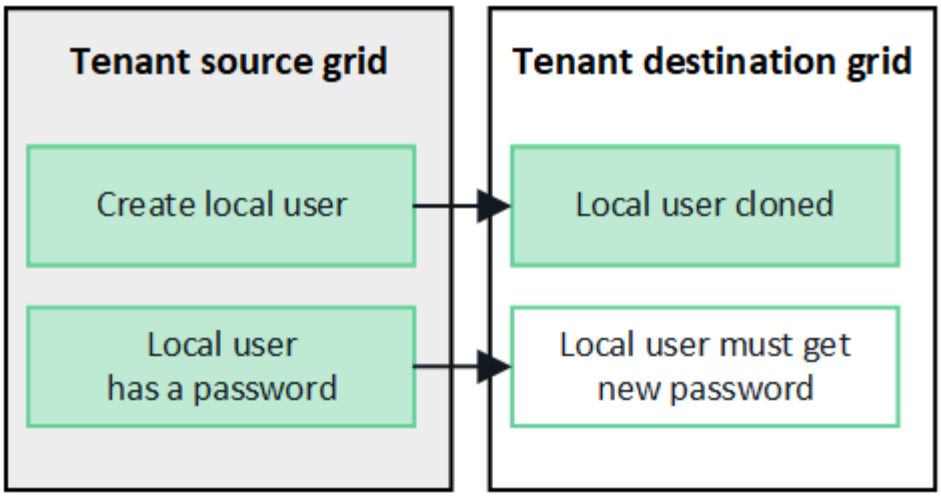


Tous les utilisateurs sélectionnés lors de la création d'un groupe local sur la grille source ne sont pas inclus lorsque le groupe est cloné dans la grille de destination. Pour cette raison, ne sélectionnez pas d'utilisateurs lorsque vous créez le groupe. Sélectionnez plutôt le groupe lorsque vous créez les utilisateurs.

Les utilisateurs locaux créés dans la grille source sont clonés

Lorsque vous créez un utilisateur local sur la grille source, StorageGRID le clone automatiquement dans la grille de destination. L'utilisateur d'origine et son clone ont tous les deux le même nom complet, le même nom d'utilisateur et le même paramètre **deny Access**. Les deux utilisateurs appartiennent également aux mêmes groupes. Pour obtenir des instructions, reportez-vous à la section "Gérez les utilisateurs locaux".

Pour des raisons de sécurité, les mots de passe des utilisateurs locaux ne sont pas clonés dans la grille de destination. Si un utilisateur local doit accéder au gestionnaire de locataires sur la grille de destination, l'utilisateur root du compte de locataire doit ajouter un mot de passe pour cet utilisateur sur la grille de destination. Pour obtenir des instructions, reportez-vous à la section "Gérez les utilisateurs locaux".

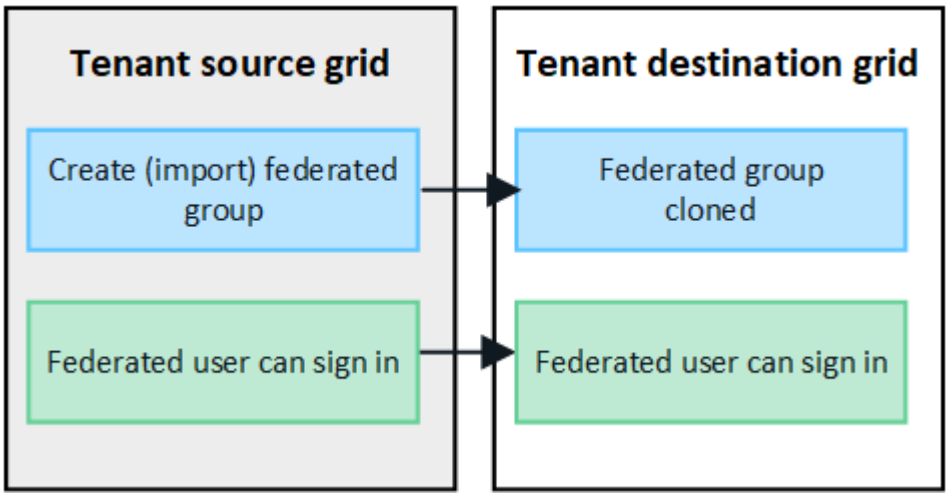


Les groupes fédérés créés dans la grille source sont clonés

Suppose les conditions requises pour l'utilisation du clone du compte avec "authentification unique" et "fédération des identités" ont été réunis, les groupes fédérés que vous créez (importez) pour le locataire sur la grille source sont automatiquement clonés dans le locataire sur la grille de destination.

Les deux groupes disposent des mêmes mode d'accès, autorisations de groupe et règles de groupe S3.

Une fois les groupes fédérés créés pour le locataire source et clonés dans le locataire de destination, les utilisateurs fédérés peuvent se connecter au locataire dans l'une ou l'autre des grilles.

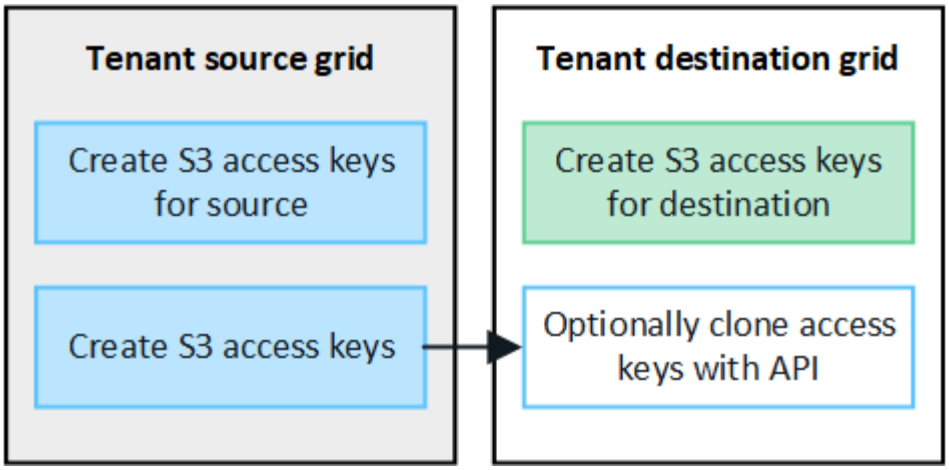


Les clés d'accès S3 peuvent être clonées manuellement

StorageGRID ne clone pas automatiquement les clés d'accès S3, car la sécurité est améliorée grâce à l'utilisation de clés différentes sur chaque grid.

Pour gérer les clés d'accès sur les deux grilles, vous pouvez effectuer l'une des opérations suivantes :

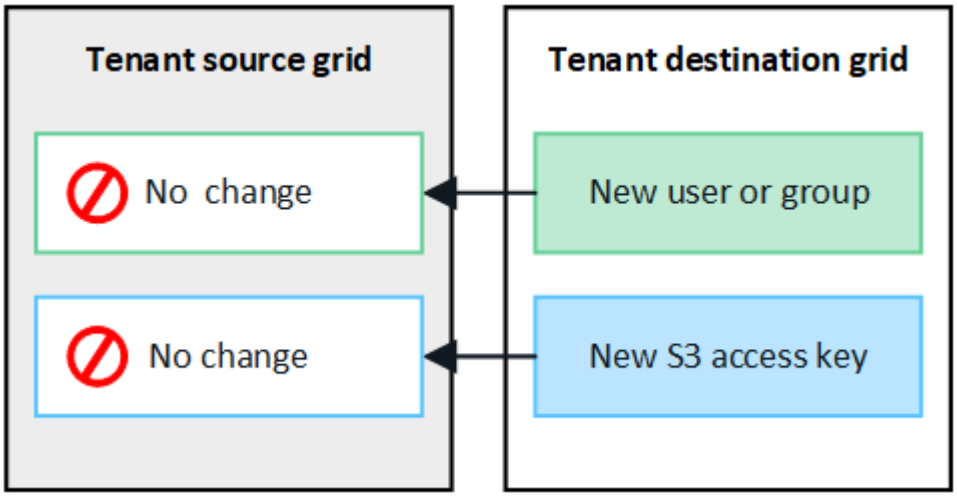
- Si vous n'avez pas besoin d'utiliser les mêmes touches pour chaque grille, vous pouvez le faire "créez vos propres clés d'accès" ou "créez les clés d'accès d'un autre utilisateur" sur chaque grille.
- Si vous devez utiliser les mêmes clés sur les deux grilles, vous pouvez créer des clés sur la grille source, puis utiliser l'API du gestionnaire de locataires pour les utiliser manuellement "cloner les clés" à la grille de destination.



Lorsque vous clonez les clés d'accès S3 d'un utilisateur fédéré, ces deux clés sont clonées dans le locataire de destination.

Les groupes et utilisateurs ajoutés à la grille de destination ne sont pas clonés

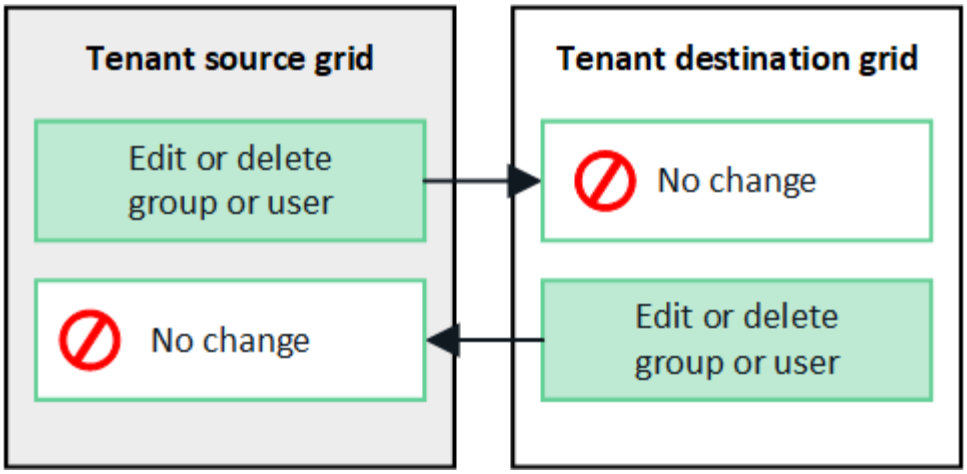
Le clonage s'effectue uniquement depuis la grille source du locataire vers la grille de destination du locataire. Si vous créez ou importez des groupes et des utilisateurs sur la grille de destination du locataire, StorageGRID ne les clonez pas dans la grille source du locataire.



Les groupes, utilisateurs et clés d'accès modifiés ou supprimés ne sont pas clonés

Le clonage a lieu uniquement lorsque vous créez de nouveaux groupes et utilisateurs.

Si vous modifiez ou supprimez des groupes, des utilisateurs ou des clés d'accès sur l'une ou l'autre grille, vos modifications ne seront pas clonées sur l'autre grille.



Cloner les clés d'accès S3 à l'aide de l'API

Si votre compte de locataire dispose de l'autorisation **utiliser la connexion de fédération grid**, vous pouvez utiliser l'API de gestion des locataires pour cloner manuellement les clés d'accès S3 du locataire de la grille source vers le locataire de la grille de destination.

Avant de commencer

- Le compte de tenant dispose de l'autorisation **utiliser la connexion de fédération de grille**.
- La connexion de fédération de grille a un **état de connexion** de **connecté**.
- Vous êtes connecté au gestionnaire de locataires sur la grille source du locataire à l'aide d'un "navigateur web pris en charge".
- Vous appartenez à un groupe d'utilisateurs qui possède le "Gérez vos propres informations d'identification S3 ou autorisations d'accès racine".
- Si vous clonez des clés d'accès pour un utilisateur local, l'utilisateur existe déjà sur les deux grilles.

> Lorsque vous clonez les clés d'accès S3 d'un utilisateur fédéré, ces deux clés sont ajoutées au locataire de destination.

Clonez vos propres clés d'accès

Vous pouvez cloner vos propres clés d'accès si vous devez accéder aux mêmes compartiments sur les deux grilles.

Étapes

1. À l'aide du gestionnaire de locataires sur la grille source, "créez vos propres clés d'accès" et téléchargez le `.csv` fichier.
2. Dans le haut du Gestionnaire de locataires, sélectionnez l'icône d'aide et sélectionnez **documentation API**.
3. Dans la section **s3**, sélectionnez le noeud final suivant :

   ```
   POST /org/users/current-user/replicate-s3-access-key
   ```

4. Sélectionnez **essayez-le**.
5. Dans la zone de texte **body**, remplacez les entrées d'exemple pour **accesskey** et **secretAccessKey** par les valeurs du fichier **.csv** que vous avez téléchargé.

   Veillez à conserver les guillemets doubles autour de chaque chaîne.

6. Si la clé expire, remplacez l'exemple de **expire** par la date et l'heure d'expiration sous forme de chaîne au format de données ISO 8601 (par exemple, `2024-02-28T22:46:33-08:00`). Si la clé n'expire pas, entrez **null** comme valeur pour l'entrée **Expires** (ou supprimez la ligne **Expires** et la virgule précédente).
7. Sélectionnez **Exécuter**.
8. Vérifiez que le code de réponse du serveur est **204**, ce qui indique que la clé a été correctement clonée dans la grille de destination.

Cloner les clés d'accès d'un autre utilisateur

Vous pouvez cloner les clés d'accès d'un autre utilisateur s'il doit accéder aux mêmes compartiments sur les deux grilles.

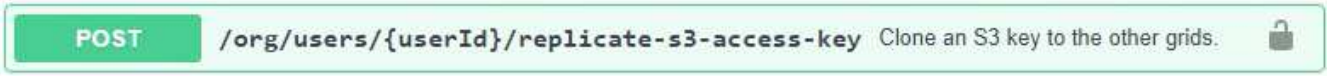
Étapes

1. À l'aide du gestionnaire de locataires sur la grille source, "Créez les clés d'accès S3 de l'autre utilisateur" et téléchargez le `.csv` fichier.
2. Dans le haut du Gestionnaire de locataires, sélectionnez l'icône d'aide et sélectionnez **documentation API**.
3. Obtenez l'ID utilisateur. Vous aurez besoin de cette valeur pour cloner les clés d'accès des autres utilisateurs.
   a. Dans la section **Users**, sélectionnez le noeud final suivant :

      `GET /org/users`

   b. Sélectionnez **essayez-le**.
   c. Spécifiez les paramètres que vous souhaitez utiliser lors de la recherche d'utilisateurs.
   d. Sélectionnez **Exécuter**.
   e. Recherchez l'utilisateur dont vous souhaitez cloner les clés et copiez le numéro dans le champ **ID**.
4. Dans la section **s3**, sélectionnez le noeud final suivant :

   `POST /org/users/{userId}/replicate-s3-access-key`



5. Sélectionnez **essayez-le**.
6. Dans la zone de texte **userid**, collez l'ID utilisateur que vous avez copié.
7. Dans la zone de texte **body**, remplacez les entrées d'exemple pour **example Access key** et **secret Access key** par les valeurs du fichier **.csv** pour cet utilisateur.

   Veillez à conserver les guillemets doubles autour de la chaîne.

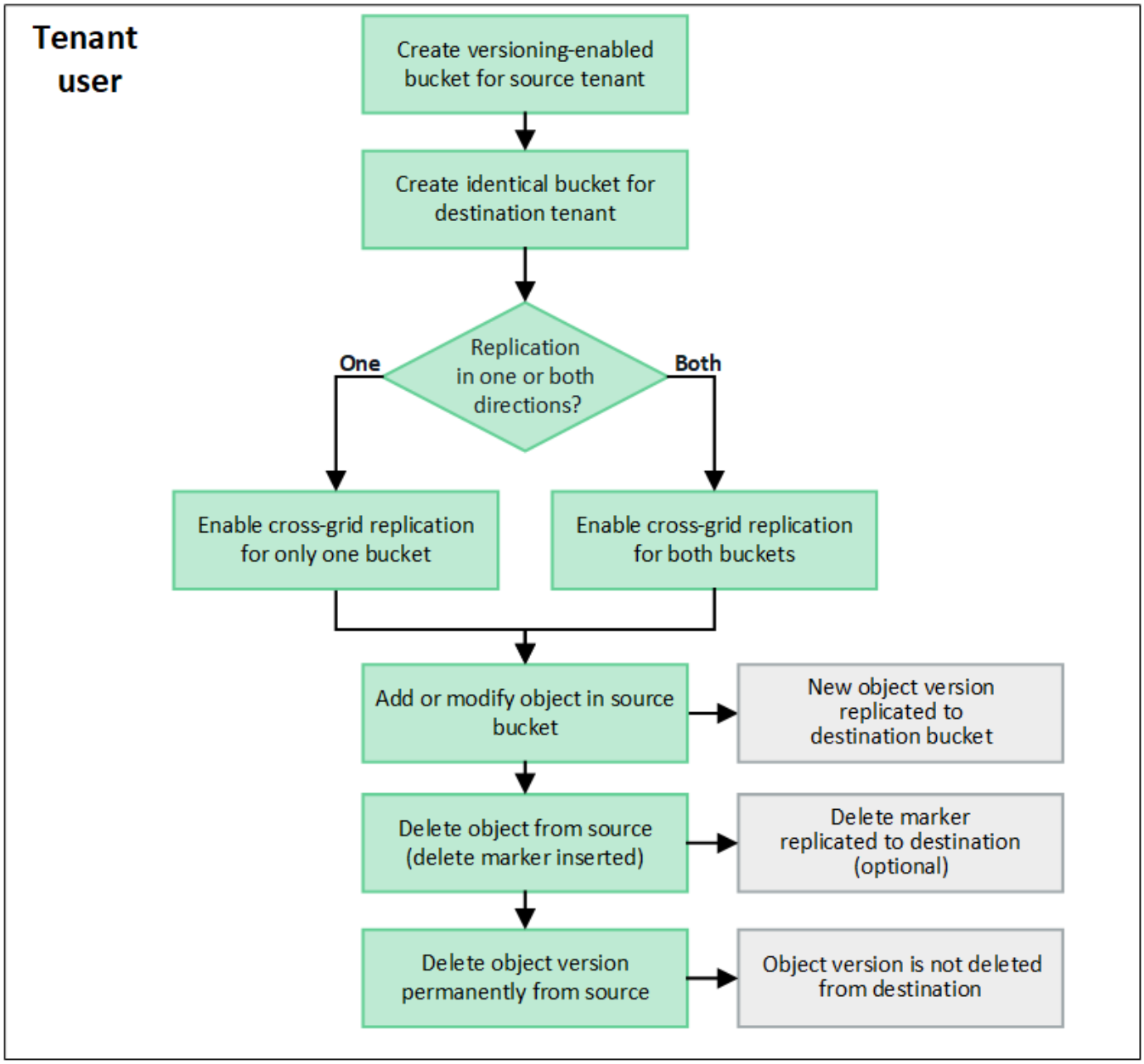
8. Si la clé expire, remplacez l'exemple de **expire** par la date et l'heure d'expiration sous forme de chaîne au format de données ISO 8601 (par exemple, `2023-02-28T22:46:33-08:00`). Si la clé n'expire pas, entrez **null** comme valeur pour l'entrée **Expires** (ou supprimez la ligne **Expires** et la virgule précédente).
9. Sélectionnez **Exécuter**.
10. Vérifiez que le code de réponse du serveur est **204**, ce qui indique que la clé a été correctement clonée dans la grille de destination.

Gérer la réplication entre les grilles

Si l'autorisation **utiliser la connexion de fédération de grille** a été attribuée à votre compte de locataire lors de sa création, vous pouvez utiliser la réplication multigrille pour répliquer automatiquement les objets entre les compartiments de la grille source du locataire et les compartiments de la grille de destination du locataire. La réplication inter-grille peut se produire dans une ou les deux directions.

Flux de production pour la réplication entre les grilles

Le diagramme de flux de travail récapitule les étapes que vous allez effectuer pour configurer la réplication inter-grille entre les compartiments sur deux grilles. Ces étapes sont décrites plus en détail ci-dessous.



Configurer la réplication entre les grilles

Avant de pouvoir utiliser la réplication multigrille, vous devez vous connecter aux comptes de locataires correspondants sur chaque grille et créer des compartiments identiques. Vous pouvez ensuite activer la réplication entre les grilles sur l'un ou l'autre des compartiments, ou sur les deux.

Avant de commencer

- Vous avez examiné les exigences relatives à la réplication intergrid. Voir "Qu'est-ce que la réplication cross-grid".
- Vous utilisez un "navigateur web pris en charge".
- Le compte de tenant possède l'autorisation **utiliser la connexion de fédération de grille** et des comptes de tenant identiques existent sur les deux grilles. Voir "Gérez les locataires autorisés pour la connexion de fédération de grille".
- L'utilisateur locataire auquel vous vous connectez, car il existe déjà sur les deux grilles et appartient à un groupe d'utilisateurs qui possède le "Autorisation d'accès racine".

- Si vous vous connectez à la grille de destination du locataire en tant qu'utilisateur local, l'utilisateur root du compte locataire a défini un mot de passe pour votre compte utilisateur sur cette grille .

Créer deux compartiments identiques

Dans un premier temps, connectez-vous aux comptes de locataires correspondants sur chaque grille et créez des compartiments identiques.

Étapes

1. En commençant à partir de l'une des grilles de la connexion de fédération de grille, créez un nouveau compartiment :
   a. Connectez-vous au compte de tenant à l'aide des informations d'identification d'un utilisateur de tenant qui existe sur les deux grilles.

      Si vous ne parvenez pas à vous connecter à la grille de destination du locataire en tant qu'utilisateur local, vérifiez que l'utilisateur root du compte locataire a défini un mot de passe pour votre compte utilisateur.

   b. Suivez les instructions à "Créer un compartiment S3".
   c. Dans l'onglet **gérer les paramètres d'objet**, sélectionnez **Activer la gestion des versions d'objet**.
   d. Si le verrouillage objet S3 est activé pour votre système StorageGRID, n'activez pas le verrouillage objet S3 pour le compartiment.
   e. Sélectionnez **Créer un compartiment**.
   f. Sélectionnez **Terminer**.
2. Répétez ces étapes pour créer un compartiment identique pour le même compte locataire sur l'autre grille de la connexion de fédération de grille.

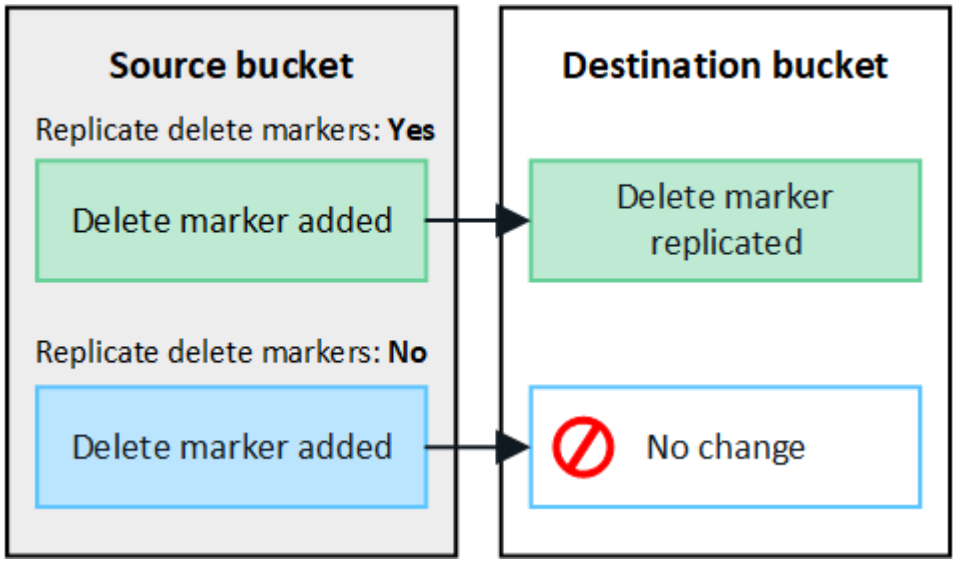
Activer la réplication entre les grilles

Vous devez effectuer ces étapes avant d'ajouter des objets à l'un ou l'autre compartiment.

Étapes

1. À partir d'une grille dont vous souhaitez répliquer les objets, activez "réplication multigrille dans une direction":
   a. Connectez-vous au compte du locataire pour le compartiment.
   b. Sélectionnez **Afficher les compartiments** dans le tableau de bord ou sélectionnez **STOCKAGE (S3)** > **compartiments**.
   c. Sélectionnez le nom du compartiment dans le tableau pour accéder à la page de détails du compartiment.
   d. Sélectionnez l'onglet **réplication multigrille**.
   e. Sélectionnez **Activer** et consultez la liste des exigences.
   f. Si toutes les exigences ont été satisfaites, sélectionnez la connexion de fédération de grille que vous souhaitez utiliser.
   g. Vous pouvez également modifier le paramètre **replicate delete markers** pour déterminer ce qui se passe sur la grille de destination si un client S3 envoie une demande de suppression à la grille source qui n'inclut pas d'ID de version :

- Si **Yes** (par défaut), un marqueur de suppression est ajouté au compartiment source et répliqué dans le compartiment de destination.
- Si **non**, un marqueur de suppression est ajouté au compartiment source mais n'est pas répliqué dans le compartiment de destination.



> Si la demande de suppression inclut un ID de version, cette version de l'objet est définitivement supprimée du compartiment source. StorageGRID ne réplique pas les demandes de suppression qui incluent un ID de version, de sorte que la même version d'objet n'est pas supprimée de la destination.

Voir "Qu'est-ce que la réplication cross-grid" pour plus d'informations.

a. Vérifiez vos sélections. Vous ne pouvez pas modifier ces paramètres à moins que les deux compartiments ne soient vides.

b. Sélectionnez **Activer et tester**.

   Après quelques instants, un message de réussite s'affiche. Les objets ajoutés à ce compartiment seront désormais automatiquement répliqués sur l'autre grille. **La réplication multigrille** est affichée sous la forme d'une fonction activée sur la page de détails du compartiment.

2. Si vous le souhaitez, accédez au compartiment correspondant sur l'autre grille et "activez la réplication entre les grilles dans les deux sens".

Tester la réplication entre les grilles

Si la réplication inter-grid est activée pour un compartiment, vous devrez peut-être vérifier que la connexion et la réplication inter-grid fonctionnent correctement et que les compartiments source et de destination répondent toujours à toutes les exigences (par exemple, la gestion des versions est toujours activée).

Avant de commencer

- Vous utilisez un "navigateur web pris en charge".
- Vous appartenez à un groupe d'utilisateurs qui possède le "Autorisation d'accès racine".

Étapes

1. Connectez-vous au compte du locataire pour le compartiment.

2. Sélectionnez **Afficher les compartiments** dans le tableau de bord ou sélectionnez **STOCKAGE (S3)** > **compartiments**.
3. Sélectionnez le nom du compartiment dans le tableau pour accéder à la page de détails du compartiment.
4. Sélectionnez l'onglet **réplication multigrille**.
5. Sélectionnez **Tester la connexion**.

   Si la connexion est bonne, une bannière de réussite s'affiche. Sinon, un message d'erreur s'affiche, que vous et l'administrateur de la grille pouvez utiliser pour résoudre le problème. Pour plus de détails, voir "Dépanner les erreurs de fédération de grille".

6. Si la réplication inter-grille est configurée pour se produire dans les deux sens, allez dans le compartiment correspondant sur l'autre grille et sélectionnez **Tester la connexion** pour vérifier que la réplication inter-grille fonctionne dans l'autre sens.

Désactiver la réplication entre les grilles

Vous pouvez arrêter définitivement la réplication multigrille si vous ne souhaitez plus copier d'objets sur l'autre grille.

Avant de désactiver la réplication multigrille, notez ce qui suit :

- La désactivation de la réplication multigrille ne supprime pas les objets qui ont déjà été copiés entre les grilles. Par exemple, les objets dans `my-bucket` Sur la grille 1 qui a été copiée dans `my-bucket` Sur la grille 2 ne sont pas supprimés si vous désactivez la réplication inter-grid pour ce compartiment. Si vous souhaitez supprimer ces objets, vous devez les supprimer manuellement.
- Si la réplication inter-grid a été activée pour chacun des compartiments (c'est-à-dire si la réplication se produit dans les deux directions), vous pouvez désactiver la réplication inter-grid pour l'un ou les deux compartiments. Par exemple, vous pouvez désactiver la réplication d'objets à partir de `my-bucket` Sur la grille 1 à `my-bucket` Sur la grille 2, tout en continuant à répliquer les objets à partir de `my-bucket` Sur la grille 2 à `my-bucket` Sur la grille 1.
- Vous devez désactiver la réplication multigrille avant de pouvoir supprimer l'autorisation d'un locataire d'utiliser la connexion de fédération de grille. Voir "Gérer les locataires autorisés".
- Si vous désactivez la réplication inter-grid pour un compartiment contenant des objets, vous ne pourrez pas réactiver la réplication inter-grid à moins de supprimer tous les objets des compartiments source et de destination.

> ⚠ Vous ne pouvez pas réactiver la réplication sauf si les deux compartiments sont vides.

Avant de commencer

- Vous utilisez un "navigateur web pris en charge".
- Vous appartenez à un groupe d'utilisateurs qui possède le "Autorisation d'accès racine".

Étapes

1. Depuis la grille dont vous ne souhaitez plus répliquer les objets, arrêtez la réplication inter-grid pour le compartiment :
   a. Connectez-vous au compte du locataire pour le compartiment.
   b. Sélectionnez **Afficher les compartiments** dans le tableau de bord ou sélectionnez **STOCKAGE (S3)** > **compartiments**.

c. Sélectionnez le nom du compartiment dans le tableau pour accéder à la page de détails du compartiment.

d. Sélectionnez l'onglet **réplication multigrille**.

e. Sélectionnez **Désactiver la réplication**.

f. Si vous êtes sûr de vouloir désactiver la réplication inter-grille pour ce compartiment, tapez **Yes** dans la zone de texte et sélectionnez **Disable**.

   Après quelques instants, un message de réussite s'affiche. Les nouveaux objets ajoutés à ce compartiment ne peuvent plus être automatiquement répliqués sur l'autre grille. **La réplication multigrille** n'est plus affichée comme fonction activée sur la page compartiments.

2. Si la réplication inter-grille a été configurée pour se produire dans les deux directions, allez dans le compartiment correspondant sur l'autre grille et arrêtez la réplication inter-grille dans l'autre direction.

Afficher les connexions de fédération de grille

Si votre compte de locataire dispose de l'autorisation **utiliser la connexion de fédération de grille**, vous pouvez afficher les connexions autorisées.

Avant de commencer

- Le compte de tenant dispose de l'autorisation **utiliser la connexion de fédération de grille**.
- Vous êtes connecté au Gestionnaire de locataires à l'aide d'un "navigateur web pris en charge".
- Vous appartenez à un groupe d'utilisateurs qui possède le "Autorisation d'accès racine".

Étapes

1. Sélectionnez **STORAGE (S3)** > **Grid federation connections**.

   La page de connexion de fédération de grille s'affiche et comprend un tableau qui résume les informations suivantes :

Colonne	Description
Nom de la connexion	Les connexions de fédération de grille que ce locataire a l'autorisation d'utiliser.
Compartiments avec réplication inter-grid	Pour chaque connexion de fédération de grid, les compartiments de locataire pour lesquels la réplication inter-grid est activée. Les objets ajoutés à ces compartiments seront répliqués sur l'autre grille de la connexion.
Dernière erreur	Pour chaque connexion de fédération de grille, l'erreur la plus récente se produit, le cas échéant, lors de la réplication des données vers l'autre grille. Voir Effacez la dernière erreur.

2. Si vous le souhaitez, sélectionnez un nom de compartiment "afficher les détails du compartiment".

efface la dernière erreur

Une erreur peut apparaître dans la colonne **dernière erreur** pour l'une des raisons suivantes :

- La version de l'objet source est introuvable.
- Le compartiment source est introuvable.
- Le compartiment de destination a été supprimé.
- Le compartiment de destination a été recréé par un autre compte.
- La gestion des versions du compartiment de destination est suspendue.
- Le compartiment de destination a été recréé par le même compte, mais il n'est plus versionné.

> Cette colonne affiche uniquement la dernière erreur de réplication inter-grille à se produire ; les erreurs précédentes qui se sont peut-être produites ne seront pas affichées.

Étapes

1. Si un message apparaît dans la colonne **dernière erreur**, affichez le texte du message.

   Par exemple, cette erreur indique que le compartiment de destination de la réplication inter-grid était dans un état non valide, probablement parce que la gestion de version a été suspendue ou que le verrouillage d'objet S3 a été activé.

2. Effectuez toutes les actions recommandées. Par exemple, si la gestion des versions a été suspendue dans le compartiment de destination pour la réplication inter-grid, réactivez la gestion des versions pour ce compartiment.
3. Sélectionnez la connexion dans le tableau.
4. Sélectionnez **Effacer erreur**.
5. Sélectionnez **Oui** pour effacer le message et mettre à jour l'état du système.
6. Patientez 5-6 minutes, puis ingérer un nouvel objet dans le compartiment. Vérifiez que le message d'erreur ne réapparaît pas.

   > Pour vous assurer que le message d'erreur est effacé, attendez au moins 5 minutes après l'horodatage dans le message avant d'ingérer un nouvel objet.

7. Pour déterminer si des objets n'ont pas pu être répliqués en raison d'une erreur de compartiment, reportez-vous à la section "Identifier et réessayer les opérations de réplication ayant échoué".

Gestion des groupes et des utilisateurs

Utiliser la fédération des identités

L'utilisation de la fédération des identités accélère la configuration des groupes de locataires et des utilisateurs, et permet aux utilisateurs de se connecter au compte du locataire à l'aide des identifiants familiers.

Configurez la fédération des identités pour le gestionnaire des locataires

Vous pouvez configurer la fédération des identités pour le Gestionnaire de locataires si vous souhaitez que les groupes et les utilisateurs de locataires soient gérés dans un autre système, tel qu'Active Directory, Azure Active Directory (Azure AD), OpenLDAP ou Oracle Directory Server.

Avant de commencer

- Vous êtes connecté au Gestionnaire de locataires à l'aide d'un "navigateur web pris en charge".
- Vous appartenez à un groupe d'utilisateurs qui possède le "Autorisation d'accès racine".
- Vous utilisez Active Directory, Azure AD, OpenLDAP ou Oracle Directory Server comme fournisseur d'identité.

> Si vous souhaitez utiliser un service LDAP v3 non répertorié, contactez le support technique.

- Si vous avez l'intention d'utiliser OpenLDAP, vous devez configurer le serveur OpenLDAP. Voir Instructions de configuration du serveur OpenLDAP.
- Si vous prévoyez d'utiliser TLS (transport Layer Security) pour les communications avec le serveur LDAP, le fournisseur d'identité doit utiliser TLS 1.2 ou 1.3. Voir "Chiffrement pris en charge pour les connexions TLS sortantes".

Description de la tâche

La configuration d'un service de fédération des identités pour votre locataire dépend de la configuration de votre compte locataire. Votre locataire peut partager le service de fédération des identités configuré pour Grid Manager. Si ce message s'affiche lorsque vous accédez à la page Fédération des identités, vous ne pouvez pas configurer un référentiel d'identité fédéré distinct pour ce locataire.

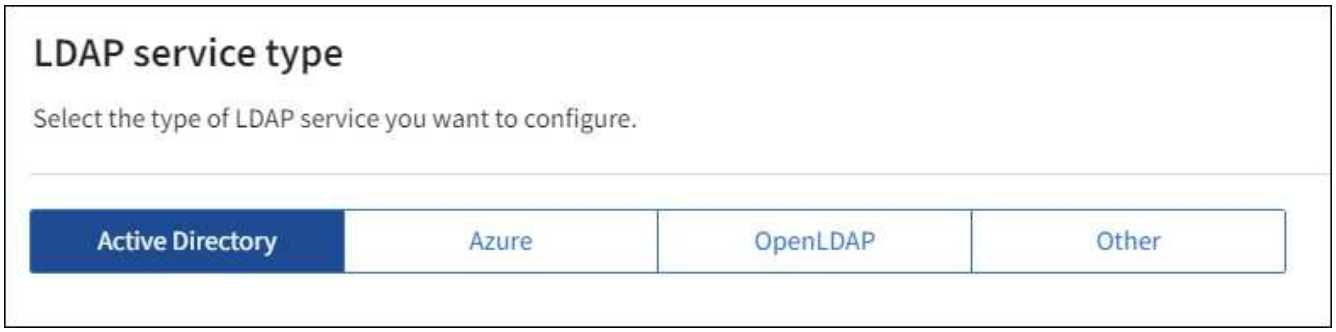
> This tenant account uses the LDAP server that is configured for the Grid Manager. Contact the grid administrator for information or to change this setting.

Entrez la configuration

Lorsque vous configurez la fédération Identify, vous fournissez les valeurs dont StorageGRID a besoin pour se connecter à un service LDAP.

Étapes

1. Sélectionnez **ACCESS MANAGEMENT** > **identity federation**.
2. Sélectionnez **Activer la fédération d'identités**.
3. Dans la section Type de service LDAP, sélectionnez le type de service LDAP que vous souhaitez configurer.



Sélectionnez **autre** pour configurer les valeurs d'un serveur LDAP qui utilise Oracle Directory Server.

4. Si vous avez sélectionné **autre**, renseignez les champs de la section attributs LDAP. Dans le cas contraire, passez à l'étape suivante.
   - **Nom unique utilisateur** : nom de l'attribut qui contient l'identifiant unique d'un utilisateur LDAP. Cet attribut est équivalent à `sAMAccountName` Pour Active Directory et `uid` Pour OpenLDAP. Si vous configurez Oracle Directory Server, entrez `uid`.
   - **UUID d'utilisateur** : nom de l'attribut qui contient l'identifiant unique permanent d'un utilisateur LDAP. Cet attribut est équivalent à `objectGUID` Pour Active Directory et `entryUUID` Pour OpenLDAP. Si vous configurez Oracle Directory Server, entrez `nsuniqueid`. La valeur de chaque utilisateur pour l'attribut spécifié doit être un nombre hexadécimal à 32 chiffres au format 16 octets ou chaîne, où les tirets sont ignorés.
   - **Nom unique de groupe** : nom de l'attribut qui contient l'identifiant unique d'un groupe LDAP. Cet attribut est équivalent à `sAMAccountName` Pour Active Directory et `cn` Pour OpenLDAP. Si vous configurez Oracle Directory Server, entrez `cn`.
   - **UUID de groupe** : nom de l'attribut qui contient l'identificateur unique permanent d'un groupe LDAP. Cet attribut est équivalent à `objectGUID` Pour Active Directory et `entryUUID` Pour OpenLDAP. Si vous configurez Oracle Directory Server, entrez `nsuniqueid`. La valeur de chaque groupe pour l'attribut spécifié doit être un nombre hexadécimal à 32 chiffres au format 16 octets ou chaîne, où les tirets sont ignorés.
5. Pour tous les types de services LDAP, entrez les informations de connexion réseau et de serveur LDAP requises dans la section configurer le serveur LDAP.
   - **Nom d'hôte** : le nom de domaine complet (FQDN) ou l'adresse IP du serveur LDAP.
   - **Port** : port utilisé pour se connecter au serveur LDAP.

     Le port par défaut de STARTTLS est 389 et le port par défaut de LDAPS est 636. Cependant, vous pouvez utiliser n'importe quel port tant que votre pare-feu est configuré correctement.

   - **Nom d'utilisateur** : chemin complet du nom distinctif (DN) de l'utilisateur qui se connectera au serveur LDAP.

     Pour Active Directory, vous pouvez également spécifier le nom de connexion bas niveau ou le nom principal d'utilisateur.

     L'utilisateur spécifié doit être autorisé à répertorier les groupes et les utilisateurs et à accéder aux attributs suivants :

     - `sAMAccountName` ou `uid`

- `objectGUID`, `entryUUID`, ou `nsuniqueid`
- `cn`
- `memberOf` ou `isMemberOf`
- **Active Directory** : `objectSid`, `primaryGroupID`, `userAccountControl`, et `userPrincipalName`
- **Azure**: `accountEnabled` et `userPrincipalName`

◦ **Mot de passe** : mot de passe associé au nom d'utilisateur.

◦ **DN de base de groupe** : chemin complet du nom distinctif (DN) pour une sous-arborescence LDAP que vous voulez rechercher des groupes. Dans l'exemple Active Directory (ci-dessous), tous les groupes dont le nom unique est relatif au DN de base (DC=storagegrid,DC=exemple,DC=com) peuvent être utilisés comme groupes fédérés.

> Les valeurs **Nom unique de groupe** doivent être uniques dans le **DN de base de groupe** auquel elles appartiennent.

◦ **DN de base d'utilisateurs** : le chemin complet du nom distinctif (DN) d'une sous-arborescence LDAP que vous voulez rechercher des utilisateurs.

> Les valeurs **Nom unique utilisateur** doivent être uniques dans le **DN de base utilisateur** auquel elles appartiennent.

◦ **Bind username format** (facultatif) : le nom d'utilisateur par défaut StorageGRID devrait utiliser si le modèle ne peut pas être déterminé automatiquement.

Il est recommandé de fournir le format **Bind username** car il peut permettre aux utilisateurs de se connecter si StorageGRID ne parvient pas à se lier avec le compte de service.

Entrez l'un des motifs suivants :

- **Modèle UserPrincipalName (Active Directory et Azure)** : `[USERNAME]@*example*.com`
- **Modèle de nom de connexion bas niveau (Active Directory et Azure)** : `*example*\[USERNAME]`
- **Modèle de nom unique** : `CN=[USERNAME],CN=Users,DC=*example*,DC=com`

  Inclure **[NOM D'UTILISATEUR]** exactement comme écrit.

6. Dans la section transport Layer Security (TLS), sélectionnez un paramètre de sécurité.

◦ **Utilisez STARTTLS** : utilisez STARTTLS pour sécuriser les communications avec le serveur LDAP. Il s'agit de l'option recommandée pour Active Directory, OpenLDAP ou autre, mais cette option n'est pas prise en charge pour Azure.

◦ **Utilisez LDAPS** : l'option LDAPS (LDAP sur SSL) utilise TLS pour établir une connexion au serveur LDAP. Vous devez sélectionner cette option pour Azure.

◦ **N'utilisez pas TLS** : le trafic réseau entre le système StorageGRID et le serveur LDAP ne sera pas sécurisé. Cette option n'est pas prise en charge pour Azure.

> L'utilisation de l'option **ne pas utiliser TLS** n'est pas prise en charge si votre serveur Active Directory applique la signature LDAP. Vous devez utiliser STARTTLS ou LDAPS.

7. Si vous avez sélectionné STARTTLS ou LDAPS, choisissez le certificat utilisé pour sécuriser la connexion.
   - **Utilisez le certificat CA du système d'exploitation** : utilisez le certificat CA de la grille par défaut installé sur le système d'exploitation pour sécuriser les connexions.
   - **Utilisez un certificat d'autorité de certification personnalisé** : utilisez un certificat de sécurité personnalisé.

     Si vous sélectionnez ce paramètre, copiez et collez le certificat de sécurité personnalisé dans la zone de texte certificat de l'autorité de certification.

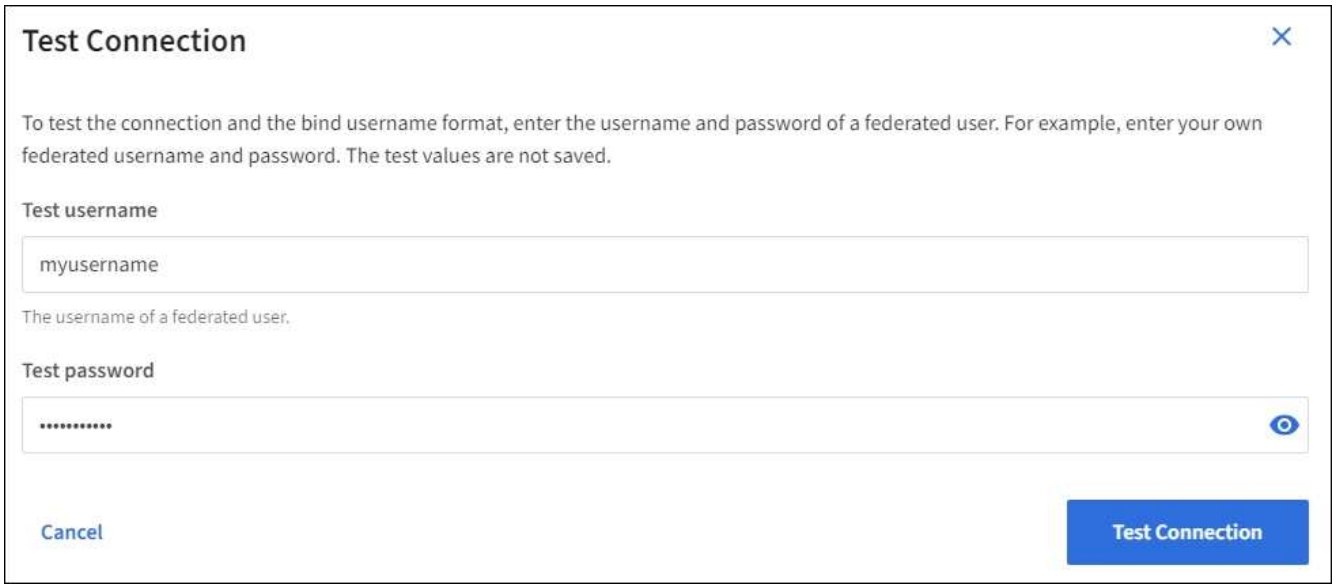
Testez la connexion et enregistrez la configuration

Après avoir saisi toutes les valeurs, vous devez tester la connexion avant de pouvoir enregistrer la configuration. StorageGRID vérifie les paramètres de connexion pour le serveur LDAP et le format de nom d'utilisateur BIND, si vous en avez fourni un.

Étapes

1. Sélectionnez **Tester la connexion**.
2. Si vous n'avez pas fourni de format de nom d'utilisateur de liaison :
   - Un message « Test connexion réussie » s'affiche si les paramètres de connexion sont valides. Sélectionnez **Enregistrer** pour enregistrer la configuration.
   - Un message « Impossible d'établir la connexion test » s'affiche si les paramètres de connexion ne sont pas valides. Sélectionnez **Fermer**. Ensuite, résolvez tout problème et testez à nouveau la connexion.
3. Si vous avez fourni un format de nom d'utilisateur BIND, entrez le nom d'utilisateur et le mot de passe d'un utilisateur fédéré valide.

   Par exemple, entrez votre nom d'utilisateur et votre mot de passe. N'incluez pas de caractères spéciaux dans le nom d'utilisateur, tels que @ ou /.



   - Un message « Test connexion réussie » s'affiche si les paramètres de connexion sont valides. Sélectionnez **Enregistrer** pour enregistrer la configuration.
   - Un message d'erreur s'affiche si les paramètres de connexion, le format du nom d'utilisateur de liaison ou le nom d'utilisateur et le mot de passe du test sont incorrects. Résolvez tout problème et testez à nouveau la connexion.

Forcer la synchronisation avec le référentiel d'identité

Le système StorageGRID synchronise régulièrement les groupes fédérés et les utilisateurs à partir du référentiel d'identité. Vous pouvez forcer la synchronisation à démarrer si vous souhaitez activer ou restreindre les autorisations utilisateur le plus rapidement possible.

Étapes

1. Accédez à la page fédération des identités.
2. Sélectionnez **serveur de synchronisation** en haut de la page.

   Le processus de synchronisation peut prendre un certain temps en fonction de votre environnement.

> L'alerte **échec de synchronisation de la fédération d'identités** est déclenchée en cas de problème de synchronisation des groupes fédérés et des utilisateurs à partir du référentiel d'identité.

Désactiver la fédération des identités

Vous pouvez désactiver temporairement ou définitivement la fédération des identités pour les groupes et les utilisateurs. Lorsque la fédération des identités est désactivée, il n'y a aucune communication entre StorageGRID et le référentiel d'identité. Cependant, tous les paramètres que vous avez configurés sont conservés, ce qui vous permet de réactiver facilement la fédération d'identités à l'avenir.

Description de la tâche

Avant de désactiver la fédération des identités, vous devez prendre connaissance des points suivants :

- Les utilisateurs fédérés ne pourront pas se connecter.
- Les utilisateurs fédérés qui sont actuellement connectés conservent l'accès au système StorageGRID jusqu'à l'expiration de leur session, mais ils ne pourront pas se connecter après l'expiration de leur session.
- La synchronisation entre le système StorageGRID et le référentiel d'identité ne se produira pas et des alertes ou des alarmes ne seront pas émises pour les comptes qui n'ont pas été synchronisés.
- La case **Activer la fédération d'identité** est désactivée si l'authentification unique (SSO) est définie sur **activé** ou **mode Sandbox**. Le statut SSO sur la page connexion unique doit être **désactivé** avant de pouvoir désactiver la fédération d'identités. Voir "Désactiver l'authentification unique".

Étapes

1. Accédez à la page fédération des identités.
2. Décochez la case **Activer la fédération d'identité**.

Instructions de configuration du serveur OpenLDAP

Si vous souhaitez utiliser un serveur OpenLDAP pour la fédération des identités, vous devez configurer des paramètres spécifiques sur le serveur OpenLDAP.

> Pour les référentiels d'identité qui ne sont pas ActiveDirectory ou Azure, StorageGRID ne bloquera pas automatiquement l'accès S3 aux utilisateurs désactivés en externe. Pour bloquer l'accès S3, supprimez les clés S3 de l'utilisateur ou supprimez l'utilisateur de tous les groupes.

Recouvrements de memberOf et de raffint

Les recouvrements de membre et de raffinage doivent être activés. Pour plus d'informations, reportez-vous aux instructions relatives à la maintenance de l'adhésion au groupe inverse dans lehttp://www.openldap.org/doc/admin24/index.html["Documentation OpenLDAP : version 2.4 - Guide de l'administrateur"^].

Indexation

Vous devez configurer les attributs OpenLDAP suivants avec les mots-clés d'index spécifiés :

- `olcDbIndex: objectClass eq`
- `olcDbIndex: uid eq,pres,sub`
- `olcDbIndex: cn eq,pres,sub`
- `olcDbIndex: entryUUID eq`

De plus, assurez-vous que les champs mentionnés dans l'aide pour le nom d'utilisateur sont indexés pour des performances optimales.

Reportez-vous aux informations relatives à la maintenance de l'adhésion au groupe inverse dans lehttp://www.openldap.org/doc/admin24/index.html["Documentation OpenLDAP : version 2.4 - Guide de l'administrateur"^].

Gestion des groupes de locataires

Créez des groupes pour un locataire S3

Vous pouvez gérer les autorisations des groupes d'utilisateurs S3 en important des groupes fédérés ou en créant des groupes locaux.

Avant de commencer

- Vous êtes connecté au Gestionnaire de locataires à l'aide d'un "navigateur web pris en charge".
- Vous appartenez à un groupe d'utilisateurs qui possède le "Autorisation d'accès racine".
- Si vous prévoyez d'importer un groupe fédéré, vous avez "fédération des identités configurée", et le groupe fédéré existe déjà dans le référentiel d'identité configuré.
- Si votre compte locataire dispose de l'autorisation **utiliser la connexion de fédération de grille**, vous avez examiné le flux de travail et les considérations pour "clonage de groupes de locataires et d'utilisateurs", et vous êtes connecté à la grille source du locataire.

Accédez à l'assistant de création de groupe

Pour la première étape, accédez à l'assistant de création de groupe.

Étapes

1. Sélectionnez **ACCESS MANAGEMENT** > **Groups**.
2. Si votre compte locataire dispose de l'autorisation **utiliser la connexion de fédération de grille**, vérifiez qu'une bannière bleue s'affiche, indiquant que les nouveaux groupes créés sur cette grille seront clonés sur le même locataire sur l'autre grille de la connexion. Si cette bannière n'apparaît pas, vous pouvez être connecté à la grille de destination du locataire.

3. Sélectionnez **Créer groupe**.

Choisissez un type de groupe

Vous pouvez créer un groupe local ou importer un groupe fédéré.

Étapes

1. Sélectionnez l'onglet **Groupe local** pour créer un groupe local ou sélectionnez l'onglet **Groupe fédéré** pour importer un groupe à partir du référentiel d'identité configuré précédemment.

   Si l'authentification unique (SSO) est activée pour votre système StorageGRID, les utilisateurs appartenant à des groupes locaux ne pourront pas se connecter au Gestionnaire de locataires, bien qu'ils puissent utiliser les applications client pour gérer les ressources du locataire, en fonction des autorisations de groupe.

2. Entrez le nom du groupe.
   - **Groupe local** : saisissez à la fois un nom d'affichage et un nom unique. Vous pouvez modifier le nom d'affichage ultérieurement.

     Si votre compte de locataire dispose de l'autorisation **utiliser la connexion de fédération de grille**, une erreur de clonage se produit si le même **nom unique** existe déjà pour le locataire sur la grille de destination.

   - **Groupe fédéré** : saisissez le nom unique. Pour Active Directory, le nom unique est le nom associé à l' `sAMAccountName` attribut. Pour OpenLDAP, le nom unique est le nom associé à `uid` attribut.
3. Sélectionnez **Continuer**.

Gérer les autorisations de groupe

Les autorisations de groupe contrôlent les tâches que les utilisateurs peuvent effectuer dans le Gestionnaire de locataires et l'API de gestion des locataires.

Étapes

1. Pour **Access mode**, sélectionnez l'une des options suivantes :
   - **Lecture-écriture** (par défaut) : les utilisateurs peuvent se connecter au gestionnaire de locataires et gérer la configuration du locataire.

- **Lecture seule** : les utilisateurs peuvent uniquement afficher les paramètres et les fonctionnalités. Ils ne peuvent pas apporter de modifications ni exécuter d'opérations dans le gestionnaire de locataires ou l'API de gestion des locataires. Les utilisateurs locaux en lecture seule peuvent modifier leurs propres mots de passe.

> Si un utilisateur appartient à plusieurs groupes et qu'un groupe est défini sur lecture seule, l'utilisateur dispose d'un accès en lecture seule à tous les paramètres et fonctions sélectionnés.

2. Sélectionnez une ou plusieurs autorisations pour ce groupe.

   Voir "Autorisations de gestion des locataires".

3. Sélectionnez **Continuer**.

Définissez la règle de groupe S3

La stratégie de groupe détermine les autorisations d'accès S3 dont disposent les utilisateurs.

Étapes

1. Sélectionnez la stratégie que vous souhaitez utiliser pour ce groupe.

Stratégie de groupe	Description
Aucun accès à S3	Par défaut. Les utilisateurs de ce groupe n'ont pas accès aux ressources S3, sauf si l'accès est accordé avec une règle de compartiment. Si vous sélectionnez cette option, seul l'utilisateur root peut accéder aux ressources S3 par défaut.
Accès en lecture seule	Les utilisateurs de ce groupe disposent d'un accès en lecture seule aux ressources S3. Par exemple, les utilisateurs de ce groupe peuvent afficher la liste des objets et lire les données d'objet, les métadonnées et les balises. Lorsque vous sélectionnez cette option, la chaîne JSON pour une stratégie de groupe en lecture seule s'affiche dans la zone de texte. Vous ne pouvez pas modifier cette chaîne.
Accès complet	Les utilisateurs de ce groupe bénéficient d'un accès complet aux ressources S3, y compris les compartiments. Lorsque vous sélectionnez cette option, la chaîne JSON pour une stratégie de groupe à accès complet s'affiche dans la zone de texte. Vous ne pouvez pas modifier cette chaîne.

Stratégie de groupe	Description
Réduction des ransomwares	Cet exemple de règle s'applique à toutes les compartiments pour ce locataire. Les utilisateurs de ce groupe peuvent effectuer des actions courantes, mais ne peuvent pas supprimer définitivement des objets des compartiments pour lesquels la gestion des versions d'objet est activée. Les utilisateurs de tenant Manager disposant de l'autorisation **gérer tous les compartiments** peuvent remplacer cette stratégie de groupe. Limitez l'autorisation gérer tous les compartiments aux utilisateurs de confiance et utilisez l'authentification multifacteur (MFA), le cas échéant.
Personnalisées	Les utilisateurs du groupe se voient accorder les autorisations que vous spécifiez dans la zone de texte.

2. Si vous avez sélectionné **personnalisé**, entrez la stratégie de groupe. Chaque stratégie de groupe a une taille limite de 5,120 octets. Vous devez entrer une chaîne au format JSON valide.

   Pour plus d'informations sur les stratégies de groupe, notamment la syntaxe de la langue et des exemples, reportez-vous à la section "Exemples de stratégies de groupe".

3. Si vous créez un groupe local, sélectionnez **Continuer**. Si vous créez un groupe fédéré, sélectionnez **Créer groupe** et **Terminer**.

Ajouter des utilisateurs (groupes locaux uniquement)

Vous pouvez enregistrer le groupe sans ajouter d'utilisateurs, ou vous pouvez éventuellement ajouter des utilisateurs locaux qui existent déjà.

> Si votre compte de locataire dispose de l'autorisation **utiliser la connexion de fédération de grille**, tous les utilisateurs que vous sélectionnez lorsque vous créez un groupe local sur la grille source ne sont pas inclus lorsque le groupe est cloné dans la grille de destination. Pour cette raison, ne sélectionnez pas d'utilisateurs lorsque vous créez le groupe. Sélectionnez plutôt le groupe lorsque vous créez les utilisateurs.

Étapes

1. Vous pouvez également sélectionner un ou plusieurs utilisateurs locaux pour ce groupe.
2. Sélectionnez **Créer groupe** et **Terminer**.

   Le groupe que vous avez créé apparaît dans la liste des groupes.

   Si votre compte locataire dispose de l'autorisation **utiliser la connexion de fédération de grille** et que vous êtes sur la grille source du locataire, le nouveau groupe est cloné dans la grille de destination du locataire. **Succès** apparaît comme l'état **clonage** dans la section vue d'ensemble de la page de détails du groupe.

Créez des groupes pour un locataire Swift

Vous pouvez gérer les autorisations d'accès pour un compte de locataire Swift en

important des groupes fédérés ou en créant des groupes locaux. Au moins un groupe doit disposer de l'autorisation Administrateur Swift, qui est requise pour gérer les conteneurs et les objets d'un compte de locataire Swift.

> La prise en charge des applications du client Swift a été obsolète et sera supprimée dans une prochaine version.

Avant de commencer

- Vous êtes connecté au Gestionnaire de locataires à l'aide d'un "navigateur web pris en charge".
- Vous appartenez à un groupe d'utilisateurs qui possède le "Autorisation d'accès racine".
- Si vous prévoyez d'importer un groupe fédéré, vous avez "fédération des identités configurée", et le groupe fédéré existe déjà dans le référentiel d'identité configuré.

Accédez à l'assistant de création de groupe

Étapes

Pour la première étape, accédez à l'assistant de création de groupe.

1. Sélectionnez **ACCESS MANAGEMENT** > **Groups**.
2. Sélectionnez **Créer groupe**.

Choisissez un type de groupe

Vous pouvez créer un groupe local ou importer un groupe fédéré.

Étapes

1. Sélectionnez l'onglet **Groupe local** pour créer un groupe local ou sélectionnez l'onglet **Groupe fédéré** pour importer un groupe à partir du référentiel d'identité configuré précédemment.

   Si l'authentification unique (SSO) est activée pour votre système StorageGRID, les utilisateurs appartenant à des groupes locaux ne pourront pas se connecter au Gestionnaire de locataires, bien qu'ils puissent utiliser les applications client pour gérer les ressources du locataire, en fonction des autorisations de groupe.

2. Entrez le nom du groupe.
   - **Groupe local** : saisissez à la fois un nom d'affichage et un nom unique. Vous pouvez modifier le nom d'affichage ultérieurement.
   - **Groupe fédéré** : saisissez le nom unique. Pour Active Directory, le nom unique est le nom associé à l' `sAMAccountName` attribut. Pour OpenLDAP, le nom unique est le nom associé à `uid` attribut.
3. Sélectionnez **Continuer**.

Gérer les autorisations de groupe

Les autorisations de groupe contrôlent les tâches que les utilisateurs peuvent effectuer dans le Gestionnaire de locataires et l'API de gestion des locataires.

Étapes

1. Pour **Access mode**, sélectionnez l'une des options suivantes :
   - **Lecture-écriture** (par défaut) : les utilisateurs peuvent se connecter au gestionnaire de locataires et

gérer la configuration du locataire.

- **Lecture seule** : les utilisateurs peuvent uniquement afficher les paramètres et les fonctionnalités. Ils ne peuvent pas apporter de modifications ni exécuter d'opérations dans le gestionnaire de locataires ou l'API de gestion des locataires. Les utilisateurs locaux en lecture seule peuvent modifier leurs propres mots de passe.

> Si un utilisateur appartient à plusieurs groupes et qu'un groupe est défini sur lecture seule, l'utilisateur dispose d'un accès en lecture seule à tous les paramètres et fonctions sélectionnés.

2. Cochez la case **accès racine** si les utilisateurs du groupe doivent se connecter à l'API tenant Manager ou tenant Management.
3. Sélectionnez **Continuer**.

Définissez la stratégie de groupe Swift

Les utilisateurs Swift ont besoin d'une autorisation d'administrateur pour s'authentifier auprès de l'API REST Swift afin de créer des conteneurs et d'ingérer des objets.

1. Cochez la case **Swift Administrator** si les utilisateurs du groupe doivent utiliser l'API REST Swift pour gérer les conteneurs et les objets.
2. Si vous créez un groupe local, sélectionnez **Continuer**. Si vous créez un groupe fédéré, sélectionnez **Créer groupe** et **Terminer**.

Ajouter des utilisateurs (groupes locaux uniquement)

Vous pouvez enregistrer le groupe sans ajouter d'utilisateurs, ou vous pouvez éventuellement ajouter des utilisateurs locaux qui existent déjà.

Étapes

1. Vous pouvez également sélectionner un ou plusieurs utilisateurs locaux pour ce groupe.

   Si vous n'avez pas encore créé d'utilisateurs locaux, vous pouvez ajouter ce groupe à l'utilisateur sur la page utilisateurs. Voir "Gérez les utilisateurs locaux".

2. Sélectionnez **Créer groupe** et **Terminer**.

   Le groupe que vous avez créé apparaît dans la liste des groupes.

Autorisations de gestion des locataires

Avant de créer un groupe de locataires, tenez compte des autorisations que vous souhaitez attribuer à ce groupe. Les autorisations de gestion des locataires déterminent les tâches que les utilisateurs peuvent effectuer à l'aide du Gestionnaire de locataires ou de l'API de gestion des locataires. Un utilisateur peut appartenir à un ou plusieurs groupes. Les autorisations sont cumulatives si un utilisateur appartient à plusieurs groupes.

Pour vous connecter au Gestionnaire de locataires ou utiliser l'API de gestion des locataires, les utilisateurs doivent appartenir à un groupe disposant d'au moins une autorisation. Tous les utilisateurs autorisés à se connecter peuvent effectuer les tâches suivantes :

- Afficher le tableau de bord
- Modifier son propre mot de passe (pour les utilisateurs locaux)

Pour toutes les autorisations, le paramètre mode d'accès du groupe détermine si les utilisateurs peuvent modifier les paramètres et effectuer des opérations ou s'ils ne peuvent afficher que les paramètres et les fonctions associés.

Si un utilisateur appartient à plusieurs groupes et qu'un groupe est défini sur lecture seule, l'utilisateur dispose d'un accès en lecture seule à tous les paramètres et fonctions sélectionnés.

Vous pouvez attribuer les autorisations suivantes à un groupe. Notez que les locataires S3 et Swift disposent d'autorisations de groupe différentes.

Autorisations	Description
Accès racine	Donne un accès complet au gestionnaire des locataires et à l'API de gestion des locataires. **Remarque :** les utilisateurs Swift doivent disposer d'une autorisation d'accès racine pour se connecter au compte locataire.
Administrateur	Les locataires Swift uniquement. Fournit un accès complet aux conteneurs et objets Swift pour ce compte de locataire **Remarque :** les utilisateurs de Swift doivent disposer de l'autorisation Administrateur Swift pour effectuer toutes les opérations avec l'API REST Swift.
Gérez vos identifiants S3	Permet aux utilisateurs de créer et de supprimer leurs propres clés d'accès S3. Les utilisateurs qui ne disposent pas de cette autorisation ne voient pas l'option de menu **STORAGE (S3)** > **My S3 Access keys**.
Gestion de tous les compartiments	• Locataires S3 : permet aux utilisateurs d'utiliser le gestionnaire de locataires et l'API de gestion des locataires pour créer et supprimer des compartiments S3 et gérer les paramètres de tous les compartiments S3 du compte, indépendamment des règles du compartiment S3 ou du groupe. Les utilisateurs qui ne disposent pas de cette autorisation ne voient pas l'option de menu **rubriques**. • Locataires Swift : permet aux utilisateurs Swift de contrôler le niveau de cohérence des conteneurs Swift à l'aide de l'API de gestion des locataires. **Remarque :** vous ne pouvez attribuer l'autorisation gérer tous les compartiments aux groupes Swift qu'à partir de l'API de gestion des locataires. Vous ne pouvez pas attribuer cette autorisation à des groupes Swift à l'aide du Gestionnaire de locataires.

Autorisations	Description
Gestion des terminaux	Permet aux utilisateurs d'utiliser le gestionnaire de locataires ou l'API de gestion des locataires pour créer ou modifier des terminaux de service de plateforme, qui sont utilisés comme destination pour les services de plateforme StorageGRID. Les utilisateurs qui ne disposent pas de cette autorisation ne voient pas l'option de menu **Platform Services Endpoints**.
Gestion des objets avec la console S3	Associé à l'autorisation gérer tous les compartiments, permet aux utilisateurs d'accéder à la console S3 expérimentale à partir de la page compartiments. Les utilisateurs qui disposent de cette autorisation mais qui ne disposent pas de l'autorisation gérer tous les compartiments peuvent toujours naviguer directement vers la console S3 expérimentale.

Gérer les groupes

Vous pouvez afficher un groupe, modifier le nom, les autorisations, les stratégies et les utilisateurs d'un groupe, dupliquer un groupe ; ou supprimer un groupe.

Avant de commencer

- Vous êtes connecté au Gestionnaire de locataires à l'aide d'un "navigateur web pris en charge".
- Vous appartenez à un groupe d'utilisateurs qui possède le "Autorisation d'accès racine".

Afficher ou modifier un groupe

Vous pouvez afficher et modifier les informations de base et les détails de chaque groupe.

Étapes

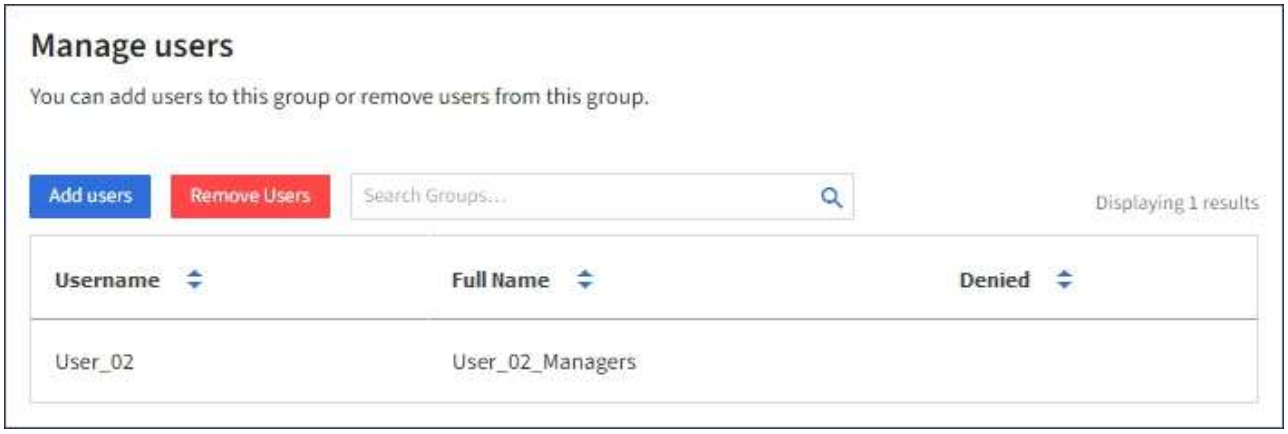
1. Sélectionnez **ACCESS MANAGEMENT** > **Groups**.
2. Consultez les informations fournies sur la page groupes, qui répertorie les informations de base pour tous les groupes locaux et fédérés pour ce compte de tenant.

   Si le compte de tenant dispose de l'autorisation **utiliser la connexion de fédération de grille** et que vous affichez des groupes sur la grille source du locataire, une bannière bleue indique que si vous modifiez ou supprimez un groupe, vos modifications ne seront pas synchronisées avec l'autre grille. Voir "Cloner des groupes de locataires et des utilisateurs".

3. Si vous souhaitez modifier le nom du groupe :
   a. Cochez la case du groupe.
   b. Sélectionnez **actions** > **Modifier le nom du groupe**.
   c. Saisissez le nouveau nom.
   d. Sélectionnez **Enregistrer les modifications.**
4. Si vous souhaitez afficher plus de détails ou apporter des modifications supplémentaires, effectuez l'une des opérations suivantes :
   - Sélectionnez le nom du groupe.
   - Cochez la case du groupe et sélectionnez **actions** > **Afficher les détails du groupe**.
5. Consultez la section Présentation, qui présente les informations suivantes pour chaque groupe :

- Nom d'affichage
- Nom unique
- Type
- Mode d'accès
- Autorisations
- Règle S3
- Nombre d'utilisateurs dans ce groupe
- Champs supplémentaires si le compte de tenant dispose de l'autorisation **utiliser la connexion de fédération de grille** et que vous affichez le groupe sur la grille source du locataire :
  - État de clonage, soit **succès** soit **échec**
  - Une bannière bleue indiquant que si vous modifiez ou supprimez ce groupe, vos modifications ne seront pas synchronisées avec l'autre grille.

6. Modifiez les paramètres de groupe selon vos besoins. Voir "Créez des groupes pour un locataire S3" et "Créez des groupes pour un locataire Swift" pour plus d'informations sur ce que vous devez saisir.
   a. Dans la section vue d'ensemble, modifiez le nom d'affichage en sélectionnant le nom ou l'icône de modification .
   b. Dans l'onglet **autorisations de groupe**, mettez à jour les autorisations et sélectionnez **Enregistrer les modifications**.
   c. Dans l'onglet **Stratégie de groupe**, apportez les modifications nécessaires et sélectionnez **Enregistrer les modifications**.
      - Si vous modifiez un groupe S3, sélectionnez une règle de groupe S3 différente ou entrez la chaîne JSON pour une règle personnalisée, si nécessaire.
      - Si vous modifiez un groupe Swift, cochez ou décochez la case **Administrateur Swift**.
7. Pour ajouter un ou plusieurs utilisateurs locaux existants au groupe :
   a. Sélectionnez l'onglet utilisateurs.



   b. Sélectionnez **Ajouter des utilisateurs**.
   c. Sélectionnez les utilisateurs existants que vous souhaitez ajouter, puis sélectionnez **Ajouter des utilisateurs**.

      Un message de réussite s'affiche en haut à droite.

8. Pour supprimer des utilisateurs locaux du groupe :

a. Sélectionnez l'onglet utilisateurs.
b. Sélectionnez **Supprimer utilisateurs**.
c. Sélectionnez les utilisateurs que vous souhaitez supprimer, puis sélectionnez **Supprimer utilisateurs**.

   Un message de réussite s'affiche en haut à droite.

9. Confirmez que vous avez sélectionné **Enregistrer les modifications** pour chaque section que vous avez modifiée.

Dupliquer le groupe

Vous pouvez dupliquer un groupe existant pour créer de nouveaux groupes plus rapidement.

> Si votre compte de locataire dispose de l'autorisation **utiliser la connexion de fédération de grille** et que vous dupliquez un groupe à partir de la grille source du locataire, le groupe dupliqué sera cloné dans la grille de destination du locataire.

Étapes

1. Sélectionnez **ACCESS MANAGEMENT** > **Groups**.
2. Cochez la case du groupe que vous souhaitez dupliquer.
3. Sélectionnez **actions** > **Dupliquer le groupe**.
4. Voir "Créez des groupes pour un locataire S3" ou "Créez des groupes pour un locataire Swift" pour plus d'informations sur ce que vous devez saisir.
5. Sélectionnez **Créer groupe**.

Supprimer un ou plusieurs groupes

Vous pouvez supprimer un ou plusieurs groupes. Les utilisateurs qui appartiennent uniquement à un groupe supprimé ne pourront plus se connecter au gestionnaire de tenant ni utiliser le compte de tenant.

> Si votre compte de locataire dispose de l'autorisation **utiliser la connexion de fédération de grille** et que vous supprimez un groupe, StorageGRID ne supprimera pas le groupe correspondant sur l'autre grille. Si vous devez conserver ces informations synchronisées, vous devez supprimer le même groupe des deux grilles.

Étapes

1. Sélectionnez **ACCESS MANAGEMENT** > **Groups**.
2. Cochez la case correspondant à chaque groupe à supprimer.
3. Sélectionnez **actions** > **Supprimer groupe** ou **actions** > **Supprimer groupes**.

   Une boîte de dialogue de confirmation s'affiche.

4. Sélectionnez **Supprimer le groupe** ou **Supprimer les groupes**.

Gérez les utilisateurs locaux

Vous pouvez créer des utilisateurs locaux et les affecter à des groupes locaux pour déterminer les fonctions auxquelles ces utilisateurs peuvent accéder. Le gestionnaire de locataires comprend un utilisateur local prédéfini, nommé « root ». Bien que vous

puissiez ajouter et supprimer des utilisateurs locaux, vous ne pouvez pas supprimer l'utilisateur racine.

> Si l'authentification unique (SSO) est activée pour votre système StorageGRID, les utilisateurs locaux ne pourront pas se connecter au gestionnaire de locataires ou à l'API de gestion des locataires, bien qu'ils puissent utiliser des applications clientes pour accéder aux ressources du locataire, en fonction des autorisations de groupe.

Avant de commencer

- Vous êtes connecté au Gestionnaire de locataires à l'aide d'un "navigateur web pris en charge".
- Vous appartenez à un groupe d'utilisateurs qui possède le "Autorisation d'accès racine".
- Si votre compte locataire dispose de l'autorisation **utiliser la connexion de fédération de grille**, vous avez examiné le flux de travail et les considérations pour "clonage de groupes de locataires et d'utilisateurs", et vous êtes connecté à la grille source du locataire.

Créez un utilisateur local

Vous pouvez créer un utilisateur local et l'affecter à un ou plusieurs groupes locaux pour contrôler leurs autorisations d'accès.

Les utilisateurs S3 qui n'appartiennent à aucun groupe ne disposent pas d'autorisations de gestion ni de règles de groupe S3 qui leur sont appliquées. Il est possible que les utilisateurs bénéficient d'un accès par compartiment S3 accordé via une règle de compartiment.

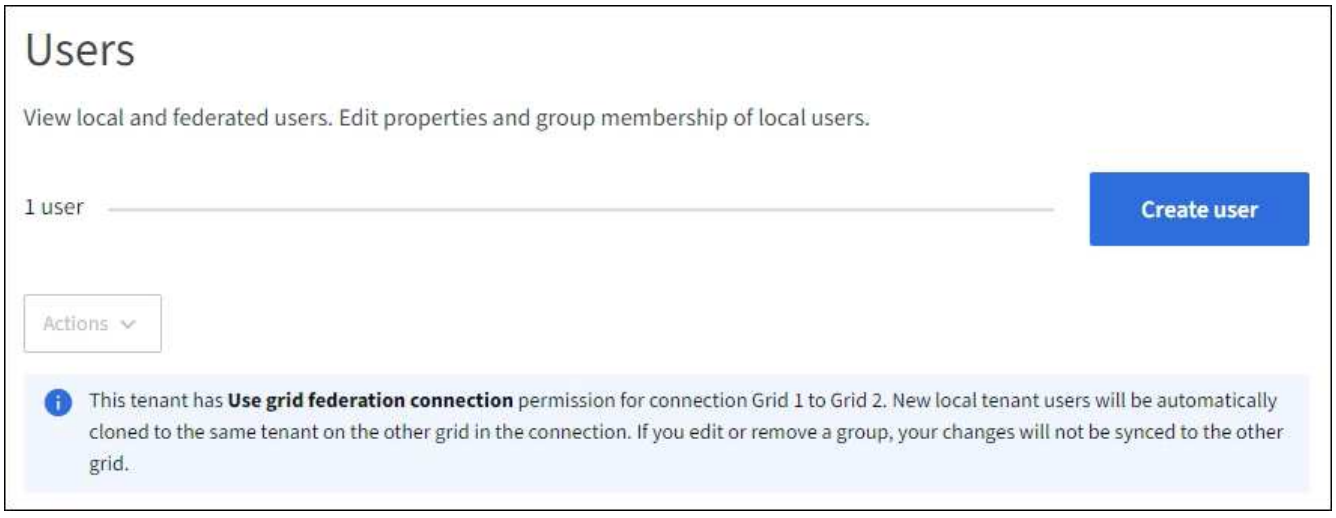
Les utilisateurs Swift qui n'appartiennent à aucun groupe ne disposent d'aucune autorisation de gestion ou d'un accès au conteneur Swift.

Accédez à l'assistant de création d'utilisateur

Étapes

1. Sélectionnez **ACCESS MANAGEMENT** > **Users**.

   Si votre compte de locataire dispose de l'autorisation **utiliser la connexion de fédération de grille**, une bannière bleue indique qu'il s'agit de la grille source du locataire. Tous les utilisateurs locaux que vous créez sur cette grille seront clonés dans l'autre grille de la connexion.



2. Sélectionnez **Créer utilisateur**.

Entrez les informations d'identification

Étapes

1. Pour l'étape **entrer les informations d'identification de l'utilisateur**, renseignez les champs suivants.

Champ	Description
Nom complet	Le nom complet de cet utilisateur, par exemple le prénom et le nom d'une personne ou le nom d'une application.
Nom d'utilisateur	Nom que cet utilisateur utilisera pour se connecter. Les noms d'utilisateur doivent être uniques et ne peuvent pas être modifiés. **Remarque** : si votre compte locataire dispose de l'autorisation **utiliser la connexion de fédération de grille**, une erreur de clonage se produit si le même **Nom d'utilisateur** existe déjà pour le locataire sur la grille de destination.
Mot de passe et confirmer le mot de passe	Le mot de passe que l'utilisateur utilisera lors de sa connexion.
Refuser l'accès	Sélectionnez **Oui** pour empêcher cet utilisateur de se connecter au compte de tenant, même s'il appartient toujours à un ou plusieurs groupes. Par exemple, sélectionnez **Oui** pour suspendre temporairement la capacité d'un utilisateur à se connecter.

2. Sélectionnez **Continuer**.

Affecter à des groupes

Étapes

1. Attribuez l'utilisateur à un ou plusieurs groupes locaux pour déterminer les tâches qu'ils peuvent effectuer.

   L'attribution d'un utilisateur à des groupes est facultative. Si vous le souhaitez, vous pouvez sélectionner des utilisateurs lorsque vous créez ou modifiez des groupes.

   Les utilisateurs qui n'appartiennent à aucun groupe ne disposent d'aucune autorisation de gestion. Les autorisations sont cumulatives. Les utilisateurs disposent de toutes les autorisations pour tous les groupes auxquels ils appartiennent. Voir "Autorisations de gestion des locataires".

2. Sélectionnez **Créer utilisateur**.

   Si votre compte locataire dispose de l'autorisation **utiliser la connexion de fédération de grille** et que vous êtes sur la grille source du locataire, le nouvel utilisateur local est cloné dans la grille de destination du locataire. **Succès** apparaît comme l'état **clonage** dans la section vue d'ensemble de la page de détails de l'utilisateur.

3. Sélectionnez **Terminer** pour revenir à la page utilisateurs.

Afficher ou modifier un utilisateur local

Étapes

1. Sélectionnez **ACCESS MANAGEMENT** > **Users**.
2. Consultez les informations fournies sur la page utilisateurs, qui répertorie les informations de base pour tous les utilisateurs locaux et fédérés pour ce compte de tenant.

   Si le compte de tenant dispose de l'autorisation **utiliser la connexion de fédération de grille** et que vous affichez l'utilisateur sur la grille source du locataire, une bannière bleue indique que si vous modifiez ou supprimez l'utilisateur, vos modifications ne seront pas synchronisées avec l'autre grille.

3. Si vous souhaitez modifier le nom complet de l'utilisateur :
   a. Cochez la case de l'utilisateur.
   b. Sélectionnez **actions** > **Modifier le nom complet**.
   c. Saisissez le nouveau nom.
   d. Sélectionnez **Enregistrer les modifications.**
4. Si vous souhaitez afficher plus de détails ou apporter des modifications supplémentaires, effectuez l'une des opérations suivantes :
   - Sélectionnez le nom d'utilisateur.
   - Cochez la case de l'utilisateur et sélectionnez **actions** > **Afficher les détails de l'utilisateur**.
5. Consultez la section Présentation, qui présente les informations suivantes pour chaque utilisateur :
   - Nom complet
   - Nom d'utilisateur
   - Type d'utilisateur
   - Accès refusé
   - Mode d'accès
   - Appartenance à un groupe
   - Champs supplémentaires si le compte de tenant dispose de l'autorisation **utiliser la connexion de fédération de grille** et que vous affichez l'utilisateur sur la grille source du locataire :
     - État de clonage, soit **succès** soit **échec**
     - Une bannière bleue indiquant que si vous modifiez cet utilisateur, vos modifications ne seront pas synchronisées avec l'autre grille.
6. Modifiez les paramètres utilisateur selon vos besoins. Voir Créer un utilisateur local pour plus d'informations sur ce que vous devez saisir.
   a. Dans la section vue d'ensemble, modifiez le nom complet en sélectionnant le nom ou l'icône de modification .

      Vous ne pouvez pas modifier le nom d'utilisateur.

   b. Dans l'onglet **Mot de passe**, modifiez le mot de passe de l'utilisateur et sélectionnez **Enregistrer les modifications**.
   c. Dans l'onglet **accès**, sélectionnez **non** pour permettre à l'utilisateur de se connecter ou sélectionnez **Oui** pour empêcher l'utilisateur de se connecter. Sélectionnez ensuite **Enregistrer les modifications**.
   d. Dans l'onglet **clés d'accès**, sélectionnez **Créer une clé** et suivez les instructions de "Création des clés d'accès S3 d'un autre utilisateur".

e. Dans l'onglet **groupes**, sélectionnez **Modifier les groupes** pour ajouter l'utilisateur à des groupes ou supprimer l'utilisateur des groupes. Sélectionnez ensuite **Enregistrer les modifications**.

7. Confirmez que vous avez sélectionné **Enregistrer les modifications** pour chaque section que vous avez modifiée.

Dupliquer l'utilisateur local

Vous pouvez dupliquer un utilisateur local pour créer un nouvel utilisateur plus rapidement.

> Si votre compte locataire dispose de l'autorisation **utiliser la connexion de fédération de grille** et que vous dupliquez un utilisateur de la grille source du locataire, l'utilisateur dupliqué sera cloné dans la grille de destination du locataire.

Étapes

1. Sélectionnez **ACCESS MANAGEMENT** > **Users**.
2. Cochez la case correspondant à l'utilisateur que vous souhaitez dupliquer.
3. Sélectionnez **actions** > **Dupliquer utilisateur**.
4. Voir Créer un utilisateur local pour plus d'informations sur ce que vous devez saisir.
5. Sélectionnez **Créer utilisateur**.

Supprimez un ou plusieurs utilisateurs locaux

Vous pouvez supprimer définitivement un ou plusieurs utilisateurs locaux qui n'ont plus besoin d'accéder au compte de locataire StorageGRID.

> Si votre compte de tenant dispose de l'autorisation **utiliser la connexion de fédération de grille** et que vous supprimez un utilisateur local, StorageGRID ne supprimera pas l'utilisateur correspondant sur l'autre grille. Si vous devez conserver ces informations synchronisées, vous devez supprimer le même utilisateur des deux grilles.

> Vous devez utiliser le référentiel d'identité fédéré pour supprimer des utilisateurs fédérés.

Étapes

1. Sélectionnez **ACCESS MANAGEMENT** > **Users**.
2. Cochez la case correspondant à chaque utilisateur à supprimer.
3. Sélectionnez **actions** > **Supprimer utilisateur** ou **actions** > **Supprimer utilisateurs**.

   Une boîte de dialogue de confirmation s'affiche.

4. Sélectionnez **Supprimer utilisateur** ou **Supprimer utilisateurs**.

Gestion des clés d'accès S3

Présentation de la gestion des clés d'accès S3

Chaque utilisateur d'un compte de locataire S3 doit disposer d'une clé d'accès pour stocker et récupérer des objets dans le système StorageGRID. Une clé d'accès se compose d'un ID de clé d'accès et d'une clé d'accès secrète.

Les clés d'accès S3 peuvent être gérées de la manière suivante :

- Les utilisateurs disposant de l'autorisation **gérer vos propres informations d'identification S3** peuvent créer ou supprimer leurs propres clés d'accès S3.
- Les utilisateurs disposant de l'autorisation **Root Access** peuvent gérer les clés d'accès du compte root S3 et de tous les autres utilisateurs. Les clés d'accès racine offrent un accès complet à toutes les compartiments et objets du locataire, sauf si une règle de compartiment est explicitement désactivée.

StorageGRID prend en charge l'authentification Signature version 2 et Signature version 4. L'accès entre comptes n'est pas autorisé sauf si cette règle est explicitement activée par une règle de compartiment.

Créez vos propres clés d'accès S3

Si vous utilisez un locataire S3 et que vous disposez de l'autorisation appropriée, vous pouvez créer vos propres clés d'accès S3. Vous devez disposer d'une clé d'accès pour accéder à vos compartiments et objets.

Avant de commencer

- Vous êtes connecté au Gestionnaire de locataires à l'aide d'un "navigateur web pris en charge".
- Vous appartenez à un groupe d'utilisateurs qui possède le "Gérez vos propres informations d'identification S3 ou autorisations d'accès racine".

Description de la tâche

Vous pouvez créer une ou plusieurs clés d'accès S3 qui vous permettent de créer et de gérer des compartiments pour votre compte de locataire. Après avoir créé une nouvelle clé d'accès, mettez à jour l'application avec votre nouvel ID de clé d'accès et votre clé d'accès secrète. Pour des raisons de sécurité, ne créez pas plus de clés que nécessaire et supprimez les clés que vous n'utilisez pas. Si vous n'avez qu'une seule clé et que vous êtes sur le point d'expirer, créez une nouvelle clé avant l'expiration de l'ancienne, puis supprimez l'ancienne.

Chaque clé peut avoir une heure d'expiration spécifique ou pas d'expiration. Suivez les directives ci-dessous pour l'heure d'expiration :

- Définissez une durée d'expiration pour vos clés afin de limiter votre accès à une certaine période. La définition d'un délai d'expiration court peut vous aider à réduire le risque si votre ID de clé d'accès et votre clé secrète sont exposés accidentellement. Les clés expirées sont supprimées automatiquement.
- Si le risque de sécurité dans votre environnement est faible et que vous n'avez pas besoin de créer régulièrement de nouvelles clés, vous n'avez pas besoin de définir une heure d'expiration pour vos clés. Si vous décidez plus tard de créer de nouvelles clés, supprimez les anciennes clés manuellement.

> Vous pouvez accéder aux compartiments S3 et aux objets appartenant à votre compte à l'aide de l'ID de clé d'accès et de la clé secrète affichée pour votre compte dans le Gestionnaire des locataires. Pour cette raison, protégez les clés d'accès comme vous le feriez avec un mot de passe. Faites pivoter les clés d'accès régulièrement, supprimez les clés inutilisées de votre compte et ne les partagez jamais avec d'autres utilisateurs.

Étapes

1. Sélectionnez **STORAGE (S3)** > **Mes clés d'accès**.

   La page Mes touches d'accès s'affiche et répertorie toutes les clés d'accès existantes.

2. Sélectionnez **Créer clé**.
3. Effectuez l'une des opérations suivantes :
   - Sélectionnez **ne définissez pas d'heure d'expiration** pour créer une clé qui n'expire pas. (Valeur par défaut)
   - Sélectionnez **définissez une heure d'expiration** et définissez la date et l'heure d'expiration.

   > La date d'expiration peut être au maximum de cinq ans à compter de la date actuelle. La durée d'expiration peut être d'au moins une minute à partir de l'heure actuelle.

4. Sélectionnez **Créer une clé d'accès**.

   La boîte de dialogue Télécharger la clé d'accès s'affiche, avec la liste de votre ID de clé d'accès et de votre clé secrète d'accès.

5. Copiez l'ID de la clé d'accès et la clé secrète dans un emplacement sûr, ou sélectionnez **Download .csv** pour enregistrer un fichier de feuille de calcul contenant l'ID de la clé d'accès et la clé secrète d'accès.

   > Ne fermez pas cette boîte de dialogue tant que vous n'avez pas copié ou téléchargé ces informations. Vous ne pouvez pas copier ou télécharger de clés après la fermeture de la boîte de dialogue.

6. Sélectionnez **Terminer**.

   La nouvelle clé apparaît sur la page Mes clés d'accès.

7. Si votre compte de locataire dispose de l'autorisation **utiliser la connexion de fédération grid**, vous pouvez utiliser l'API de gestion des locataires pour cloner manuellement les clés d'accès S3 du locataire de la grille source vers le locataire de la grille de destination. Voir "Cloner les clés d'accès S3 à l'aide de l'API".

Affichez vos clés d'accès S3

Si vous utilisez un locataire S3 et que vous disposez des autorisations appropriées, vous pouvez afficher la liste de vos clés d'accès S3. Vous pouvez trier la liste en fonction de l'heure d'expiration afin de déterminer quelles clés vont bientôt expirer. Si nécessaire, c'est possible "créer de nouvelles clés" ou "supprimer les clés" que vous n'utilisez plus.

> Vous pouvez accéder aux compartiments S3 et aux objets appartenant à votre compte à l'aide de l'ID de clé d'accès et de la clé secrète affichée pour votre compte dans le Gestionnaire des locataires. Pour cette raison, protégez les clés d'accès comme vous le feriez avec un mot de passe. Faites pivoter les clés d'accès régulièrement, supprimez les clés inutilisées de votre compte et ne les partagez jamais avec d'autres utilisateurs.

Avant de commencer

- Vous êtes connecté au Gestionnaire de locataires à l'aide d'un "navigateur web pris en charge".
- Vous appartenez à un groupe d'utilisateurs disposant des informations d'identification Manage your own S3 "permission".

Étapes

1. Sélectionnez **STORAGE (S3)** > **Mes clés d'accès**.

2. À partir de la page Mes clés d'accès, triez toutes les clés d'accès existantes par **heure d'expiration** ou **ID de clé d'accès**.
3. Au besoin, créez de nouvelles clés ou supprimez les clés que vous n'utilisez plus.

   Si vous créez de nouvelles clés avant l'expiration des clés existantes, vous pouvez commencer à utiliser les nouvelles clés sans perdre temporairement l'accès aux objets du compte.

   Les clés expirées sont supprimées automatiquement.

Supprimez vos propres clés d'accès S3

Si vous utilisez un locataire S3 et que vous disposez des autorisations appropriées, vous pouvez supprimer vos propres clés d'accès S3. Une fois la clé d'accès supprimée, elle ne peut plus être utilisée pour accéder aux objets et aux compartiments du compte du locataire.

Avant de commencer

- Vous êtes connecté au Gestionnaire de locataires à l'aide d'un "navigateur web pris en charge".
- Vous disposez de l'autorisation gérer vos propres informations d'identification S3. Voir "Autorisations de gestion des locataires".

> Vous pouvez accéder aux compartiments S3 et aux objets appartenant à votre compte à l'aide de l'ID de clé d'accès et de la clé secrète affichée pour votre compte dans le Gestionnaire des locataires. Pour cette raison, protégez les clés d'accès comme vous le feriez avec un mot de passe. Faites pivoter les clés d'accès régulièrement, supprimez les clés inutilisées de votre compte et ne les partagez jamais avec d'autres utilisateurs.

Étapes

1. Sélectionnez **STORAGE (S3)** > **Mes clés d'accès**.
2. Sur la page Mes clés d'accès, cochez la case correspondant à chaque clé d'accès que vous souhaitez supprimer.
3. Sélectionnez **Supprimer la touche**.
4. Dans la boîte de dialogue de confirmation, sélectionnez **touche Suppr**.

   Un message de confirmation s'affiche dans le coin supérieur droit de la page.

Créez les clés d'accès S3 d'un autre utilisateur

Si vous utilisez un locataire S3 avec l'autorisation appropriée, vous pouvez créer des clés d'accès S3 pour d'autres utilisateurs, comme les applications qui ont besoin d'accéder à des compartiments et des objets.

Avant de commencer

- Vous êtes connecté au Gestionnaire de locataires à l'aide d'un "navigateur web pris en charge".
- Vous appartenez à un groupe d'utilisateurs qui possède le "Autorisation d'accès racine".

Description de la tâche

Vous pouvez créer une ou plusieurs clés d'accès S3 pour les autres utilisateurs afin qu'ils puissent créer et

gérer des compartiments pour leur compte de locataire. Après avoir créé une nouvelle clé d'accès, mettez à jour l'application avec le nouvel ID de clé d'accès et la clé d'accès secrète. Pour des raisons de sécurité, ne créez pas plus de clés que les besoins de l'utilisateur et supprimez les clés qui ne sont pas utilisées. Si vous n'avez qu'une seule clé et que vous êtes sur le point d'expirer, créez une nouvelle clé avant l'expiration de l'ancienne, puis supprimez l'ancienne.

Chaque clé peut avoir une heure d'expiration spécifique ou pas d'expiration. Suivez les directives ci-dessous pour l'heure d'expiration :

- Définissez un délai d'expiration pour les clés afin de limiter l'accès de l'utilisateur à une certaine période. La définition d'un délai d'expiration court peut aider à réduire le risque si l'ID de clé d'accès et la clé secrète sont exposés accidentellement. Les clés expirées sont supprimées automatiquement.
- Si le risque de sécurité dans votre environnement est faible et que vous n'avez pas besoin de créer régulièrement de nouvelles clés, vous n'avez pas besoin de définir une heure d'expiration pour les clés. Si vous décidez plus tard de créer de nouvelles clés, supprimez les anciennes clés manuellement.

> Les compartiments S3 et les objets appartenant à un utilisateur sont accessibles à l'aide de l'ID de clé d'accès et de la clé secrète affichée pour cet utilisateur dans le Gestionnaire de locataires. Pour cette raison, protégez les clés d'accès comme vous le feriez avec un mot de passe. Faites pivoter les clés d'accès régulièrement, supprimez les clés inutilisées du compte et ne les partagez jamais avec d'autres utilisateurs.

Étapes

1. Sélectionnez **ACCESS MANAGEMENT** > **Users**.
2. Sélectionnez l'utilisateur dont vous souhaitez gérer les clés d'accès S3.

   La page de détails utilisateur s'affiche.

3. Sélectionnez **touches d'accès**, puis **touche Créer**.
4. Effectuez l'une des opérations suivantes :
   - Sélectionnez **ne pas définir de délai d'expiration** pour créer une clé qui n'expire pas. (Valeur par défaut)
   - Sélectionnez **définissez une heure d'expiration** et définissez la date et l'heure d'expiration.

     > La date d'expiration peut être au maximum de cinq ans à compter de la date actuelle. La durée d'expiration peut être d'au moins une minute à partir de l'heure actuelle.

5. Sélectionnez **Créer une clé d'accès**.

   La boîte de dialogue Télécharger la clé d'accès s'affiche, avec la liste de l'ID de clé d'accès et de la clé secrète.

6. Copiez l'ID de la clé d'accès et la clé secrète dans un emplacement sûr, ou sélectionnez **Download .csv** pour enregistrer un fichier de feuille de calcul contenant l'ID de la clé d'accès et la clé secrète d'accès.

   > Ne fermez pas cette boîte de dialogue tant que vous n'avez pas copié ou téléchargé ces informations. Vous ne pouvez pas copier ou télécharger de clés après la fermeture de la boîte de dialogue.

7. Sélectionnez **Terminer**.

La nouvelle clé est répertoriée dans l'onglet touches d'accès de la page des détails de l'utilisateur.

8. Si votre compte de locataire dispose de l'autorisation **utiliser la connexion de fédération grid**, vous pouvez utiliser l'API de gestion des locataires pour cloner manuellement les clés d'accès S3 du locataire de la grille source vers le locataire de la grille de destination. Voir "Cloner les clés d'accès S3 à l'aide de l'API".

Afficher les clés d'accès S3 d'un autre utilisateur

Si vous utilisez un locataire S3 et que vous disposez des autorisations appropriées, vous pouvez afficher les clés d'accès S3 d'un autre utilisateur. Vous pouvez trier la liste par heure d'expiration pour déterminer quelles clés vont bientôt expirer. Au besoin, vous pouvez créer de nouvelles clés et supprimer des clés qui ne sont plus utilisées.

Avant de commencer

- Vous êtes connecté au Gestionnaire de locataires à l'aide d'un "navigateur web pris en charge".
- Vous disposez de l'autorisation d'accès racine.

> Les compartiments S3 et les objets appartenant à un utilisateur sont accessibles à l'aide de l'ID de clé d'accès et de la clé secrète affichée pour cet utilisateur dans le Gestionnaire de locataires. Pour cette raison, protégez les clés d'accès comme vous le feriez avec un mot de passe. Faites pivoter les clés d'accès régulièrement, supprimez les clés inutilisées du compte et ne les partagez jamais avec d'autres utilisateurs.

Étapes

1. Sélectionnez **ACCESS MANAGEMENT** > **Users**.
2. Sur la page utilisateurs, sélectionnez l'utilisateur dont vous souhaitez afficher les clés d'accès S3.
3. Dans la page Détails de l'utilisateur, sélectionnez **touches d'accès**.
4. Trier les clés par **heure d'expiration** ou **ID de clé d'accès**.
5. Si nécessaire, créez de nouvelles clés et supprimez manuellement les clés que le n'est plus utilisé.

   Si vous créez de nouvelles clés avant l'expiration des clés existantes, l'utilisateur peut commencer à utiliser les nouvelles clés sans perdre temporairement l'accès aux objets du compte.

   Les clés expirées sont supprimées automatiquement.

Informations associées

"Créez les clés d'accès S3 d'un autre utilisateur"

"Supprimez les clés d'accès S3 d'un autre utilisateur"

Supprimez les clés d'accès S3 d'un autre utilisateur

Si vous utilisez un locataire S3 et que vous disposez des autorisations appropriées, vous pouvez supprimer les clés d'accès S3 d'un autre utilisateur. Une fois la clé d'accès supprimée, elle ne peut plus être utilisée pour accéder aux objets et aux compartiments du compte du locataire.

Avant de commencer

- Vous êtes connecté au Gestionnaire de locataires à l'aide d'un "navigateur web pris en charge".
- Vous disposez de l'autorisation d'accès racine. Voir "Autorisations de gestion des locataires".

> Les compartiments S3 et les objets appartenant à un utilisateur sont accessibles à l'aide de l'ID de clé d'accès et de la clé secrète affichée pour cet utilisateur dans le Gestionnaire de locataires. Pour cette raison, protégez les clés d'accès comme vous le feriez avec un mot de passe. Faites pivoter les clés d'accès régulièrement, supprimez les clés inutilisées du compte et ne les partagez jamais avec d'autres utilisateurs.

Étapes

1. Sélectionnez **ACCESS MANAGEMENT** > **Users**.
2. Sur la page utilisateurs, sélectionnez l'utilisateur dont vous souhaitez gérer les clés d'accès S3.
3. Sur la page Détails de l'utilisateur, sélectionnez **touches d'accès**, puis cochez la case correspondant à chaque clé d'accès que vous souhaitez supprimer.
4. Sélectionnez **actions** > **Supprimer la touche sélectionnée**.
5. Dans la boîte de dialogue de confirmation, sélectionnez **touche Suppr**.

   Un message de confirmation s'affiche dans le coin supérieur droit de la page.

Gestion des compartiments S3

Créer un compartiment S3

Vous pouvez utiliser le Gestionnaire des locataires pour créer des compartiments S3 pour les données d'objet.

Avant de commencer

- Vous êtes connecté au Gestionnaire de locataires à l'aide d'un "navigateur web pris en charge".
- Vous appartenez à un groupe d'utilisateurs disposant de l'accès racine ou de la fonction gérer tous les compartiments "permission". Ces autorisations remplacent les paramètres d'autorisations des stratégies de groupes ou de compartiments.

  > Les autorisations de définir ou de modifier les propriétés de verrouillage d'objet S3 des compartiments ou des objets peuvent être accordées par "politique de compartiment ou règle de groupe".

- Si vous prévoyez d'activer le verrouillage objet S3 pour un compartiment, un administrateur du grid a activé le paramètre de verrouillage objet S3 global pour le système StorageGRID. Vous avez également passé en revue les exigences relatives aux compartiments et aux objets S3 Object Lock. Voir "Utilisez le verrouillage d'objet S3 pour conserver les objets".

Accéder à l'assistant

Étapes

1. Sélectionnez **Afficher les compartiments** dans le tableau de bord ou sélectionnez **STOCKAGE (S3)** > **compartiments**.
2. Sélectionnez **Créer un compartiment**.

Entrez les détails

Étapes

1. Entrez les détails du compartiment.

Champ	Description
Nom du compartiment	Nom du compartiment conforme aux règles suivantes : • Il doit être unique sur chaque système StorageGRID (et pas seulement au sein du compte du locataire). • Doit être conforme DNS. • Doit contenir au moins 3 caractères et pas plus de 63 caractères. • Chaque étiquette doit commencer et se terminer par une lettre ou un chiffre en minuscules et ne peut utiliser que des lettres minuscules, des chiffres et des tirets. • Ne doit pas utiliser de périodes dans des demandes de type hébergement virtuel. Les périodes provoquera des problèmes avec la vérification du certificat générique du serveur. Pour plus d'informations, reportez-vous à la section "Documentation Amazon Web Services (AWS) sur les règles d'attribution de nom de compartiment". **Remarque** : vous ne pouvez pas modifier le nom du compartiment après avoir créé le compartiment.
Région	La région du godet. L'administrateur StorageGRID gère les régions disponibles. Ce compartiment peut affecter la règle de protection des données appliquée aux objets. Par défaut, tous les compartiments sont créés dans le `us-east-1` région. **Remarque** : vous ne pouvez pas modifier la région après avoir créé le compartiment.

2. Sélectionnez **Continuer**.

Gestion des paramètres d'objet

Étapes

1. Activez éventuellement le contrôle de version d'objet pour le compartiment.

   Activez la gestion des versions d'objet si vous souhaitez stocker chaque version de chaque objet dans ce compartiment. Vous pouvez ensuite récupérer les versions précédentes d'un objet si nécessaire. Vous devez activer la gestion des versions d'objet si le compartiment est utilisé pour la réplication entre plusieurs grilles.

2. Si le paramètre global S3 Object Lock est activé, activez éventuellement S3 Object Lock pour que le compartiment stocke des objets à l'aide d'un modèle WORM (Write-once-read-many).

   Activez le verrouillage des objets S3 pour un compartiment uniquement si vous devez conserver les objets pendant une durée fixe, par exemple, pour répondre à certaines exigences réglementaires. Le verrouillage

objet S3 est un paramètre permanent qui vous permet d'empêcher la suppression ou l'écrasement d'objets pendant une durée fixe ou indéfiniment.

> Une fois le paramètre S3 Object Lock activé pour un compartiment, il ne peut pas être désactivé. Toute personne disposant des autorisations appropriées peut ajouter à ce compartiment des objets qui ne peuvent pas être modifiés. Il se peut que vous ne puissiez pas supprimer ces objets ou le compartiment lui-même.

Si vous activez le verrouillage des objets S3 pour un compartiment, le contrôle de version des compartiments est automatiquement activé.

3. Si vous avez sélectionné **Activer le verrouillage d'objet S3**, vous pouvez activer **rétention par défaut** pour ce compartiment.

   Lorsque **Default Retention** est activé, les nouveaux objets ajoutés au compartiment sont automatiquement protégés contre la suppression ou l'écrasement. Le paramètre **rétention par défaut** ne s'applique pas aux objets qui ont leurs propres périodes de rétention.

   a. Si **Default Retention** est activé, spécifiez un **mode de rétention par défaut** pour le compartiment.

Mode de rétention par défaut	Description
La conformité	• L'objet ne peut pas être supprimé tant que sa date de conservation jusqu'à n'est pas atteinte. • La date de conservation de l'objet peut être augmentée, mais elle ne peut pas être réduite. • La date de conservation de l'objet jusqu'à ne peut pas être supprimée tant que cette date n'est pas atteinte.
La gouvernance	• Utilisateurs avec le `s3:BypassGovernanceRetention` l'autorisation peut utiliser le `x-amz-bypass-governance-retention: true` demander à l'en-tête de contourner les paramètres de rétention. • Ces utilisateurs peuvent supprimer une version d'objet avant d'atteindre sa date de conservation jusqu'à. • Ces utilisateurs peuvent augmenter, diminuer ou supprimer la date de conservation d'un objet.

   b. Si **Default Retention** est activé, spécifiez la **période de rétention par défaut** pour le compartiment.

      La **période de conservation par défaut** indique la durée pendant laquelle les nouveaux objets ajoutés à ce compartiment doivent être conservés, à partir du moment où ils sont ingérés. Spécifiez une valeur comprise entre 1 et 36,500 jours ou entre 1 et 100 ans.

4. Sélectionnez **Créer un compartiment**.

   Le godet est créé et ajouté au tableau sur la page godets.

5. Si vous le souhaitez, sélectionnez **aller à la page des détails du compartiment** à "afficher les détails du compartiment" et effectuer une configuration supplémentaire.

Afficher les détails du compartiment

Vous pouvez afficher les compartiments de votre compte de locataire.

Avant de commencer

- Vous êtes connecté au Gestionnaire de locataires à l'aide d'un "navigateur web pris en charge".

Étapes

1. Sélectionnez **Afficher les compartiments** dans le tableau de bord ou sélectionnez **STOCKAGE (S3)** > **compartiments**.

   La page compartiments s'affiche.

2. Passez en revue les informations récapitulatives pour chaque compartiment.

   Si nécessaire, vous pouvez trier les informations par colonne, ou vous pouvez avancer et revenir à la liste.

   > Les valeurs nombre d'objets et espace utilisé affichées sont des estimations. Ces estimations sont affectées par le moment de l'ingestion, la connectivité réseau et l'état des nœuds. Si la gestion des versions des compartiments est activée, les versions des objets supprimés sont incluses dans le nombre d'objets.

Colonne	Description
Nom	Nom unique du compartiment, qui ne peut pas être modifié.
Fonctionnalités activées	Liste des fonctions activées pour le compartiment.
Verrouillage d'objet S3	Indique si le verrouillage d'objet S3 est activé pour le compartiment. Cette colonne apparaît uniquement si le verrouillage objet S3 est activé pour la grille. Cette colonne affiche également des informations pour tous les compartiments conformes existants.
Région	La région du compartiment, qui ne peut pas être modifiée.
Nombre d'objets	Nombre d'objets dans ce compartiment. Lorsque des objets sont ajoutés ou supprimés, il est possible que cette valeur ne soit pas mise à jour immédiatement. Si la gestion des versions des compartiments est activée, les versions d'objets non actuelles sont incluses dans cette valeur.
Espace utilisé	Taille logique de tous les objets du compartiment. La taille logique n'inclut pas l'espace réel requis pour les copies répliquées ou avec code d'effacement, ni pour les métadonnées d'objet.
Date de création	Date et heure de création du compartiment.

3. Pour afficher les détails d'un compartiment spécifique, sélectionnez le nom du compartiment dans le tableau.

   La page des détails du compartiment s'affiche. À partir de cette page, vous pouvez effectuer les tâches

suivantes :

- Configurez et gérez des options de compartiment, notamment "niveau de cohérence", "mises à jour de l'heure du dernier accès", "gestion des versions d'objets", "Verrouillage d'objet S3" et "rétention de compartiments par défaut"
- Configurez l'accès au compartiment, par exemple "Partage des ressources d'origine croisée (CORS)"
- Gérez "services de plateforme" (si autorisé pour le locataire), y compris la réplication, les notifications d'événements et l'intégration de la recherche
- Activer et "gérer la réplication entre les grilles" (Si le locataire est autorisé) pour répliquer les objets ingérés dans ce compartiment vers un autre système StorageGRID
- Accédez au "Console S3 expérimentale" pour gérer les objets dans le compartiment
- "Supprime tous les objets d'un compartiment"
- "Supprimer un compartiment" c'est déjà vide

Modifiez le niveau de cohérence d'un compartiment

Si vous utilisez un locataire S3, vous pouvez modifier le niveau de cohérence des opérations effectuées sur les objets dans des compartiments S3.

Avant de commencer

- Vous êtes connecté au Gestionnaire de locataires à l'aide d'un "navigateur web pris en charge".
- Vous appartenez à un groupe d'utilisateurs qui possède le "Gérez tous les compartiments ou l'autorisation d'accès racine". Ces autorisations remplacent les paramètres d'autorisations des stratégies de groupes ou de compartiments.

Description de la tâche

Les contrôles de cohérence assurent un équilibre entre la disponibilité des objets et la cohérence de ces objets entre plusieurs nœuds de stockage et sites. En général, vous devez utiliser le niveau de cohérence **Read-After-New-write** pour vos compartiments.

Si le niveau de cohérence **Read-After-New-write** ne répond pas aux exigences de l'application client, vous pouvez modifier le niveau de cohérence en définissant le niveau de cohérence du compartiment ou en utilisant le `Consistency-Control` en-tête. Le `Consistency-Control` le cueilleur remplace le niveau de cohérence du godet.

> Lorsque vous modifiez le niveau de cohérence d'un compartiment, seuls les objets ingérées après la modification sont garantis pour satisfaire le niveau révisé.

Étapes

1. Sélectionnez **Afficher les compartiments** dans le tableau de bord ou sélectionnez **STOCKAGE (S3)** > **compartiments**.
2. Sélectionnez le nom du compartiment dans la table.

   La page des détails du compartiment s'affiche.

3. Dans l'onglet **Bucket options**, sélectionnez l'accordéon **Consistency level**.
4. Sélectionnez un niveau de cohérence pour les opérations effectuées sur les objets de ce compartiment.
   - **Tous** : fournit le plus haut niveau de cohérence. Tous les nœuds reçoivent les données immédiatement, sinon la requête échoue.

- **Strong-global** : garantit la cohérence lecture après écriture pour toutes les demandes client sur tous les sites.
- **Strong-site** : garantit la cohérence lecture après écriture pour toutes les demandes client au sein d'un site.
- **Read-After-New-write** (par défaut) : fournit une cohérence lecture-après-écriture pour les nouveaux objets et une cohérence éventuelle pour les mises à jour d'objets. Offre une haute disponibilité et une protection des données garanties. Recommandé dans la plupart des cas.
- **Disponible** : assure la cohérence finale pour les nouveaux objets et les mises à jour d'objets. Pour les compartiments S3, utilisez uniquement si nécessaire (par exemple, pour un compartiment qui contient des valeurs de journal rarement lues ou pour les opérations HEAD ou GET sur des clés qui n'existent pas). Non pris en charge pour les compartiments FabricPool S3.

5. Sélectionnez **Enregistrer les modifications**.

Activez ou désactivez les mises à jour de l'heure du dernier accès

Les administrateurs du grid créent les règles de gestion du cycle de vie des informations d'un système StorageGRID. Ils ont la possibilité de spécifier la date d'accès de dernier objet afin de déterminer si celui-ci doit être déplacé vers un autre emplacement de stockage. Si vous utilisez un locataire S3, vous pouvez activer ces règles en activant les mises à jour de l'heure du dernier accès pour les objets dans un compartiment S3.

Ces instructions s'appliquent uniquement aux systèmes StorageGRID qui incluent au moins une règle ILM utilisant l'option **Last Access Time** comme filtre avancé ou comme heure de référence. Vous pouvez ignorer ces instructions si votre système StorageGRID n'inclut pas une telle règle. Voir "Utiliser l'heure du dernier accès dans les règles ILM" pour plus d'informations.

Avant de commencer

- Vous êtes connecté au Gestionnaire de locataires à l'aide d'un "navigateur web pris en charge".
- Vous appartenez à un groupe d'utilisateurs qui possède le "Gérez tous les compartiments ou l'autorisation d'accès racine". Ces autorisations remplacent les paramètres d'autorisations des stratégies de groupes ou de compartiments.

Description de la tâche

Last Access Time est l'une des options disponibles pour l'instruction de placement **Reference Time** pour une règle ILM. La définition de l'heure de référence d'une règle sur heure du dernier accès permet aux administrateurs de la grille de spécifier que les objets doivent être placés dans certains emplacements de stockage en fonction du moment où ces objets ont été récupérés (lus ou affichés) pour la dernière fois.

Par exemple, pour s'assurer que les objets récemment affichés restent dans un stockage plus rapide, un administrateur du grid peut créer une règle ILM spécifiant ce qui suit :

- Les objets récupérés au cours du mois dernier doivent rester sur les nœuds de stockage locaux.
- Les objets qui n'ont pas été récupérés au cours du dernier mois doivent être déplacés vers un emplacement hors site.

Par défaut, les mises à jour de l'heure du dernier accès sont désactivées. Si votre système StorageGRID inclut une règle ILM qui utilise l'option **Last Access Time** et que vous souhaitez que cette option s'applique aux objets de ce compartiment, vous devez activer les mises à jour de l'heure du dernier accès pour les compartiments S3 spécifiés dans cette règle.

La mise à jour du dernier accès lors de l'extraction d'un objet peut réduire les performances du StorageGRID, en particulier pour les petits objets.

Un impact sur les performances se produit lors des mises à jour des temps de dernier accès, car StorageGRID doit effectuer ces étapes supplémentaires chaque fois que les objets sont récupérés :

- Mettre à jour les objets avec de nouveaux horodatages
- Ajoutez ces objets à la file d'attente ILM pour une réévaluation des règles et règles ILM actuelles

Le tableau récapitule le comportement appliqué à tous les objets du compartiment lorsque l'heure du dernier accès est désactivée ou activée.

Type de demande	Comportement si l'heure du dernier accès est désactivée (par défaut)		Comportement si l'heure du dernier accès est activée	
	Heure du dernier accès mise à jour ?	Objet ajouté à la file d'attente d'évaluation ILM ?	Heure du dernier accès mise à jour ?	Objet ajouté à la file d'attente d'évaluation ILM ?
Demande de récupération d'un objet, de sa liste de contrôle d'accès ou de ses métadonnées	Non	Non	Oui.	Oui.
Demande de mise à jour des métadonnées d'un objet	Oui.	Oui.	Oui.	Oui.
Demander de copier un objet d'un compartiment à un autre	• Non, pour la copie source • Oui, pour la copie de destination	• Non, pour la copie source • Oui, pour la copie de destination	• Oui, pour la copie source • Oui, pour la copie de destination	• Oui, pour la copie source • Oui, pour la copie de destination
Demander de terminer un téléchargement partitionné	Oui, pour l'objet assemblé	Oui, pour l'objet assemblé	Oui, pour l'objet assemblé	Oui, pour l'objet assemblé

Étapes

1. Sélectionnez **Afficher les compartiments** dans le tableau de bord ou sélectionnez **STOCKAGE (S3)** > **compartiments**.
2. Sélectionnez le nom du compartiment dans la table.

   La page des détails du compartiment s'affiche.

3. Dans l'onglet **Bucket options**, sélectionnez l'accordéon **Last Access Time Updates**.
4. Activer ou désactiver les mises à jour des heures du dernier accès.
5. Sélectionnez **Enregistrer les modifications**.

Modifiez le contrôle de version d'objet pour un compartiment

Si vous utilisez un locataire S3, vous pouvez modifier l'état de gestion des versions des compartiments S3.

Avant de commencer

- Vous êtes connecté au Gestionnaire de locataires à l'aide d'un "navigateur web pris en charge".
- Vous appartenez à un groupe d'utilisateurs qui possède le "Gérez tous les compartiments ou l'autorisation d'accès racine". Ces autorisations remplacent les paramètres d'autorisations des stratégies de groupes ou de compartiments.

Description de la tâche

Vous pouvez activer ou suspendre la gestion des versions d'objet pour un compartiment. Une fois que vous avez activé la gestion des versions pour un compartiment, il ne peut plus revenir à un état sans version. Toutefois, vous pouvez suspendre le contrôle de version du compartiment.

- Désactivé : le contrôle de version n'a jamais été activé
- Activé : la gestion des versions est activée
- Suspendu : la gestion des versions a déjà été activée et est suspendue

Pour plus d'informations, reportez-vous aux sections suivantes :

- "Gestion des versions d'objet"
- "Règles et règles ILM pour les objets avec version S3 (exemple 4)"
- "Comment supprimer les objets"

Étapes

1. Sélectionnez **Afficher les compartiments** dans le tableau de bord ou sélectionnez **STOCKAGE (S3)** > **compartiments**.
2. Sélectionnez le nom du compartiment dans la table.

   La page des détails du compartiment s'affiche.

3. Dans l'onglet **Bucket options**, sélectionnez l'accordéon **Object multiversion**.
4. Sélectionnez un état de gestion des versions pour les objets de ce compartiment.

   La gestion des versions d'objet doit rester activée pour un compartiment utilisé pour la réplication entre plusieurs grilles. Si le verrouillage d'objet S3 ou la conformité héritée est activée, les options **Object versionnage** sont désactivées.

Option	Description
Activez le contrôle des versions	Activez la gestion des versions d'objet si vous souhaitez stocker chaque version de chaque objet dans ce compartiment. Vous pouvez ensuite récupérer les versions précédentes d'un objet si nécessaire. Les objets qui se trouvent déjà dans le compartiment sont avec gestion de version lorsqu'ils sont modifiés par l'utilisateur.
Suspendre la gestion des versions	Suspendre la gestion des versions d'objet si vous ne souhaitez plus créer de nouvelles versions d'objet. Vous pouvez toujours récupérer toutes les versions d'objet existantes.

5. Sélectionnez **Enregistrer les modifications**.

Utilisez le verrouillage d'objet S3 pour conserver les objets

Vous pouvez utiliser le verrouillage objet S3 si les compartiments et les objets doivent respecter les exigences réglementaires en matière de conservation des données.

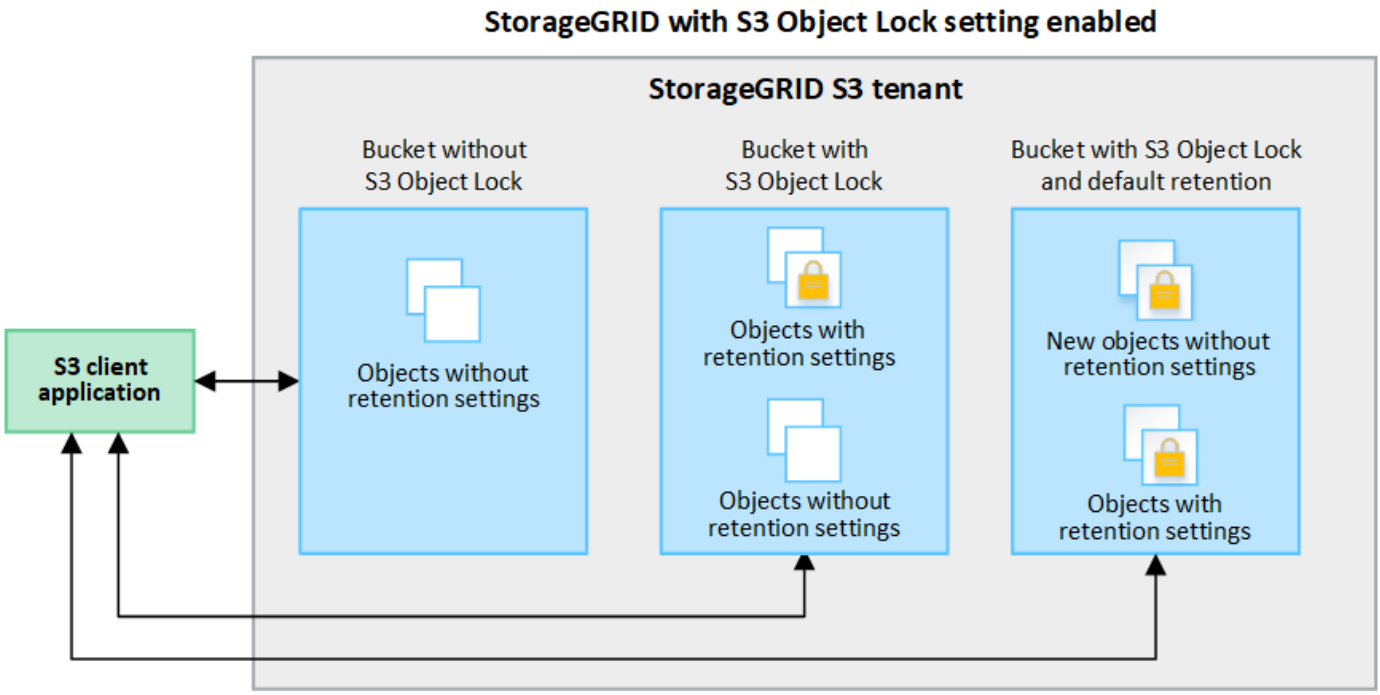
Qu'est-ce que le verrouillage objet S3 ?

La fonctionnalité de verrouillage objet StorageGRID S3 est une solution de protection des objets équivalente au verrouillage objet S3 dans Amazon simple Storage Service (Amazon S3).

Comme illustré dans la figure, lorsque le paramètre global de verrouillage d'objet S3 est activé pour un système StorageGRID, un compte de locataire S3 peut créer des compartiments avec ou sans verrouillage d'objet S3 activé. Si le verrouillage objet S3 est activé pour un compartiment, la gestion des versions de compartiment est requise et elle est automatiquement activée.

Si le verrouillage objet S3 est activé dans un compartiment, les applications client S3 peuvent spécifier des paramètres de conservation pour toute version d'objet enregistrée dans ce compartiment.

En outre, un compartiment dans lequel le verrouillage objet S3 est activé peut choisir entre un mode de conservation et une période de conservation par défaut. Les paramètres par défaut s'appliquent uniquement aux objets ajoutés au compartiment sans leurs propres paramètres de conservation.



Modes de rétention

La fonction de verrouillage d'objet StorageGRID S3 prend en charge deux modes de conservation pour appliquer différents niveaux de protection aux objets. Ces modes sont équivalents aux modes de conservation Amazon S3.

- En mode conformité :
  - L'objet ne peut pas être supprimé tant que sa date de conservation jusqu'à n'est pas atteinte.
  - La date de conservation de l'objet peut être augmentée, mais elle ne peut pas être réduite.
  - La date de conservation de l'objet jusqu'à ne peut pas être supprimée tant que cette date n'est pas atteinte.
- En mode gouvernance :
  - Les utilisateurs disposant d'une autorisation spéciale peuvent utiliser un en-tête de contournement dans les demandes pour modifier certains paramètres de conservation.
  - Ces utilisateurs peuvent supprimer une version d'objet avant d'atteindre sa date de conservation jusqu'à.
  - Ces utilisateurs peuvent augmenter, diminuer ou supprimer la date de conservation d'un objet.

Paramètres de conservation pour les versions d'objet

Si un compartiment est créé avec le verrouillage objet S3 activé, les utilisateurs peuvent utiliser l'application client S3 pour spécifier éventuellement les paramètres de conservation suivants pour chaque objet ajouté au compartiment :

- **Mode de conservation** : conformité ou gouvernance.
- **Conserver-jusqu'à-date**: Si la date de conservation d'une version d'objet est dans le futur, l'objet peut être récupéré, mais il ne peut pas être supprimé.
- **Mise en garde légale** : l'application d'une mise en garde légale à une version d'objet verrouille immédiatement cet objet. Par exemple, vous devrez peut-être mettre une obligation légale sur un objet lié

à une enquête ou à un litige juridique. Une obligation légale n'a pas de date d'expiration, mais reste en place jusqu'à ce qu'elle soit explicitement supprimée. Les dispositions légales sont indépendantes de la date de conservation.

> Si un objet fait l'objet d'une conservation légale, personne ne peut le supprimer, quel que soit son mode de conservation.

Pour plus d'informations sur les paramètres d'objet, reportez-vous à la section "Utilisez l'API REST S3 pour configurer le verrouillage objet S3".

Paramètre de rétention par défaut pour les compartiments

Si un compartiment est créé avec le verrouillage objet S3 activé, les utilisateurs peuvent spécifier les paramètres par défaut suivants pour le compartiment :

- **Mode de rétention par défaut** : conformité ou gouvernance.
- **Période de rétention par défaut** : durée pendant laquelle les nouvelles versions d'objets ajoutées à ce compartiment doivent être conservées, à partir du jour où elles sont ajoutées.

Les paramètres de compartiment par défaut s'appliquent uniquement aux nouveaux objets qui ne disposent pas de leurs propres paramètres de conservation. Les objets de compartiment existants ne sont pas affectés lorsque vous ajoutez ou modifiez ces paramètres par défaut.

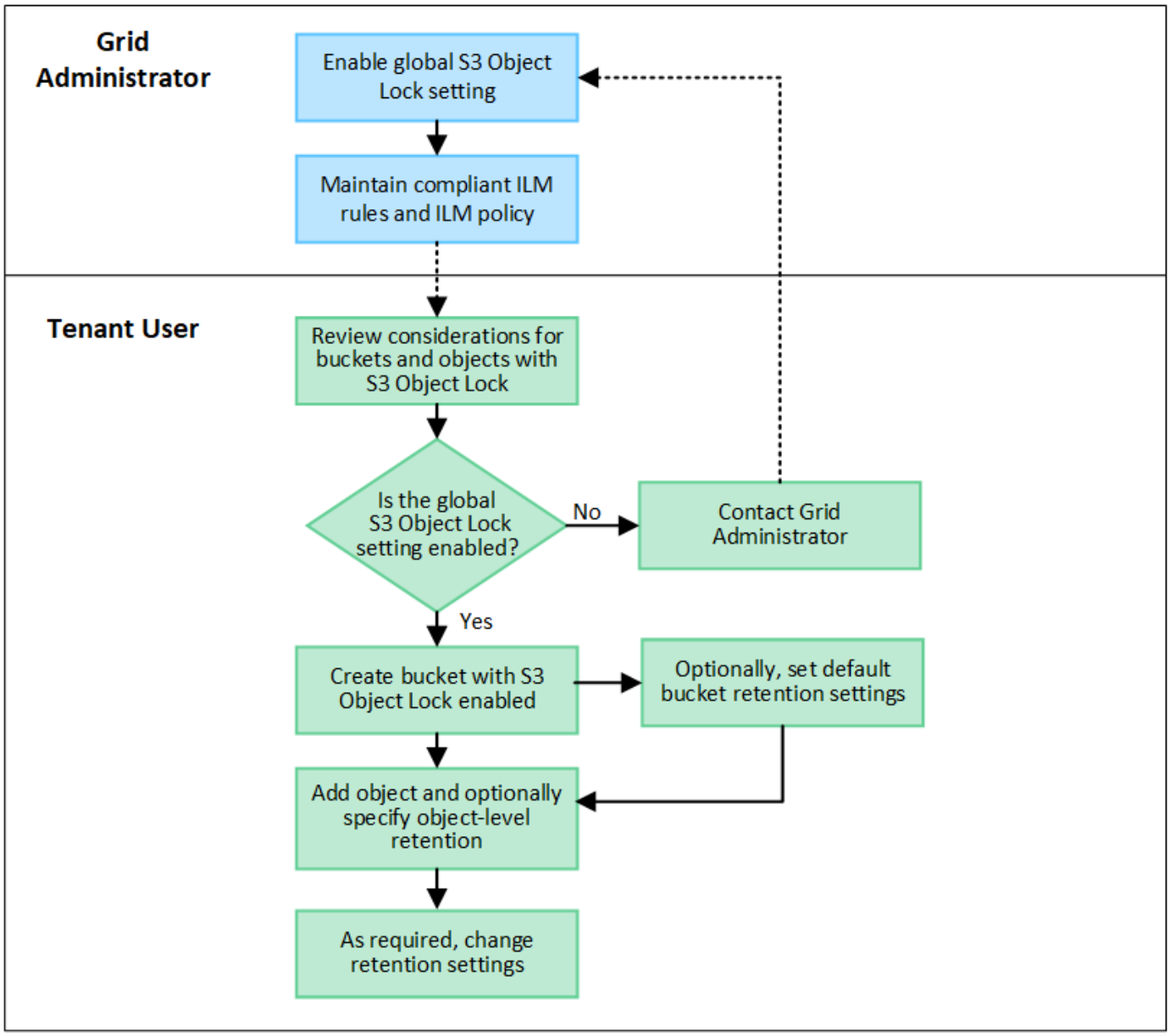
Voir "Créer un compartiment S3" et "Mettre à jour la conservation par défaut du verrouillage d'objet S3".

Workflow de verrouillage d'objet S3

Le schéma de workflow montre les étapes générales d'utilisation de la fonction de verrouillage d'objet S3 dans StorageGRID.

Avant de créer des compartiments avec le verrouillage d'objet S3 activé, l'administrateur de la grille doit activer le paramètre de verrouillage d'objet S3 global pour l'ensemble du système StorageGRID. L'administrateur du grid doit également s'assurer que la politique de gestion du cycle de vie de l'information est « conforme ». Elle doit répondre aux exigences des compartiments lorsque le verrouillage objet S3 est activé. Pour plus de détails, contactez votre administrateur de grille ou consultez les instructions de "Gestion des objets avec le verrouillage objet S3".

Une fois le paramètre global S3 Object Lock activé, vous pouvez créer des compartiments avec S3 Object Lock activé et spécifier éventuellement des paramètres de conservation par défaut pour chaque compartiment. En outre, vous pouvez utiliser l'application client S3 pour spécifier des paramètres de conservation pour chaque version d'objet.



Conditions requises pour les compartiments avec verrouillage objet S3 activé

- Si le paramètre global de verrouillage objet S3 est activé pour le système StorageGRID, vous pouvez utiliser le gestionnaire de locataires, l'API de gestion des locataires ou l'API REST S3 pour créer des compartiments avec le verrouillage objet S3 activé.
- Si vous prévoyez d'utiliser le verrouillage d'objet S3, vous devez activer le verrouillage d'objet S3 lors de la création du compartiment. Vous ne pouvez pas activer le verrouillage objet S3 pour un compartiment existant.
- Lorsque le verrouillage d'objet S3 est activé pour un compartiment, StorageGRID active automatiquement le contrôle de version pour ce compartiment. Vous ne pouvez pas désactiver le verrouillage objet S3 ou suspendre la gestion des versions pour le compartiment.
- Vous pouvez également spécifier un mode de conservation et une période de conservation par défaut pour chaque compartiment à l'aide du gestionnaire des locataires, de l'API de gestion des locataires ou de l'API REST S3. Les paramètres de conservation par défaut du compartiment s'appliquent uniquement aux nouveaux objets ajoutés au compartiment qui ne disposent pas de leurs propres paramètres de conservation. Vous pouvez remplacer ces paramètres par défaut en spécifiant un mode de conservation et une date de conservation jusqu'à pour chaque version d'objet lors du téléchargement.

- La configuration du cycle de vie des compartiments est prise en charge pour les compartiments avec le verrouillage objet S3 activé.
- La réplication CloudMirror n'est pas prise en charge pour les compartiments avec le verrouillage objet S3 activé.

Exigences relatives aux objets dans les compartiments avec le verrouillage d'objet S3 activé

- Pour protéger une version d'objet, vous pouvez spécifier les paramètres de conservation par défaut du compartiment ou les paramètres de conservation pour chaque version d'objet. Les paramètres de conservation au niveau objet peuvent être spécifiés à l'aide de l'application client S3 ou de l'API REST S3.
- Les paramètres de conservation s'appliquent aux versions d'objet individuelles. Une version d'objet peut avoir à la fois un paramètre de conservation à la date et un paramètre de conservation légal, l'un mais pas l'autre, ou l'autre. La spécification d'un paramètre de conservation à la date ou d'un paramètre de conservation légal pour un objet protège uniquement la version spécifiée dans la demande. Vous pouvez créer de nouvelles versions de l'objet, tandis que la version précédente de l'objet reste verrouillée.

Cycle de vie des objets dans des compartiments avec verrouillage objet S3 activé

Chaque objet enregistré dans un compartiment lorsque le verrouillage objet S3 est activé passe par les étapes suivantes :

1. **Entrée d'objet**

   Lors de l'ajout d'une version d'objet à un compartiment pour lequel S3 Object Lock est activé, les paramètres de conservation sont appliqués comme suit :

   - Si des paramètres de rétention sont spécifiés pour l'objet, les paramètres de niveau objet sont appliqués. Tous les paramètres de compartiment par défaut sont ignorés.
   - Si aucun paramètre de conservation n'est spécifié pour l'objet, les paramètres de compartiment par défaut sont appliqués, s'ils existent.
   - Si aucun paramètre de conservation n'est spécifié pour l'objet ou le compartiment, l'objet n'est pas protégé par le verrouillage objet S3.

   Si les paramètres de conservation sont appliqués, l'objet et les métadonnées S3 définies par l'utilisateur sont protégés.

2. **Conservation et suppression d'objets**

   StorageGRID stocke plusieurs copies de chaque objet protégé pendant la période de conservation spécifiée. Le nombre et le type exacts de copies d'objet et d'emplacements de stockage sont déterminés par les règles de conformité de la politique ILM active. La possibilité de supprimer un objet protégé avant d'atteindre sa date de conservation jusqu'à dépend de son mode de conservation.

   - Si un objet fait l'objet d'une conservation légale, personne ne peut le supprimer, quel que soit son mode de conservation.

Est-il toujours possible de gérer des compartiments existants conformes ?

La fonction de verrouillage d'objet S3 remplace la fonction de conformité disponible dans les versions StorageGRID précédentes. Si vous avez créé des compartiments conformes à l'aide d'une version précédente de StorageGRID, vous pouvez continuer à gérer les paramètres de ces compartiments. Toutefois, vous ne pouvez plus créer de compartiments conformes. Pour obtenir des instructions, reportez-vous à la sectionhttps://kb.netapp.com/Advice_and_Troubleshooting/Hybrid_Cloud_Infrastructure/StorageGRID/How_to_manage_legacy_Compliant_buckets_in_StorageGRID_11.5["Base de connaissances NetApp : comment

gérer des compartiments conformes aux ancienne génération dans StorageGRID 11.5"^].

Mettre à jour la conservation par défaut du verrouillage d'objet S3

Si vous avez activé le verrouillage objet S3 lors de la création du compartiment, vous pouvez modifier ce dernier pour modifier les paramètres de conservation par défaut. Vous pouvez activer (ou désactiver) la rétention par défaut et définir un mode de rétention et une période de rétention par défaut.

Avant de commencer

- Vous êtes connecté au Gestionnaire de locataires à l'aide d'un "navigateur web pris en charge".
- Vous appartenez à un groupe d'utilisateurs qui possède le "Gérez tous les compartiments ou l'autorisation d'accès racine". Ces autorisations remplacent les paramètres d'autorisations des stratégies de groupes ou de compartiments.
- Le verrouillage des objets S3 est activé globalement pour votre système StorageGRID et vous avez activé le verrouillage des objets S3 lorsque vous avez créé le compartiment. Voir "Utilisez le verrouillage d'objet S3 pour conserver les objets".

Étapes

1. Sélectionnez **Afficher les compartiments** dans le tableau de bord ou sélectionnez **STOCKAGE (S3)** > **compartiments**.
2. Sélectionnez le nom du compartiment dans la table.

   La page des détails du compartiment s'affiche.

3. Dans l'onglet **Bucket options**, sélectionnez l'accordéon **S3 Object Lock**.
4. En option, activez ou désactivez **rétention par défaut** pour ce compartiment.

   Les modifications de ce paramètre ne s'appliquent pas aux objets qui se trouvent déjà dans le compartiment ni aux objets qui peuvent avoir leurs propres périodes de conservation.

5. Si **Default Retention** est activé, spécifiez un **mode de rétention par défaut** pour le compartiment.

Mode de rétention par défaut	Description
La conformité	• L'objet ne peut pas être supprimé tant que sa date de conservation jusqu'à n'est pas atteinte. • La date de conservation de l'objet peut être augmentée, mais elle ne peut pas être réduite. • La date de conservation de l'objet jusqu'à ne peut pas être supprimée tant que cette date n'est pas atteinte.

Mode de rétention par défaut	Description
La gouvernance	• Utilisateurs avec le `s3:BypassGovernanceRetention` l'autorisation peut utiliser le `x-amz-bypass-governance-retention: true` demander à l'en-tête de contourner les paramètres de rétention. • Ces utilisateurs peuvent supprimer une version d'objet avant d'atteindre sa date de conservation jusqu'à. • Ces utilisateurs peuvent augmenter, diminuer ou supprimer la date de conservation d'un objet.

6. Si **Default Retention** est activé, spécifiez la **période de rétention par défaut** pour le compartiment.

   La **période de conservation par défaut** indique la durée pendant laquelle les nouveaux objets ajoutés à ce compartiment doivent être conservés, à partir du moment où ils sont ingérés. Spécifiez une valeur comprise entre 1 et 36,500 jours ou entre 1 et 100 ans.

7. Sélectionnez **Enregistrer les modifications**.

Configurer le partage de ressources inter-sources (CORS)

Vous pouvez configurer le partage de ressources entre sources (CORS) pour un compartiment S3 si vous souhaitez que ce compartiment et ces objets soient accessibles aux applications web d'autres domaines.

Avant de commencer

- Vous êtes connecté au Gestionnaire de locataires à l'aide d'un "navigateur web pris en charge".
- Vous appartenez à un groupe d'utilisateurs qui possède le "Gérez tous les compartiments ou l'autorisation d'accès racine". Ces autorisations remplacent les paramètres d'autorisations des stratégies de groupes ou de compartiments.

Description de la tâche

Le partage de ressources d'origine croisée (CORS) est un mécanisme de sécurité qui permet aux applications Web clientes d'un domaine d'accéder aux ressources d'un domaine différent. Supposons par exemple que vous utilisez un compartiment S3 nommé `Images` pour stocker des graphiques. En configurant CORS pour l'`Images` le champ permet d'afficher les images de ce compartiment sur le site web `http://www.example.com`.

Activer le CORS pour un godet

Étapes

1. Utilisez un éditeur de texte pour créer le fichier XML requis.

   Cet exemple montre le code XML utilisé pour activer le code commande pour un compartiment S3. Ce XML permet à n'importe quel domaine d'envoyer des requêtes GET au compartiment, mais il n'autorise que le `http://www.example.com` Domaine pour envoyer des demandes POST et DE SUPPRESSION. Tous les en-têtes de demande sont autorisés.

```
<CORSConfiguration
    xmlns="http://s3.amazonaws.com/doc/2020-10-22/">
    <CORSRule>
        <AllowedOrigin>*</AllowedOrigin>
        <AllowedMethod>GET</AllowedMethod>
        <AllowedHeader>*</AllowedHeader>
    </CORSRule>
    <CORSRule>
        <AllowedOrigin>http://www.example.com</AllowedOrigin>
        <AllowedMethod>GET</AllowedMethod>
        <AllowedMethod>POST</AllowedMethod>
        <AllowedMethod>DELETE</AllowedMethod>
        <AllowedHeader>*</AllowedHeader>
    </CORSRule>
</CORSConfiguration>
```

Pour plus d'informations sur le XML de configuration CORS, voir "Documentation Amazon Web Services (AWS) : guide du développeur Amazon simple Storage Service".

2. Sélectionnez **Afficher les compartiments** dans le tableau de bord ou sélectionnez **STOCKAGE (S3)** > **compartiments**.
3. Sélectionnez le nom du compartiment dans la table.

   La page des détails du compartiment s'affiche.

4. Dans l'onglet **Bucket Access**, sélectionnez l'accordéon **Cross-Origin Resource Sharing (CORS)**.
5. Cochez la case **Activer CORS**.
6. Collez le fichier XML de configuration CORS dans la zone de texte.
7. Sélectionnez **Enregistrer les modifications**.

Modifier le paramètre CORS

Étapes

1. Mettez à jour le XML de configuration CORS dans la zone de texte ou sélectionnez **Effacer** pour recommencer.
2. Sélectionnez **Enregistrer les modifications**.

Désactiver le paramètre CORS

Étapes

1. Décochez la case **Activer CORS**.
2. Sélectionnez **Enregistrer les modifications**.

Supprime les objets du compartiment

Vous pouvez utiliser le Gestionnaire de locataires pour supprimer les objets d'une ou de plusieurs compartiments.

Considérations et exigences

Avant d'effectuer ces étapes, notez les points suivants :

- Lorsque vous supprimez les objets d'un compartiment, StorageGRID supprime définitivement tous les objets et toutes les versions d'objets de chaque compartiment sélectionné de tous les nœuds et sites de votre système StorageGRID. StorageGRID supprime également les métadonnées d'objet associées. Vous ne pourrez pas récupérer ces informations.
- La suppression de tous les objets d'un compartiment peut prendre plusieurs minutes, jours, voire semaines, en fonction du nombre d'objets, de copies d'objet et d'opérations simultanées.
- Si un godet a "Verrouillage objet S3 activé", Il peut rester à l'état **Suppression d'objets : lecture seule** pendant *années*.

Un compartiment qui utilise le verrouillage d'objet S3 restera à l'état **Suppression d'objets : lecture seule** jusqu'à ce que la date de conservation soit atteinte pour tous les objets et que toutes les mises en suspens légales soient supprimées.

- Pendant la suppression des objets, l'état du compartiment est **Suppression d'objets : lecture seule**. Dans cet état, vous ne pouvez pas ajouter de nouveaux objets au compartiment.
- Une fois tous les objets supprimés, le compartiment reste à l'état en lecture seule. Vous pouvez effectuer l'une des opérations suivantes :
  - Ramener le compartiment en mode écriture et le réutiliser pour de nouveaux objets
  - Supprimez le compartiment
  - Conservez le compartiment en mode lecture seule pour réserver son nom pour une utilisation ultérieure
- Si la gestion des versions d'un objet est activée dans un compartiment, les marqueurs de suppression qui se trouvent dans le compartiment au démarrage de ces étapes ne seront pas supprimés par l'opération de suppression d'objets. Si vous souhaitez supprimer un compartiment versionné après la suppression de tous les objets, vous devez supprimer tous les marqueurs de suppression préexistants.
- Si vous utilisez "réplication entre plusieurs grilles", noter ce qui suit :
  - L'utilisation de cette option ne supprime aucun objet du compartiment de l'autre grille.
  - Si vous sélectionnez cette option pour le compartiment source, l'alerte **échec de réplication multigrille** est déclenchée si vous ajoutez des objets au compartiment de destination sur l'autre grille. Si vous ne pouvez pas garantir que personne n'ajoutera d'objets au compartiment de l'autre grille, "désactiver la réplication entre les grilles" ce compartiment avant la suppression de tous les objets de compartiment.

Avant de commencer

- Vous êtes connecté au Gestionnaire de locataires à l'aide d'un "navigateur web pris en charge".
- Vous appartenez à un groupe d'utilisateurs qui possède le "Autorisation d'accès racine". Cette autorisation remplace les paramètres d'autorisations dans les stratégies de groupe ou de compartiment.

Étapes

1. Sélectionnez **Afficher les compartiments** dans le tableau de bord ou sélectionnez **STOCKAGE (S3)** > **compartiments**.

   La page compartiments s'affiche et affiche tous les compartiments S3 existants.

2. Utilisez le menu **actions** ou la page de détails pour un compartiment spécifique.

Menu actions

a. Cochez la case correspondant à chaque compartiment dans lequel vous souhaitez supprimer des objets.

b. Sélectionnez **actions** > **Supprimer les objets dans le compartiment**.

Page de détails

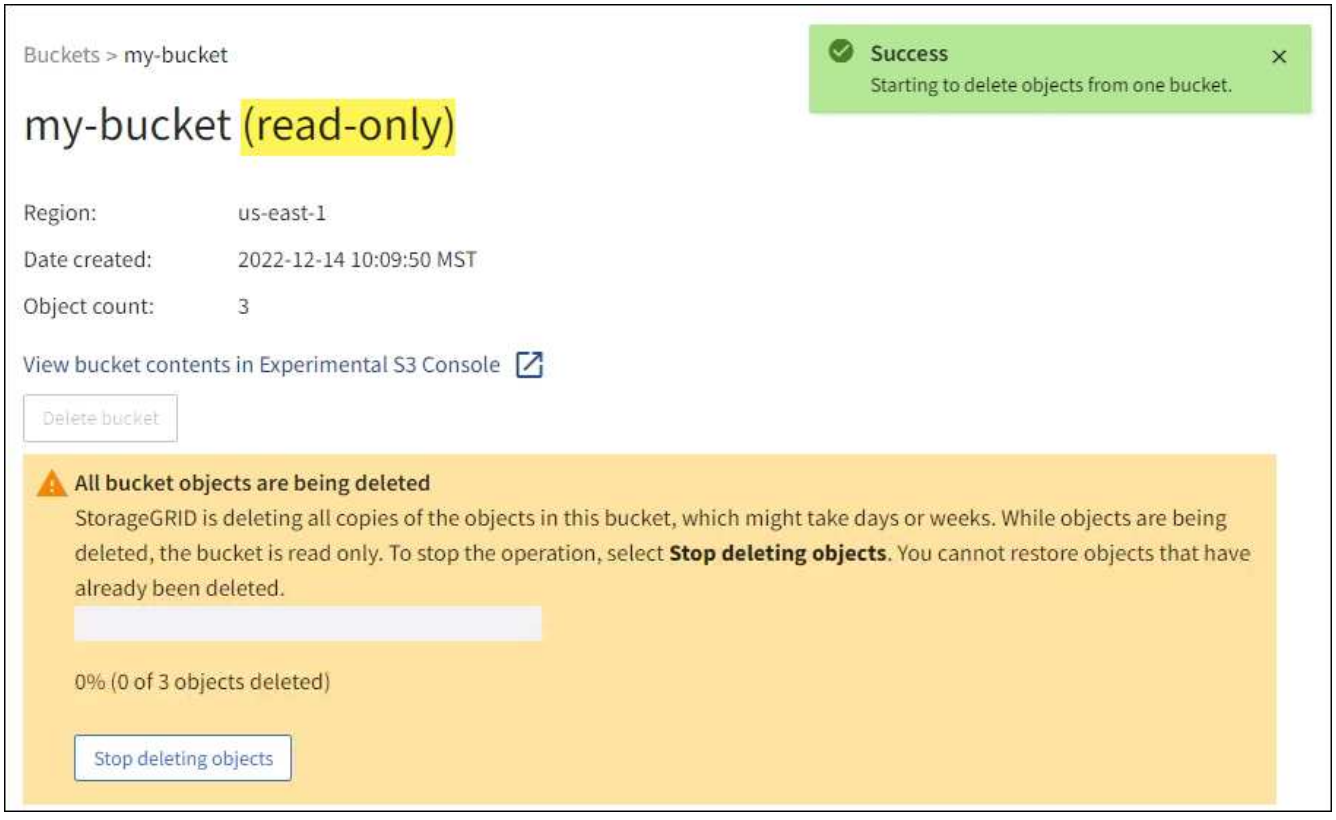
a. Sélectionnez un nom de compartiment pour afficher ses détails.

b. Sélectionnez **Supprimer les objets dans le compartiment**.

3. Lorsque la boîte de dialogue de confirmation s'affiche, vérifiez les détails, entrez **Oui** et sélectionnez **OK**.
4. Attendez que l'opération de suppression commence.

   Au bout de quelques minutes :

   - Une bannière d'état jaune s'affiche sur la page de détails du compartiment. La barre de progression représente le pourcentage d'objets supprimés.
   - **(lecture seule)** apparaît après le nom du compartiment sur la page de détails du compartiment.
   - **(Suppression d'objets : lecture seule)** apparaît à côté du nom du compartiment sur la page compartiments.

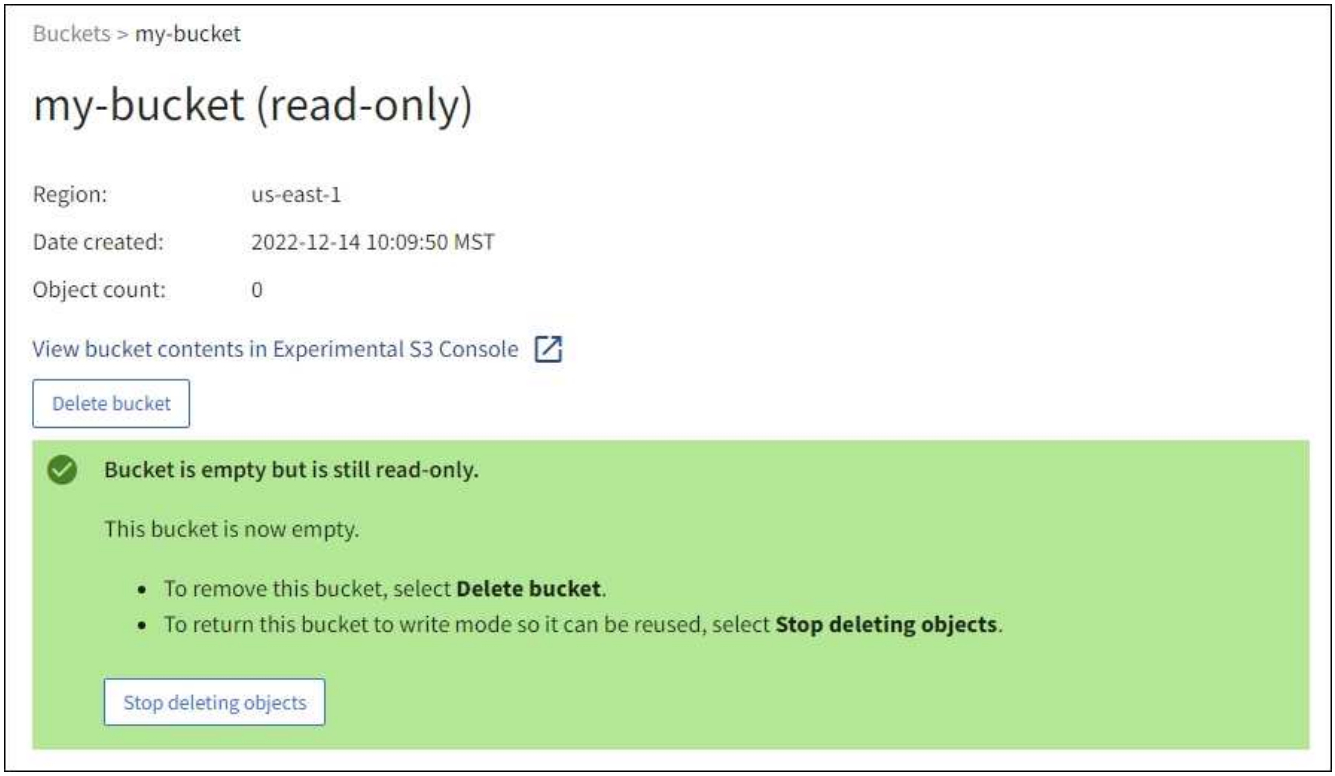


5. Si nécessaire pendant l'exécution de l'opération, sélectionnez **Arrêter la suppression d'objets** pour arrêter le processus. Sélectionnez ensuite **Supprimer les objets dans le compartiment** pour reprendre le processus.

   Lorsque vous sélectionnez **Arrêter la suppression d'objets**, le compartiment est remis en mode écriture ; cependant, vous ne pouvez pas accéder aux objets qui ont été supprimés ni les restaurer.

6. Attendez la fin de l'opération.

   Lorsque le compartiment est vide, la bannière d'état est mise à jour, mais le compartiment reste en lecture seule.



7. Effectuez l'une des opérations suivantes :
   - Quittez la page pour garder le compartiment en mode lecture seule. Par exemple, vous pouvez conserver un compartiment vide en mode lecture seule afin de réserver le nom du compartiment pour une utilisation ultérieure.
   - Supprimer le compartiment. Vous pouvez sélectionner **Supprimer un compartiment** pour supprimer un seul compartiment ou retourner à la page compartiments et sélectionner **actions** > **Supprimer** compartiments pour supprimer plusieurs compartiments.

     Si vous ne pouvez pas supprimer un compartiment multiversion après la suppression de tous les objets, les marqueurs de suppression peuvent rester. Pour supprimer le godet, vous devez supprimer tous les marqueurs de suppression restants.

   - Ramenez le compartiment en mode écriture et réutilisez-le éventuellement pour de nouveaux objets. Vous pouvez sélectionner **Arrêter la suppression d'objets** pour un seul compartiment ou revenir à la page compartiments et sélectionner **action** > **Arrêter la suppression d'objets** pour plusieurs compartiments.

Supprimez le compartiment S3

Vous pouvez utiliser le Gestionnaire de locataires pour supprimer une ou plusieurs compartiments S3 vides.

Avant de commencer

- Vous êtes connecté au Gestionnaire de locataires à l'aide d'un "navigateur web pris en charge".

- Vous appartenez à un groupe d'utilisateurs qui possède le "Gérez tous les compartiments ou l'autorisation d'accès racine". Ces autorisations remplacent les paramètres d'autorisations des stratégies de groupes ou de compartiments.
- Les compartiments à supprimer sont vides.

Description de la tâche

Ces instructions expliquent comment supprimer un compartiment S3 à l'aide du Gestionnaire des locataires. Vous pouvez également supprimer des compartiments S3 à l'aide du "API de gestion des locataires" ou le "L'API REST S3".

Vous ne pouvez pas supprimer un compartiment S3 s'il contient des objets, des versions d'objets non actuelles ou des marqueurs de suppression. Pour plus d'informations sur la suppression des objets avec version S3, reportez-vous à la section "Comment supprimer les objets".

Étapes

1. Sélectionnez **Afficher les compartiments** dans le tableau de bord ou sélectionnez **STOCKAGE (S3)** > **compartiments**.

   La page compartiments s'affiche et affiche tous les compartiments S3 existants.

2. Utilisez le menu **actions** ou la page de détails pour un compartiment spécifique.

   Menu actions

   a. Cochez la case correspondant à chaque compartiment à supprimer.

   b. Sélectionnez **actions** > **Supprimer des compartiments**.

   Page de détails

   a. Sélectionnez un nom de compartiment pour afficher ses détails.

   b. Sélectionnez **Supprimer le compartiment**.

3. Lorsque la boîte de dialogue de confirmation s'affiche, sélectionnez **Oui**.

   La fonction StorageGRID confirme que chaque compartiment est vide, puis supprime chaque compartiment. Cette opération peut prendre quelques minutes.

   Si un compartiment n'est pas vide, un message d'erreur s'affiche. Vous devez supprimer tous les objets et tous les marqueurs de suppression du compartiment avant de pouvoir le supprimer.

Utilisation de la console Experimental S3

Vous pouvez utiliser la console S3 pour afficher les objets d'un compartiment S3.

Vous pouvez également utiliser la console S3 pour :

- Ajouter et supprimer des objets, des versions d'objet et des dossiers
- Renommez les objets
- Déplacer et copier des objets entre des compartiments et des dossiers
- Gérer les balises d'objet

- Afficher les métadonnées d'objet
- Télécharger des objets

> La console S3 est marquée comme « expérimentale » car elle n'est pas encore complète ou approuvée pour une utilisation dans un environnement de production. Les locataires ne doivent utiliser la console S3 que lors de l'exécution de fonctions sur un petit nombre d'objets, par exemple lors du chargement d'objets pour simuler une nouvelle règle ILM, pour résoudre les problèmes d'ingestion ou via des grilles de validation technique ou non-production.

Avant de commencer

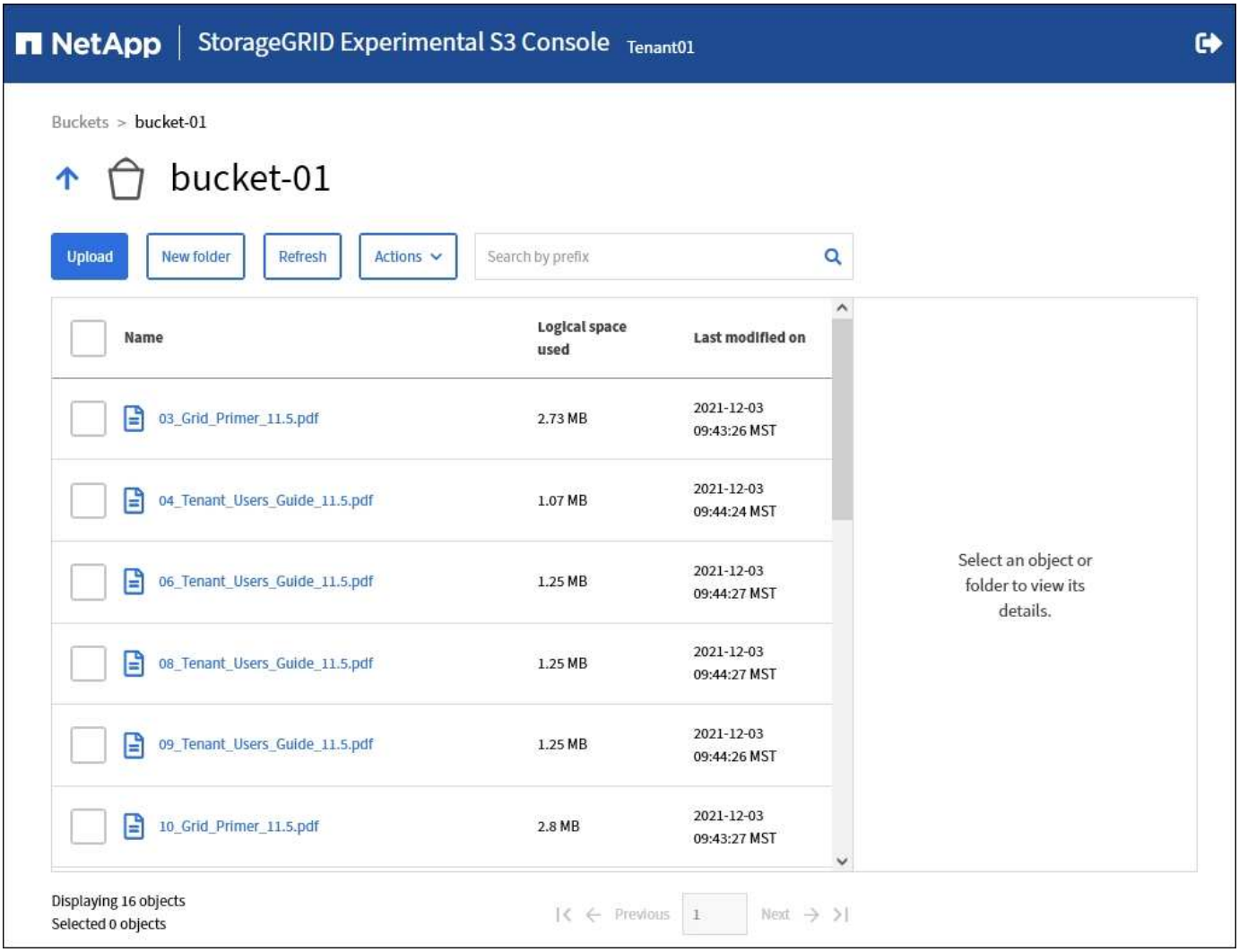
- Vous êtes connecté au Gestionnaire de locataires à l'aide d'un "navigateur web pris en charge".
- Vous appartenez à un groupe d'utilisateurs disposant de l'autorisation d'accès racine ou disposant à la fois des options gérer tous les compartiments et gérer les objets avec la console S3 "autorisations".

> Les utilisateurs disposant de l'autorisation gérer les objets avec la console S3, mais qui ne disposent pas de l'autorisation gérer tous les compartiments, peuvent toujours naviguer directement vers la console S3 expérimentale.

- Vous avez créé un compartiment.
- Une règle de groupe S3 ou de compartiment a été configurée pour l'utilisateur.
- Vous connaissez l'ID de clé d'accès de l'utilisateur et la clé d'accès secrète. Si vous le souhaitez, vous avez un `.csv` fichier contenant ces informations. Voir la "instructions pour la création de clés d'accès".

Étapes

1. Sélectionnez **godets**.
2. Sélectionnez Experimental S3 Console . Vous pouvez également accéder à ce lien à partir de la page des détails du compartiment.
3. Sur la page de connexion de la console Experimental S3, collez l'ID de clé d'accès et la clé secrète dans les champs. Sinon, sélectionnez **Télécharger les touches d'accès** et sélectionnez votre `.csv` fichier.
4. Sélectionnez **connexion**.
5. Gérez les objets selon vos besoins.



Gérez les services de la plateforme S3

Qu'est-ce que les services de plateforme ?

Les services de plateforme StorageGRID vous aident à mettre en œuvre une stratégie de cloud hybride en vous permettant d'envoyer des notifications d'événements et des copies d'objets S3 et de métadonnées d'objet à des destinations externes.

Si l'utilisation des services de plateforme est autorisée pour votre compte de locataire, vous pouvez configurer les services suivants pour n'importe quel compartiment S3 :

- **Réplication CloudMirror** : utilisation "Service de réplication StorageGRID CloudMirror" Pour mettre en miroir des objets spécifiques d'un compartiment StorageGRID vers une destination externe spécifiée.

  Vous pouvez, par exemple, utiliser la réplication CloudMirror pour mettre en miroir des enregistrements client spécifiques dans Amazon S3, puis exploiter les services AWS pour analyser vos données.

  > La réplication CloudMirror n'est pas prise en charge si le compartiment source est activé pour le verrouillage objet S3.

- **Notifications**: Utilisation "notifications d'événement par compartiment" Pour envoyer des notifications sur

des actions spécifiques effectuées sur des objets à un service Amazon simple notification Service™ (SNS) externe spécifié.

Par exemple, vous pouvez configurer l'envoi d'alertes aux administrateurs pour chaque objet ajouté à un compartiment, où les objets représentent les fichiers de journal associés à un événement système critique.

> Bien que la notification d'événement puisse être configurée sur un compartiment avec l'option de verrouillage d'objet S3 activée, les métadonnées S3 Object Lock (conservation jusqu'à la date et état de conservation légale) des objets ne seront pas incluses dans les messages de notification.

- **Service d'intégration de recherche** : utilisez le "service d'intégration de la recherche" Permet d'envoyer des métadonnées d'objet S3 à un index Elasticsearch spécifié pour rechercher ou analyser les métadonnées à l'aide du service externe.

  Vous pouvez, par exemple, configurer des compartiments pour envoyer les métadonnées d'objet S3 vers un service Elasticsearch distant. Vous pouvez ensuite utiliser Elasticsearch pour effectuer des recherches dans des compartiments et effectuer des analyses sophistiquées des modèles présents dans les métadonnées de l'objet.

  > Bien que l'intégration avec Elasticsearch puisse être configurée sur un compartiment avec l'option S3 Object Lock activée, les métadonnées S3 Object Lock (conservation jusqu'à la date et état de conservation légale) des objets ne seront pas incluses dans les messages de notification.

L'emplacement cible des services de plateforme étant généralement externe à votre déploiement StorageGRID, les services de plateforme vous offrent la puissance et la flexibilité offertes par l'utilisation de ressources de stockage externes, de services de notification et de services de recherche ou d'analyse pour vos données.

Toute combinaison de services de plateforme peut être configurée pour un seul compartiment S3. Par exemple, vous pouvez configurer le service CloudMirror et les notifications sur un compartiment StorageGRID S3 afin de pouvoir mettre en miroir des objets spécifiques sur Amazon simple Storage Service, tout en envoyant une notification sur chacun de ces objets à une application de surveillance tierce pour vous aider à suivre vos dépenses AWS.

> L'utilisation des services de la plateforme doit être activée pour chaque compte de locataire par un administrateur StorageGRID à l'aide de Grid Manager ou de l'API de gestion du grid.

Configuration des services de plate-forme

Les services de plateforme communiquent avec les terminaux externes que vous configurez à l'aide de "Gestionnaire de locataires" ou le "API de gestion des locataires". Chaque terminal représente une destination externe, par exemple un compartiment StorageGRID S3, un compartiment Amazon Web Services, un sujet SNS (simple notification Service) ou un cluster Elasticsearch hébergé localement, dans AWS ou ailleurs.

Après avoir créé un noeud final externe, vous pouvez activer un service de plate-forme pour un compartiment en ajoutant une configuration XML au compartiment. La configuration XML identifie les objets sur lesquels le compartiment doit agir, l'action que le compartiment doit effectuer et le point de terminaison que le compartiment doit utiliser pour le service.

Vous devez ajouter des configurations XML distinctes pour chaque service de plate-forme que vous souhaitez configurer. Par exemple :

- Si vous souhaitez que tous les objets dont les clés commencent par `/images` Pour la réplication vers un compartiment Amazon S3, vous devez ajouter une configuration de réplication dans le compartiment source.
- Si vous souhaitez également envoyer des notifications lorsque ces objets sont stockés dans le compartiment, vous devez ajouter une configuration de notifications.
- Enfin, si vous voulez indexer les métadonnées de ces objets, vous devez ajouter la configuration de notification de métadonnées utilisée pour implémenter l'intégration de la recherche.

Le format du XML de configuration est régi par les API REST S3 utilisées pour mettre en œuvre les services de plateforme StorageGRID :

Service de plateforme	L'API REST S3
"Réplication CloudMirror"	• RÉPLICATION des compartiments • RÉPLICATION des compartiments
"Notifications"	• GET Bucket notification • PUT Bucket notification
"Intégration de la recherche"	• CONFIGURATION DES notifications de métadonnées de compartiment • CONFIGURATION de notification des métadonnées de compartiment Ces opérations sont personnalisées pour StorageGRID.

Informations associées

"Considérations relatives aux services de plateforme"

"UTILISEZ L'API REST S3"

Service de réplication CloudMirror

Vous pouvez activer la réplication CloudMirror pour un compartiment S3 si vous souhaitez que StorageGRID réplique des objets spécifiés ajoutés au compartiment dans un ou plusieurs compartiments de destination.

La réplication CloudMirror fonctionne indépendamment de la règle ILM active de la grille. Le service CloudMirror réplique les objets au fur et à mesure qu'ils sont stockés dans le compartiment source et les fournit au compartiment de destination dès que possible. La livraison des objets répliqués est déclenchée lors de la réussite de l'acquisition de l'objet.

> La réplication CloudMirror présente des similarités et des différences importantes avec la fonction de réplication multigrille. Pour en savoir plus, voir "Comparez la réplication entre les grilles et la réplication CloudMirror".

Si vous activez la réplication CloudMirror pour un compartiment existant, seuls les nouveaux objets ajoutés à ce compartiment sont répliqués. Les objets existants dans le compartiment ne sont pas répliqués. Pour forcer la réplication d'objets existants, vous pouvez mettre à jour les métadonnées de l'objet existant en effectuant

une copie d'objet.

> Si vous utilisez la réplication CloudMirror pour copier des objets vers une destination Amazon S3, sachez qu'Amazon S3 limite la taille des métadonnées définies par l'utilisateur dans chaque en-tête de la requête PUT à 2 Ko. Si un objet possède des métadonnées définies par l'utilisateur supérieures à 2 Ko, cet objet ne sera pas répliqué.

Dans StorageGRID, vous pouvez répliquer les objets dans un compartiment unique vers plusieurs compartiments de destination. Pour ce faire, spécifiez la destination de chaque règle dans le XML de configuration de réplication. Vous ne pouvez pas répliquer un objet dans plusieurs compartiments en même temps.

En outre, vous pouvez configurer la réplication CloudMirror pour les compartiments avec version ou sans version, et spécifier un compartiment avec version ou sans version comme destination. Vous pouvez utiliser n'importe quelle combinaison de compartiments avec version et sans version. Par exemple, vous pouvez spécifier un compartiment avec version comme destination pour un compartiment source sans version, ou vice-versa. Vous pouvez également répliquer les compartiments sans version.

Le comportement de suppression du service de réplication CloudMirror est identique au comportement de suppression du service CRR (Cross Region Replication) fourni par Amazon S3 — la suppression d'un objet dans un compartiment source ne supprime jamais un objet répliqué dans la destination. Si le compartiment source et le compartiment de destination sont multiversion, le marqueur de suppression est répliqué. Si le compartiment de destination n'est pas multiversion, la suppression d'un objet du compartiment source ne réplique pas le marqueur de suppression vers le compartiment de destination ou supprime l'objet de destination.

Lors de la réplication des objets dans le compartiment de destination, StorageGRID les désigne par « duplicaas ». Un compartiment StorageGRID de destination ne réplique pas les objets marqués comme répliques, ce qui vous protège des boucles de réplication accidentelles. Ce marquage de réplication est interne à StorageGRID et ne vous empêche pas d'utiliser AWS CRR lorsque vous utilisez un compartiment Amazon S3 comme destination.

> L'en-tête personnalisé utilisé pour marquer une réplique est `x-ntap-sg-replica`. Ce marquage empêche un miroir en cascade. StorageGRID prend en charge un CloudMirror bidirectionnel entre deux grilles.

L'unicité et l'ordre des événements dans le compartiment de destination ne sont pas garantis. Plusieurs copies identiques d'un objet source peuvent être livrées à la destination du fait des opérations effectuées pour garantir le succès de la livraison. Dans de rares cas, lorsque le même objet est mis à jour simultanément depuis deux sites StorageGRID ou plus, il peut ne pas correspondre au ordre d'événements du compartiment source.

La réplication CloudMirror est généralement configurée pour utiliser un compartiment S3 externe comme destination. Vous pouvez cependant également configurer la réplication afin d'utiliser un autre déploiement StorageGRID ou tout service compatible S3.

Description des notifications pour les compartiments

Vous pouvez activer la notification des événements pour un compartiment S3 si vous souhaitez que StorageGRID envoie des notifications sur les événements spécifiés à un service Amazon simple notification Service (SNS) de destination.

C'est possible "configurer les notifications d'événements" En associant XML de configuration de notification à un compartiment source. Le XML de configuration de notification respecte les conventions S3 pour la

configuration des notifications de compartiment, avec la rubrique SNS de destination spécifiée comme URN d'un terminal.

Les notifications d'événements sont créées au niveau du compartiment source, comme indiqué dans la configuration de la notification, et sont envoyées vers le compartiment de destination. Si un événement associé à un objet réussit, une notification concernant cet événement est créée et mise en file d'attente pour la livraison.

L'unicité et l'ordre des notifications ne sont pas garantis. Plusieurs notifications d'événement peuvent être envoyées vers la destination après les opérations effectuées pour garantir la réussite de la livraison. La livraison étant asynchrone, l'ordre dans le temps des notifications au niveau de la destination n'est pas garanti correspondant à l'ordre des événements dans le compartiment source, en particulier pour les opérations provenant de différents sites StorageGRID. Vous pouvez utiliser le `sequencer` Key dans le message d'événement pour déterminer l'ordre des événements pour un objet particulier, tel que décrit dans la documentation Amazon S3.

Notifications et messages pris en charge

Les notifications d'événements StorageGRID suivent l'API Amazon S3 avec quelques limitations :

- Les types d'événements suivants sont pris en charge :
  - s3:ObjectCreated:*
  - s3:ObjectCreated:put
  - s3:ObjectCreated:Post
  - s3:ObjectCreated:Copier
  - s3:ObjectCreated:CompleteMultipartUpload
  - s3:ObjectRemoved:*
  - s3:ObjectRemoved:Supprimer
  - s3:ObjectRemoved:DeleteMarkerCreated
  - s3:ObjectRestore:Post
- Les notifications d'événements envoyées par StorageGRID utilisent le format JSON standard, mais n'incluent pas certaines clés et utilisent des valeurs spécifiques pour d'autres, comme illustré dans le tableau :

Nom de la clé	Valeur ajoutée de StorageGRID
Source d'événements	`sgws:s3`
Région de l'awsRegion	non inclus
x-amz-id-2	non inclus
arn	`urn:sgws:s3:::bucket_name`

Comprendre le service d'intégration de la recherche

Si vous souhaitez utiliser un service externe de recherche et d'analyse de données pour

vos métadonnées d'objet, vous pouvez activer l'intégration de la recherche pour un compartiment S3.

Le service d'intégration de recherche est un service StorageGRID personnalisé qui envoie automatiquement et de manière asynchrone des métadonnées d'objet S3 vers un terminal de destination lors de la mise à jour d'un objet ou de ses métadonnées. Vous pouvez ensuite utiliser des outils sophistiqués de recherche, d'analyse de données, de visualisation ou de machine learning proposés par le service de destination pour rechercher, analyser et obtenir des informations exploitables à partir de vos données d'objet.

Vous pouvez activer le service d'intégration de la recherche pour tout compartiment avec version ou sans version. L'intégration des recherches est configurée en associant le XML de configuration des notifications de métadonnées au compartiment qui spécifie les objets à utiliser et la destination des métadonnées de l'objet.

Les notifications sont générées sous la forme d'un document JSON nommé avec le nom de compartiment, le nom de l'objet et l'ID de version, le cas échéant. Chaque notification de métadonnées contient un ensemble standard de métadonnées système pour l'objet, en plus de toutes les balises de l'objet et de toutes les métadonnées utilisateur.

> Pour les balises et les métadonnées d'utilisateur, StorageGRID transmet des dates et des chiffres à Elasticsearch en tant que chaînes ou notifications d'événement S3. Pour configurer Elasticsearch afin d'interpréter ces chaînes comme des dates ou des chiffres, suivez les instructions Elasticsearch pour un mappage dynamique des champs et un mappage des formats de date. Vous devez activer les mappages de champs dynamiques sur l'index avant de configurer le service d'intégration de la recherche. Une fois qu'un document est indexé, vous ne pouvez pas modifier les types de champ du document dans l'index.

Les notifications sont générées et mises en file d'attente pour livraison chaque fois que :

- Un objet est créé.
- Un objet est supprimé, notamment lorsque des objets sont supprimés suite au fonctionnement de la règle ILM de la grille.
- Les métadonnées ou les balises d'objet sont ajoutées, mises à jour ou supprimées. L'ensemble complet de métadonnées et de balises est toujours envoyé lors de la mise à jour, et pas seulement les valeurs modifiées.

Après avoir ajouté le XML de configuration de notification des métadonnées à un compartiment, des notifications sont envoyées pour tout nouvel objet que vous créez et pour tout objet que vous modifiez en mettant à jour ses données, métadonnées utilisateur ou balises. Cependant, aucune notification n'est envoyée pour les objets qui se trouvaient déjà dans le compartiment. Pour vous assurer que les métadonnées d'objet de tous les objets du compartiment sont envoyées à la destination, effectuez l'une des opérations suivantes :

- Configurez le service d'intégration de la recherche immédiatement après avoir créé le compartiment et avant d'ajouter des objets.
- Exécutez une action sur tous les objets déjà dans le compartiment pour déclencher un message de notification des métadonnées à envoyer à la destination.

Le service d'intégration de recherche StorageGRID prend en charge un cluster Elasticsearch. Comme pour les autres services de plate-forme, la destination est spécifiée dans le noeud final dont l'URN est utilisé dans le XML de configuration du service. Utilisez le "Matrice d'interopérabilité NetApp" Afin de déterminer les versions prises en charge par Elasticsearch.

Informations associées

"XML de configuration pour l'intégration de la recherche"

"Métadonnées d'objet incluses dans les notifications de métadonnées"

"JSON généré par le service d'intégration de la recherche"

"Configurez le service d'intégration de la recherche"

Considérations relatives aux services de plateforme

Avant de mettre en œuvre des services de plateforme, examinez les recommandations et les considérations relatives à l'utilisation de ces services.

Pour plus d'informations sur S3, reportez-vous à la section "UTILISEZ L'API REST S3".

Considérations relatives à l'utilisation des services de plate-forme

Réflexion	Détails
Surveillance des terminaux de destination	Vous devez surveiller la disponibilité de chaque point final de destination. Si la connexion au point final de destination est perdue pendant une période prolongée et qu'il existe un important retard de requêtes, les demandes client supplémentaires (telles QUE LES requêtes ENVOYÉES) à StorageGRID échoueront. Vous devez réessayer ces demandes ayant échoué lorsque le noeud final devient accessible.
Limitation du terminal de destination	Le logiciel StorageGRID peut canaliser les demandes S3 entrantes pour un compartiment si le taux d'envoi des demandes dépasse le taux à partir duquel le terminal de destination peut recevoir les demandes. La restriction ne se produit que lorsqu'il existe un arriéré de demandes en attente d'envoi vers le noeud final de destination. Le seul effet visible est que les requêtes S3 entrantes prennent plus de temps à s'exécuter. Si vous commencez à détecter les performances beaucoup plus lentes, vous devez réduire le taux d'entrée ou utiliser un terminal avec une capacité plus élevée. Si l'carnet de commandes des requêtes continue d'augmenter, les opérations S3 des clients (par EXEMPLE, LES requêtes PUT) finiront par échouer. Les demandes CloudMirror sont plus susceptibles d'être affectées par les performances du terminal de destination, car ces demandes impliquent généralement plus de transfert de données que les demandes d'intégration de recherche ou de notification d'événements.
Garanties de commande	StorageGRID garantit l'ordre des opérations sur un objet d'un site. Tant que toutes les opérations relatives à un objet se trouvent sur le même site, l'état final de l'objet (pour la réplication) sera toujours égal à l'état dans StorageGRID. StorageGRID tente également de commander des demandes lorsque des opérations sont effectuées sur des sites StorageGRID. Par exemple, si vous écrivez un objet initialement sur le site A, puis que vous le remplacez par un autre objet au niveau du site B, le dernier objet répliqué par CloudMirror vers le compartiment de destination n'est pas garanti que ce nouvel objet soit.

Réflexion	Détails
Suppressions d'objets basées sur des règles ILM	Pour correspondre au comportement de suppression des services CRR et SNS d'AWS, les requêtes CloudMirror et de notification d'événement ne sont pas envoyées lorsqu'un objet du compartiment source est supprimé en raison des règles ILM de StorageGRID. Par exemple, aucune demande de notification de CloudMirror ou d'événement n'est envoyée si une règle ILM supprime un objet au bout de 14 jours. Au contraire, les demandes d'intégration de la recherche sont envoyées lorsque les objets sont supprimés du fait de ILM.

Considérations relatives à l'utilisation du service de réplication CloudMirror

Réflexion	Détails
État de la réplication	StorageGRID ne prend pas en charge le `x-amz-replication-status` en-tête.
Taille de l'objet	La taille maximale des objets qui peuvent être répliqués dans un compartiment de destination par le service de réplication CloudMirror est de 5 Tio, soit la même que la taille maximale de l'objet *pris en charge*. **Remarque** : la taille maximale *recommandée* pour une opération d'objet PUT simple est de 5 Gio (5,368,709,120 octets). Si vos objets sont supérieurs à 5 Gio, utilisez le téléchargement partitionné.
Gestion des versions du compartiment et ID de version	Si le compartiment S3 source de StorageGRID est activé pour la gestion des versions, vous devez également activer la gestion des versions pour le compartiment de destination. Lors de l'utilisation du contrôle de version, notez que l'ordre des versions d'objet dans le compartiment de destination est meilleur effort et n'est pas garanti par le service CloudMirror, en raison des limites du protocole S3. **Remarque** : les ID de version du compartiment source dans StorageGRID ne sont pas liés aux ID de version du compartiment de destination.
Balisage des versions d'objets	Le service CloudMirror ne réplique pas les demandes DE balisage d'objets PUT ou DELETE Object tagging qui fournissent un ID de version, en raison des limitations du protocole S3. Étant donné que les ID de version de la source et de la destination ne sont pas liés, il n'est pas possible de s'assurer qu'une mise à jour de balise vers un ID de version spécifique sera répliquée. En revanche, le service CloudMirror réplique les demandes DE balisage D'objets PUT ou SUPPRIME les demandes de balisage d'objets qui ne spécifient pas d'ID de version. Ces demandes mettent à jour les balises pour la clé la plus récente (ou la dernière version si le compartiment est versionné). Les ings normaux avec des étiquettes (et non les mises à jour de marquage) sont également répliqués.

Réflexion	Détails
Téléchargements partitionnés et `ETag` valeurs	Lors de la mise en miroir d'objets qui ont été téléchargés à l'aide d'un téléchargement partitionné, le service CloudMirror ne conserve pas les pièces. En conséquence, le `ETag` la valeur de l'objet symétrique sera différente de la `ETag` valeur de l'objet d'origine.
Chiffrement des objets avec SSE-C (chiffrement côté serveur avec clés fournies par le client)	Le service CloudMirror ne prend pas en charge les objets chiffrés avec SSE-C. Si vous tentez d'ingérer un objet dans le compartiment source pour la réplication CloudMirror et que la demande inclut les en-têtes de requête SSE-C, l'opération échoue.
Compartiment avec verrouillage objet S3 activé	Si le compartiment S3 de destination pour la réplication CloudMirror est activé pour le verrouillage des objets S3, la tentative de configuration de la réplication de compartiment (RÉPLICATION PUT bucket) échoue avec une erreur AccessDenied.

Configurer les terminaux des services de plateforme

Avant de pouvoir configurer un service de plateforme pour un compartiment, vous devez configurer au moins un point de terminaison afin qu'il soit la destination du service de plateforme.

L'accès aux services de plateforme est activé par locataire par administrateur StorageGRID. Pour créer ou utiliser un noeud final de services de plate-forme, vous devez être un utilisateur locataire disposant de l'autorisation gérer les noeuds finaux ou accès racine, dans une grille dont la mise en réseau a été configurée pour permettre aux noeuds de stockage d'accéder aux ressources de noeuds finaux externes. Pour plus d'informations, contactez votre administrateur StorageGRID.

Qu'est-ce qu'un terminal de services de plateforme ?

Lorsque vous créez un noeud final de services de plate-forme, vous spécifiez les informations dont StorageGRID a besoin pour accéder à la destination externe.

Par exemple, si vous souhaitez répliquer des objets à partir d'un compartiment StorageGRID vers un compartiment Amazon S3, vous créez un terminal des services de plateforme qui inclut les informations et les identifiants dont StorageGRID a besoin pour accéder au compartiment de destination sur Amazon.

Chaque type de service de plate-forme nécessite son propre terminal, vous devez donc configurer au moins un point final pour chaque service de plate-forme que vous prévoyez d'utiliser. Après avoir défini un noeud final de services de plate-forme, vous utilisez l'URN du noeud final comme destination dans le XML de configuration utilisé pour activer le service.

Vous pouvez utiliser le même point final que la destination pour plusieurs compartiments source. Par exemple, vous pouvez configurer plusieurs compartiments source pour envoyer les métadonnées d'objet vers le même point de terminaison d'intégration de la recherche, afin d'effectuer des recherches dans plusieurs compartiments. Vous pouvez également configurer un compartiment source pour utiliser plusieurs points de terminaison comme cible, ce qui vous permet d'envoyer des notifications sur la création d'objet à une rubrique SNS et des notifications sur la suppression d'objet à une autre rubrique SNS.

Terminaux pour la réplication CloudMirror

StorageGRID prend en charge les terminaux de réplication qui représentent des compartiments S3. Ces compartiments peuvent être hébergés sur Amazon Web Services, sur le même déploiement StorageGRID, sur un autre service ou sur un autre déploiement à distance.

Terminaux pour les notifications

StorageGRID prend en charge les terminaux SNS (simple notification Service). Les terminaux SQS (simple Queue Service) ou Lambda d'AWS ne sont pas pris en charge.

Points d'extrémité du service d'intégration de la recherche

StorageGRID prend en charge des terminaux d'intégration de recherche représentant les clusters Elasticsearch. Ces clusters Elasticsearch peuvent se trouver dans un data Center local ou être hébergés dans un cloud AWS ou ailleurs.

Le point final de l'intégration de la recherche fait référence à un index et à un type Elasticsearch spécifiques. Vous devez créer l'index dans Elasticsearch avant la création du noeud final dans StorageGRID, sinon la création du noeud final échouera. Il n'est pas nécessaire de créer le type avant de créer le noeud final. StorageGRID crée le type si nécessaire lors de l'envoi de métadonnées d'objet au terminal.

Informations associées

"Administrer StorageGRID"

Spécifiez l'URN du terminal des services de plateforme

Lorsque vous créez un noeud final de services de plate-forme, vous devez spécifier un Nom de ressource unique (URN). Vous utiliserez l'URN pour référencer le noeud final lorsque vous créez un XML de configuration pour le service de plate-forme. L'URN de chaque terminal doit être unique.

StorageGRID valide les terminaux de services de plateforme lors de leur création. Avant de créer un noeud final de services de plate-forme, vérifiez que la ressource spécifiée dans le noeud final existe et qu'elle peut être atteinte.

Éléments DE RETOUR

L'URN d'un terminal de services de plateforme doit commencer par l'un ou l'autre `arn:aws` ou `urn:mysite`, comme suit:

- Si ce service est hébergé sur Amazon Web Services (AWS), utilisez `arn:aws`.
- Si ce service est hébergé sur Google Cloud Platform (GCP), utilisez `arn:aws`.
- Si le service est hébergé localement, utilisez `urn:mysite`

Par exemple, si vous spécifiez l'URN pour un terminal CloudMirror hébergé sur StorageGRID, il peut commencer par l'URN `urn:sgws`.

L'élément suivant de l'URN spécifie le type de service de plateforme, comme suit :

Service	Type
Réplication CloudMirror	s3
Notifications	sns
Intégration de la recherche	es

Par exemple, pour continuer à spécifier l'URN d'un terminal CloudMirror hébergé sur StorageGRID, vous devez ajouter `s3` pour obtenir `urn:sgws:s3`.

L'élément final de l'URN identifie la ressource cible spécifique au niveau de l'URI de destination.

Service	Ressource spécifique
Réplication CloudMirror	nom du compartiment
Notifications	nom-rubrique-sns
Intégration de la recherche	`domain-name/index-name/type-name` **Remarque :** si le cluster Elasticsearch est **NOT** configuré pour créer automatiquement des index, vous devez créer l'index manuellement avant de créer le noeud final.

Urns pour les services hébergés sur AWS et GCP

Pour les entités AWS et GCP, l'URN complet est un ARN AWS valide. Par exemple :

- Réplication CloudMirror :

```
arn:aws:s3:::bucket-name
```

- Notifications :

```
arn:aws:sns:region:account-id:topic-name
```

- Intégration de la recherche :

```
arn:aws:es:region:account-id:domain/domain-name/index-name/type-name
```

Pour un terminal d'intégration de recherche AWS, le `domain-name` doit inclure la chaîne littérale `domain/`, comme indiqué ici.

Urnes pour des services hébergés localement

Lors de l'utilisation de services hébergés localement au lieu de services cloud, vous pouvez spécifier l'URN de toute façon qui crée un URN valide et unique, tant que l'URN inclut les éléments requis dans les troisième et dernière positions. Vous pouvez laisser les éléments indiqués en blanc facultatif, ou vous pouvez les spécifier de quelque manière que ce soit pour vous aider à identifier la ressource et à rendre l'URN unique. Par exemple :

- Réplication CloudMirror :

```
urn:mysite:s3:optional:optional:bucket-name
```

  Pour un terminal CloudMirror hébergé sur StorageGRID, vous pouvez spécifier un URN valide commençant par `urn:sgws`:

```
urn:sgws:s3:optional:optional:bucket-name
```

- Notifications :

```
urn:mysite:sns:optional:optional:sns-topic-name
```

- Intégration de la recherche :

```
urn:mysite:es:optional:optional:domain-name/index-name/type-name
```

> ⓘ Pour les points de terminaison d'intégration de recherche hébergés localement, le `domain-name` L'élément peut être n'importe quelle chaîne tant que l'URN du terminal est unique.

Créer un terminal de services de plate-forme

Vous devez créer au moins un noeud final du type correct avant d'activer un service de plate-forme.

Avant de commencer

- Vous êtes connecté au Gestionnaire de locataires à l'aide d'un "navigateur web pris en charge".
- Les services de plateforme ont été activés pour votre compte de locataire par un administrateur StorageGRID.
- Vous appartenez à un groupe d'utilisateurs qui possède le "Gestion des noeuds finaux ou des autorisations d'accès racine".
- La ressource référencée par le noeud final des services de plate-forme a été créée :
  - Réplication CloudMirror : compartiment S3
  - Notification d'événement : rubrique SNS
  - Notification de recherche : index Elasticsearch, si le cluster de destination n'est pas configuré pour

créer automatiquement des index.

- Vous disposez des informations relatives à la ressource de destination :
  - Hôte et port pour l'URI (Uniform Resource identifier)

    > Si vous prévoyez d'utiliser un compartiment hébergé sur un système StorageGRID comme point de terminaison pour la réplication CloudMirror, contactez l'administrateur de la grille pour déterminer les valeurs à saisir.

  - Nom de ressource unique (URN)

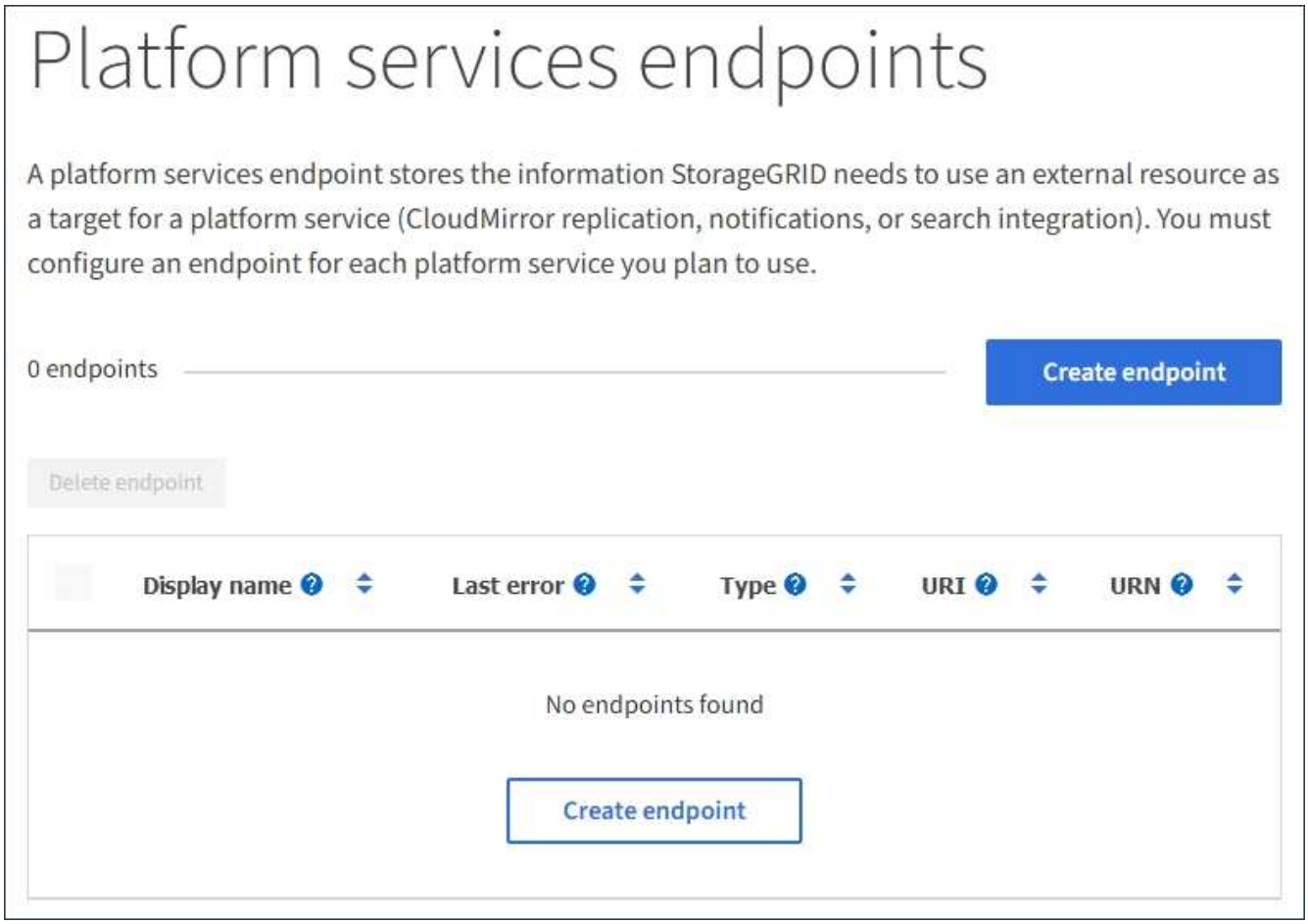
    "Spécifiez l'URN du terminal des services de plateforme"

  - Informations d'authentification (si nécessaire) :
    - Clé d'accès : ID de clé d'accès et clé d'accès secrète
    - HTTP de base : nom d'utilisateur et mot de passe
    - CAP (C2S Access Portal) : URL d'informations d'identification temporaires, certificats de serveur et de client, clés client et phrase de passe de clé privée de client facultative.
  - Certificat de sécurité (en cas d'utilisation d'un certificat d'autorité de certification personnalisé)
- Si les fonctions de sécurité de Elasticsearch sont activées, vous disposez du privilège Monitor cluster pour les tests de connectivité et du privilège write index ou des privilèges index and delete index pour les mises à jour de documents.

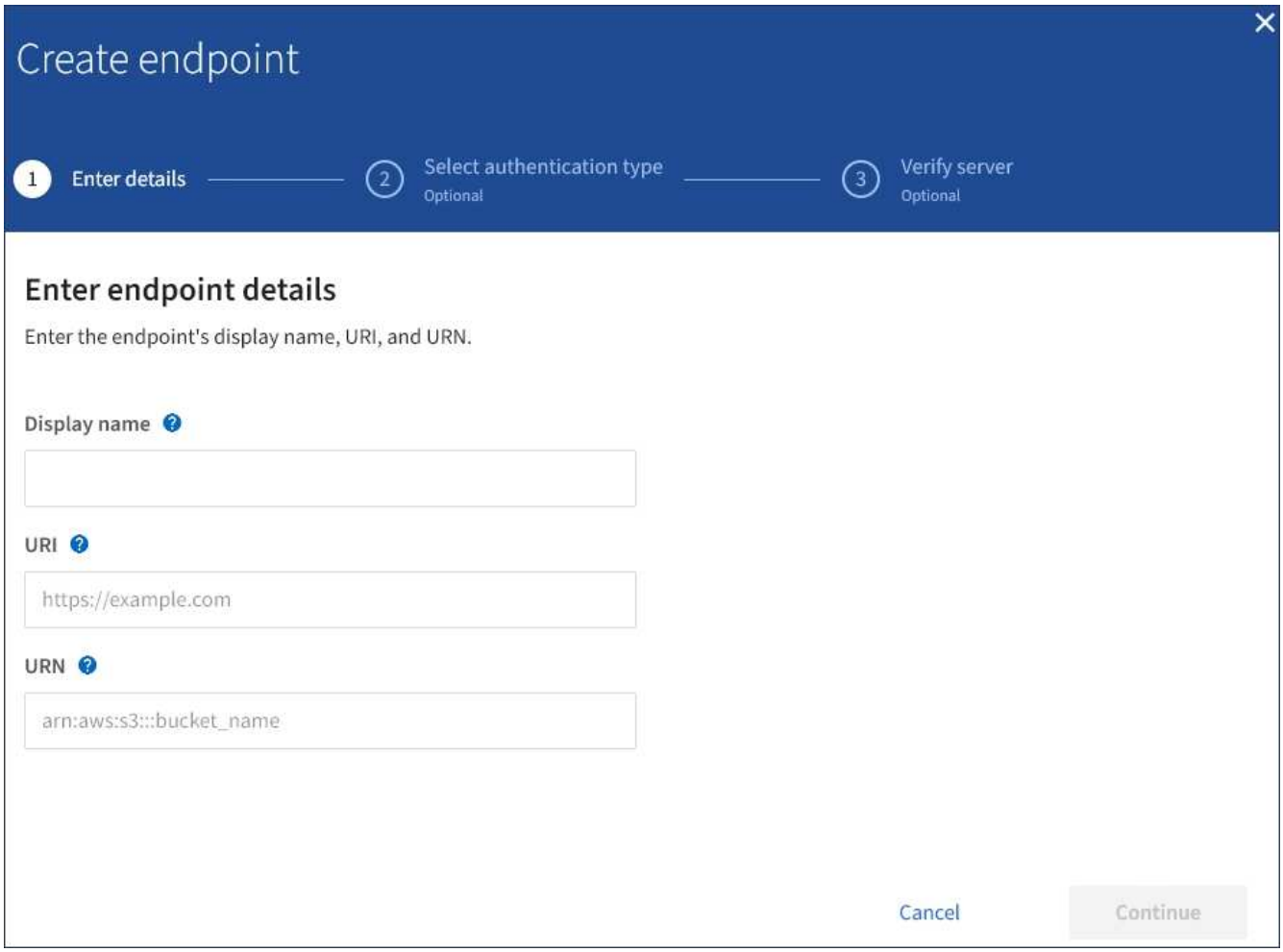
Étapes

1. Sélectionnez **STORAGE (S3)** > **Platform services Endpoints**.

   La page noeuds finaux des services de plate-forme s'affiche.



2. Sélectionnez **Créer un noeud final**.



3. Entrez un nom d'affichage pour décrire brièvement le point final et son objectif.

   Le type de service de plate-forme pris en charge par le noeud final est affiché à côté du nom du noeud final lorsqu'il est répertorié sur la page noeuds finaux, de sorte que vous n'avez pas besoin d'inclure ces informations dans le nom.

4. Dans le champ **URI**, spécifiez l'identificateur de ressource unique (URI) du noeud final.

   Utilisez l'un des formats suivants :

   ```
   https://host:port
   http://host:port
   ```

   Si vous ne spécifiez pas de port, le port 443 est utilisé pour les URI HTTPS et le port 80 est utilisé pour les URI HTTP.

   Par exemple, l'URI d'un compartiment hébergé sur StorageGRID peut être :

   ```
   https://s3.example.com:10443
   ```

   Dans cet exemple, `s3.example.com` Représente l'entrée DNS pour l'adresse IP virtuelle (VIP) du groupe

haute disponibilité StorageGRID, et `10443` représente le port défini dans le noeud final de l'équilibreur de charge.

> Si possible, vous devez vous connecter à un groupe haute disponibilité de nœuds d'équilibrage de la charge pour éviter un point de défaillance unique.

De la même manière, l'URI d'un compartiment hébergé sur AWS peut être :

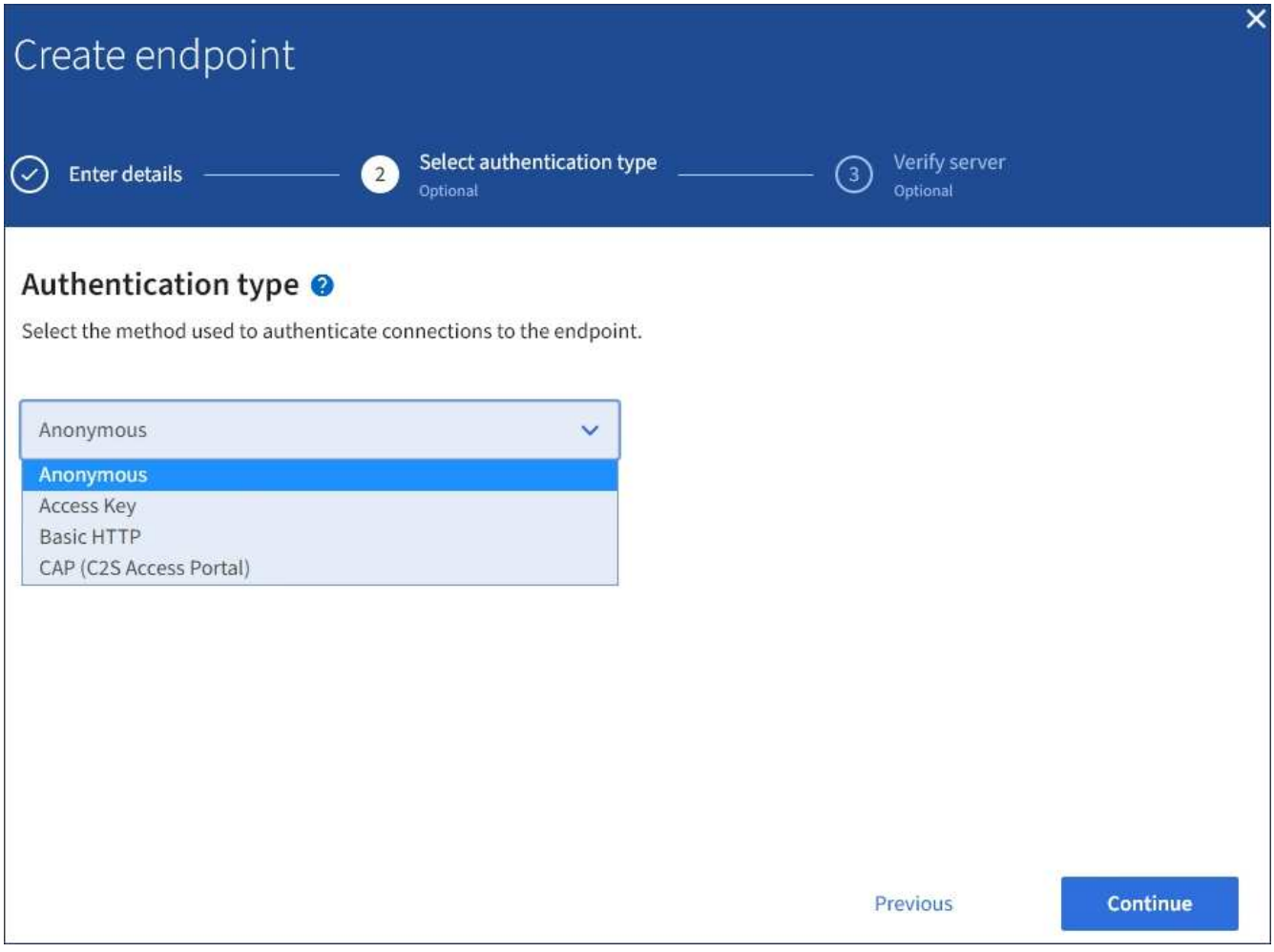
```
https://s3-aws-region.amazonaws.com
```

> Si le noeud final est utilisé pour le service de réplication CloudMirror, n'incluez pas le nom de compartiment dans l'URI. Vous incluez le nom du compartiment dans le champ **URN**.

5. Entrez le nom de ressource unique (URN) du noeud final.

> Vous ne pouvez pas modifier l'URN d'un noeud final après sa création.

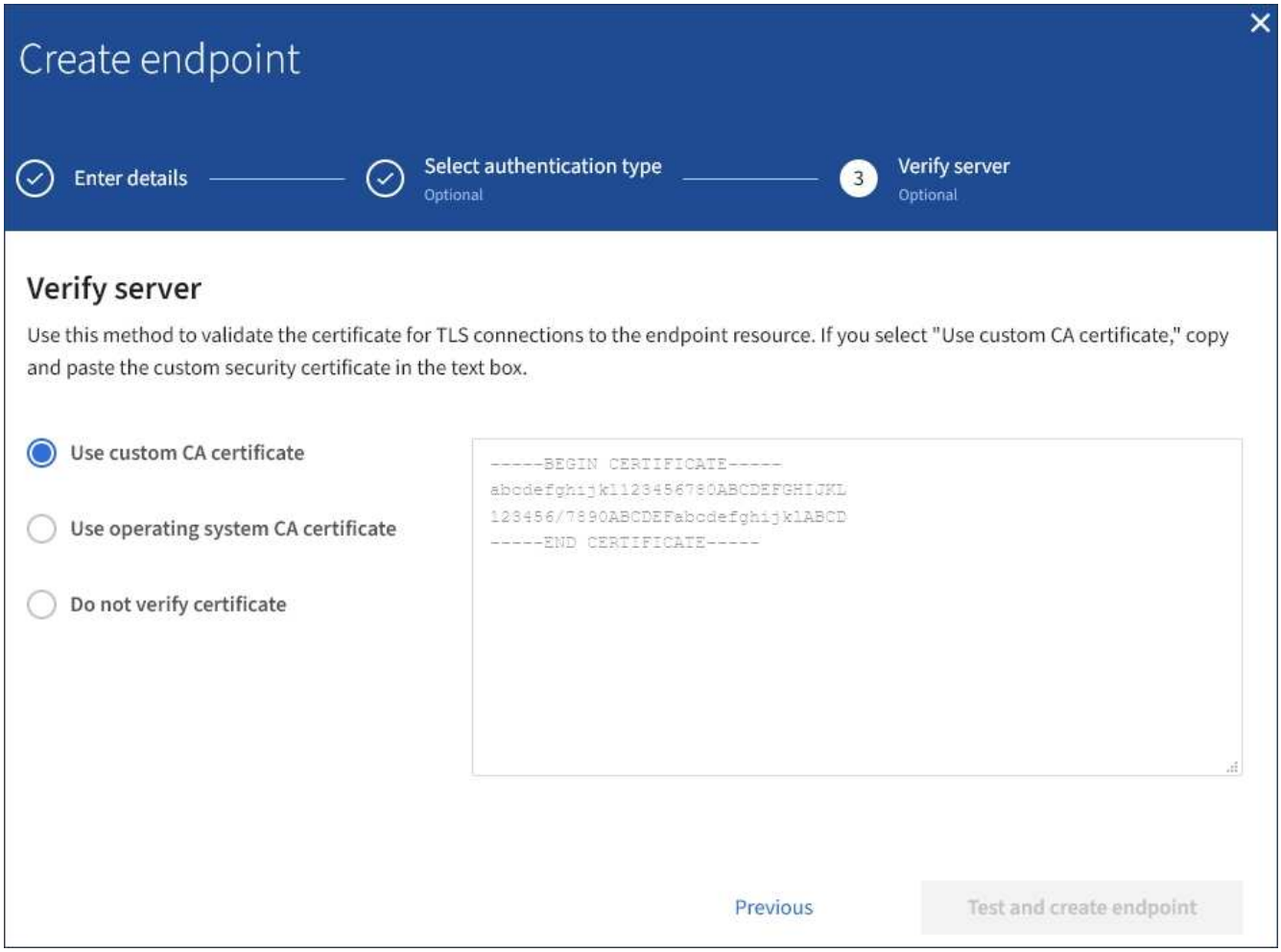
6. Sélectionnez **Continuer**.
7. Sélectionnez une valeur pour **Type d'authentification**, puis saisissez ou téléchargez les informations d'identification requises.



Les informations d'identification que vous fournissez doivent disposer d'autorisations d'écriture pour la ressource de destination.

Type d'authentification	Description	Informations d'identification
Anonyme	Fournit un accès anonyme à la destination. Fonctionne uniquement pour les terminaux dont la sécurité est désactivée.	Pas d'authentification.
Clé d'accès	Utilise des identifiants de style AWS pour authentifier les connexions avec la destination.	• ID de clé d'accès • Clé d'accès secrète
HTTP de base	Utilise un nom d'utilisateur et un mot de passe pour authentifier les connexions à la destination.	• Nom d'utilisateur • Mot de passe
CAP (portail d'accès C2S)	Utilise des certificats et des clés pour authentifier les connexions à la destination.	• URL des informations d'identification temporaires • Certificat autorité de certification du serveur (téléchargement de fichiers PEM) • Certificat client (téléchargement de fichier PEM) • Clé privée client (téléchargement de fichiers PEM, format crypté OpenSSL ou format de clé privée non crypté) • Phrase de passe de clé privée du client (facultatif)

8. Sélectionnez **Continuer**.
9. Sélectionnez un bouton radio pour **Verify Server** pour choisir la manière dont la connexion TLS au noeud final est vérifiée.



Type de vérification du certificat	Description
Utiliser un certificat d'autorité de certification personnalisé	Utilisez un certificat de sécurité personnalisé. Si vous sélectionnez ce paramètre, copiez et collez le certificat de sécurité personnalisé dans la zone de texte **certificat CA**.
Utiliser le certificat CA du système d'exploitation	Utilisez le certificat d'autorité de certification Grid par défaut installé sur le système d'exploitation pour sécuriser les connexions.
Ne vérifiez pas le certificat	Le certificat utilisé pour la connexion TLS n'est pas vérifié. Cette option n'est pas sécurisée.

10. Sélectionnez **Test et Créer un noeud final**.
    - Un message de réussite s'affiche si le noeud final peut être atteint à l'aide des informations d'identification spécifiées. La connexion au noeud final est validée à partir d'un nœud sur chaque site.
    - Un message d'erreur s'affiche si la validation du noeud final échoue. Si vous devez modifier le noeud final pour corriger l'erreur, sélectionnez **Retour aux détails du noeud final** et mettez à jour les informations. Sélectionnez ensuite **Test et Créer un noeud final**.

> La création du terminal échoue si les services de plate-forme ne sont pas activés pour votre compte de locataire. Veuillez contacter votre administrateur StorageGRID.

Après avoir configuré un noeud final, vous pouvez utiliser son URN pour configurer un service de plate-forme.

Informations associées

"Spécifiez l'URN du terminal des services de plateforme"

"Configurez la réplication CloudMirror"

"Configurer les notifications d'événements"

"Configurez le service d'intégration de la recherche"

Tester la connexion pour le point final des services de plate-forme

Si la connexion à un service de plate-forme a changé, vous pouvez tester la connexion du noeud final pour vérifier que la ressource de destination existe et qu'elle peut être atteinte à l'aide des informations d'identification que vous avez spécifiées.

Avant de commencer

- Vous êtes connecté au Gestionnaire de locataires à l'aide d'un "navigateur web pris en charge".
- Vous appartenez à un groupe d'utilisateurs qui possède le "Gestion des noeuds finaux ou des autorisations d'accès racine".

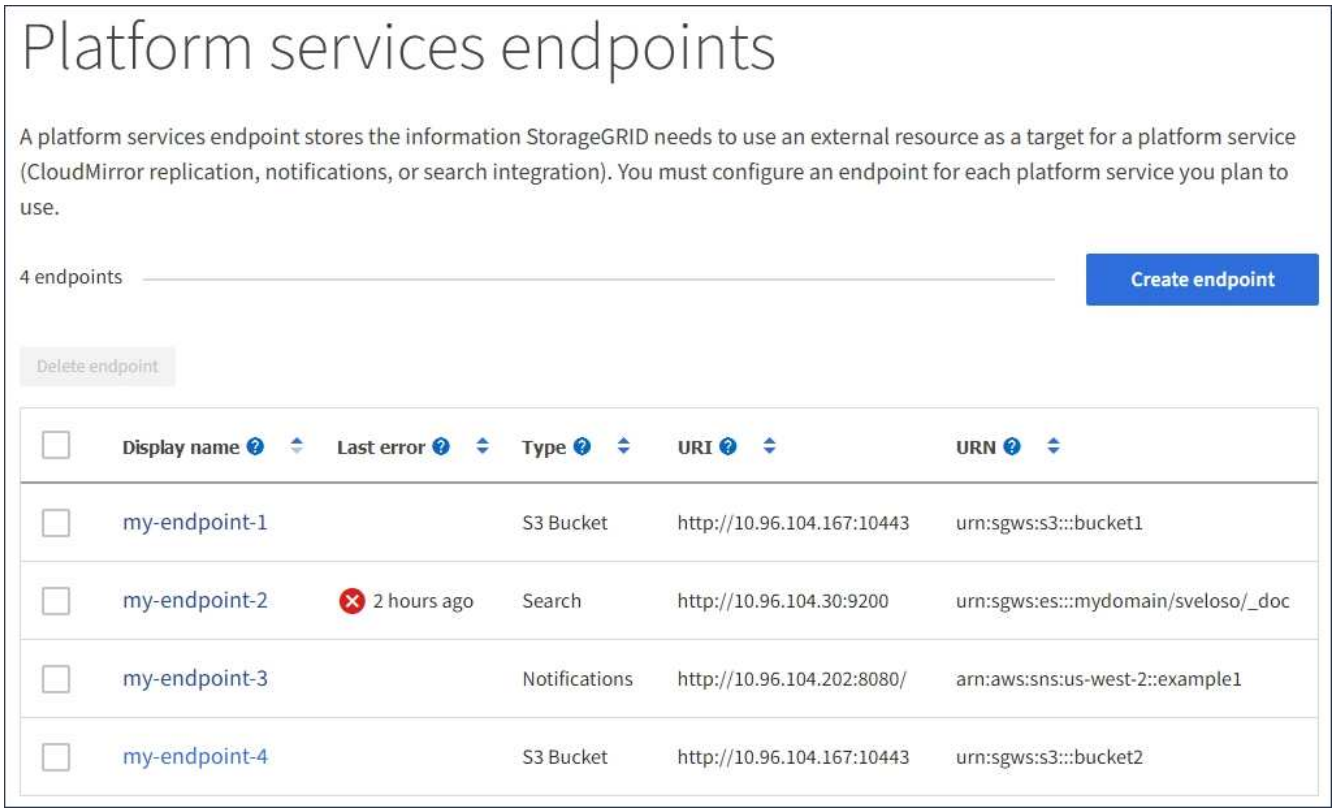
Description de la tâche

StorageGRID ne vérifie pas que les informations d'identification disposent des autorisations appropriées.

Étapes

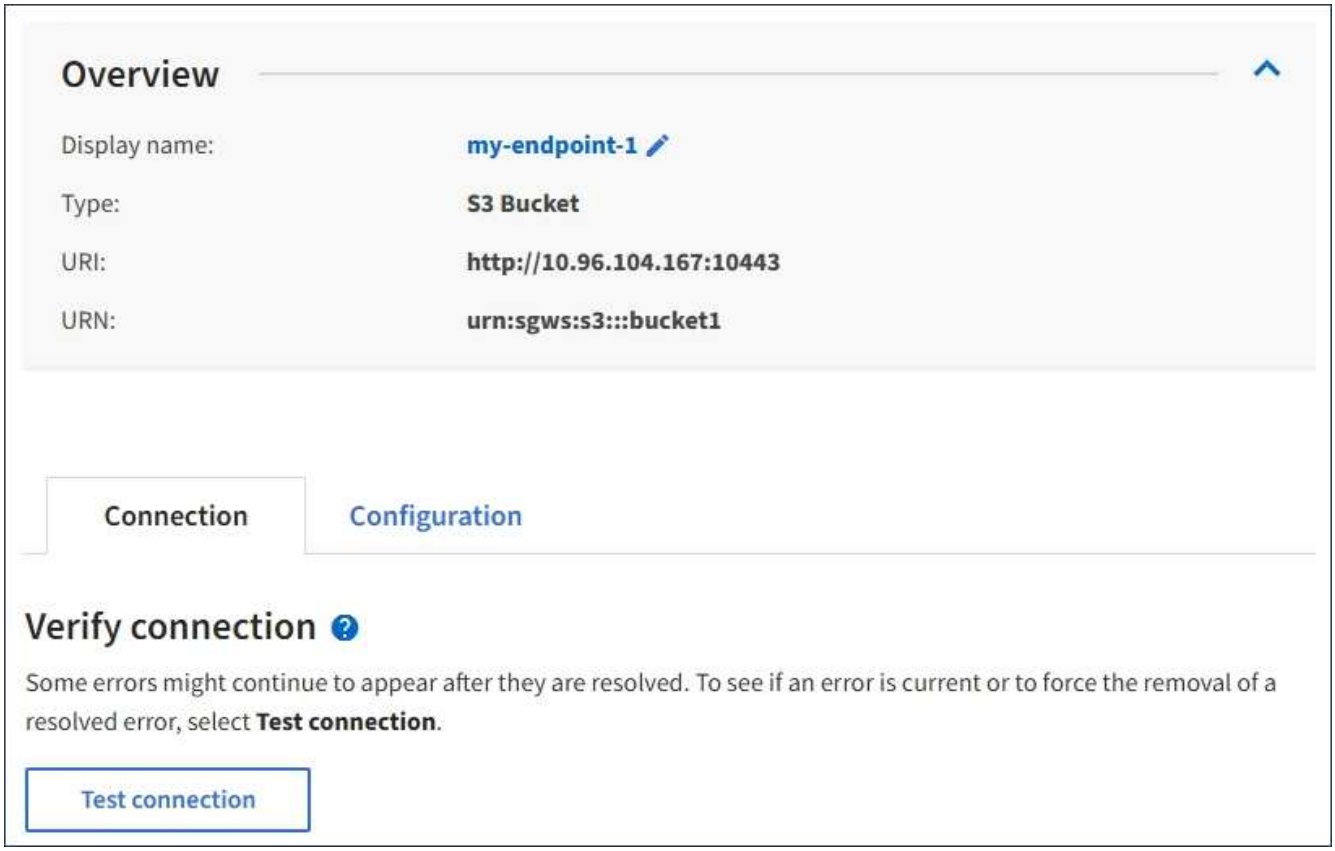
1. Sélectionnez **STORAGE (S3)** > **Platform services Endpoints**.

   La page noeuds finaux des services de plate-forme s'affiche et affiche la liste des noeuds finaux des services de plate-forme déjà configurés.



2. Sélectionnez le noeud final dont vous souhaitez tester la connexion.

   La page des détails du point final s'affiche.



3. Sélectionnez **Tester la connexion**.

- Un message de réussite s'affiche si le noeud final peut être atteint à l'aide des informations d'identification spécifiées. La connexion au noeud final est validée à partir d'un nœud sur chaque site.
- Un message d'erreur s'affiche si la validation du noeud final échoue. Si vous devez modifier le noeud final pour corriger l'erreur, sélectionnez **Configuration** et mettez à jour les informations. Sélectionnez ensuite **Test et enregistrer les modifications**.

Modifier le point final des services de plate-forme

Vous pouvez modifier la configuration d'un point de terminaison de services de plate-forme pour modifier son nom, son URI ou d'autres détails. Par exemple, vous devrez peut-être mettre à jour les informations d'identification expirées ou modifier l'URI pour qu'il pointe vers un index Elasticsearch de sauvegarde pour le basculement. Vous ne pouvez pas modifier l'URN d'un terminal de services de plate-forme.

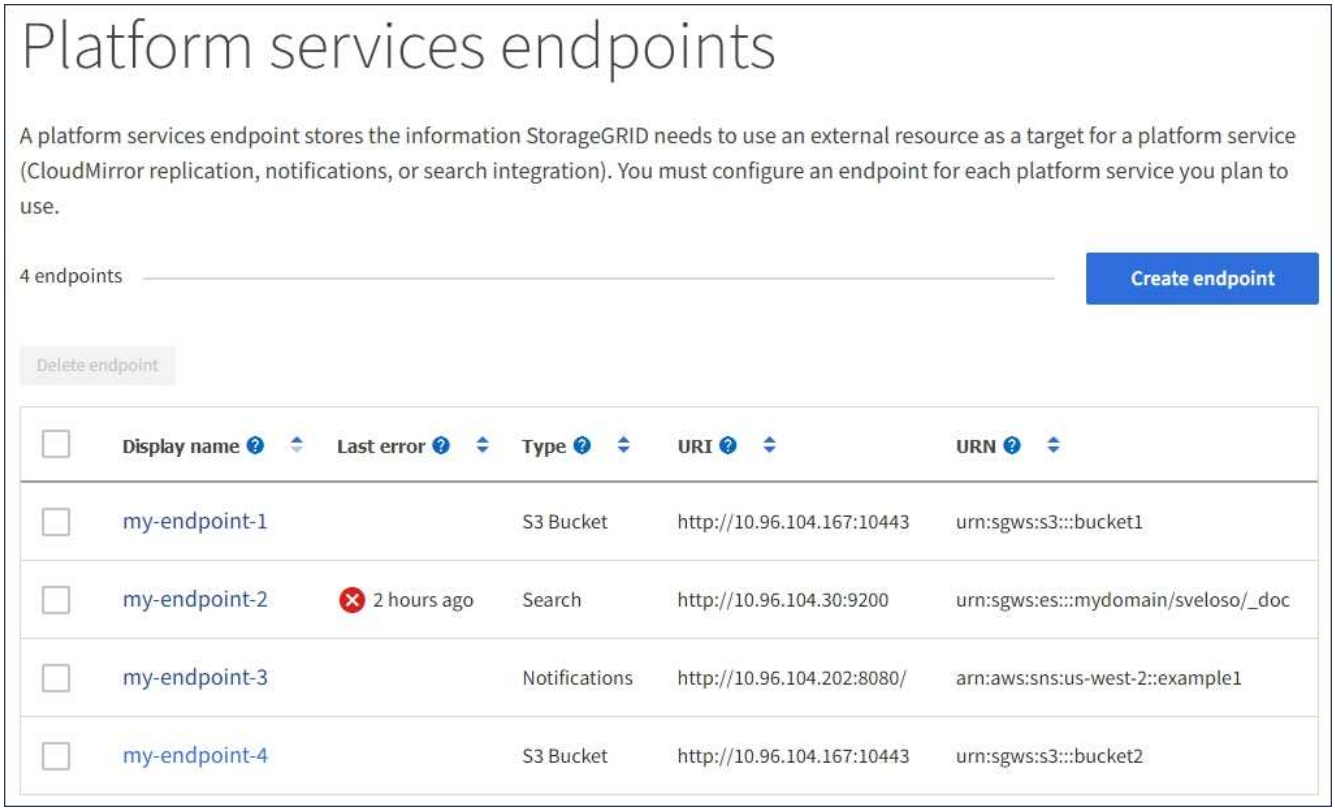
Avant de commencer

- Vous êtes connecté au Gestionnaire de locataires à l'aide d'un "navigateur web pris en charge".
- Vous appartenez à un groupe d'utilisateurs qui possède le "Gestion des noeuds finaux ou des autorisations d'accès racine".

Étapes

1. Sélectionnez **STORAGE (S3)** > **Platform services Endpoints**.

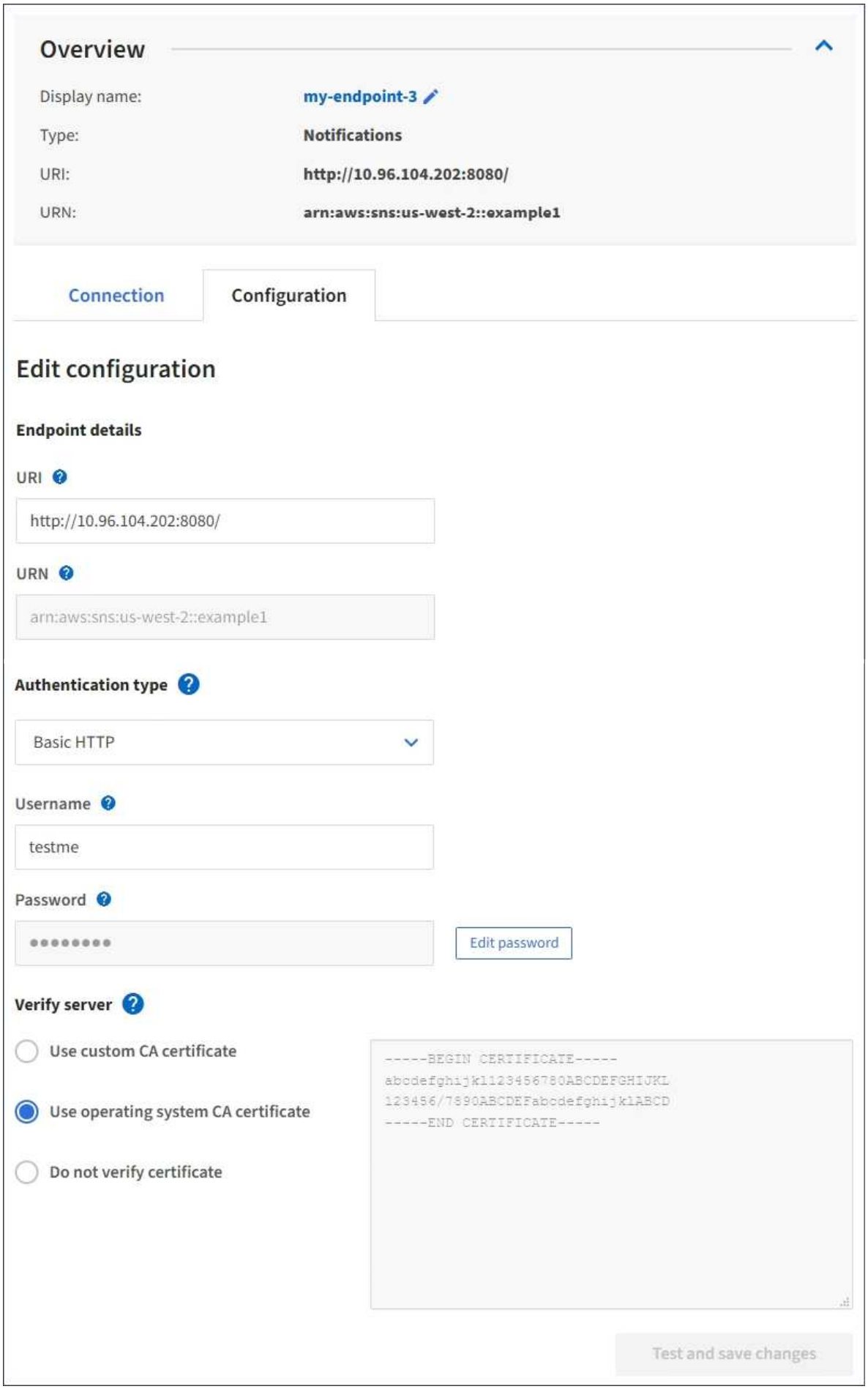
   La page noeuds finaux des services de plate-forme s'affiche et affiche la liste des noeuds finaux des services de plate-forme déjà configurés.



2. Sélectionnez le point final que vous souhaitez modifier.

   La page des détails du point final s'affiche.

3. Sélectionnez **Configuration**.


Overview
Display name:
my-endpoint-3
Type:
Notifications
URI:
http://10.96.104.202:8080/
URN:
arn:aws:sns:us-west-2::example1
Connection
Configuration
Edit configuration
Endpoint details
URI
http://10.96.104.202:8080/
URN
arn:aws:sns:us-west-2::example1
Authentication type
Basic HTTP
Username
testme
Password
Edit password
Verify server
Use custom CA certificate
Use operating system CA certificate
Do not verify certificate
-----BEGIN CERTIFICATE-----
abcdefghijkl123456780ABCDEFGHIJKL
123456/7890ABCDEFabcdefghijklABCD
-----END CERTIFICATE-----
Test and save changes

4. Modifiez la configuration du noeud final selon les besoins.

   Vous ne pouvez pas modifier l'URN d'un noeud final après sa création.

   a. Pour modifier le nom d'affichage du noeud final, sélectionnez l'icône d'édition .
   b. Modifiez l'URI si nécessaire.
   c. Si nécessaire, modifiez le type d'authentification.
      - Pour l'authentification par clé d'accès, modifiez la clé selon vos besoins en sélectionnant **Modifier la clé S3** et en collant une nouvelle ID de clé d'accès et une nouvelle clé d'accès secrète. Si vous devez annuler vos modifications, sélectionnez **Revert S3 key edit**.
      - Pour l'authentification HTTP de base, modifiez le nom d'utilisateur si nécessaire. Modifiez le mot de passe selon vos besoins en sélectionnant **Modifier le mot de passe** et en saisissant le nouveau mot de passe. Si vous devez annuler vos modifications, sélectionnez **Revert password edit**.
      - Pour l'authentification CAP (C2S Access Portal), modifiez l'URL des informations d'identification temporaires ou la phrase de passe de la clé privée du client facultative et téléchargez de nouveaux certificats et fichiers de clés selon les besoins.

        La clé privée du client doit être au format crypté OpenSSL ou au format de clé privée non crypté.

   d. Si nécessaire, modifiez la méthode de vérification du serveur.
5. Sélectionnez **Tester et enregistrer les modifications**.
   - Un message de réussite s'affiche si le noeud final peut être atteint à l'aide des informations d'identification spécifiées. La connexion au noeud final est vérifiée à partir d'un noeud sur chaque site.
   - Un message d'erreur s'affiche si la validation du noeud final échoue. Modifiez le noeud final pour corriger l'erreur, puis sélectionnez **Test et enregistrer les modifications**.

Supprimer le noeud final des services de plate-forme

Vous pouvez supprimer un noeud final si vous ne souhaitez plus utiliser le service de plate-forme associé.

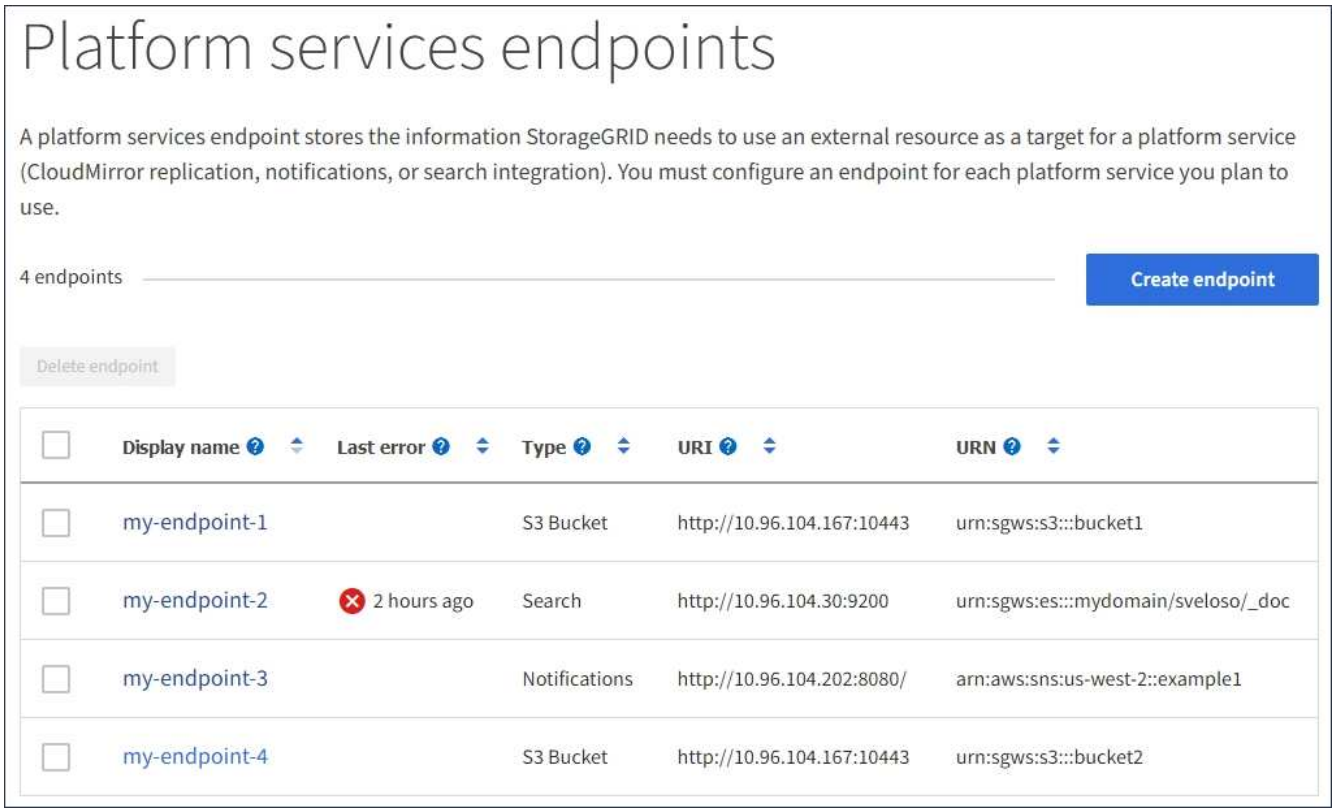
Avant de commencer

- Vous êtes connecté au Gestionnaire de locataires à l'aide d'un "navigateur web pris en charge".
- Vous appartenez à un groupe d'utilisateurs qui possède le "Gestion des noeuds finaux ou des autorisations d'accès racine".

Étapes

1. Sélectionnez **STORAGE (S3)** > **Platform services Endpoints**.

   La page noeuds finaux des services de plate-forme s'affiche et affiche la liste des noeuds finaux des services de plate-forme déjà configurés.

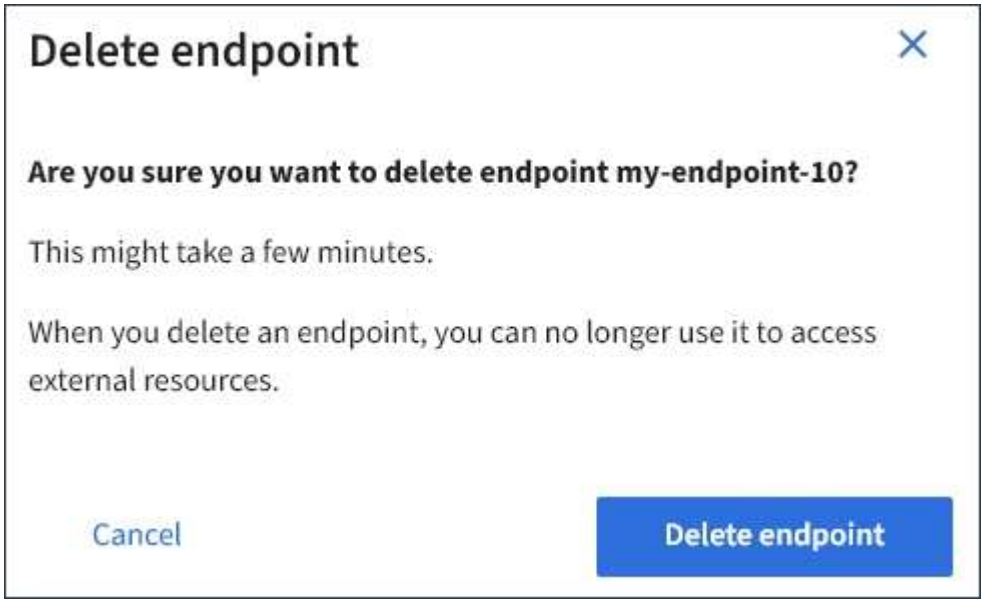


2. Cochez la case correspondant à chaque point final à supprimer.

> Si vous supprimez un noeud final de services de plate-forme en cours d'utilisation, le service de plate-forme associé sera désactivé pour tous les compartiments qui utilisent le noeud final. Toutes les demandes qui n'ont pas encore été traitées seront supprimées. Toutes les nouvelles demandes seront toujours générées jusqu'à ce que vous modifiiez la configuration de compartiment pour ne plus référencer l'URN supprimé. StorageGRID signale ces demandes comme des erreurs irrécupérables.

3. Sélectionnez **actions** > **Supprimer le point final**.

   Un message de confirmation s'affiche.



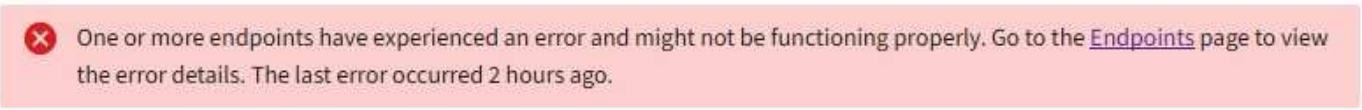
4. Sélectionnez **Supprimer le point final**.

Dépanner les erreurs de point final des services de plate-forme

Si une erreur se produit lorsque StorageGRID tente de communiquer avec un noeud final de services de plate-forme, un message s'affiche sur le tableau de bord. Sur la page noeuds finaux des services de plate-forme, la colonne dernière erreur indique il y a combien de temps l'erreur s'est produite. Aucune erreur ne s'affiche si les autorisations associées aux informations d'identification d'un noeud final sont incorrectes.

Déterminez si l'erreur s'est produite

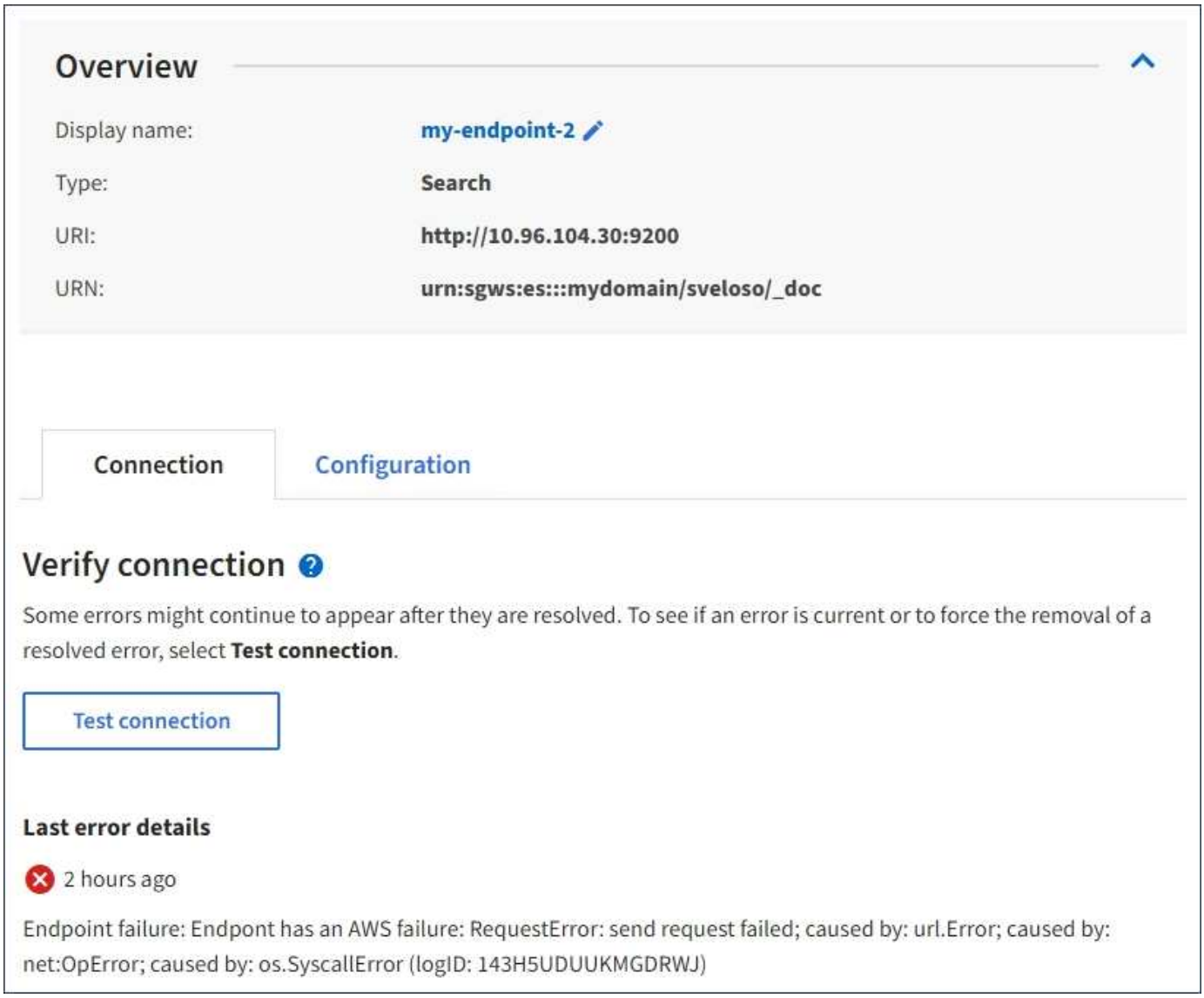
Si des erreurs de noeud final de services de plateforme se sont produites au cours des 7 derniers jours, le tableau de bord du gestionnaire de locataires affiche un message d'alerte. Vous pouvez accéder à la page noeuds finaux des services de plate-forme pour obtenir plus de détails sur l'erreur.



La même erreur qui s'affiche sur le tableau de bord s'affiche également en haut de la page noeuds finaux Platform Services. Pour afficher un message d'erreur plus détaillé :

Étapes

1. Dans la liste des noeuds finaux, sélectionnez le noeud final qui contient l'erreur.
2. Sur la page des détails du noeud final, sélectionnez **connexion**. Cet onglet affiche uniquement l'erreur la plus récente pour un noeud final et indique il y a combien de temps l'erreur s'est produite. Erreurs incluant l'icône X rouge s'est produit au cours des 7 derniers jours.



Vérifiez si l'erreur est toujours à jour

Certaines erreurs peuvent continuer à s'afficher dans la colonne **dernière erreur**, même après leur résolution. Pour voir si une erreur est active ou pour forcer la suppression d'une erreur résolue du tableau :

Étapes

1. Sélectionnez l'extrémité.

   La page des détails du point final s'affiche.

2. Sélectionnez **connexion** > **Tester la connexion**.

La sélection de **Test Connection** permet à StorageGRID de valider l'existence du noeud final des services de plate-forme et de l'atteindre avec les informations d'identification actuelles. La connexion au noeud final est validée à partir d'un nœud sur chaque site.

Résoudre les erreurs de point final

Vous pouvez utiliser le message **dernière erreur** sur la page des détails du noeud final pour déterminer ce qui est à l'origine de l'erreur. Certaines erreurs peuvent vous obliger à modifier le noeud final pour résoudre le

problème. Par exemple, une erreur CloudMirroring peut se produire si StorageGRID ne parvient pas à accéder au compartiment S3 de destination, car il ne dispose pas des autorisations d'accès correctes ou si la clé d'accès a expiré. Le message est ""les identifiants de point de terminaison ou l'accès de destination doivent être mis à jour", et les détails sont "AccessDenied" ou "InvalidAccessKeyId."".

Si vous devez modifier le noeud final pour résoudre une erreur, la sélection de **Test et enregistrer les modifications** fait que StorageGRID valide le noeud final mis à jour et confirme qu'il peut être atteint avec les informations d'identification actuelles. La connexion au noeud final est validée à partir d'un nœud sur chaque site.

Étapes

1. Sélectionnez l'extrémité.
2. Sur la page des détails du noeud final, sélectionnez **Configuration**.
3. Modifiez la configuration de point final selon vos besoins.
4. Sélectionnez **connexion** > **Tester la connexion**.

Identifiants de point de terminaison avec autorisations insuffisantes

Lorsque StorageGRID valide un terminal de services de plateforme, il confirme que les identifiants du terminal peuvent être utilisés pour contacter la ressource de destination et il vérifie les autorisations de base. Cependant, StorageGRID ne valide pas toutes les autorisations requises pour certaines opérations de services de plateforme. Pour cette raison, si vous recevez une erreur lors de la tentative d'utilisation d'un service de plate-forme (par exemple « 403 interdit »), vérifiez les autorisations associées aux identifiants du noeud final.

Informations associées

- "Administration de StorageGRID ; dépannage des services de plate-forme"
- "Créer un terminal de services de plate-forme"
- "Tester la connexion pour le point final des services de plate-forme"
- "Modifier le point final des services de plate-forme"

Configurez la réplication CloudMirror

Le "Service de réplication CloudMirror" Est l'un des trois services de plateforme StorageGRID. Vous pouvez utiliser la réplication CloudMirror pour répliquer automatiquement les objets dans un compartiment S3 externe.

Avant de commencer

- Les services de plateforme ont été activés pour votre compte de locataire par un administrateur StorageGRID.
- Vous avez déjà créé un compartiment qui servira de source de réplication.
- Le noeud final que vous prévoyez d'utiliser comme destination pour la réplication CloudMirror existe déjà, et vous avez son URN.
- Vous appartenez à un groupe d'utilisateurs qui possède le "Gérez tous les compartiments ou l'autorisation d'accès racine". Ces autorisations remplacent les paramètres d'autorisation des stratégies de groupe ou de compartiment lors de la configuration du compartiment à l'aide du Gestionnaire de locataires.

Description de la tâche

La réplication CloudMirror copie les objets à partir d'un compartiment source vers un compartiment de destination spécifié dans un terminal.

La réplication CloudMirror présente des similarités et des différences importantes avec la fonction de réplication multigrille. Pour en savoir plus, voir "Comparez la réplication entre les grilles et la réplication CloudMirror".

Pour activer la réplication CloudMirror pour un compartiment, vous devez créer et appliquer un fichier XML de configuration de réplication de compartiment valide. Le XML de configuration de réplication doit utiliser l'URN d'un terminal de compartiment S3 pour chaque destination.

La réplication n'est pas prise en charge pour les compartiments source ou de destination lorsque le verrouillage d'objet S3 est activé.

Pour obtenir des informations générales sur la réplication de compartiment et la configuration de celle-ci, reportez-vous à la section "Documentation d'Amazon simple Storage Service (S3) : réplication d'objets". Pour plus d'informations sur la manière dont StorageGRID implémente GetBuckeReplication, DeleteBuckeReplication et PutBuckeReplication, reportez-vous au "Opérations sur les compartiments".

Si vous activez la réplication CloudMirror sur un compartiment qui contient des objets, les nouveaux objets ajoutés au compartiment sont répliqués, mais les objets existants du compartiment ne sont pas répliqués. Vous devez mettre à jour des objets existants pour déclencher la réplication.

Si vous spécifiez une classe de stockage dans le fichier XML de configuration de réplication, StorageGRID utilise cette classe lors des opérations sur le terminal S3 de destination. Le noeud final de destination doit également prendre en charge la classe de stockage spécifiée. Veillez à suivre les recommandations fournies par le fournisseur du système de destination.

Étapes

1. Activer la réplication pour le compartiment source :

   Utilisez un éditeur de texte pour créer le XML de configuration de réplication requis pour activer la réplication, comme spécifié dans l'API de réplication S3. Lors de la configuration du XML :

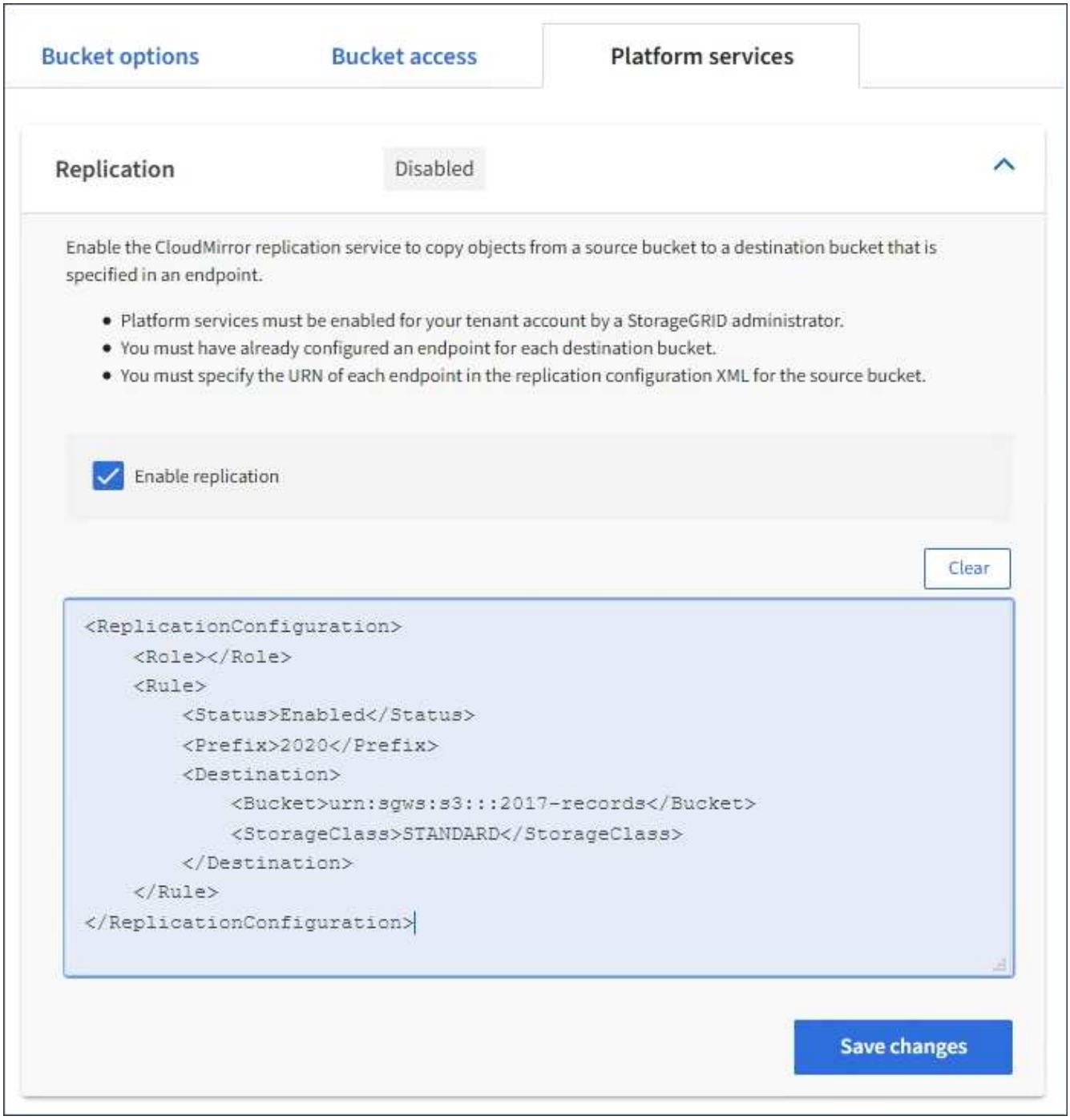
   - Notez que StorageGRID ne prend en charge que le V1 de la configuration de la réplication. Cela signifie que StorageGRID ne prend pas en charge l'utilisation de `Filter` Elément pour les règles, et suit les conventions V1 pour la suppression des versions d'objet. Pour plus d'informations, reportez-vous à la documentation Amazon sur la configuration de la réplication.
   - Utiliser l'URN d'un terminal du compartiment S3 comme destination.
   - Vous pouvez éventuellement ajouter le `<StorageClass>` et spécifiez l'un des éléments suivants :
     - `STANDARD`: La classe de stockage par défaut. Si vous ne spécifiez pas de classe de stockage lors du téléchargement d'un objet, le `STANDARD` la classe de stockage est utilisée.
     - `STANDARD_IA`: (Standard - accès peu fréquent.) Utilisez cette classe de stockage pour les données auxquelles vous accédez moins fréquemment, mais qui exige toujours un accès rapide lorsque cela est nécessaire.
     - `REDUCED_REDUNDANCY`: Utilisez cette classe de stockage pour les données non stratégiques reproductibles qui peuvent être stockées avec moins de redondance que le `STANDARD` classe de stockage.
   - Si vous spécifiez un `Role` Dans le XML de configuration, il sera ignoré. Cette valeur n'est pas utilisée par StorageGRID.

```
<ReplicationConfiguration>
    <Role></Role>
    <Rule>
        <Status>Enabled</Status>
        <Prefix>2020</Prefix>
        <Destination>
           <Bucket>urn:sgws:s3:::2017-records</Bucket>
           <StorageClass>STANDARD</StorageClass>
         </Destination>
     </Rule>
</ReplicationConfiguration>
```

2. Sélectionnez **Afficher les compartiments** dans le tableau de bord ou sélectionnez **STOCKAGE (S3)** > **compartiments**.
3. Sélectionnez le nom du compartiment source.

   La page des détails du compartiment s'affiche.

4. Sélectionnez **Platform Services** > **Replication**.
5. Cochez la case **Activer la réplication**.
6. Collez le XML de configuration de réplication dans la zone de texte et sélectionnez **Enregistrer les modifications**.



Les services de plateforme doivent être activés pour chaque compte de locataire par un administrateur StorageGRID à l'aide de Grid Manager ou de l'API de gestion du grid. Contactez votre administrateur StorageGRID si une erreur se produit lors de l'enregistrement du XML de configuration.

7. Vérifiez que la réplication est configurée correctement :
   a. Ajoutez un objet au compartiment source qui répond aux exigences de réplication telles que spécifiées dans la configuration de la réplication.

      Dans l'exemple présenté précédemment, les objets qui correspondent au préfixe « 2020 » sont répliqués.

b. Confirmer que l'objet a été répliqué vers le compartiment de destination.

   Pour les objets de petite taille, la réplication s'effectue rapidement.

Informations associées

"Créer un terminal de services de plate-forme"

Configurer les notifications d'événements

Le service de notifications est l'un des trois services de plate-forme StorageGRID. Vous pouvez activer les notifications d'un compartiment pour envoyer des informations sur les événements spécifiés vers un service de destination qui prend en charge le service SNS (simple notification Service™) d'AWS.

Avant de commencer

- Les services de plateforme ont été activés pour votre compte de locataire par un administrateur StorageGRID.
- Vous avez déjà créé un compartiment qui sert de source de notifications.
- Le noeud final que vous avez l'intention d'utiliser comme destination pour les notifications d'événements existe déjà, et vous avez son URN.
- Vous appartenez à un groupe d'utilisateurs qui possède le "Gérez tous les compartiments ou l'autorisation d'accès racine". Ces autorisations remplacent les paramètres d'autorisation des stratégies de groupe ou de compartiment lors de la configuration du compartiment à l'aide du Gestionnaire de locataires.

Description de la tâche

Après avoir configuré les notifications d'événements, chaque fois qu'un événement spécifié se produit pour un objet dans le compartiment source, une notification est générée et envoyée à la rubrique SNS (simple notification Service) utilisée comme point final de destination. Pour activer les notifications pour un compartiment, vous devez créer et appliquer un XML de configuration de notification valide. Le XML de configuration de notification doit utiliser l'URN d'un terminal de notification d'événement pour chaque destination.

Pour obtenir des informations générales sur les notifications d'événements et leur configuration, consultez la documentation Amazon. Pour plus d'informations sur l'implémentation de l'API de configuration des notifications du compartiment S3 par StorageGRID, reportez-vous aux instructions d'implémentation des applications client S3.

Si vous activez les notifications d'événements pour un compartiment contenant des objets, les notifications sont envoyées uniquement pour les actions qui sont effectuées après l'enregistrement de la configuration de notification.

Étapes

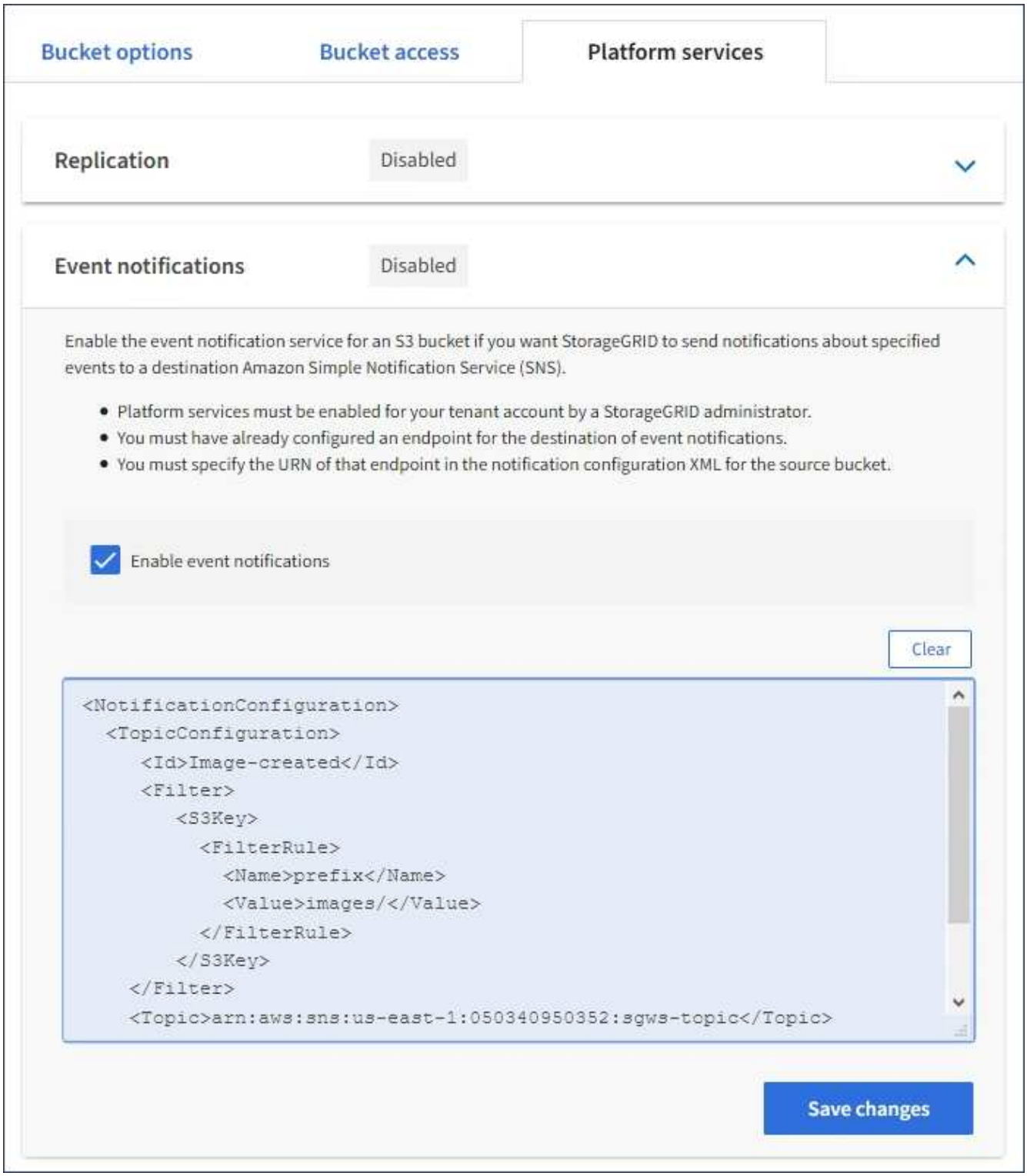
1. Activer les notifications pour le compartiment source :
   - Utilisez un éditeur de texte pour créer le XML de configuration de notification requis pour activer les notifications d'événement, comme spécifié dans l'API de notification S3.
   - Lors de la configuration du XML, utilisez l'URN d'un terminal de notification d'événements comme sujet de destination.

```
<NotificationConfiguration>
  <TopicConfiguration>
     <Id>Image-created</Id>
     <Filter>
        <S3Key>
          <FilterRule>
            <Name>prefix</Name>
            <Value>images/</Value>
          </FilterRule>
        </S3Key>
    </Filter>
    <Topic>arn:aws:sns:us-east-1:050340950352:sgws-topic</Topic>
    <Event>s3:ObjectCreated:*</Event>
   </TopicConfiguration>
 </NotificationConfiguration>
```

2. Dans le Gestionnaire de locataires, sélectionnez **STORAGE (S3)** > **seaux**.
3. Sélectionnez le nom du compartiment source.

   La page des détails du compartiment s'affiche.

4. Sélectionnez **Platform Services** > **Event Notifications**.
5. Cochez la case **Activer les notifications d'événements**.
6. Collez le XML de configuration de notification dans la zone de texte, puis sélectionnez **Enregistrer les modifications**.



Les services de plateforme doivent être activés pour chaque compte de locataire par un administrateur StorageGRID à l'aide de Grid Manager ou de l'API de gestion du grid. Contactez votre administrateur StorageGRID si une erreur se produit lors de l'enregistrement du XML de configuration.

7. Vérifiez que les notifications d'événements sont correctement configurées :

   a. Exécutez une action sur un objet du compartiment source qui répond aux exigences de déclenchement d'une notification telles qu'elles sont configurées dans le fichier XML de configuration.

Dans l'exemple, une notification d'événement est envoyée chaque fois qu'un objet est créé avec le `images/` préfixe.

b. Confirmez qu'une notification a été envoyée à la rubrique SNS de destination.

Par exemple, si le sujet de votre destination est hébergé sur le service SNS (simple notification Service) d'AWS, vous pouvez configurer le service pour vous envoyer un e-mail une fois la notification envoyée.


```
{
   "Records":[
      {
         "eventVersion":"2.0",
         "eventSource":"sgws:s3",
         "eventTime":"2017-08-08T23:52:38Z",
         "eventName":"ObjectCreated:Put",
         "userIdentity":{
            "principalId":"11111111111111111"
         },
         "requestParameters":{
            "sourceIPAddress":"193.51.100.20"
         },
         "responseElements":{
            "x-amz-request-id":"122047343"
         },
         "s3":{
            "s3SchemaVersion":"1.0",
            "configurationId":"Image-created",
            "bucket":{
               "name":"test1",
               "ownerIdentity":{
                  "principalId":"11111111111111111"
               },
               "arn":"arn:sgws:s3:::test1"
            },
            "object":{
               "key":"images/cat.jpg",
               "size":0,
               "eTag":"d41d8cd98f00b204e9800998ecf8427e",
               "sequencer":"14D90402421461C7"
            }
         }
      }
   ]
}
```

Si la notification est reçue dans la rubrique de destination, vous avez configuré votre compartiment source pour les notifications StorageGRID.

Informations associées

"Description des notifications pour les compartiments"

"UTILISEZ L'API REST S3"

"Créer un terminal de services de plate-forme"

Utilisez le service d'intégration de la recherche

Le service d'intégration de la recherche est l'un des trois services de plate-forme StorageGRID. Vous pouvez activer ce service pour envoyer des métadonnées d'objet à un index de recherche de destination chaque fois qu'un objet est créé ou supprimé, ou que ses métadonnées ou balises sont mises à jour.

Vous pouvez configurer l'intégration de la recherche à l'aide du Gestionnaire de locataires pour appliquer un code XML de configuration StorageGRID personnalisé à un compartiment.

> Comme le service d'intégration de recherche entraîne l'envoi des métadonnées d'objet vers une destination, son XML de configuration est appelé *metadata notification configuration XML*. Ce XML de configuration est différent de la configuration de *notification XML* utilisée pour activer les notifications d'événements.

Voir la "Instructions d'implémentation des applications client S3" Pour plus d'informations sur les opérations d'API REST personnalisées suivantes de StorageGRID S3 :

- SUPPRIMEZ la configuration de notification des métadonnées de compartiment
- CONFIGURATION DES notifications de métadonnées de compartiment
- CONFIGURATION de notification des métadonnées de compartiment

Informations associées

"XML de configuration pour l'intégration de la recherche"

"Métadonnées d'objet incluses dans les notifications de métadonnées"

"JSON généré par le service d'intégration de la recherche"

"Configurez le service d'intégration de la recherche"

"UTILISEZ L'API REST S3"

XML de configuration pour l'intégration de la recherche

Le service d'intégration de recherche est configuré à l'aide d'un ensemble de règles contenues dans `<MetadataNotificationConfiguration>` et `</MetadataNotificationConfiguration>` balises. Chaque règle spécifie les objets auxquels la règle s'applique, et la destination vers laquelle StorageGRID doit envoyer les métadonnées de ces objets.

Les objets peuvent être filtrés sur le préfixe du nom de l'objet. Par exemple, vous pouvez envoyer les métadonnées pour les objets avec le préfixe `images` à une destination et aux métadonnées pour les objets avec le préfixe `videos` à un autre. Les configurations avec des préfixes qui se chevauchent ne sont pas valides et sont rejetées lorsqu'elles sont soumises. Par exemple, une configuration qui inclut une règle pour les objets avec le préfixe `test` et une seconde règle pour les objets avec le préfixe `test2` n'est pas autorisé.

Les destinations doivent être spécifiées à l'aide de l'URN d'un terminal StorageGRID créé pour le service d'intégration de la recherche. Ces terminaux font référence à un index et à un type définis dans un cluster Elasticsearch.

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>rule-status</Status>
        <Prefix>key-prefix</Prefix>
        <Destination>
           <Urn>arn:aws:es:region:account-
ID:domain/mydomain/myindex/mytype</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Rule-2</ID>
         ...
    </Rule>
     ...
</MetadataNotificationConfiguration>
```

Le tableau décrit les éléments du XML de configuration de notification des métadonnées.

Nom	Description	Obligatoire
Configuration de la MetadaNotificationConfiguration	Balise de conteneur pour les règles utilisées pour spécifier les objets et la destination des notifications de métadonnées. Contient un ou plusieurs éléments de règle.	Oui.
Règle	Balise de conteneur d'une règle qui identifie les objets dont les métadonnées doivent être ajoutées à un index spécifié. Les règles avec des préfixes qui se chevauchent sont rejetées. Inclus dans l'élément MetadaNotificationConfiguration.	Oui.

Nom	Description	Obligatoire
ID	Identifiant unique de la règle. Inclus dans l'élément règle.	Non
État	L'état peut être « activé » ou « désactivé ». Aucune action n'est prise pour les règles désactivées. Inclus dans l'élément règle.	Oui.
Préfixe	Les objets qui correspondent au préfixe sont affectés par la règle et leurs métadonnées sont envoyées à la destination spécifiée. Pour faire correspondre tous les objets, spécifiez un préfixe vide. Inclus dans l'élément règle.	Oui.
Destination	Balise de conteneur pour la destination d'une règle. Inclus dans l'élément règle.	Oui.
Urne	URN de la destination où les métadonnées d'objet sont envoyées. Doit être l'URN d'un terminal StorageGRID avec les propriétés suivantes : • `es` doit être le troisième élément. • L'URN doit se terminer par l'index et le type où les métadonnées sont stockées, sous la forme `domain-name/myindex/mytype`. Les terminaux sont configurés à l'aide du Gestionnaire de locataires ou de l'API de gestion des locataires. Ils se présentent sous la forme suivante : • `arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype` • `urn:mysite:es:::mydomain/myindex/mytype` Le noeud final doit être configuré avant la soumission du XML de configuration, ou la configuration échouera avec une erreur 404. L'URNE est incluse dans l'élément destination.	Oui.

Utilisez l'exemple de XML de configuration de notification de métadonnées pour apprendre à construire votre propre XML.

Configuration de notification des métadonnées qui s'applique à tous les objets

Dans cet exemple, les métadonnées d'objet de tous les objets sont envoyées vers la même destination.

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>Enabled</Status>
        <Prefix></Prefix>
        <Destination>
           <Urn>urn:myes:es:::sgws-notifications/test1/all</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

Configuration des notifications de métadonnées avec deux règles

Dans cet exemple, les métadonnées d'objet pour les objets qui correspondent au préfixe `/images` est envoyée à une destination, tandis que les métadonnées d'objet correspondent au préfixe `/videos` est envoyé à une seconde destination.

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Images-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/images</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-east-1:3333333:domain/es-
domain/graphics/imagetype</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Videos-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/videos</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-west-1:22222222:domain/es-
domain/graphics/videotype</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

Informations associées

"UTILISEZ L'API REST S3"

"Métadonnées d'objet incluses dans les notifications de métadonnées"

"JSON généré par le service d'intégration de la recherche"

"Configurez le service d'intégration de la recherche"

Configurer le service d'intégration de la recherche

Le service d'intégration de recherche envoie des métadonnées d'objet à un index de recherche de destination chaque fois qu'un objet est créé ou supprimé, ou que ses métadonnées ou balises sont mises à jour.

Avant de commencer

- Les services de plateforme ont été activés pour votre compte de locataire par un administrateur StorageGRID.
- Vous avez déjà créé un compartiment S3 dont vous souhaitez indexer le contenu.
- Le noeud final que vous avez l'intention d'utiliser comme destination pour le service d'intégration de recherche existe déjà, et vous avez son URN.
- Vous appartenez à un groupe d'utilisateurs qui possède le "Gérez tous les compartiments ou l'autorisation d'accès racine". Ces autorisations remplacent les paramètres d'autorisation des stratégies de groupe ou de compartiment lors de la configuration du compartiment à l'aide du Gestionnaire de locataires.

Description de la tâche

Une fois que vous avez configuré le service d'intégration de recherche pour un compartiment source, la création d'un objet ou la mise à jour des métadonnées ou des balises d'un objet déclenche l'envoi des métadonnées d'objet vers le terminal de destination. Si vous activez le service d'intégration de recherche pour un compartiment qui contient déjà des objets, les notifications de métadonnées ne sont pas automatiquement envoyées pour les objets existants. Vous devez mettre à jour ces objets existants pour vous assurer que leurs métadonnées sont ajoutées à l'index de recherche de destination.

Étapes

1. Utilisez un éditeur de texte pour créer le XML de notification de métadonnées requis pour activer l'intégration de la recherche.
   - Voir les informations sur le XML de configuration pour l'intégration de la recherche.
   - Lors de la configuration du XML, utilisez l'URN d'un noeud final d'intégration de recherche comme destination.

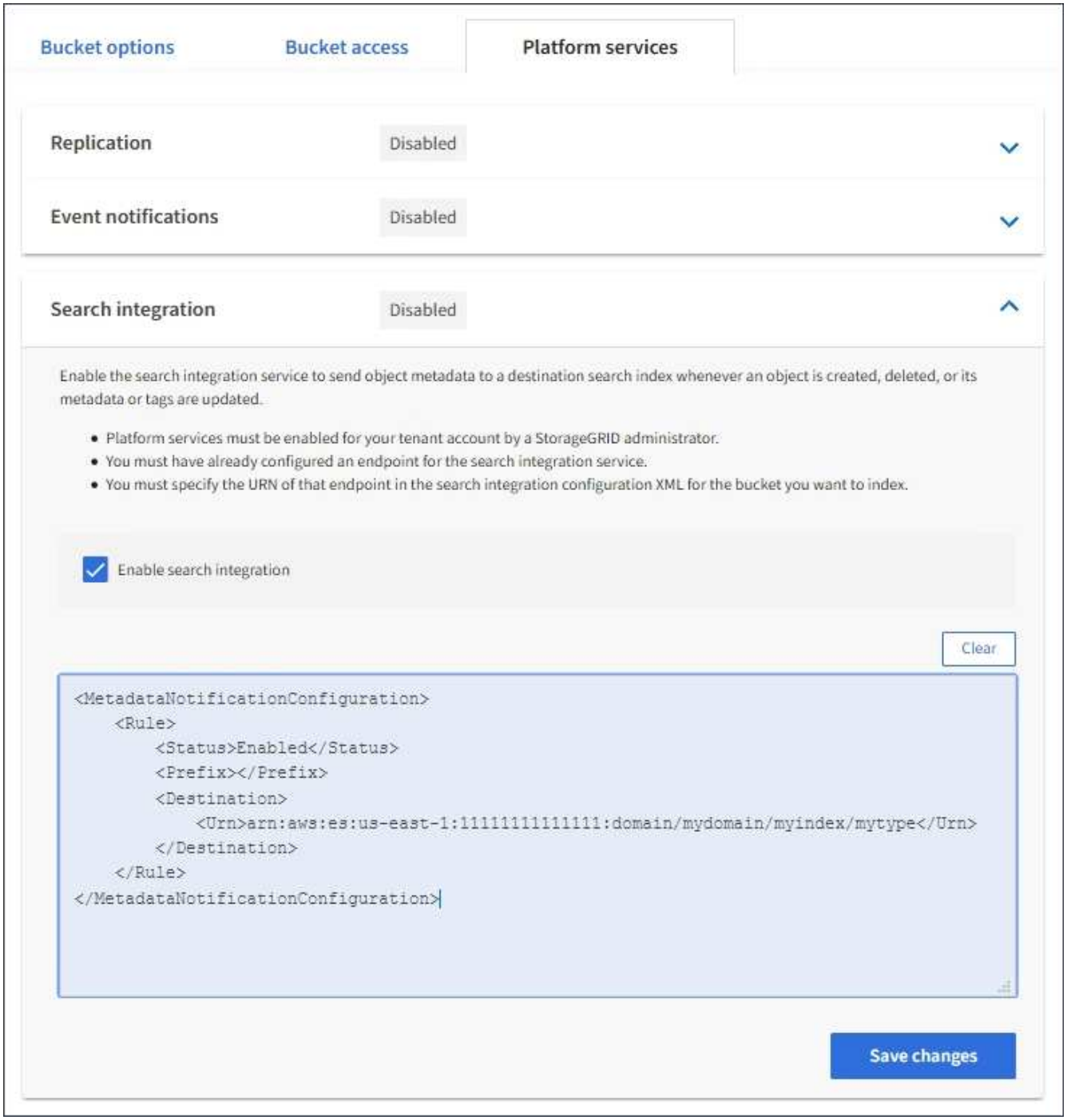
```
<MetadataNotificationConfiguration>
 <Rule>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
       <Urn>arn:aws:es:us-east-
1:11111111111111:domain/mydomain/myindex/mytype</Urn>
       </Destination>
 </Rule>
</MetadataNotificationConfiguration>
```

2. Dans le Gestionnaire de locataires, sélectionnez **STORAGE (S3)** > **seaux**.

3. Sélectionnez le nom du compartiment source.

   La page des détails du compartiment s'affiche.

4. Sélectionnez **Platform Services** > **Search Integration**
5. Cochez la case **Activer l'intégration de la recherche**.
6. Collez la configuration de notification de métadonnées dans la zone de texte, puis sélectionnez **Enregistrer les modifications**.



> Les services de plateforme doivent être activés pour chaque compte de locataire par un administrateur StorageGRID à l'aide de l'API Grid Manager ou de gestion. Contactez votre administrateur StorageGRID si une erreur se produit lors de l'enregistrement du XML de configuration.

7. Vérifiez que le service d'intégration de la recherche est configuré correctement :
   a. Ajoutez un objet au compartiment source qui répond aux exigences relatives au déclenchement d'une notification de métadonnées comme spécifié dans le XML de configuration.

      Dans l'exemple présenté précédemment, tous les objets ajoutés au compartiment déclenchent une notification de métadonnées.

   b. Vérifiez qu'un document JSON contenant les métadonnées et les balises de l'objet a été ajouté à l'index de recherche spécifié dans le noeud final.

Une fois que vous avez terminé

Si nécessaire, vous pouvez désactiver l'intégration de la recherche pour un compartiment à l'aide de l'une des méthodes suivantes :

- Sélectionnez **STORAGE (S3)** > **Buckets** et décochez la case **Enable search Integration**.
- Si vous utilisez directement l'API S3, utilisez une demande de notification DE suppression des métadonnées du compartiment. Pour plus d'informations sur l'implémentation des applications client S3, reportez-vous aux instructions.

Informations associées

"Comprendre le service d'intégration de la recherche"

"XML de configuration pour l'intégration de la recherche"

"UTILISEZ L'API REST S3"

"Créer un terminal de services de plate-forme"

JSON généré par le service d'intégration de la recherche

Lorsque vous activez le service d'intégration de la recherche pour un compartiment, un document JSON est généré et envoyé au terminal de destination à chaque ajout, mise à jour ou suppression de métadonnées d'objet.

Cet exemple montre un exemple de fichier JSON qui peut être généré lorsqu'un objet doté de la clé est associé `SGWS/Tagging.txt` est créé dans un compartiment nommé `test`. Le `test` le compartiment n'est pas multiversion `versionId` l'étiquette est vide.

```
{
  "bucket": "test",
  "key": "SGWS/Tagging.txt",
  "versionId": "",
  "accountId": "86928401983529626822",
  "size": 38,
  "md5": "3d6c7634a85436eee06d43415012855",
  "region":"us-east-1"
  "metadata": {
    "age": "25"
  },
  "tags": {
    "color": "yellow"
  }
}
```

Métadonnées d'objet incluses dans les notifications de métadonnées

Le tableau répertorie tous les champs inclus dans le document JSON qui est envoyé au noeud final de destination lorsque l'intégration de la recherche est activée.

Le nom du document inclut le nom du compartiment, le nom de l'objet et l'ID de version, le cas échéant.

Type	Nom et description de l'élément
Informations sur les compartiments et les objets	`bucket`: Nom du compartiment
`key`: Nom de la clé d'objet	`versionID`: Version d'objet, pour les objets dans les compartiments multiversion
`region`: Région godet, par exemple `us-east-1`	Métadonnées de système
`size`: Taille de l'objet (en octets) visible par un client HTTP	`md5`: Hachage d'objet
Métadonnées d'utilisateur	`metadata`: Toutes les métadonnées utilisateur de l'objet, en tant que paires clé-valeur `key:value`
Étiquettes	`tags`: Toutes les balises d'objet définies pour l'objet, en tant que paires clé-valeur `key:value`

Pour les balises et les métadonnées d'utilisateur, StorageGRID transmet des dates et des chiffres à Elasticsearch en tant que chaînes ou notifications d'événement S3. Pour configurer Elasticsearch afin d'interpréter ces chaînes comme des dates ou des chiffres, suivez les instructions Elasticsearch pour un mappage dynamique des champs et un mappage des formats de date. Vous devez activer les mappages de champs dynamiques sur l'index avant de configurer le service d'intégration de la recherche. Une fois qu'un document est indexé, vous ne pouvez pas modifier les types de champ du document dans l'index.

UTILISEZ L'API REST S3

Versions et mises à jour prises en charge par l'API REST S3

StorageGRID prend en charge l'API simple Storage Service (S3), qui est implémentée en tant que ensemble de services web REST (Representational State Transfer).

La prise en charge de l'API REST S3 vous permet de connecter les applications orientées services développées pour les services web S3 avec un stockage objet sur site qui utilise le système StorageGRID. L'utilisation actuelle des appels de l'API REST S3 par une application client requiert des modifications minimales.

Versions prises en charge

StorageGRID prend en charge les versions spécifiques suivantes de S3 et HTTP.

Élément	Version
Spécification S3	*Simple Storage Service API Reference* 2006-03-01
HTTP	1.1 Pour plus d'informations sur HTTP, consultez le document HTTP/1.1 (RFC 7230-35). **Remarque**: StorageGRID ne prend pas en charge HTTP/1.1 pipeline.

Informations associées

"IETF RFC 2616 : Protocole de transfert hypertexte (HTTP/1.1)"

"Documentation Amazon Web Services (AWS) : référence de l'API Amazon simple Storage Service"

Prise en charge des mises à jour de l'API REST S3

Relâchez	Commentaires
11.7	• Ajouté "Référence rapide : demandes d'API S3 prises en charge". • Ajout de la prise en charge du mode DE GOUVERNANCE avec S3 Object Lock. • A ajouté la prise en charge des spécificités de StorageGRID `x-ntap-sg-cgr-replication-status` En-tête de réponse pour LES requêtes GET Object et HEAD Object. Cet en-tête fournit l'état de réplication d'un objet pour la réplication inter-grid. • Les requêtes SelectObjectContent prennent désormais en charge les objets parquet.
11.6	• Ajout de la prise en charge de l'utilisation du `partNumber` Paramètre de demande dans DEMANDES OBJET GET et objet TÊTE. • Ajout de la prise en charge d'un mode de conservation par défaut et d'une période de conservation par défaut au niveau du compartiment pour le verrouillage d'objet S3. • Prise en charge ajoutée de `s3:object-lock-remaining-retention-days` la touche condition de police permet de définir la plage de périodes de conservation autorisées pour vos objets. • Modification de la taille *recommandée* maximale pour une opération objet PUT unique à 5 Gio (5,368,709,120 octets). Si vos objets sont supérieurs à 5 Gio, utilisez le téléchargement partitionné.
11.5	• Ajout de la prise en charge de la gestion du chiffrement de compartiment. • Ajout de la prise en charge des demandes de verrouillage d'objet S3 et des demandes de conformité héritées obsolètes. • Ajout de la prise en charge de L'utilisation DE LA SUPPRESSION de plusieurs objets sur les compartiments multiversion. • Le `Content-MD5` l'en-tête de demande est désormais correctement pris en charge.
11.4	• Prise en charge accrue du balisage de compartiment, DE L'étiquetage DES compartiments ET DU balisage de compartiment. Les étiquettes de répartition des coûts ne sont pas prises en charge. • Pour les compartiments créés dans StorageGRID 11.4, il n'est plus nécessaire de limiter les noms de clés d'objet pour respecter les bonnes pratiques de performance. • Ajout de la prise en charge des notifications de compartiment sur le `s3:ObjectRestore:Post` type d'événement. • Les limites de taille d'AWS pour les pièces partitionnés sont maintenant appliquées. Chaque partie d'un téléchargement partitionné doit être comprise entre 5 MIB et 5 Gio. La dernière partie peut être plus petite que 5 MIB. • Ajout de la prise en charge de TLS 1.3

Relâchez	Commentaires
11.3	• Ajout de la prise en charge du chiffrement côté serveur des données d'objet avec les clés fournies par le client (SSE-C). • Ajout de la prise en charge des opérations DE SUPPRESSION, D'OBTENTION et DE REMPLACEMENT du cycle de vie des compartiments (action d'expiration uniquement) et pour le `x-amz-expiration` en-tête de réponse. • PUT Object mis à jour, PUT Object - copie et Multipart Upload pour décrire l'impact des règles ILM utilisant un placement synchrone à l'entrée. • Les chiffrements TLS 1.1 ne sont plus pris en charge.
11.2	Ajout de la prise en charge de la restauration POST-objet pour l'utilisation avec les pools de stockage cloud. Ajout de la prise en charge de l'utilisation de la syntaxe AWS pour ARN, des clés de condition de règle et des variables de règles de groupe et de compartiment Les règles de compartiment et de groupe qui utilisent la syntaxe StorageGRID restent prises en charge. **Remarque :** les utilisations de l'ARN/URN dans d'autres configurations JSON/XML, y compris celles utilisées dans les fonctions StorageGRID personnalisées, n'ont pas changé.
11.1	Ajout de la prise en charge du partage de ressources entre les sources (CORS), du protocole HTTP pour les connexions client S3 aux nœuds de grid et des paramètres de conformité dans les compartiments.
11.0	Ajout de la prise en charge de la configuration des services de plateforme (réplication CloudMirror, notifications et intégration de la recherche Elasticsearch) pour les compartiments Ajout également de la prise en charge des contraintes d'emplacement de balisage d'objets pour les compartiments, ainsi que du paramètre de contrôle de cohérence disponible.
10.4	Ajout de la prise en charge des modifications de l'analyse ILM sur la gestion des versions, mises à jour de la page noms de domaine de point final, conditions et variables dans les règles, exemples de règles et autorisation PutOverwriteObject.
10.3	Prise en charge ajoutée pour la gestion des versions.
10.2	Ajout de la prise en charge des règles d'accès de groupe et de compartiment, ainsi que de la copie multipart (Télécharger la pièce - copie).
10.1	Ajout de la prise en charge du téléchargement partitionné, des demandes de type hébergement virtuel et de l'authentification v4.
10.0	Prise en charge initiale de l'API REST S3 par le système StorageGRID.la version actuellement prise en charge de *simple Storage Service API Reference* est 2006-03-01.

Référence rapide : demandes d'API S3 prises en charge

Cette page explique comment StorageGRID prend en charge les API Amazon simple Storage Service (S3).

Cette page inclut uniquement les opérations S3 prises en charge par StorageGRID.

Pour afficher la documentation AWS pour chaque opération, sélectionnez le lien dans l'en-tête.

Paramètres de requête URI courants et en-têtes de requête

Sauf mention contraire, les paramètres de requête URI courants suivants sont pris en charge :

- `versionId` (comme requis pour les opérations d'objet)

Sauf mention contraire, les en-têtes de requête courants suivants sont pris en charge :

- `Authorization`
- `Connection`
- `Content-Length`
- `Content-MD5`
- `Content-Type`
- `Date`
- `Expect`
- `Host`
- `x-amz-date`

Informations associées

- "Détails de l'implémentation de l'API REST S3"
- "Référence de l'API Amazon simple Storage Service : en-têtes de demande communs"

"AbortMultipartUpload"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les paramètres et en-têtes communs Pour cette demande, plus ce paramètre de requête URI supplémentaire :

- `uploadId`

Corps de la demande

Aucune

Documentation StorageGRID

"Opérations pour les téléchargements partitionnés"

"CompleteMultipartUpload"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les paramètres et en-têtes communs Pour cette demande, plus ce paramètre de requête URI supplémentaire :

- `uploadId`

Demander des balises XML de corps

StorageGRID prend en charge les balises XML de corps de requête suivantes :

- `CompleteMultipartUpload`
- `Part`
- `ETag`
- `PartNumber`

Documentation StorageGRID

"Chargement de pièces multiples complet"

"Objet de copie"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les paramètres et en-têtes communs pour cette demande, plus les en-têtes supplémentaires suivants :

- `x-amz-copy-source`
- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-modified-since`
- `x-amz-copy-source-if-none-match`
- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-server-side-encryption-customer-algorithm`
- `x-amz-copy-source-server-side-encryption-customer-key`
- `x-amz-copy-source-server-side-encryption-customer-key-MD5`
- `x-amz-metadata-directive`
- `x-amz-object-lock-legal-hold`
- `x-amz-object-lock-mode`
- `x-amz-object-lock-retain-until-date`
- `x-amz-server-side-encryption`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `x-amz-storage-class`

- `x-amz-tagging`
- `x-amz-tagging-directive`
- `x-amz-meta-<metadata-name>`

Corps de la demande

Aucune

Documentation StorageGRID

"PLACER une copie d'objet"

"CreateBucket"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les paramètres et en-têtes communs pour cette demande, plus les en-têtes supplémentaires suivants :

- `x-amz-bucket-object-lock-enabled`

Corps de la demande

StorageGRID prend en charge tous les paramètres du corps de demande définis par l'API REST Amazon S3 au moment de l'implémentation.

Documentation StorageGRID

"Opérations sur les compartiments"

"CreateMultipartUpload"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les paramètres et en-têtes communs pour cette demande, plus les en-têtes supplémentaires suivants :

- `Cache-Control`
- `Content-Disposition`
- `Content-Encoding`
- `Content-Language`
- `Expires`
- `x-amz-server-side-encryption`
- `x-amz-storage-class`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `x-amz-tagging`
- `x-amz-object-lock-mode`
- `x-amz-object-lock-retain-until-date`

- `x-amz-object-lock-legal-hold`
- `x-amz-meta-<metadata-name>`

Corps de la demande

Aucune

Documentation StorageGRID

"Lancer le téléchargement de pièces multiples"

"DeleteBucket"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les paramètres et en-têtes communs pour cette demande.

Documentation StorageGRID

"Opérations sur les compartiments"

"DeleteBuckeCors"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les paramètres et en-têtes communs pour cette demande.

Corps de la demande

Aucune

Documentation StorageGRID

"Opérations sur les compartiments"

"DeleteBuckeEncryption"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les paramètres et en-têtes communs pour cette demande.

Corps de la demande

Aucune

Documentation StorageGRID

"Opérations sur les compartiments"

"DeleteBuckeLifecycle"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les paramètres et en-têtes communs pour cette demande.

Corps de la demande

Aucune

Documentation StorageGRID

- "Opérations sur les compartiments"
- "Création de la configuration du cycle de vie S3"

"DeleteBucketPolicy"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les paramètres et en-têtes communs pour cette demande.

Corps de la demande

Aucune

Documentation StorageGRID

"Opérations sur les compartiments"

"DeleteBuckeReplication"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les paramètres et en-têtes communs pour cette demande.

Corps de la demande

Aucune

Documentation StorageGRID

"Opérations sur les compartiments"

"DeleteBucketTagging"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les paramètres et en-têtes communs pour cette demande.

Corps de la demande

Aucune

Documentation StorageGRID

"Opérations sur les compartiments"

"DeleteObject"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les paramètres et en-têtes communs pour cette demande, plus cet en-tête de demande supplémentaire :

- `x-amz-bypass-governance-retention`

Corps de la demande

Aucune

Documentation StorageGRID

"Opérations sur les objets"

"DeleteObjects"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les paramètres et en-têtes communs pour cette demande, plus cet en-tête de demande supplémentaire :

- `x-amz-bypass-governance-retention`

Corps de la demande

StorageGRID prend en charge tous les paramètres du corps de demande définis par l'API REST Amazon S3 au moment de l'implémentation.

Documentation StorageGRID

"Opérations sur les objets" (SUPPRIMER plusieurs objets)

"DeleteObjectTagging"

StorageGRID prend en charge tous les paramètres et en-têtes communs pour cette demande.

Corps de la demande

Aucune

Documentation StorageGRID

"Opérations sur les objets"

"GetBucketAcl"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les paramètres et en-têtes communs pour cette demande.

Corps de la demande

Aucune

Documentation StorageGRID

"Opérations sur les compartiments"

"GetBucketCors"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les paramètres et en-têtes communs pour cette demande.

Corps de la demande

Aucune

Documentation StorageGRID

"Opérations sur les compartiments"

"GetBucketEncryption"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les paramètres et en-têtes communs pour cette demande.

Corps de la demande

Aucune

Documentation StorageGRID

"Opérations sur les compartiments"

"GetBucketLifecycleConfiguration"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les paramètres et en-têtes communs pour cette demande.

Corps de la demande

Aucune

Documentation StorageGRID

- "Opérations sur les compartiments" (GET Bucket Lifecycle)
- "Création de la configuration du cycle de vie S3"

"GetBuckeLocation"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les paramètres et en-têtes communs pour cette demande.

Corps de la demande

Aucune

Documentation StorageGRID

"Opérations sur les compartiments"

"GetBucketNotifationConfiguration"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les paramètres et en-têtes communs pour cette demande.

Corps de la demande

Aucune

Documentation StorageGRID

"Opérations sur les compartiments" (GET Bucket notification)

"GetBucketPolicy"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les paramètres et en-têtes communs pour cette demande.

Corps de la demande

Aucune

Documentation StorageGRID

"Opérations sur les compartiments"

"GetBuckeReplication"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les paramètres et en-têtes communs pour cette demande.

Corps de la demande

Aucune

Documentation StorageGRID

"Opérations sur les compartiments"

"GetBucketTagging"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les paramètres et en-têtes communs pour cette demande.

Corps de la demande

Aucune

Documentation StorageGRID

"Opérations sur les compartiments"

"GetBucketVersioning"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les paramètres et en-têtes communs pour cette demande.

Corps de la demande

Aucune

Documentation StorageGRID

"Opérations sur les compartiments"

"GetObject"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les paramètres et en-têtes communs Pour cette demande, plus les paramètres de requête URI supplémentaires suivants :

- `partNumber`
- `response-cache-control`
- `response-content-disposition`
- `response-content-encoding`
- `response-content-language`
- `response-content-type`
- `response-expires`

Et ces en-têtes de demande supplémentaires :

- `Range`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`

- `If-Match`
- `If-Modified-Since`
- `If-None-Match`
- `If-Unmodified-Since`

Corps de la demande

Aucune

Documentation StorageGRID

"OBTENIR l'objet"

"GetObjectAcl"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les paramètres et en-têtes communs pour cette demande.

Corps de la demande

Aucune

Documentation StorageGRID

"Opérations sur les objets"

"GetObjectLegalHold"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les paramètres et en-têtes communs pour cette demande.

Corps de la demande

Aucune

Documentation StorageGRID

"Utilisez l'API REST S3 pour configurer le verrouillage objet S3"

"GetObjectLockConfiguration"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les paramètres et en-têtes communs pour cette demande.

Corps de la demande

Aucune

Documentation StorageGRID

"Utilisez l'API REST S3 pour configurer le verrouillage objet S3"

"GetObjectRetention"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les paramètres et en-têtes communs pour cette demande.

Corps de la demande

Aucune

Documentation StorageGRID

"Utilisez l'API REST S3 pour configurer le verrouillage objet S3"

"GetObjectTagging"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les paramètres et en-têtes communs pour cette demande.

Corps de la demande

Aucune

Documentation StorageGRID

"Opérations sur les objets"

"Godet principal"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les paramètres et en-têtes communs pour cette demande.

Corps de la demande

Aucune

Documentation StorageGRID

"Opérations sur les compartiments"

"Objet principal"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les paramètres et en-têtes communs pour cette demande, plus les en-têtes supplémentaires suivants :

- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `If-Match`
- `If-Modified-Since`
- `If-None-Match`
- `If-Unmodified-Since`
- `Range`

Corps de la demande

Aucune

Documentation StorageGRID

"Objet TÊTE"

"Listseaux"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les paramètres et en-têtes communs pour cette demande.

Corps de la demande

Aucune

Documentation StorageGRID

"Opérations sur le service et gt ; OBTENIR le service"

"ListMultipartUploads"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les paramètres et en-têtes communs pour cette demande, plus les paramètres supplémentaires suivants :

- `delimiter`
- `encoding-type`
- `key-marker`
- `max-uploads`
- `prefix`
- `upload-id-marker`

Corps de la demande

Aucune

Documentation StorageGRID

"Liste des téléchargements partitionnés"

"ListObjects"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les paramètres et en-têtes communs pour cette demande, plus les paramètres supplémentaires suivants :

- `delimiter`
- `encoding-type`
- `marker`
- `max-keys`
- `prefix`

Corps de la demande

Aucune

Documentation StorageGRID

"Opérations sur les compartiments" (TÉLÉCHARGER le compartiment)

"ListentsV2"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les paramètres et en-têtes communs pour cette demande, plus les paramètres supplémentaires suivants :

- `continuation-token`
- `delimiter`
- `encoding-type`
- `fetch-owner`
- `max-keys`
- `prefix`
- `start-after`

Corps de la demande

Aucune

Documentation StorageGRID

"Opérations sur les compartiments" (TÉLÉCHARGER le compartiment)

"ListObjectVersions"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les paramètres et en-têtes communs pour cette demande, plus les paramètres supplémentaires suivants :

- `delimiter`
- `encoding-type`
- `key-marker`
- `max-keys`
- `prefix`
- `version-id-marker`

Corps de la demande

Aucune

Documentation StorageGRID

"Opérations sur les compartiments" (OBTENIR les versions d'objet compartiment)

"ListParts"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les paramètres et en-têtes communs pour cette demande, plus les paramètres supplémentaires suivants :

- `max-parts`

- `part-number-marker`
- `uploadId`

Corps de la demande

Aucune

Documentation StorageGRID

"Liste des téléchargements partitionnés"

"PutBucketCors"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les paramètres et en-têtes communs pour cette demande.

Corps de la demande

StorageGRID prend en charge tous les paramètres du corps de demande définis par l'API REST Amazon S3 au moment de l'implémentation.

Documentation StorageGRID

"Opérations sur les compartiments"

"PutBucketEncryption"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les paramètres et en-têtes communs pour cette demande.

Demander des balises XML de corps

StorageGRID prend en charge les balises XML de corps de requête suivantes :

- `ServerSideEncryptionConfiguration`
- `Rule`
- `ApplyServerSideEncryptionByDefault`
- `SSEAlgorithm`

Documentation StorageGRID

"Opérations sur les compartiments"

"PutBucketLifecycleConfiguration"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les paramètres et en-têtes communs pour cette demande.

Demander des balises XML de corps

StorageGRID prend en charge les balises XML de corps de requête suivantes :

- `NewerNoncurrentVersions`
- `LifecycleConfiguration`
- `Rule`

- `Expiration`
- `Days`
- `Filter`
- `And`
- `Prefix`
- `Tag`
- `Key`
- `Value`
- `Prefix`
- `Tag`
- `Key`
- `Value`
- `ID`
- `NoncurrentVersionExpiration`
- `NoncurrentDays`
- `Prefix`
- `Status`

Documentation StorageGRID

- "Opérations sur les compartiments" (Cycle de vie DU godet PUT)
- "Création de la configuration du cycle de vie S3"

"PutBucketNotifationConfiguration"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les paramètres et en-têtes communs pour cette demande.

Demander des balises XML de corps

StorageGRID prend en charge les balises XML de corps de requête suivantes :

- `Prefix`
- `Suffix`
- `NotificationConfiguration`
- `TopicConfiguration`
- `Event`
- `Filter`
- `S3Key`
- `FilterRule`

- `Name`
- `Value`
- `Id`
- `Topic`

Documentation StorageGRID

"Opérations sur les compartiments" (Notification PUT Bucket)

"PutBuckePolicy"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les paramètres et en-têtes communs pour cette demande.

Corps de la demande

Pour plus d'informations sur les champs de corps JSON pris en charge, reportez-vous à la section"Utilisez les règles d'accès au compartiment et au groupe".

"PutBuckeReplication"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les paramètres et en-têtes communs pour cette demande.

Demander des balises XML de corps

- `ReplicationConfiguration`
- `Status`
- `Prefix`
- `Destination`
- `Bucket`
- `StorageClass`
- `Rule`

Documentation StorageGRID

"Opérations sur les compartiments"

"Étiquetage PutBucketTagging"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les paramètres et en-têtes communs pour cette demande.

Corps de la demande

StorageGRID prend en charge tous les paramètres du corps de demande définis par l'API REST Amazon S3 au moment de l'implémentation.

Documentation StorageGRID

"Opérations sur les compartiments"

"PutBuckeVersioning"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les paramètres et en-têtes communs pour cette demande.

Demander les paramètres du corps

StorageGRID prend en charge les paramètres de corps de demande suivants :

- `VersioningConfiguration`
- `Status`

Documentation StorageGRID

"Opérations sur les compartiments"

"PutObject"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les paramètres et en-têtes communs pour cette demande, plus les en-têtes supplémentaires suivants :

- `Cache-Control`
- `Content-Disposition`
- `Content-Encoding`
- `Content-Language`
- `x-amz-server-side-encryption`
- `x-amz-storage-class`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `x-amz-tagging`
- `x-amz-object-lock-mode`
- `x-amz-object-lock-retain-until-date`
- `x-amz-object-lock-legal-hold`
- `x-amz-meta-<metadata-name>`

Corps de la demande

- Données binaires de l'objet

Documentation StorageGRID

"PLACER l'objet"

"PutObjectLegalHold"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les paramètres et en-têtes communs pour cette demande.

Corps de la demande

StorageGRID prend en charge tous les paramètres du corps de demande définis par l'API REST Amazon S3 au moment de l'implémentation.

Documentation StorageGRID

"Utilisez l'API REST S3 pour configurer le verrouillage objet S3"

"PutObjectLockConfiguration"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les paramètres et en-têtes communs pour cette demande.

Corps de la demande

StorageGRID prend en charge tous les paramètres du corps de demande définis par l'API REST Amazon S3 au moment de l'implémentation.

Documentation StorageGRID

"Utilisez l'API REST S3 pour configurer le verrouillage objet S3"

"PutObjectRetention"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les paramètres et en-têtes communs pour cette demande, plus cet en-tête supplémentaire :

- `x-amz-bypass-governance-retention`

Corps de la demande

StorageGRID prend en charge tous les paramètres du corps de demande définis par l'API REST Amazon S3 au moment de l'implémentation.

Documentation StorageGRID

"Utilisez l'API REST S3 pour configurer le verrouillage objet S3"

"Marquage PutObject"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les paramètres et en-têtes communs pour cette demande.

Corps de la demande

StorageGRID prend en charge tous les paramètres du corps de demande définis par l'API REST Amazon S3 au moment de l'implémentation.

Documentation StorageGRID

"Opérations sur les objets"

"SelectObjectContent"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les paramètres et en-têtes communs pour cette demande.

Corps de la demande

Pour plus d'informations sur les champs de corps pris en charge, reportez-vous aux sections suivantes :

- "Utiliser S3 Select"
- "Sélectionnez contenu de l'objet"

"UploadPart"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les paramètres et en-têtes communs Pour cette demande, plus les paramètres de requête URI supplémentaires suivants :

- `partNumber`
- `uploadId`

Et ces en-têtes de demande supplémentaires :

- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`

Corps de la demande

- Données binaires de la pièce

Documentation StorageGRID

"Télécharger la pièce"

"UploadPartCopy"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les paramètres et en-têtes communs Pour cette demande, plus les paramètres de requête URI supplémentaires suivants :

- `partNumber`
- `uploadId`

Et ces en-têtes de demande supplémentaires :

- `x-amz-copy-source`
- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-modified-since`
- `x-amz-copy-source-if-none-match`
- `x-amz-copy-source-if-unmodified-since`

- `x-amz-copy-source-range`
- `x-amz-server-side-encryption-customer-algorithm`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-key-MD5`
- `x-amz-copy-source-server-side-encryption-customer-algorithm`
- `x-amz-copy-source-server-side-encryption-customer-key`
- `x-amz-copy-source-server-side-encryption-customer-key-MD5`

Corps de la demande

Aucune

Documentation StorageGRID

"Télécharger la pièce - Copier"

Configurez les comptes et les connexions des locataires

Pour configurer StorageGRID pour accepter les connexions à partir des applications client, vous devez créer un ou plusieurs comptes de tenant et configurer les connexions.

Créez et configurez des comptes de locataire S3

Un compte de locataire S3 est requis avant que les clients d'API S3 ne puissent stocker et récupérer des objets sur StorageGRID. Chaque compte de locataire possède son propre ID de compte, ses propres groupes, utilisateurs, compartiments et objets.

Les comptes de locataires S3 sont créés par un administrateur grid StorageGRID à l'aide de Grid Manager ou de l'API de gestion du grid. Voir "Gérer les locataires" pour plus d'informations. Une fois le compte d'un locataire S3 créé, les utilisateurs peuvent accéder au gestionnaire des locataires pour gérer les groupes, les utilisateurs, les clés d'accès et les compartiments. Voir "Utilisez un compte de locataire" pour plus d'informations.

Les locataires S3 peuvent créer et gérer des clés d'accès S3 et des compartiments avec le gestionnaire de locataires. Ils doivent utiliser une application client S3 pour ingérer et gérer les objets. Voir "UTILISEZ L'API REST S3" pour plus d'informations.

Comment configurer les connexions client

Un administrateur du grid fait des choix de configuration qui affectent la façon dont les clients S3 se connectent à StorageGRID pour stocker et récupérer les données. La connexion d'StorageGRID à une application S3 se fait en quatre étapes de base :

- Effectuez les tâches requises dans StorageGRID, en fonction de la façon dont l'application client se connecte à StorageGRID.
- Utilisez StorageGRID pour obtenir les valeurs dont l'application a besoin pour se connecter à la grille. Vous pouvez l'un ou l'autre "Utilisez l'assistant d'installation S3" Ou configurez chaque entité StorageGRID manuellement.
- Utilisez l'application S3 pour terminer la connexion à StorageGRID. Créez des entrées DNS pour associer des adresses IP à tous les noms de domaine que vous prévoyez d'utiliser.

- Effectuez des tâches continues dans l'application et dans StorageGRID afin de gérer et de surveiller le stockage objet au fil du temps.

Pour plus de détails sur ces étapes, reportez-vous à la section "Configurer les connexions client".

Informations requises pour les connexions client

Pour stocker ou récupérer des objets, les applications client S3 se connectent au service Load Balancer, qui est inclus sur tous les nœuds d'administration et les nœuds de passerelle, ou au service LDR (local distribution Router), qui est inclus sur tous les nœuds de stockage.

Les applications client peuvent se connecter à StorageGRID en utilisant l'adresse IP d'un nœud grid et le numéro de port du service sur ce nœud. Vous pouvez également créer des groupes haute disponibilité de nœuds d'équilibrage de la charge pour fournir des connexions haute disponibilité utilisant des adresses IP virtuelles (VIP). Si vous souhaitez vous connecter à StorageGRID à l'aide d'un nom de domaine complet (FQDN) au lieu d'une adresse IP ou VIP, vous pouvez configurer des entrées DNS.

Voir "Résumé : adresses IP et ports pour les connexions client" pour en savoir plus.

Choisissez d'utiliser des connexions HTTPS ou HTTP

Lorsque les connexions client sont effectuées à l'aide d'un noeud final Load Balancer, les connexions doivent être effectuées à l'aide du protocole (HTTP ou HTTPS) spécifié pour ce noeud final. Pour utiliser HTTP pour les connexions client aux nœuds de stockage, vous devez activer son utilisation.

Par défaut, lorsque les applications client se connectent aux nœuds de stockage, elles doivent utiliser le protocole HTTPS chiffré pour toutes les connexions. Vous pouvez également activer des connexions HTTP moins sécurisées en sélectionnant **CONFIGURATION** > **Paramètres de sécurité** > **réseau et objets** > **Activer HTTP pour les connexions de noeud de stockage** dans le gestionnaire de grille. Par exemple, une application client peut utiliser HTTP lors du test de la connexion à un noeud de stockage dans un environnement non-production.

> Soyez prudent lorsque vous activez HTTP pour une grille de production car les requêtes et les réponses seront envoyées sans cryptage.

Informations associées

"Administrer StorageGRID"

"Avantages des connexions HTTP actives, inactives et simultanées"

Noms de domaine de terminaux S3 pour les requêtes S3

Avant d'utiliser les noms de domaine de terminaux S3 pour les demandes client, un administrateur StorageGRID doit configurer le système pour qu'il accepte les connexions qui utilisent les noms de domaine de terminaux S3 dans les demandes de type chemin d'accès S3 et de type hébergement virtuel S3.

Description de la tâche

Pour pouvoir utiliser des demandes de style hébergement virtuel S3, un administrateur grid doit effectuer les tâches suivantes :

- Utilisez le Gestionnaire de grille pour ajouter les noms de domaine de points de terminaison S3 au système StorageGRID.
- Vérifiez que le certificat utilisé par le client pour les connexions HTTPS à StorageGRID est signé pour tous les noms de domaine requis par le client.

Par exemple, si le terminal du domaine de terminal du service d'API S3 est `s3.company.com`, L'administrateur de la grille doit s'assurer que le certificat utilisé pour les connexions HTTPS a `s3.company.com` En tant que nom commun du sujet et dans les autres noms du sujet, et `*.s3.company.com` Dans les autres noms du sujet.

- "Configurer le serveur DNS" Utilisé par le client pour inclure des enregistrements DNS qui correspondent aux noms de domaine du noeud final S3, y compris tous les enregistrements génériques requis.

Si le client se connecte à l'aide du service Load Balancer, le certificat que l'administrateur de la grille configure est le certificat du noeud final de l'équilibreur de charge utilisé par le client.

> Chaque terminal de l'équilibreur de charge possède son propre certificat, et chaque terminal peut être configuré pour reconnaître différents noms de domaine de terminal S3.

Si le client se connecte aux nœuds de stockage, le certificat que l'administrateur de la grille configure est le certificat de serveur personnalisé unique utilisé pour la grille.

Reportez-vous aux instructions pour "Administration d'StorageGRID" pour en savoir plus.

Une fois ces étapes terminées, vous pouvez utiliser des requêtes de type hébergement virtuel.

Testez la configuration de l'API REST S3

Vous pouvez utiliser l'interface de ligne de commande d'Amazon Web Services (AWS CLI) pour tester votre connexion au système et vérifier que vous pouvez lire et écrire des objets sur le système.

Avant de commencer

- Vous avez téléchargé et installé l'interface de ligne de commandes AWS depuis "aws.amazon.com/cli".
- Vous avez créé un compte de locataire S3 dans le système StorageGRID.
- Vous avez créé une clé d'accès dans le compte de locataire.

Étapes

1. Configurez les paramètres de l'interface de ligne de commande AWS pour utiliser le compte que vous avez créé dans le système StorageGRID :
   a. Passer en mode configuration : `aws configure`
   b. Entrez l'ID de clé d'accès du compte que vous avez créé.
   c. Entrez la clé d'accès secrète pour le compte que vous avez créé.
   d. Entrez la région par défaut à utiliser, par exemple US-East-1.
   e. Entrez le format de sortie par défaut à utiliser ou appuyez sur **entrée** pour sélectionner JSON.
2. Créer un compartiment.

   Cet exemple suppose que vous avez configuré un noeud final d'équilibreur de charge pour utiliser l'adresse IP 10.96.101.17 et le port 10443.

   ```
   aws s3api --endpoint-url https://10.96.101.17:10443
   --no-verify-ssl create-bucket --bucket testbucket
   ```

   Si le compartiment est créé avec succès, l'emplacement du compartiment est renvoyé, comme illustré

dans l'exemple suivant :

```
"Location": "/testbucket"
```

3. Télécharger un objet.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
put-object --bucket testbucket --key s3.pdf --body C:\s3-
test\upload\s3.pdf
```

Si l'objet est téléchargé avec succès, un ETAG est renvoyé, qui est un hachage des données de l'objet.

4. Répertorier le contenu du compartiment pour vérifier que l'objet a été téléchargé.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
list-objects --bucket testbucket
```

5. Supprimez l'objet.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
delete-object --bucket testbucket --key s3.pdf
```

6. Supprimer le compartiment.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
delete-bucket --bucket testbucket
```

La prise en charge des services de plateforme StorageGRID

La plateforme StorageGRID permet aux comptes locataires d'StorageGRID d'utiliser des services tels qu'un compartiment S3 distant, un point de terminaison SNS (simple notification Service) ou un cluster Elasticsearch afin d'élargir les services fournis par un grid.

Le tableau suivant récapitule les services de plateforme disponibles et les API S3 utilisés pour les configurer.

Service de plateforme	Objectif	API S3 utilisée pour configurer le service
Réplication CloudMirror	Réplique les objets à partir d'un compartiment StorageGRID source vers le compartiment S3 distant configuré.	PUT Bucket Replication (réplication de compartiment) (voir "Opérations sur les compartiments")
Notifications	Envoie des notifications sur les événements d'un compartiment StorageGRID source vers un point de terminaison SNS (simple notification Service) configuré.	Notification PUT Bucket (PLACER le compartiment) (voir "Opérations sur les compartiments")
Intégration de la recherche	Envoie les métadonnées d'objet des objets stockés dans un compartiment StorageGRID vers un index Elasticsearch configuré.	"CONFIGURATION de notification des métadonnées de compartiment" **Remarque :** il s'agit d'une API S3 personnalisée StorageGRID.

L'administrateur du grid doit activer les services de plateforme pour un compte de locataire avant de pouvoir les utiliser. Voir "Administrer StorageGRID". Ensuite, un administrateur de tenant doit créer un noeud final qui représente le service distant dans le compte de tenant. Cette étape est requise avant la configuration d'un service. Voir "Utilisez un compte de locataire".

Recommandations relatives à l'utilisation des services de plate-forme

Avant d'utiliser les services de plateforme, vous devez connaître les recommandations suivantes :

- NetApp recommande de ne pas autoriser plus de 100 locataires actifs avec les demandes S3 nécessitant la réplication CloudMirror, les notifications et l'intégration de la recherche. Avec plus de 100 locataires actifs, les performances des clients S3 sont plus lentes.
- Si la gestion des versions et la réplication CloudMirror sont activées pour un compartiment S3 dans le système StorageGRID, NetApp recommande que la gestion des versions du compartiment S3 soit également activée sur le terminal de destination. Cela permet à la réplication CloudMirror de générer des versions d'objet similaires sur le noeud final.
- La réplication CloudMirror n'est pas prise en charge si le compartiment source est activé pour le verrouillage objet S3.
- La réplication CloudMirror échoue avec une erreur AccessDenied si la conformité héritée du compartiment de destination est activée.

Implémentation de l'API REST S3 par StorageGRID

Requêtes des clients en conflit

Les demandes contradictoires des clients, telles que deux clients qui écrivent sur la même clé, sont résolues sur une base de « derniers-victoires ».

La chronologie de l'évaluation « derniers-victoires » repose sur la date à laquelle le système StorageGRID termine une demande donnée et non sur la date à laquelle les clients S3 commencent une opération.

Contrôles de cohérence

Les contrôles de cohérence assurent un équilibre entre la disponibilité des objets et la cohérence de ces objets entre plusieurs nœuds et sites de stockage, selon les exigences de votre application.

Par défaut, StorageGRID garantit la cohérence de lecture après écriture pour les nouveaux objets. Tout GET suivant un PUT réussi sera en mesure de lire les données nouvellement écrites. Les écrasements d'objets existants, les mises à jour de métadonnées et les suppressions sont cohérents. La propagation des écrasements ne prend généralement que quelques secondes ou minutes, mais peut prendre jusqu'à 15 jours.

Pour effectuer des opérations d'objet à un niveau de cohérence différent, vous pouvez définir un contrôle de cohérence pour chaque compartiment ou pour chaque opération d'API.

Contrôles de cohérence

Le contrôle de cohérence affecte la façon dont les métadonnées utilisées par StorageGRID pour suivre les objets sont distribuées entre les nœuds, et donc la disponibilité des objets pour les requêtes client.

Vous pouvez définir le contrôle de cohérence pour une opération de compartiment ou API sur l'une des valeurs suivantes :

- **All** : tous les nœuds reçoivent immédiatement les données, sinon la demande échouera.
- **Forte-global**: Garantit la cohérence lecture-après-écriture pour toutes les demandes client sur tous les sites.
- **Site fort** : garantit la cohérence de lecture après écriture pour toutes les demandes de clients au sein d'un site.
- **Read-after-New-write**: (Par défaut) fournit la cohérence lecture-après-écriture pour les nouveaux objets et éventuellement la cohérence pour les mises à jour d'objets. Offre une haute disponibilité et une protection des données garanties. Recommandé dans la plupart des cas.
- **Disponible** : assure la cohérence finale pour les nouveaux objets et les mises à jour d'objets. Pour les compartiments S3, utilisez uniquement si nécessaire (par exemple, pour un compartiment qui contient des valeurs de journal rarement lues ou pour les opérations HEAD ou GET sur des clés qui n'existent pas). Non pris en charge pour les compartiments FabricPool S3.

Utilisez des contrôles de cohérence « en cas de nouvelle écriture » et « disponibles »

Lorsqu'une OPÉRATION EN TÊTE ou GET utilise le contrôle de cohérence « en cas de nouvelle écriture », StorageGRID effectue la recherche en plusieurs étapes, comme suit :

- Il recherche tout d'abord l'objet à partir d'une faible cohérence.
- Si cette recherche échoue, elle répète la recherche au niveau de cohérence suivant jusqu'à ce qu'elle atteigne un niveau de cohérence équivalent au comportement de Strong-global.

Si une opération HEAD ou GET utilise le contrôle de cohérence « read-after-New-write », mais que l'objet n'existe pas, la recherche d'objets atteindra toujours un niveau de cohérence équivalent au comportement pour les groupes globaux forts. Ce niveau de cohérence exigeant la disponibilité de plusieurs copies des métadonnées d'objet sur chaque site, vous pouvez recevoir un nombre élevé d'erreurs de serveur interne 500 si deux nœuds de stockage ou plus sur le même site sont indisponibles.

À moins que vous n'ayez besoin de garanties de cohérence similaires à Amazon S3, vous pouvez empêcher ces erreurs de TÊTE et D'OBTENIR des opérations en définissant le contrôle de cohérence sur « disponible ». Lorsqu'une OPÉRATION DE TÊTE OU D'OBTENTION utilise le contrôle de cohérence « disponible », StorageGRID n'offre qu'une cohérence éventuelle. Elle n'essaie pas d'effectuer une opération ayant échoué à des niveaux de cohérence toujours plus élevés. Il n'est donc pas nécessaire que plusieurs copies des métadonnées de l'objet soient disponibles.

Spécifiez le contrôle de cohérence pour les opérations d'API

Pour définir le contrôle de cohérence pour une opération API individuelle, les contrôles de cohérence doivent être pris en charge pour l'opération, et vous devez spécifier le contrôle de cohérence dans l'en-tête de la demande. Cet exemple définit le contrôle de cohérence sur "site de segmentation" pour une opération D'OBTENTION d'objet.

```
GET /bucket/object HTTP/1.1
Date: date
Authorization: authorization name
Host: host
Consistency-Control: strong-site
```

> Vous devez utiliser le même contrôle de cohérence pour les opérations PLACER l'objet et OBTENIR l'objet.

Contrôle de cohérence du compartiment

Pour définir le contrôle de cohérence du compartiment, vous pouvez utiliser la demande de cohérence StorageGRID PUT bucket et la demande DE cohérence GET bucket. Vous pouvez également utiliser le Gestionnaire de locataires ou l'API de gestion des locataires.

Lors du réglage des commandes de cohérence pour un godet, tenez compte des éléments suivants :

- La configuration du contrôle de cohérence d'un compartiment détermine quel contrôle de cohérence est utilisé pour les opérations S3 effectuées sur les objets dans le compartiment ou sur la configuration du compartiment. Cela n'affecte pas les opérations du compartiment lui-même.
- Le contrôle de cohérence d'une opération API individuelle remplace le contrôle de cohérence du compartiment.
- En général, les compartiments doivent utiliser le contrôle de cohérence par défaut, « read-after-New-write ». Si les demandes ne fonctionnent pas correctement, modifiez le comportement du client d'application si possible. Ou configurez le client afin de spécifier le contrôle de cohérence pour chaque requête d'API. Réglez le contrôle de cohérence au niveau du godet uniquement en dernier recours.

[[comment les contrôles-cohérence-et-règles-ILM-interagissent]]Comment les contrôles de cohérence et les règles ILM interagissent pour protéger les données

Le contrôle de cohérence et la règle ILM de votre choix affectent la protection des objets. Ces paramètres peuvent interagir.

Par exemple, le contrôle de cohérence utilisé lorsqu'un objet est stocké affecte le placement initial des métadonnées d'objet, tandis que le comportement d'ingestion sélectionné pour la règle ILM affecte le placement initial des copies d'objet. Étant donné que StorageGRID nécessite l'accès aux métadonnées d'un objet et à ses données pour répondre aux demandes client, la sélection de niveaux de protection

correspondant au niveau de cohérence et au comportement d'ingestion permet d'améliorer la protection des données initiale et de mieux prévoir les réponses du système.

Les comportements d'ingestion suivants sont disponibles pour les règles ILM :

- **Dual commit** : StorageGRID effectue immédiatement des copies intermédiaires de l'objet et renvoie le succès au client. Les copies spécifiées dans la règle ILM sont effectuées lorsque cela est possible.
- **Strict** : toutes les copies spécifiées dans la règle ILM doivent être effectuées avant que le succès ne soit renvoyé au client.
- **Équilibré**: StorageGRID tente de faire toutes les copies spécifiées dans la règle ILM à l'entrée; si ce n'est pas possible, des copies intermédiaires sont faites et le succès est renvoyé au client. Les copies spécifiées dans la règle ILM sont effectuées lorsque cela est possible.

> Avant de sélectionner le comportement d'entrée d'une règle ILM, lisez la description complète de ces paramètres dans les instructions de gestion des objets avec la gestion du cycle de vie des informations.

Exemple d'interaction du contrôle de cohérence et de la règle ILM

Supposons que vous disposez d'une grille à deux sites avec la règle ILM suivante et le paramètre de niveau de cohérence suivant :

- **Règle ILM** : créez deux copies d'objet, une sur le site local et une sur un site distant. Le comportement d'entrée strict est sélectionné.
- **Niveau de cohérence**: "Sept-global" (les métadonnées d'objet sont immédiatement distribuées à tous les sites).

Lorsqu'un client stocke un objet dans la grille, StorageGRID effectue à la fois des copies d'objet et distribue les métadonnées aux deux sites avant de rétablir la réussite du client.

L'objet est entièrement protégé contre la perte au moment du message d'ingestion. Par exemple, si le site local est perdu peu de temps après l'ingestion, des copies des données de l'objet et des métadonnées de l'objet existent toujours sur le site distant. L'objet est entièrement récupérable.

Si vous utilisez à la place la même règle ILM et le niveau de cohérence "sept-site", le client peut recevoir un message de réussite après la réplication des données d'objet vers le site distant, mais avant que les métadonnées d'objet ne soient distribuées sur ce site. Dans ce cas, le niveau de protection des métadonnées d'objet ne correspond pas au niveau de protection des données d'objet. Si le site local est perdu peu de temps après l'ingestion, les métadonnées d'objet sont perdues. Impossible de récupérer l'objet.

L'interdépendance entre les niveaux de cohérence et les règles ILM peut être complexe. Contactez NetApp si vous avez besoin d'aide.

Informations associées

"Gestion des objets avec ILM"

"OPTIMISEZ la cohérence des compartiments"

"PRÉSERVER la cohérence du godet"

Gestion des objets par les règles StorageGRID ILM

L'administrateur du grid crée des règles de gestion du cycle de vie des informations pour

gérer les données d'objet ingérées sur le système StorageGRID à partir des applications client de l'API REST S3. Ces règles sont ensuite ajoutées à la règle ILM pour déterminer la façon dont et l'emplacement de stockage des données d'objet au fil du temps.

Les paramètres ILM déterminent les aspects suivants d'un objet :

- **Géographie**

  L'emplacement des données d'un objet, dans le système StorageGRID (pool de stockage) ou dans un pool de stockage cloud.

- **Grade de stockage**

  Type de stockage utilisé pour stocker les données d'objet : par exemple, Flash ou disque rotatif.

- * Protection contre les pertes*

  Le nombre de copies effectuées et les types de copies créées : réplication, code d'effacement, ou les deux.

- * Rétention*

  Évolution au fil du temps de la gestion des données d'un objet, de leur emplacement de stockage et de leur protection contre la perte.

- * Protection pendant l'ingestion*

  Méthode de protection des données d'objet lors de l'ingestion : placement synchrone (avec options équilibrées ou strictes pour le comportement d'ingestion) ou copies intermédiaires (avec l'option de double validation).

Les règles ILM peuvent filtrer et sélectionner des objets. Pour les objets ingérées à l'aide du protocole S3, les règles ILM peuvent filtrer les objets en fonction des métadonnées suivantes :

- Compte locataire
- Nom du compartiment
- Temps d'ingestion
- Clé
- Heure du dernier accès

> Par défaut, les mises à jour de l'heure du dernier accès sont désactivées pour tous les compartiments S3. Si votre système StorageGRID inclut une règle ILM utilisant l'option heure du dernier accès, vous devez activer les mises à jour à l'heure du dernier accès pour les compartiments S3 spécifiés dans cette règle. Utilisez la demande DE l'heure du dernier accès du compartiment PUT, le Gestionnaire de locataires (voir "Activez ou désactivez les mises à jour de l'heure du dernier accès") Ou l'API de gestion des locataires. Lors de l'activation des mises à jour du dernier accès, notez que les performances du StorageGRID peuvent être réduites, notamment dans les systèmes dotés d'objets de petite taille.

- Contrainte d'emplacement
- Taille de l'objet

- Métadonnées d'utilisateur
- Balise d'objet

Informations associées

"Utilisez un compte de locataire"

"Gestion des objets avec ILM"

"METTRE l'heure du dernier accès au compartiment"

Gestion des versions d'objet

Vous pouvez utiliser la gestion des versions pour conserver plusieurs versions d'un objet, ce qui vous protège contre la suppression accidentelle d'objets et vous permet d'extraire et de restaurer les versions antérieures d'un objet.

Le système StorageGRID implémente la gestion des versions avec prise en charge de la plupart des fonctionnalités et avec certaines limites. StorageGRID prend en charge jusqu'à 1,000 versions de chaque objet.

Le contrôle de version d'objets peut être associé à la gestion du cycle de vie des informations (ILM) d'StorageGRID ou à la configuration du cycle de vie des compartiments S3. Vous devez activer explicitement la gestion des versions pour chaque compartiment pour activer cette fonctionnalité. Chaque objet du compartiment est associé à un ID de version, généré par le système StorageGRID.

La suppression de l'authentification multifacteur (MFA) n'est pas prise en charge.

> Le contrôle de version ne peut être activé que pour les compartiments créés avec StorageGRID version 10.3 ou ultérieure.

ILM et gestion des versions

Les règles ILM sont appliquées à chaque version d'un objet. Un processus d'analyse ILM analyse en continu tous les objets, puis les évalue à nouveau en fonction de la règle ILM actuelle. Toute modification apportée aux règles ILM est appliquée à tous les objets précédemment ingérées. Ceci inclut les versions préalablement ingérées si la gestion des versions est activée. L'analyse ILM applique les modifications de l'ILM aux objets précédemment ingérées.

Pour les objets S3 dans les compartiments avec gestion des versions, la prise en charge des versions vous permet de créer des règles ILM qui utilisent « Noncurrent Time » comme heure de référence (sélectionnez **Yes** pour la question, « Apply this rule to Older versions only? ») po "Étape 1 de l'assistant de création de règles ILM"). Lorsqu'un objet est mis à jour, ses versions précédentes deviennent non actuelles. L'utilisation d'un filtre « Noncurrent Time » vous permet de créer des règles qui réduisent l'impact sur le stockage des versions précédentes d'objets.

> Lorsque vous téléchargez une nouvelle version d'un objet à l'aide d'une opération de téléchargement partitionné, l'heure qui n'est pas à jour pour la version d'origine de l'objet correspond à la création du téléchargement partitionné pour la nouvelle version, et non à la fin du téléchargement partitionné. Dans des cas limités, l'heure non actuelle de la version d'origine peut être des heures ou des jours plus tôt que l'heure de la version actuelle.

Voir "Règles et règles ILM pour les objets avec version S3 (exemple 4)".

Utilisez l'API REST S3 pour configurer le verrouillage objet S3

Si le paramètre global de verrouillage des objets S3 est activé pour votre système StorageGRID, vous pouvez créer des compartiments avec le verrouillage des objets S3 activé. Vous pouvez spécifier des paramètres de conservation par défaut pour chaque compartiment ou pour chaque version d'objet.

Activation du verrouillage objet S3 pour un compartiment

Si le paramètre global de verrouillage d'objet S3 est activé pour votre système StorageGRID, vous pouvez activer le verrouillage d'objet S3 lorsque vous créez chaque compartiment.

Le verrouillage objet S3 est un paramètre permanent qui ne peut être activé que lorsque vous créez un compartiment. Une fois un compartiment créé, vous ne pouvez ni ajouter ni désactiver le verrouillage objet S3.

Pour activer le verrouillage objet S3 pour un compartiment, utilisez l'une des méthodes suivantes :

- Créez le compartiment à l'aide du Gestionnaire des locataires. Voir "Créer un compartiment S3".
- Créer le compartiment à l'aide d'une demande PUT bucket avec le `x-amz-bucket-object-lock-enabled` en-tête de demande. Voir "Opérations sur les compartiments".

Le verrouillage objet S3 requiert la gestion des versions des compartiments, qui est automatiquement activée lors de la création du compartiment. Vous ne pouvez pas suspendre la gestion des versions pour le compartiment. Voir "Gestion des versions d'objet".

Paramètres de conservation par défaut d'un compartiment

Lorsque le verrouillage objet S3 est activé pour un compartiment, vous pouvez éventuellement activer la conservation par défaut du compartiment et spécifier un mode de conservation par défaut et une période de conservation par défaut.

Mode de rétention par défaut

- En mode CONFORMITÉ :
  - L'objet ne peut pas être supprimé tant que sa date de conservation jusqu'à n'est pas atteinte.
  - La date de conservation de l'objet peut être augmentée, mais elle ne peut pas être réduite.
  - La date de conservation de l'objet jusqu'à ne peut pas être supprimée tant que cette date n'est pas atteinte.
- En mode GOUVERNANCE :
  - Utilisateurs avec le `s3:BypassGovernanceRetention` l'autorisation peut utiliser le `x-amz-bypass-governance-retention: true` demander à l'en-tête de contourner les paramètres de rétention.
  - Ces utilisateurs peuvent supprimer une version d'objet avant d'atteindre sa date de conservation jusqu'à.
  - Ces utilisateurs peuvent augmenter, diminuer ou supprimer la date de conservation d'un objet.

Période de conservation par défaut

Une période de conservation par défaut peut être spécifiée en années ou en jours pour chaque compartiment.

Comment définir la conservation par défaut d'un compartiment

Pour définir la rétention par défaut d'un compartiment, utilisez l'une des méthodes suivantes :

- Gérez les paramètres de compartiment depuis le gestionnaire de locataires. Voir "Créer un compartiment S3" et "Mettre à jour la conservation par défaut du verrouillage d'objet S3".
- Émettre une demande DE configuration DE verrouillage d'objet PUT pour le compartiment afin de spécifier le mode par défaut et le nombre de jours ou d'années par défaut.

CONFIGURATION du verrouillage de l'objet

La demande PUT Object Lock Configuration vous permet de définir et de modifier le mode de rétention par défaut et la période de rétention par défaut pour un compartiment pour lequel S3 Object Lock est activé. Vous pouvez également supprimer les paramètres de conservation par défaut configurés précédemment.

Lorsque de nouvelles versions d'objet sont ingérées sur le compartiment, le mode de conservation par défaut est appliqué si `x-amz-object-lock-mode` et `x-amz-object-lock-retain-until-date` ne sont pas spécifiés. La période de rétention par défaut est utilisée pour calculer la date de conservation si `x-amz-object-lock-retain-until-date` n'est pas spécifié.

Si la période de conservation par défaut est modifiée après l'ingestion d'une version d'objet, la conservation à la date de la version de l'objet reste la même et n'est pas recalculée en utilisant la nouvelle période de conservation par défaut.

Vous devez avoir le `s3:PutBucketObjectLockConfiguration` autorisation, ou être root de compte, pour terminer cette opération.

Le `Content-MD5` L'en-tête de demande doit être spécifié dans la demande PUT.

Exemple de demande

Cet exemple active le verrouillage objet S3 pour un compartiment et définit le mode de conservation par défaut sur CONFORMITÉ et la période de conservation par défaut sur 6 ans.

```
PUT /bucket?object-lock HTTP/1.1
Accept-Encoding: identity
Content-Length: 308
Host: host
Content-MD5: request header
User-Agent: s3sign/1.0.0 requests/2.24.0 python/3.8.2
X-Amz-Date: date
X-Amz-Content-SHA256: authorization-string
Authorization: authorization-string

<ObjectLockConfiguration>
    <ObjectLockEnabled>Enabled</ObjectLockEnabled>
    <Rule>
        <DefaultRetention>
            <Mode>COMPLIANCE</Mode>
            <Years>6</Years>
        </DefaultRetention>
    </Rule>
</ObjectLockConfiguration>
```

Comment déterminer la conservation par défaut d'un compartiment

Pour déterminer si le verrouillage objet S3 est activé pour un compartiment et pour afficher le mode de conservation et la période de conservation par défaut, utilisez l'une des méthodes suivantes :

- Affichez le compartiment dans le gestionnaire de locataires. Voir "Afficher les compartiments S3".
- Émettre une demande OBTENIR la configuration de verrouillage d'objet.

OBTENIR la configuration de verrouillage d'objet

La demande OBTENIR la configuration du verrouillage d'objet vous permet de déterminer si le verrouillage d'objet S3 est activé pour un compartiment et, si ce dernier est activé, vérifiez si un mode de conservation et une période de conservation par défaut sont configurés pour ce compartiment.

Lorsque de nouvelles versions d'objet sont ingérées sur le compartiment, le mode de conservation par défaut est appliqué si `x-amz-object-lock-mode` n'est pas spécifié. La période de rétention par défaut est utilisée pour calculer la date de conservation si `x-amz-object-lock-retain-until-date` n'est pas spécifié.

Vous devez avoir le `s3:GetBucketObjectLockConfiguration` autorisation, ou être root de compte, pour terminer cette opération.

Exemple de demande

```
GET /bucket?object-lock HTTP/1.1
Host: host
Accept-Encoding: identity
User-Agent: aws-cli/1.18.106 Python/3.8.2 Linux/4.4.0-18362-Microsoft
botocore/1.17.29
x-amz-date: date
x-amz-content-sha256: authorization-string
Authorization: authorization-string
```

Exemple de réponse

```
HTTP/1.1 200 OK
x-amz-id-2:
iVmcB7OXXJRkRH1FiVq1151/T24gRfpwpuZrEG11Bb9ImOMAAe98oxSpXlknabA0LTvBYJpSIX
k=
x-amz-request-id: B34E94CACB2CEF6D
Date: Fri, 04 Sep 2020 22:47:09 GMT
Transfer-Encoding: chunked
Server: AmazonS3

<?xml version="1.0" encoding="UTF-8"?>
<ObjectLockConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
    <ObjectLockEnabled>Enabled</ObjectLockEnabled>
    <Rule>
        <DefaultRetention>
            <Mode>COMPLIANCE</Mode>
            <Years>6</Years>
        </DefaultRetention>
    </Rule>
</ObjectLockConfiguration>
```

Comment spécifier les paramètres de conservation d'un objet

Un compartiment lorsque le verrouillage objet S3 est activé peut contenir une combinaison d'objets avec ou sans paramètres de conservation du verrouillage objet S3.

Les paramètres de conservation au niveau objet sont spécifiés à l'aide de l'API REST S3. Les paramètres de conservation d'un objet remplacent les paramètres de conservation par défaut du compartiment.

Vous pouvez spécifier les paramètres suivants pour chaque objet :

- **Mode de conservation** : CONFORMITÉ ou GOUVERNANCE.
- **Conserver-jusqu'à-date** : une date spécifiant la durée pendant laquelle la version de l'objet doit être conservée par StorageGRID.
  - En mode CONFORMITÉ, si la date de conservation jusqu'à est dans le futur, l'objet peut être récupéré, mais il ne peut pas être modifié ou supprimé. La date de conservation jusqu'à peut être augmentée,

mais cette date ne peut pas être réduite ou supprimée.

  - En mode GOUVERNANCE, les utilisateurs disposant d'une autorisation spéciale peuvent contourner le paramètre conserver jusqu'à la date. Ils peuvent supprimer une version d'objet avant la fin de sa période de conservation. Ils peuvent également augmenter, diminuer ou même supprimer la date de conservation jusqu'à.

- **Mise en garde légale** : l'application d'une mise en garde légale à une version d'objet verrouille immédiatement cet objet. Par exemple, vous devrez peut-être mettre une obligation légale sur un objet lié à une enquête ou à un litige juridique. Une obligation légale n'a pas de date d'expiration, mais reste en place jusqu'à ce qu'elle soit explicitement supprimée.

  Le paramètre de conservation légale d'un objet est indépendant du mode de conservation et de la date de conservation jusqu'à. Si une version d'objet est en attente légale, personne ne peut supprimer cette version.

Pour spécifier les paramètres de verrouillage d'objet S3 lors de l'ajout d'une version d'objet à un compartiment, émettez un "PLACER l'objet", "PLACER l'objet - Copier", ou "Lancer le téléchargement de pièces multiples" demande.

Vous pouvez utiliser les éléments suivants :

- `x-amz-object-lock-mode`, Qui peut être CONFORMITÉ ou GOUVERNANCE (sensible à la casse).

  > Si vous spécifiez `x-amz-object-lock-mode`, vous devez également spécifier `x-amz-object-lock-retain-until-date`.

- `x-amz-object-lock-retain-until-date`
  - La valeur conserver jusqu'à la date doit être au format `2020-08-10T21:46:00Z`. Les secondes fractionnaires sont autorisées, mais seuls 3 chiffres après la virgule sont conservés (précision des millisecondes). Les autres formats ISO 8601 ne sont pas autorisés.
  - La date de conservation doit être ultérieure.
- `x-amz-object-lock-legal-hold`

  Si la conservation légale est ACTIVÉE (sensible à la casse), l'objet est placé sous une obligation légale. Si la mise en attente légale est désactivée, aucune mise en attente légale n'est mise. Toute autre valeur entraîne une erreur 400 Bad Request (InvalidArgument).

Si vous utilisez l'un de ces en-têtes de demande, tenez compte des restrictions suivantes :

- Le `Content-MD5` l'en-tête de demande est requis le cas échéant `x-amz-object-lock-*` L'en-tête de la demande est présent dans la demande D'objet PUT. `Content-MD5` N'est pas nécessaire pour PLACER l'objet - Copier ou lancer le téléchargement de pièces multiples.
- Si le verrouillage d'objet S3 n'est pas activé dans le compartiment et qu'un `x-amz-object-lock-*` L'en-tête de la demande est présent, une erreur 400 Bad Request (InvalidRequest) est renvoyée.
- La requête PUT Object prend en charge l'utilisation de `x-amz-storage-class: REDUCED_REDUNDANCY` Pour correspondre au comportement AWS. Cependant, lors de l'ingestion d'un objet dans un compartiment lorsque le verrouillage objet S3 est activé, StorageGRID effectue toujours une entrée à double validation.
- Une réponse ultérieure DE la version D'objet GET ou HEAD inclura les en-têtes `x-amz-object-lock-mode`, `x-amz-object-lock-retain-until-date`, et `x-amz-object-lock-legal-hold`, si

configuré et si l'expéditeur de la demande est correct `s3:Get*` autorisations.

Vous pouvez utiliser le `s3:object-lock-remaining-retention-days` clé de condition de règle pour limiter les périodes de conservation minimale et maximale autorisée pour vos objets.

Comment mettre à jour les paramètres de conservation d'un objet

Si vous devez mettre à jour les paramètres de conservation légale ou de conservation d'une version d'objet existante, vous pouvez effectuer les opérations de sous-ressource d'objet suivantes :

- `PUT Object legal-hold`

  Si la nouvelle valeur de conservation légale est ACTIVÉE, l'objet est placé sous une mise en attente légale. Si la valeur de retenue légale est OFF, la suspension légale est levée.

- `PUT Object retention`
  - La valeur du mode peut être CONFORMITÉ ou GOUVERNANCE (sensible à la casse).
  - La valeur conserver jusqu'à la date doit être au format `2020-08-10T21:46:00Z`. Les secondes fractionnaires sont autorisées, mais seuls 3 chiffres après la virgule sont conservés (précision des millisecondes). Les autres formats ISO 8601 ne sont pas autorisés.
  - Si une version d'objet possède une date de conservation existante, vous pouvez uniquement l'augmenter. La nouvelle valeur doit être future.

Comment utiliser le mode GOUVERNANCE

Les utilisateurs qui disposent de `s3:BypassGovernanceRetention` L'autorisation peut contourner les paramètres de rétention actifs d'un objet qui utilise le mode DE GOUVERNANCE. Toute opération DE SUPPRESSION ou DE CONSERVATION D'objet PUT doit inclure le `x-amz-bypass-governance-retention:true` en-tête de demande. Ces utilisateurs peuvent effectuer les opérations supplémentaires suivantes :

- Effectuez DES opérations DE SUPPRESSION d'objet ou DE SUPPRESSION de plusieurs objets pour supprimer une version d'objet avant la fin de sa période de conservation.

  Impossible de supprimer les objets qui sont en attente légale. La mise en attente légale doit être désactivée.

- Exécutez des opérations PUT Object Retention qui font passer le mode d'une version d'objet DE GOUVERNANCE À LA CONFORMITÉ avant que la période de conservation de l'objet ne soit écoulée.

  Le passage du mode DE CONFORMITÉ À LA GOUVERNANCE n'est jamais autorisé.

- Exécutez des opérations PUT Object Retention pour augmenter, diminuer ou supprimer la période de conservation d'une version d'objet.

Informations associées

- "Gestion des objets avec le verrouillage d'objets S3"
- "Utilisez le verrouillage d'objet S3 pour conserver les objets"
- "Guide de l'utilisateur Amazon simple Storage Service : utilisation du verrouillage d'objets S3"

Création de la configuration du cycle de vie S3

Vous pouvez créer une configuration de cycle de vie S3 afin de contrôler la suppression d'objets spécifiques du système StorageGRID.

L'exemple simple de cette section illustre la façon dont une configuration du cycle de vie S3 peut contrôler la suppression de certains objets (expirés) dans des compartiments S3 spécifiques. L'exemple de cette section est fourni à titre d'illustration uniquement. Pour plus d'informations sur la création de configurations de cycle de vie S3, reportez-vous à la section "Amazon simple Storage Service Developer Guide : gestion du cycle de vie des objets". Notez que StorageGRID prend uniquement en charge les actions d'expiration, mais pas les actions de transition.

La configuration du cycle de vie

La configuration du cycle de vie est un ensemble de règles appliquées aux objets dans des compartiments S3 spécifiques. Chaque règle indique quels objets sont affectés et quand ces objets vont expirer (à une date spécifique ou après un certain nombre de jours).

StorageGRID prend en charge jusqu'à 1,000 règles de cycle de vie dans une configuration cycle de vie. Chaque règle peut inclure les éléments XML suivants :

- Expiration : supprimez un objet lorsqu'une date spécifiée est atteinte ou lorsqu'un nombre de jours spécifié est atteint, à partir de l'ingestion de l'objet.
- NonactuelVersionExexpiration : supprimez un objet lorsque le nombre de jours spécifié est atteint, à partir de quand l'objet est devenu non courant.
- Filtre (préfixe, étiquette)
- État
- ID

Si vous appliquez une configuration de cycle de vie à un compartiment, les paramètres de cycle de vie du compartiment prévalent toujours sur les paramètres ILM de StorageGRID. StorageGRID utilise les paramètres d'expiration du compartiment et non ILM pour déterminer s'il faut supprimer ou conserver des objets spécifiques.

Par conséquent, il est possible de supprimer un objet de la grille, même si les instructions de placement d'une règle ILM s'appliquent toujours à l'objet. Il est également possible de conserver un objet dans la grille même après l'expiration des instructions de placement ILM de l'objet. Pour plus de détails, voir "Fonctionnement de ILM tout au long de la vie d'un objet".

> La configuration du cycle de vie des compartiments avec des compartiments dont le verrouillage objet S3 est activé, mais la configuration du cycle de vie des compartiments n'est pas prise en charge pour les compartiments conformes.

StorageGRID prend en charge les opérations suivantes des compartiments pour gérer les configurations du cycle de vie :

- SUPPRIMER le cycle de vie du compartiment
- OPTIMISEZ le cycle de vie des compartiments
- CYCLE de vie des compartiments

Créer une configuration de cycle de vie

Comme première étape de la création de la configuration du cycle de vie, vous créez un fichier JSON qui inclut une ou plusieurs règles. Par exemple, ce fichier JSON contient trois règles, comme suit :

1. La règle 1 s'applique uniquement aux objets qui correspondent au préfixe `category1/` et qui ont un `key2` valeur de `tag2`. Le `Expiration` Le paramètre spécifie que les objets correspondant au filtre expireront à minuit le 22 août 2020.
2. La règle 2 s'applique uniquement aux objets qui correspondent au préfixe `category2/`. Le `Expiration` le paramètre indique que les objets correspondant au filtre expirent 100 jours après leur ingestion.

   > Les règles spécifiant un nombre de jours sont relatives à l'ingestion de l'objet. Si la date actuelle dépasse la date d'ingestion et le nombre de jours, certains objets peuvent être supprimés du compartiment dès que la configuration de cycle de vie est appliquée.

3. La règle 3 s'applique uniquement aux objets qui correspondent au préfixe `category3/`. Le `Expiration` paramètre spécifie que toute version non actuelle des objets de correspondance expirera 50 jours après leur non-mise à jour.

```
{
    "Rules": [
        {
            "ID": "rule1",
            "Filter": {
                "And": {
                    "Prefix": "category1/",
                    "Tags": [
                        {
                            "Key": "key2",
                            "Value": "tag2"
                        }
                    ]
                }
            },
            "Expiration": {
                "Date": "2020-08-22T00:00:00Z"
            },
            "Status": "Enabled"
        },
        {
            "ID": "rule2",
            "Filter": {
                "Prefix": "category2/"
            },
            "Expiration": {
                "Days": 100
            },
            "Status": "Enabled"
        },
        {
            "ID": "rule3",
            "Filter": {
                "Prefix": "category3/"
            },
            "NoncurrentVersionExpiration": {
                "NoncurrentDays": 50
            },
            "Status": "Enabled"
        }
    ]
}
```

Appliquez la configuration du cycle de vie au compartiment

Une fois que vous avez créé le fichier de configuration du cycle de vie, vous l'appliquez à un compartiment en émettant une demande DE cycle de vie PUT bucket.

Cette demande applique la configuration du cycle de vie dans le fichier exemple aux objets d'un compartiment nommé `testbucket`.

```
aws s3api --endpoint-url <StorageGRID endpoint> put-bucket-lifecycle-
configuration
--bucket testbucket --lifecycle-configuration file://bktjson.json
```

Pour vérifier qu'une configuration du cycle de vie a été appliquée avec succès au compartiment, émettez une demande GET Lifecycle. Par exemple :

```
aws s3api --endpoint-url <StorageGRID endpoint> get-bucket-lifecycle-
configuration
 --bucket testbucket
```

Une réponse réussie répertorie la configuration de cycle de vie que vous venez d'appliquer.

Vérifiez que l'expiration du cycle de vie du compartiment s'applique à l'objet

Vous pouvez déterminer si une règle d'expiration dans la configuration de cycle de vie s'applique à un objet spécifique lors de l'émission d'une requête D'objet PUT, HEAD Object ou GET Object. Si une règle s'applique, la réponse comprend un `Expiration` paramètre qui indique quand l'objet expire et quelle règle d'expiration a été mise en correspondance.

> Le cycle de vie des compartiments ignore ILM, le `expiry-date` l'illustration représente la date réelle à laquelle l'objet sera supprimé. Pour plus de détails, voir "Méthode de détermination de la conservation des objets".

Par exemple, cette requête PUT Object a été émise le 22 juin 2020 et place un objet dans le `testbucket` godet.

```
aws s3api --endpoint-url <StorageGRID endpoint> put-object
--bucket testbucket --key obj2test2 --body bktjson.json
```

La réponse de réussite indique que l'objet expirera dans 100 jours (01 oct 2020) et qu'il correspond à la règle 2 de la configuration de cycle de vie.

```
{
      *"Expiration": "expiry-date=\"Thu, 01 Oct 2020 09:07:49 GMT\", rule-
id=\"rule2\"",
      "ETag": "\"9762f8a803bc34f5340579d4446076f7\""
}
```

Par exemple, cette demande d'objet TÊTE a été utilisée pour obtenir les métadonnées du même objet dans le compartiment test.

```
aws s3api --endpoint-url <StorageGRID endpoint> head-object
--bucket testbucket --key obj2test2
```

La réponse de réussite inclut les métadonnées de l'objet et indique que l'objet expirera dans 100 jours et qu'il correspond à la règle 2.

```
{
      "AcceptRanges": "bytes",
      *"Expiration": "expiry-date=\"Thu, 01 Oct 2020 09:07:48 GMT\", rule-
id=\"rule2\"",
      "LastModified": "2020-06-23T09:07:48+00:00",
      "ContentLength": 921,
      "ETag": "\"9762f8a803bc34f5340579d4446076f7\""
      "ContentType": "binary/octet-stream",
      "Metadata": {}
}
```

Recommandations pour l'implémentation de l'API REST S3

Suivez ces recommandations lors de l'implémentation de l'API REST S3 pour une utilisation avec StorageGRID.

Recommandations pour les têtes à des objets inexistants

Si votre application vérifie régulièrement si un objet existe dans un chemin où vous ne vous attendez pas à ce que l'objet existe réellement, vous devez utiliser le contrôle de cohérence « disponible ». Par exemple, vous devez utiliser le contrôle de cohérence « disponible » si votre application dirige un emplacement avant DE LE PLACER.

Sinon, si l'opération HEAD ne trouve pas l'objet, vous pouvez recevoir un nombre élevé de 500 erreurs de serveur interne si un ou plusieurs nœuds de stockage ne sont pas disponibles.

Vous pouvez définir le contrôle de cohérence « disponible » pour chaque compartiment à l'aide de la demande DE cohérence PUT bucket, ou spécifier le contrôle de cohérence dans l'en-tête de demande pour une opération API individuelle.

Recommandations pour les clés d'objet

Suivez ces recommandations pour les noms de clés d'objet, en fonction de la date de création du compartiment.

Compartiments créés dans StorageGRID 11.4 ou version antérieure

- N'utilisez pas de valeurs aléatoires comme les quatre premiers caractères des clés d'objet. Cela contraste avec l'ancienne recommandation AWS pour les préfixes de clés. Utilisez plutôt des préfixes non aléatoires et non uniques, tels que `image`.
- Si vous suivez les recommandations d'AWS pour utiliser des caractères aléatoires et uniques dans les préfixes de clés, préfixez les clés d'objet à l'aide d'un nom de répertoire. C'est-à-dire, utilisez le format suivant :

  ```
  mybucket/mydir/f8e3-image3132.jpg
  ```

  Au lieu de ce format :

  ```
  mybucket/f8e3-image3132.jpg
  ```

Compartiments créés dans StorageGRID 11.4 ou version ultérieure

Il n'est pas nécessaire de restreindre les noms de clés d'objet pour répondre aux bonnes pratiques de performances. Dans la plupart des cas, vous pouvez utiliser des valeurs aléatoires pour les quatre premiers caractères des noms de clé d'objet.

> À cela s'exception près un workload S3 qui supprime en continu tous les objets après une courte période de temps. Pour minimiser l'impact sur les performances de ce cas d'utilisation, il est possible de faire varier la première partie du nom de clé tous les mille objets avec une date comme la date. Supposons par exemple qu'un client S3 écrit généralement 2,000 objets/seconde et que la règle de cycle de vie ILM ou compartiment supprime tous les objets au bout de trois jours. Pour réduire l'impact sur les performances, vous pouvez nommer les clés comme suit : `/mybucket/mydir/yyyymmddhhmmss-random_UUID.jpg`

Recommandations pour « plages de lectures »

Si le "option globale pour compresser les objets stockés" Est activé, les applications client S3 doivent éviter d'effectuer des opérations GET Object qui spécifient une plage d'octets à renvoyer. Ces opérations de « lecture à plage » sont inefficaces, car StorageGRID doit décompresser efficacement les objets pour accéder aux octets demandés. LES opérations GET Object qui demandent une petite plage d'octets provenant d'un objet très volumineux sont particulièrement inefficaces. Par exemple, il est inefficace de lire une plage de 10 Mo sur un objet compressé de 50 Go.

Si les plages sont lues à partir d'objets compressés, les demandes client peuvent être en attente.

> Si vous devez compresser des objets et que votre application client doit utiliser des lectures de plage, augmentez le délai de lecture de l'application.

Informations associées

- "Contrôles de cohérence"
- "PRÉSERVER la cohérence du godet"
- "Administrer StorageGRID"

Prise en charge de l'API REST Amazon S3

Détails de l'implémentation de l'API REST S3

Le système StorageGRID implémente l'API simple Storage Service (API version 2006-03-01) avec la prise en charge de la plupart des opérations et avec certaines limites. Vous devez connaître les détails d'implémentation lorsque vous intégrez des applications client de l'API REST S3.

Le système StorageGRID prend en charge les demandes de type hébergement virtuel et les demandes de type chemin d'accès.

Traitement de la date

L'implémentation StorageGRID de l'API REST S3 ne prend en charge que les formats de date HTTP valides.

Le système StorageGRID prend uniquement en charge les formats de date HTTP valides pour tous les en-têtes qui acceptent les valeurs de date. La partie heure de la date peut être spécifiée au format heure de Greenwich (GMT) ou au format heure coordonnée universelle (UTC) sans décalage de fuseau horaire (+0000 doit être spécifié). Si vous incluez le `x-amz-date` En-tête de votre demande, elle remplace toute valeur spécifiée dans l'en-tête de la demande de date. Lors de l'utilisation de la signature AWS version 4, le `x-amz-date` l'en-tête doit être présent dans la demande signée car l'en-tête de date n'est pas pris en charge.

En-têtes de demande commune

Le système StorageGRID prend en charge les en-têtes de requête communs définis par "Référence de l'API Amazon simple Storage Service : en-têtes de demande communs", à une exception près.

En-tête de demande	Mise en place
Autorisation	Prise en charge complète de la signature AWS version 2 Prise en charge de la signature AWS version 4, à l'exception des cas suivants : • La valeur SHA256 n'est pas calculée pour le corps de la demande. La valeur soumise par l'utilisateur est acceptée sans validation, comme si la valeur `UNSIGNED-PAYLOAD` avait été prévu pour le `x-amz-content-sha256` en-tête.
jeton de sécurité x-amz	Non mis en œuvre. Retours `XNotImplemented`.

En-têtes de réponse commune

Le système StorageGRID prend en charge tous les en-têtes de réponse courants définis par l'API *simple Storage Service Reference*, à une exception près.

En-tête de réponse	Mise en place
x-amz-id-2	Non utilisé

Authentifier les demandes

Le système StorageGRID prend en charge l'accès authentifié et anonyme aux objets à l'aide de l'API S3.

L'API S3 prend en charge la version 2 de Signature et la version 4 de Signature pour authentifier les requêtes API S3.

Les demandes authentifiées doivent être signées à l'aide de votre ID de clé d'accès et de votre clé secrète d'accès.

Le système StorageGRID prend en charge deux méthodes d'authentification : le protocole HTTP `Authorization` en-tête et utilisation des paramètres de requête.

Utilisez l'en-tête HTTP Authorization

Le HTTP `Authorization` L'en-tête est utilisé par toutes les opérations de l'API S3 à l'exception des demandes anonymes lorsque la stratégie de compartiment l'autorise. Le `Authorization` en-tête contient toutes les informations de signature requises pour authentifier une demande.

Utiliser les paramètres de requête

Vous pouvez utiliser les paramètres de requête pour ajouter des informations d'authentification à une URL. Il s'agit de la présignature de l'URL, qui peut être utilisée pour accorder un accès temporaire à des ressources spécifiques. Les utilisateurs avec l'URL présignée n'ont pas besoin de connaître la clé d'accès secrète pour accéder à la ressource, ce qui vous permet de fournir un accès limité tiers à une ressource.

Opérations sur le service

Le système StorageGRID prend en charge les opérations suivantes sur ce service.

Fonctionnement	Mise en place
ACCÉDER au service `(ListBuckets)`	Mise en œuvre avec tout le comportement de l'API REST Amazon S3. D'être modifiées sans préavis.
DÉCOUVREZ l'utilisation du stockage	La demande GET Storage usage vous indique la quantité totale de stockage utilisée par un compte et pour chaque compartiment associé au compte. Il s'agit d'une opération sur le service avec un chemin de / et un paramètre de requête personnalisé (`?x-ntap-sg-usage`) ajouté.
OPTIONS /	Les applications client peuvent émettre `OPTIONS /` Requêtes vers le port S3 d'un nœud de stockage, sans identifiants d'authentification S3, pour déterminer si le nœud de stockage est disponible. Vous pouvez utiliser cette requête pour la surveillance ou permettre aux équilibreurs de charge externes d'identifier lorsqu'un nœud de stockage est arrêté.

Informations associées

"DÉCOUVREZ l'utilisation du stockage"

Opérations sur les compartiments

Le système StorageGRID prend en charge un maximum de 1,000 compartiments pour chaque compte de locataire S3.

Les restrictions relatives aux noms de compartiment respectent les restrictions régionales standard AWS, mais vous devez les restreindre à une nomenclature DNS pour prendre en charge les demandes de type hébergement virtuel S3.

Pour plus d'informations, reportez-vous aux sections suivantes :

- "Documentation Amazon Web Services (AWS) : restrictions et limites des compartiments"
- "Configuration des noms de domaine de terminaux S3"

Les opérations GET Bucket (List Objects) et GET compartiment versions prennent en charge les contrôles de cohérence StorageGRID.

Vous pouvez vérifier si les mises à jour de l'heure du dernier accès sont activées ou désactivées pour les compartiments individuels.

Le tableau suivant décrit la façon dont StorageGRID implémente les opérations des compartiments de l'API REST S3. Pour effectuer l'une de ces opérations, les informations d'identification d'accès nécessaires doivent être fournies pour le compte.

Fonctionnement	Mise en place
SUPPRIMER le compartiment	Cette opération supprime le godet.
SUPPRIMER les godets	Cette opération supprime la configuration CORS pour le compartiment.
SUPPRIMER le chiffrement du compartiment	Cette opération supprime le chiffrement par défaut du compartiment. Les objets chiffrés existants restent chiffrés, mais aucun nouvel objet ajouté au compartiment n'est chiffré.
SUPPRIMER le cycle de vie du compartiment	Cette opération supprime la configuration du cycle de vie du compartiment. Voir "Création de la configuration du cycle de vie S3".
SUPPRIMER la règle de compartiment	Cette opération supprime la règle attachée au compartiment.
SUPPRIMER la réplication du compartiment	Cette opération supprime la configuration de réplication attachée au compartiment.
SUPPRIMER le balisage du compartiment	Cette opération utilise le `tagging` sous-ressource pour supprimer toutes les balises d'un compartiment.

Fonctionnement	Mise en place
RUBRIQUE GET (ListObjects) (ListObjectsV2)	Cette opération renvoie une partie ou la totalité (jusqu'à 1,000) des objets dans un godet. La classe de stockage pour les objets peut avoir l'une ou l'autre des deux valeurs, même si l'objet a été ingéré avec le `REDUCED_REDUNDANCY` option de classe de stockage : • `STANDARD`, Qui indique que l'objet est stocké dans un pool de stockage composé de nœuds de stockage. • `GLACIER`, Qui indique que l'objet a été déplacé vers le compartiment externe spécifié par le pool de stockage cloud. Si le compartiment contient un grand nombre de clés supprimées qui ont le même préfixe, la réponse peut inclure une partie `CommonPrefixes` qui ne contiennent pas de clés.
OBTENIR les versions d'objet de compartiment (ListObjectVersions)	Avec accès EN LECTURE sur un godet, cette opération avec le `versions` sous-ressource répertorie les métadonnées de toutes les versions des objets dans le compartiment.
OBTENIR l'acl du compartiment	Cette opération renvoie une réponse positive et l'ID, le DisplayName et l'autorisation du propriétaire du compartiment, indiquant que le propriétaire a un accès complet au compartiment.
OBTENIR les godets	Cette opération renvoie le `cors` configuration du compartiment.
CHIFFREMENT des compartiments	Cette opération renvoie la configuration de cryptage par défaut pour le compartiment.
OPTIMISEZ le cycle de vie des compartiments (GetBucketLifecycleConfiguration)	Cette opération retourne la configuration du cycle de vie du godet. Voir "Création de la configuration du cycle de vie S3".
ACCÉDER à l'emplacement du compartiment	Cette opération renvoie la région définie à l'aide de `LocationConstraint` Élément dans la demande PUT Bucket. Si la région du godet est de `us-east-1`, une chaîne vide est renvoyée pour la région.
GET Bucket notification (GetBucketNotifationConfiguration)	Cette opération renvoie la configuration de notification attachée au compartiment.
GET Bucket policy	Cette opération renvoie la politique attachée au godet.
RÉPLICATION des compartiments	Cette opération renvoie la configuration de réplication attachée au compartiment.

Fonctionnement	Mise en place
GET Bucket tagging	Cette opération utilise le `tagging` sous-ressource pour renvoyer toutes les balises d'un compartiment.
GESTION des versions des compartiments	Cette implémentation utilise le `versioning` sous-ressource pour retourner l'état de gestion des versions d'un compartiment. • *Blank*: La gestion des versions n'a jamais été activée (le compartiment est « non versionné ») • Activé : la gestion des versions est activée • Suspendu : la gestion des versions a déjà été activée et est suspendue
OBTENIR la configuration de verrouillage d'objet	Cette opération renvoie le mode de rétention par défaut du compartiment et la période de conservation par défaut, si configuré. Voir "Utilisez l'API REST S3 pour configurer le verrouillage objet S3".
Godet DE TÊTE	Cette opération détermine si un compartiment existe et que vous êtes autorisé à y accéder. Cette opération renvoie : • `x-ntap-sg-bucket-id`: L'UUID du godet au format UUID. • `x-ntap-sg-trace-id`: ID de trace unique de la demande associée.

Fonctionnement	Mise en place
PLACER le godet	Cette opération crée un nouveau godet. C'est en créant le compartiment que vous devenez le propriétaire. • Les noms de compartiment doivent être conformes aux règles suivantes : ◦ Il doit être unique sur chaque système StorageGRID (et pas seulement au sein du compte du locataire). ◦ Doit être conforme DNS. ◦ Doit contenir au moins 3 caractères et pas plus de 63 caractères. ◦ Peut être une série d'une ou plusieurs étiquettes, avec des étiquettes adjacentes séparées par un point. Chaque étiquette doit commencer et se terminer par une lettre ou un chiffre en minuscules et ne peut utiliser que des lettres minuscules, des chiffres et des tirets. ◦ Ne doit pas ressembler à une adresse IP au format texte. ◦ Ne doit pas utiliser de périodes dans des demandes de type hébergement virtuel. Les périodes provoquera des problèmes avec la vérification du certificat générique du serveur. • Par défaut, les compartiments sont créés dans le `us-east-1` région ; cependant, vous pouvez utiliser le `LocationConstraint` élément de demande dans le corps de la demande pour spécifier une région différente. Lorsque vous utilisez le `LocationConstraint` Elément, vous devez spécifier le nom exact d'une région qui a été définie à l'aide du gestionnaire de grille ou de l'API de gestion de grille. Contactez votre administrateur système si vous ne connaissez pas le nom de région que vous devez utiliser. **Remarque** : une erreur se produit si votre demande PUT Bucket utilise une région qui n'a pas été définie dans StorageGRID. • Vous pouvez inclure le `x-amz-bucket-object-lock-enabled` Demander l'en-tête pour créer un compartiment avec le verrouillage objet S3 activé. Voir "Utilisez l'API REST S3 pour configurer le verrouillage objet S3". Vous devez activer le verrouillage d'objet S3 lors de la création du compartiment. Une fois un compartiment créé, vous ne pouvez ni ajouter ni désactiver le verrouillage objet S3. Le verrouillage objet S3 requiert la gestion des versions de compartiment, qui est activée automatiquement lors de la création du compartiment.
PLACEZ les godets	Cette opération définit la configuration du CORS pour un compartiment afin que le compartiment puisse traiter les demandes d'origine croisée. Le partage de ressources d'origine croisée (CORS) est un mécanisme de sécurité qui permet aux applications Web clientes d'un domaine d'accéder aux ressources d'un domaine différent. Supposons par exemple que vous utilisez un compartiment S3 nommé `images` pour stocker des graphiques. En définissant la configuration CORS pour le `images` le champ permet d'afficher les images de ce compartiment sur le site web `http://www.example.com`.

Fonctionnement	Mise en place
PUT Bucket Encryption	Cette opération définit l'état de cryptage par défaut d'un compartiment existant. Lorsque le chiffrement au niveau du compartiment est activé, tout nouvel objet ajouté au compartiment est chiffré.StorageGRID prend en charge le chiffrement côté serveur avec des clés gérées par StorageGRID. Lorsque vous spécifiez la règle de configuration de cryptage côté serveur, définissez l' `SSEAlgorithm` paramètre à `AES256`, et n'utilisez pas le `KMSMasterKeyID` paramètre. La configuration de cryptage par défaut du compartiment est ignorée si la demande de téléchargement d'objet spécifie déjà le cryptage (c'est-à-dire, si la demande inclut le `x-amz-server-side-encryption-*` en-tête de demande).
CYCLE de vie des compartiments (Configuration PutBucketLifecycleConfiguration)	Cette opération crée une nouvelle configuration de cycle de vie pour le compartiment ou remplace une configuration de cycle de vie existante. StorageGRID prend en charge jusqu'à 1,000 règles de cycle de vie dans une configuration cycle de vie. Chaque règle peut inclure les éléments XML suivants : • Expiration (jours, date) • NonactuelVersionExp (Nontactut Days) • Filtre (préfixe, étiquette) • État • ID StorageGRID ne prend pas en charge les actions suivantes : • AbortIncompleMultipartUpload • ExpiredObjectDeleteMarker • Transition Voir "Création de la configuration du cycle de vie S3". Pour comprendre comment l'action d'expiration d'un cycle de vie de compartiment interagit avec les instructions de placement ILM, reportez-vous à la section "Fonctionnement de ILM tout au long de la vie d'un objet". **Remarque** : la configuration du cycle de vie des compartiments peut être utilisée avec des compartiments avec le verrouillage d'objet S3 activé, mais la configuration du cycle de vie des compartiments n'est pas prise en charge pour les compartiments conformes hérités.

Fonctionnement	Mise en place

PUT Bucket notification
 	
(PutBucketNotifationConfiguration)
	Cette opération configure les notifications pour le compartiment à l'aide du XML de configuration de notification inclus dans le corps de la demande. Vous devez connaître les détails d'implémentation suivants :
	
	• StorageGRID prend en charge les rubriques SNS (simple notification Service) comme destinations. Les points finaux SQS (simple Queue Service) ou Lambda d'Amazon ne sont pas pris en charge.
	• La destination des notifications doit être spécifiée comme URN d'un terminal StorageGRID. Les terminaux peuvent être créés à l'aide du Gestionnaire de locataires ou de l'API de gestion des locataires.
	
	Le noeud final doit exister pour que la configuration des notifications réussisse. Si le noeud final n'existe pas, un `400 Bad Request` l'erreur est renvoyée avec le code `InvalidArgument`.
	
	• Vous ne pouvez pas configurer de notification pour les types d'événements suivants. Ces types d'événements sont **non** pris en charge.
	◦ `s3:ReducedRedundancyLostObject`
	◦ `s3:ObjectRestore:Completed`
	• Les notifications d'événements envoyées par StorageGRID utilisent le format JSON standard, sauf qu'elles n'incluent pas certaines clés et utilisent des valeurs spécifiques pour d'autres, comme illustré dans la liste suivante :
	◦ **EventSource**
	
	`sgws:s3`
	
	◦ **AwsRegion**
	
	non inclus
	
	◦ **x-amz-id-2**
	
	non inclus
	
	◦ **arn**
	
	`urn:sgws:s3:::bucket_name`

PUT Bucket policy	Cette opération définit la politique associée au compartiment.

Fonctionnement	Mise en place
RÉPLICATION des compartiments	Cette opération est configurée "Réplication StorageGRID CloudMirror" Pour le compartiment utilisant le XML de configuration de réplication fourni dans le corps de la requête. Pour la réplication CloudMirror, vous devez connaître les détails d'implémentation suivants : • StorageGRID ne prend en charge que le V1 de la configuration de la réplication. Cela signifie que StorageGRID ne prend pas en charge l'utilisation de `Filter` Elément pour les règles, et suit les conventions V1 pour la suppression des versions d'objet. Pour plus d'informations, reportez-vous à la "Documentation Amazon S3 sur la configuration de la réplication". • La réplication des compartiments peut être configurée sur les compartiments avec ou sans version. • Vous pouvez spécifier un compartiment de destination différent dans chaque règle du XML de configuration de réplication. Un compartiment source peut être répliqué sur plusieurs compartiments de destination. • Les compartiments de destination doivent être spécifiés en tant que URN des terminaux StorageGRID, tel que spécifié dans le Gestionnaire de locataires ou l'API de gestion des locataires. Voir "Configurez la réplication CloudMirror". Le noeud final doit exister pour que la configuration de réplication réussisse. Si le noeud final n'existe pas, la demande échoue en tant que `400 Bad Request`. Le message d'erreur indique : `Unable to save the replication policy. The specified endpoint URN does not exist: URN`. • Vous n'avez pas besoin de spécifier un `Role` Dans le XML de configuration. Cette valeur n'est pas utilisée par StorageGRID et sera ignorée si elle a été soumise. • Si vous omettez la classe de stockage du XML de configuration, StorageGRID utilise le `STANDARD` classe de stockage par défaut. • Si vous supprimez un objet du compartiment source ou que vous supprimez le compartiment source lui-même, le comportement de réplication inter-région est le suivant : ◦ Si vous supprimez l'objet ou le compartiment avant sa réplication, l'objet/le compartiment n'est pas répliqué et vous n'êtes pas averti. ◦ Si vous supprimez l'objet ou le compartiment après sa réplication, StorageGRID suit le comportement de suppression Amazon S3 standard pour la version V1 de la réplication multi-région.

Fonctionnement	Mise en place
PUT Bucket tagging	Cette opération utilise le `tagging` sous-ressource pour ajouter ou mettre à jour un ensemble de balises pour un compartiment. Lors de l'ajout de balises de compartiment, tenez compte des limites suivantes : • StorageGRID et Amazon S3 prennent en charge jusqu'à 50 balises pour chaque compartiment. • Les étiquettes associées à un compartiment doivent avoir des clés d'étiquette uniques. Une clé de balise peut comporter jusqu'à 128 caractères Unicode. • Les valeurs de balise peuvent comporter jusqu'à 256 caractères Unicode. • Les clés et les valeurs sont sensibles à la casse
GESTION des versions du compartiment	Cette implémentation utilise le `versioning` sous-ressource pour définir l'état de gestion des versions d'un compartiment existant. Vous pouvez définir l'état de la gestion des versions à l'aide de l'une des valeurs suivantes : • Activé : permet la gestion des versions des objets dans le compartiment. Tous les objets ajoutés au compartiment reçoivent un ID de version unique. • Suspendu : désactive la gestion des versions des objets dans le compartiment. Tous les objets ajoutés au compartiment reçoivent l'ID de version `null`.
CONFIGURATION du verrouillage de l'objet	Cette opération configure ou supprime le mode de conservation par défaut du compartiment et la période de conservation par défaut. Si la période de conservation par défaut est modifiée, la conservation jusqu'à la date des versions d'objet existantes reste la même et n'est pas recalculée en utilisant la nouvelle période de conservation par défaut. Voir "Utilisez l'API REST S3 pour configurer le verrouillage objet S3" pour des informations détaillées.

Informations associées

"Contrôles de cohérence"

"HEURE du dernier accès au compartiment"

"Utilisez les règles d'accès au compartiment et au groupe"

"Opérations S3 suivies dans les journaux d'audit"

Opérations personnalisées dans les compartiments

Le système StorageGRID prend en charge les opérations de compartiment personnalisées, ajoutées à l'API REST S3 et propres au système.

Le tableau suivant répertorie les opérations de compartiment personnalisées prises en charge par StorageGRID.

Fonctionnement	Description	Pour en savoir plus
OPTIMISEZ la cohérence des compartiments	Renvoie le niveau de cohérence appliqué à un compartiment spécifique.	"OPTIMISEZ la cohérence des compartiments"
PRÉSERVER la cohérence du godet	Définit le niveau de cohérence appliqué à un compartiment spécifique.	"PRÉSERVER la cohérence du godet"
HEURE du dernier accès au compartiment	Indique si les mises à jour de l'heure du dernier accès sont activées ou désactivées pour un compartiment spécifique.	"HEURE du dernier accès au compartiment"
METTRE l'heure du dernier accès au compartiment	Permet d'activer ou de désactiver les mises à jour de l'heure du dernier accès pour un compartiment spécifique.	"METTRE l'heure du dernier accès au compartiment"
SUPPRIMEZ la configuration de notification des métadonnées de compartiment	Supprime le XML de configuration de notification de métadonnées associé à un compartiment spécifique.	"SUPPRIMEZ la configuration de notification des métadonnées de compartiment"
CONFIGURATION DES notifications de métadonnées de compartiment	Renvoie le XML de configuration de notification de métadonnées associé à un compartiment spécifique.	"CONFIGURATION DES notifications de métadonnées de compartiment"
CONFIGURATION de notification des métadonnées de compartiment	Configure le service de notification des métadonnées pour un compartiment.	"CONFIGURATION de notification des métadonnées de compartiment"
PUT Bucket with Compliance settings	Obsolète et non pris en charge : vous ne pouvez plus créer de compartiments avec conformité activée.	"Obsolète : METTEZ le compartiment avec les paramètres de conformité"
ASSUREZ la conformité aux compartiments	Obsolète mais pris en charge : renvoie les paramètres de conformité actuellement en vigueur pour un compartiment compatible existant.	"Obsolète : CONFORMITÉ DES compartiments"
METTEZ le godet en conformité	Obsolète mais pris en charge : permet de modifier les paramètres de conformité d'un compartiment compatible existant.	"Obsolète : conformité DES compartiments PUT"

Informations associées

"Opérations S3 suivies dans les journaux d'audit"

Opérations sur les objets

Cette section décrit la manière dont le système StorageGRID implémente les opérations de l'API REST S3 pour les objets.

Les conditions suivantes s'appliquent à toutes les opérations d'objet :

- StorageGRID "contrôles de cohérence" sont prises en charge par toutes les opérations sur les objets, à l'exception de ce qui suit :
  - OBTENIR l'ACL d'objet
  - `OPTIONS /`
  - METTRE l'objet en attente légale
  - CONSERVATION des objets
  - SÉLECTIONNEZ contenu de l'objet
- Les demandes contradictoires des clients, telles que deux clients qui écrivent sur la même clé, sont résolues sur une base de « derniers-victoires ». Le calendrier de l'évaluation « derniers-victoires » est basé sur le moment où le système StorageGRID remplit une demande donnée et non sur le moment où les clients S3 commencent une opération.
- Tous les objets d'un compartiment StorageGRID sont détenus par le propriétaire du compartiment, y compris les objets créés par un utilisateur anonyme ou par un autre compte.
- Les objets de données ingérés dans le système StorageGRID via Swift ne sont pas accessibles via S3.

Le tableau ci-dessous décrit la manière dont StorageGRID implémente les opérations sur les objets de l'API REST S3.

Fonctionnement	Mise en place
SUPPRIMER l'objet	Authentification multifacteur (MFA) et en-tête de réponse `x-amz-mfa` ne sont pas pris en charge. Lors du traitement d'une requête DE SUPPRESSION d'objet, StorageGRID tente de supprimer immédiatement toutes les copies de l'objet des emplacements stockés. En cas de succès, StorageGRID renvoie immédiatement une réponse au client. Si toutes les copies ne peuvent pas être supprimées dans les 30 secondes (par exemple, parce qu'un emplacement est temporairement indisponible), StorageGRID met les copies en file d'attente pour suppression et indique que le client a réussi. **Gestion des versions** Pour supprimer une version spécifique, le demandeur doit être le propriétaire du compartiment et utiliser le `versionId` sous-ressource. L'utilisation de cette sous-ressource supprime définitivement la version. Si le `versionId` correspond à un marqueur de suppression, l'en-tête de réponse `x-amz-delete-marker` est renvoyé à `true`. • Si un objet est supprimé sans l' `versionId` sous-ressource sur un compartiment activé pour la version, il génère un marqueur de suppression. Le `versionId` pour le marqueur de suppression, est renvoyé à l'aide du `x-amz-version-id` en-tête de réponse, et le `x-amz-delete-marker` l'en-tête de réponse est renvoyé à `true`. • Si un objet est supprimé sans l' `versionId` sous-ressource sur un compartiment suspendu de version, elle entraîne la suppression permanente d'une version existante 'null' ou d'un marqueur de suppression 'null' et la génération d'un nouveau marqueur de suppression 'null'. Le `x-amz-delete-marker` l'en-tête de réponse est renvoyé à `true`. **Remarque** : dans certains cas, plusieurs marqueurs de suppression peuvent exister pour un objet. Voir "Utilisez l'API REST S3 pour configurer le verrouillage objet S3" Pour apprendre à supprimer des versions d'objets en mode GOUVERNANCE.
SUPPRIMER plusieurs objets (DeleteObjects)	Authentification multifacteur (MFA) et en-tête de réponse `x-amz-mfa` ne sont pas pris en charge. Plusieurs objets peuvent être supprimés dans le même message de demande. Voir "Utilisez l'API REST S3 pour configurer le verrouillage objet S3" Pour apprendre à supprimer des versions d'objets en mode GOUVERNANCE.

Fonctionnement	Mise en place
SUPPRIMER le balisage d'objets	Utilise le `tagging` sous-ressource pour supprimer toutes les balises d'un objet. **Gestion des versions** Si le `versionId` le paramètre query n'est pas spécifié dans la demande. l'opération supprime toutes les balises de la version la plus récente de l'objet dans un compartiment versionné. Si la version actuelle de l'objet est un marqueur de suppression, un état "methodNotAldue" est renvoyé avec l' `x-amz-delete-marker` réponse en-tête réglée sur `true`.
OBTENIR l'objet	"OBTENIR l'objet"
OBTENIR l'ACL d'objet	Si les informations d'identification d'accès nécessaires sont fournies pour le compte, l'opération renvoie une réponse positive ainsi que l'ID, le DisplayName et l'autorisation du propriétaire de l'objet, ce qui indique que le propriétaire dispose d'un accès complet à l'objet.
OBTENIR la mise en attente légale de l'objet	"Utilisez l'API REST S3 pour configurer le verrouillage objet S3"
OBTENIR la conservation des objets	"Utilisez l'API REST S3 pour configurer le verrouillage objet S3"
OBTENIR le balisage d'objets	Utilise le `tagging` sous-ressource pour renvoyer toutes les balises d'un objet. **Gestion des versions** Si le `versionId` le paramètre query n'est pas spécifié dans la demande, l'opération renvoie toutes les balises de la version la plus récente de l'objet dans un compartiment versionné. Si la version actuelle de l'objet est un marqueur de suppression, un état "methodNotAldue" est renvoyé avec l' `x-amz-delete-marker` réponse en-tête réglée sur `true`.
Objet TÊTE	"Objet TÊTE"
Restauration POST-objet	"Restauration POST-objet"
PLACER l'objet	"PLACER l'objet"
PLACER l'objet - Copier	"PLACER l'objet - Copier"
METTRE l'objet en attente légale	"Utilisez l'API REST S3 pour configurer le verrouillage objet S3"
CONSERVATION des objets	"Utilisez l'API REST S3 pour configurer le verrouillage objet S3"

Fonctionnement	Mise en place
PUT Object tagging	Utilise le `tagging` sous-ressource pour ajouter un ensemble de balises à un objet existant. **Limites des balises d'objet** Vous pouvez ajouter des balises à de nouveaux objets lorsque vous les téléchargez ou les ajouter à des objets existants. StorageGRID et Amazon S3 prennent en charge jusqu'à 10 balises pour chaque objet. Les balises associées à un objet doivent avoir des clés de balise uniques. Une clé de balise peut comporter jusqu'à 128 caractères Unicode et les valeurs de balise peuvent comporter jusqu'à 256 caractères Unicode. Les clés et les valeurs sont sensibles à la casse **Mises à jour des balises et comportement d'ingestion** Lorsque vous utilisez PUT Object tagging pour mettre à jour les balises d'un objet, StorageGRID ne réingérer pas l'objet. Cela signifie que l'option de comportement d'ingestion spécifiée dans la règle ILM correspondante n'est pas utilisée. Tout changement au placement d'objet déclenché par la mise à jour est apporté lors de l'évaluation de ILM par des processus ILM en arrière-plan normaux. En d'autres termes, si la règle ILM utilise l'option strict pour le comportement d'ingestion, aucune action n'est entreprise si les placements d'objet requis ne peuvent pas être effectués (par exemple, parce qu'un nouvel emplacement n'est pas disponible). L'objet mis à jour conserve son emplacement actuel jusqu'à ce que le placement requis soit possible. **Résolution des conflits** Les demandes contradictoires des clients, telles que deux clients qui écrivent sur la même clé, sont résolues sur la base des « derniers-victoires ». Le calendrier de l'évaluation « derniers-victoires » est basé sur le moment où le système StorageGRID remplit une demande donnée et non sur le moment où les clients S3 commencent une opération. **Gestion des versions** Si le `versionId` le paramètre de requête n'est pas spécifié dans la requête, l'opération ajoute des balises à la version la plus récente de l'objet dans un compartiment versionné. Si la version actuelle de l'objet est un marqueur de suppression, un état "methodNotAldue" est renvoyé avec l' `x-amz-delete-marker` réponse en-tête réglée sur `true`.
SelectObjectContent	"SelectObjectContent"

Informations associées

"Opérations S3 suivies dans les journaux d'audit"

StorageGRID prend en charge les clauses, types de données et opérateurs Amazon S3 Select suivants pour le "Commande SelectObjectContent".

Les éléments non répertoriés ne sont pas pris en charge.

Pour la syntaxe, voir "SelectObjectContent". Pour plus d'informations sur S3 Select, consultez le "Documentation AWS pour S3 Select".

Seuls les comptes de tenant dont S3 Select est activé peuvent émettre des requêtes SelectObjectContent. Voir la "Considérations et configuration requise pour l'utilisation de S3 Select".

Clauses

- SÉLECTIONNER la liste
- Clause FROM
- Clause WHERE
- Clause DE LIMITE

Types de données

- bool
- entier
- chaîne
- flottement
- décimale, numérique
- horodatage

Opérateurs

Opérateurs logiques

- ET
- PAS
- OU

Opérateurs de comparaison

- <
- >
- &lt ;=
- >=
- =
- =
- <>

- !=
- ENTRE
- DANS

Opérateurs de correspondance de répétition

- COMME
- _
- %

Opérateurs unitaires

- EST NULL
- N'EST PAS NULL

Opérateurs mathématiques

- +
- -
- *
- /
- %

StorageGRID suit la priorité de l'opérateur Amazon S3 Select.

Fonctions d'agrégation

- MOY()
- NOMBRE(*)
- MAX()
- MIN()
- SOMME()

Fonctions conditionnelles

- CASSE
- FUSIONNE
- NULLIF

Fonctions de conversion

- CAST (pour les types de données pris en charge)

Fonctions de date

- DATE_AJOUTER
- DATE_DIFF

- EXTRAIRE
- TO_STRING
- TO_TIMESTAMP
- CODE D'ARTICLE

Fonctions de chaîne

- CHAR_LENGTH, CARACTÈRE_LENGTH
- ABAISSEMENT
- SOUS-CHAÎNE
- GARNITURE
- SUPÉRIEUR

Utilisez le cryptage côté serveur

Le chiffrement côté serveur vous permet de protéger vos données au repos objet. StorageGRID crypte les données lors de leur écriture et décrypte les données lorsque vous accédez à l'objet.

Si vous souhaitez utiliser le chiffrement côté serveur, vous pouvez choisir l'une des deux options mutuellement exclusives, en fonction de la gestion des clés de cryptage :

- **SSE (chiffrement côté serveur avec clés gérées par StorageGRID)** : lorsque vous émettez une demande S3 pour stocker un objet, StorageGRID crypte l'objet avec une clé unique. Lorsque vous émettez une requête S3 pour récupérer l'objet, StorageGRID utilise la clé stockée pour décrypter l'objet.
- **SSE-C (chiffrement côté serveur avec clés fournies par le client)** : lorsque vous émettez une demande S3 pour stocker un objet, vous fournissez votre propre clé de chiffrement. Lorsque vous récupérez un objet, vous fournissez la même clé de chiffrement dans le cadre de votre demande. Si les deux clés de chiffrement correspondent, l'objet est décrypté et vos données d'objet sont renvoyées.

  StorageGRID gère toutes les opérations de cryptage et de décryptage des objets, mais vous devez gérer les clés de cryptage que vous fournissez.

> Les clés de chiffrement que vous fournissez ne sont jamais stockées. Si vous perdez une clé de chiffrement, vous perdez l'objet correspondant.

> Si un objet est chiffré avec SSE ou SSE-C, tous les paramètres de chiffrement au niveau du godet ou de la grille sont ignorés.

Utiliser SSE

Pour chiffrer un objet avec une clé unique gérée par StorageGRID, utilisez l'en-tête de demande suivant :

```
x-amz-server-side-encryption
```

L'en-tête de demande SSE est pris en charge par les opérations d'objet suivantes :

- "PLACER l'objet"

- "PLACER l'objet - Copier"
- "Lancer le téléchargement de pièces multiples"

Utiliser SSE-C

Pour crypter un objet avec une clé unique que vous gérez, vous utilisez trois en-têtes de requête :

En-tête de demande	Description
`x-amz-server-side-encryption-customer-algorithm`	Spécifiez l'algorithme de cryptage. La valeur de la barre de coupe doit être de `AES256`.
`x-amz-server-side-encryption-customer-key`	Spécifiez la clé de cryptage qui sera utilisée pour crypter ou décrypter l'objet. La valeur de la clé doit être codée en 256 bits, en base64.
`x-amz-server-side-encryption-customer-key-MD5`	Spécifiez le résumé MD5 de la clé de chiffrement selon la RFC 1321, qui est utilisé pour garantir que la clé de chiffrement a été transmise sans erreur. La valeur du résumé MD5 doit être codée en base64 à 128 bits.

Les en-têtes de demande SSE-C sont pris en charge par les opérations objet suivantes :

- "OBTENIR l'objet"
- "Objet TÊTE"
- "PLACER l'objet"
- "PLACER l'objet - Copier"
- "Lancer le téléchargement de pièces multiples"
- "Télécharger la pièce"
- "Télécharger la pièce - Copier"

Considérations relatives au chiffrement côté serveur avec clés fournies par le client (SSE-C)

Avant d'utiliser SSE-C, tenez compte des points suivants :

- Vous devez utiliser https.

> StorageGRID rejette toute demande effectuée sur http en utilisant SSE-C. Pour des considérations de sécurité, vous devez envisager toute clé que vous envoyez accidentellement en utilisant http pour être compromise. Mettez la clé au rebut et tournez-la selon les besoins.

- L'ETag dans la réponse n'est pas le MD5 des données objet.
- Vous devez gérer le mappage des clés de chiffrement aux objets. StorageGRID ne stocke pas de clés de chiffrement. Vous êtes responsable du suivi de la clé de chiffrement que vous fournissez pour chaque objet.
- Si le contrôle de version du compartiment est activé, chaque version d'objet doit disposer de sa propre clé de chiffrement. Vous êtes responsable du suivi de la clé de chiffrement utilisée pour chaque version d'objet.

- Comme vous gérez les clés de chiffrement côté client, vous devez également gérer d'autres dispositifs de protection, tels que la rotation des clés, côté client.

> Les clés de chiffrement que vous fournissez ne sont jamais stockées. Si vous perdez une clé de chiffrement, vous perdez l'objet correspondant.

- Si la réplication inter-grid ou CloudMirror est configurée pour le compartiment, vous ne pouvez pas acquérir d'objets SSE-C. L'opération d'acquisition échoue.

Informations associées

"Guide pour les développeurs Amazon S3 : protection des données à l'aide du chiffrement côté serveur avec clés de chiffrement fournies par le client (SSE-C)"

OBTENIR l'objet

Vous pouvez utiliser la requête D'objet GET S3 pour récupérer un objet à partir d'un compartiment S3.

OBTENIR un objet et des objets partitionnés

Vous pouvez utiliser le `partNumber` paramètre de demande pour récupérer une partie spécifique d'un objet partitionné ou segmenté. Le `x-amz-mp-parts-count` l'élément de réponse indique le nombre de pièces dont dispose l'objet.

Vous pouvez définir `partNumber` à 1 pour les objets segmentés/multisegments et les objets non segmentés/non-partitionnés ; cependant, le `x-amz-mp-parts-count` l'élément de réponse n'est renvoyé que pour les objets segmentés ou partitionnés.

Caractères UTF-8 dans les métadonnées utilisateur

StorageGRID n'analyse ni n'interprète pas les caractères UTF-8 qui se sont échappés dans les métadonnées définies par l'utilisateur. LES requêtes GET pour un objet avec des caractères UTF-8 échappés dans les métadonnées définies par l'utilisateur ne renvoient pas le `x-amz-missing-meta` en-tête si le nom ou la valeur de la clé comporte des caractères non imprimables.

En-tête de demande non pris en charge

L'en-tête de demande suivant n'est pas pris en charge et renvoie `XNotImplemented`:

- `x-amz-website-redirect-location`

Gestion des versions

Si un `versionId` la sous-ressource n'est pas spécifiée, l'opération extrait la version la plus récente de l'objet dans un compartiment multiversion. Si la version actuelle de l'objet est un marqueur de suppression, un état « non trouvé » est renvoyé avec le `x-amz-delete-marker` réponse en-tête réglée sur `true`.

En-têtes de demande pour chiffrement côté serveur avec clés de chiffrement fournies par le client (SSE-C)

Utilisez les trois en-têtes si l'objet est chiffré avec une clé unique que vous avez fournie.

- `x-amz-server-side-encryption-customer-algorithm`: Spécifiez `AES256`.
- `x-amz-server-side-encryption-customer-key`: Spécifiez votre clé de cryptage pour l'objet.
- `x-amz-server-side-encryption-customer-key-MD5`: Spécifiez le résumé MD5 de la clé de chiffrement de l'objet.

> Les clés de chiffrement que vous fournissez ne sont jamais stockées. Si vous perdez une clé de chiffrement, vous perdez l'objet correspondant. Avant d'utiliser des clés fournies par le client pour sécuriser les données d'objet, consultez les points à prendre en compte dans la section "Utilisez le cryptage côté serveur".

Comportement de L'objet GET pour les objets de pool de stockage cloud

Si un objet a été stocké dans un "Pool de stockage cloud", Le comportement d'une requête GET Object dépend de l'état de l'objet. Voir "Objet TÊTE" pour en savoir plus.

> Si un objet est stocké dans un pool de stockage cloud et qu'une ou plusieurs copies de cet objet existent également dans la grille, L'OBTENTION des demandes d'objet tente d'extraire les données de la grille avant de les récupérer depuis le pool de stockage cloud.

État de l'objet	Comportement de L'objet GET
Les objets sont ingéré dans StorageGRID mais pas encore évalués par ILM, ou objet stocké dans un pool de stockage traditionnel ou au moyen d'un code d'effacement	`200 OK` Une copie de l'objet est récupérée.
Objet dans Cloud Storage Pool, mais pas encore migré vers un état non récupérable	`200 OK` Une copie de l'objet est récupérée.
L'objet a été transféré à un état non récupérable	`403 Forbidden`, `InvalidObjectState` Utiliser un "Restauration POST-objet" demande de restauration de l'objet à un état récupérable.
Objet en cours de restauration à partir d'un état non récupérable	`403 Forbidden`, `InvalidObjectState` Attendez que la demande DE restauration POST Object soit terminée.
Objet entièrement restauré dans le pool de stockage cloud	`200 OK` Une copie de l'objet est récupérée.

Objets partitionnés ou segmentés dans un pool de stockage cloud

Si vous avez téléchargé un objet partitionné ou si StorageGRID le divise en segments, StorageGRID détermine si l'objet est disponible dans le pool de stockage cloud en échantillonant un sous-ensemble de parties ou de segments de l'objet. Dans certains cas, une demande GET Object peut retourner de manière

incorrecte `200 OK` lorsque certaines parties de l'objet ont déjà été migrées à un état non récupérable ou lorsque certaines parties de l'objet n'ont pas encore été restaurées.

Dans ces cas :

- La demande GET Object peut renvoyer certaines données mais s'arrête à mi-chemin du transfert.
- Une requête GET Object suivante peut revenir `403 Forbidden`.

OBTENEZ la réplication objet et inter-grid

Si vous utilisez "fédération des grilles" et "réplication entre plusieurs grilles" Est activé pour un compartiment. Le client S3 peut vérifier l'état de réplication d'un objet en envoyant une requête GET Object. La réponse inclut la réponse spécifique à StorageGRID `x-ntap-sg-cgr-replication-status` en-tête de réponse, qui aura l'une des valeurs suivantes :

Grille	État de la réplication
Source	• **SUCCÈS** : la réplication a réussi. • **EN ATTENTE** : l'objet n'a pas encore été répliqué. • **ÉCHEC** : la réplication a échoué avec une défaillance permanente. L'utilisateur doit résoudre l'erreur.
Destination	**RÉPLIQUE** : l'objet a été répliqué à partir de la grille source.

> StorageGRID ne prend pas en charge le `x-amz-replication-status` en-tête.

Informations associées

"Opérations S3 suivies dans les journaux d'audit"

Objet TÊTE

Vous pouvez utiliser la requête d'objet TÊTE S3 pour extraire les métadonnées à partir d'un objet sans y retourner. Si l'objet est stocké dans un pool de stockage cloud, vous pouvez utiliser HEAD Object pour déterminer l'état de transition de l'objet.

Objet TÊTE et objets multipart

Vous pouvez utiliser le `partNumber` paramètre de demande pour récupérer les métadonnées d'une partie spécifique d'un objet partitionné ou segmenté. Le `x-amz-mp-parts-count` l'élément de réponse indique le nombre de pièces dont dispose l'objet.

Vous pouvez définir `partNumber` à 1 pour les objets segmentés/multisegments et les objets non segmentés/non-partitionnés ; cependant, le `x-amz-mp-parts-count` l'élément de réponse n'est renvoyé que pour les objets segmentés ou partitionnés.

Caractères UTF-8 dans les métadonnées utilisateur

StorageGRID n'analyse ni n'interprète pas les caractères UTF-8 qui se sont échappés dans les métadonnées définies par l'utilisateur. Les demandes HEAD pour un objet avec des caractères UTF-8 échappés dans les métadonnées définies par l'utilisateur ne renvoient pas le `x-amz-missing-meta` en-tête si le nom ou la

valeur de la clé comporte des caractères non imprimables.

En-tête de demande non pris en charge

L'en-tête de demande suivant n'est pas pris en charge et renvoie `XNotImplemented`:

- `x-amz-website-redirect-location`

Gestion des versions

Si un `versionId` la sous-ressource n'est pas spécifiée, l'opération extrait la version la plus récente de l'objet dans un compartiment multiversion. Si la version actuelle de l'objet est un marqueur de suppression, un état « non trouvé » est renvoyé avec le `x-amz-delete-marker` réponse en-tête réglée sur `true`.

En-têtes de demande pour chiffrement côté serveur avec clés de chiffrement fournies par le client (SSE-C)

Utilisez les trois en-têtes si l'objet est chiffré avec une clé unique que vous avez fournie.

- `x-amz-server-side-encryption-customer-algorithm`: Spécifiez `AES256`.
- `x-amz-server-side-encryption-customer-key`: Spécifiez votre clé de cryptage pour l'objet.
- `x-amz-server-side-encryption-customer-key-MD5`: Spécifiez le résumé MD5 de la clé de chiffrement de l'objet.

> Les clés de chiffrement que vous fournissez ne sont jamais stockées. Si vous perdez une clé de chiffrement, vous perdez l'objet correspondant. Avant d'utiliser des clés fournies par le client pour sécuriser les données d'objet, consultez les points à prendre en compte dans la section "Utilisez le cryptage côté serveur".

Réponses D'objet PRINCIPAL pour les objets de pool de stockage cloud

Si l'objet est stocké dans un "Pool de stockage cloud", les en-têtes de réponse suivants sont renvoyés :

- `x-amz-storage-class: GLACIER`
- `x-amz-restore`

Les en-têtes de réponse fournissent des informations sur l'état d'un objet lors de son déplacement vers Cloud Storage Pool, qui peut être migré vers un état non récupérable et restauré.

État de l'objet	Réponse à l'objet TÊTE
Les objets sont ingéré dans StorageGRID mais pas encore évalués par ILM, ou objet stocké dans un pool de stockage traditionnel ou au moyen d'un code d'effacement	`200 OK` (Aucun en-tête à réponse spéciale n'est renvoyé.)

État de l'objet	Réponse à l'objet TÊTE

Objet dans Cloud Storage Pool, mais pas encore migré vers un état non récupérable	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"`
	
	Jusqu'à ce que l'objet soit transféré à un état non récupérable, la valeur de `expiry-date` est sur le point de passer un moment lointain dans le futur. L'heure exacte de la transition n'est pas contrôlée par le système StorageGRID.

L'objet est passé à l'état non récupérable, mais il existe au moins une copie sur la grille	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"`
	
	La valeur pour `expiry-date` est sur le point de passer un moment lointain dans le futur.
	
	Remarque : si la copie sur la grille n'est pas disponible (par exemple, un nœud de stockage est en panne), vous devez émettre un "Restauration POST-objet" Demande de restauration de la copie à partir du pool de stockage cloud avant que vous puissiez récupérer l'objet.

L'objet a été transféré à un état non récupérable et aucune copie n'existe sur la grille	`200 OK`
	
	`x-amz-storage-class: GLACIER`

Objet en cours de restauration à partir d'un état non récupérable	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="true"`

État de l'objet	Réponse à l'objet TÊTE

Objet entièrement restauré dans le pool de stockage cloud	`200 OK`
	
	`x-amz-storage-class: GLACIER`
	
	`x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2018 00:00:00 GMT"`
	
	Le `expiry-date` Indique quand l'objet du pool de stockage cloud sera renvoyé à un état non récupérable.

Objets partitionnés ou segmentés dans Cloud Storage Pool

Si vous avez téléchargé un objet partitionné ou si StorageGRID le divise en segments, StorageGRID détermine si l'objet est disponible dans le pool de stockage cloud en échantillonant un sous-ensemble de parties ou de segments de l'objet. Dans certains cas, une requête d'objet DE TÊTE peut revenir de manière incorrecte `x-amz-restore: ongoing-request="false"` lorsque certaines parties de l'objet ont déjà été migrées à un état non récupérable ou lorsque certaines parties de l'objet n'ont pas encore été restaurées.

HEAD réplication d'objets et de cross-grid

Si vous utilisez "fédération des grilles" et "réplication entre plusieurs grilles" Est activé pour un compartiment, le client S3 peut vérifier l'état de réplication d'un objet en émettant une requête d'objet PRINCIPAL. La réponse inclut la réponse spécifique à StorageGRID `x-ntap-sg-cgr-replication-status` en-tête de réponse, qui aura l'une des valeurs suivantes :

Grille	État de la réplication
Source	• **SUCCÈS** : la réplication a réussi. • **EN ATTENTE** : l'objet n'a pas encore été répliqué. • **ÉCHEC** : la réplication a échoué avec une défaillance permanente. L'utilisateur doit résoudre l'erreur.
Destination	**RÉPLIQUE** : l'objet a été répliqué à partir de la grille source.

> StorageGRID ne prend pas en charge le `x-amz-replication-status` en-tête.

Informations associées

"Opérations S3 suivies dans les journaux d'audit"

Restauration POST-objet

Vous pouvez utiliser la demande de restauration POST-objet S3 pour restaurer un objet stocké dans un pool de stockage cloud.

Type de demande pris en charge

StorageGRID ne prend en charge que les demandes DE restauration POST-objet pour restaurer un objet. Elle ne prend pas en charge le `SELECT` type de restauration. Sélectionnez demandes de retour `XNotImplemented`.

Gestion des versions

Spécifiez éventuellement `versionId` pour restaurer une version spécifique d'un objet dans un compartiment multiversion. Si vous ne spécifiez pas `versionId`, la version la plus récente de l'objet est restaurée

Comportement de restauration POST-objet sur les objets de pool de stockage cloud

Si un objet a été stocké dans un pool de stockage cloud (voir les instructions de gestion des objets avec gestion du cycle de vie des informations), une demande de restauration POST-objet présente le comportement suivant, en fonction de l'état de l'objet. Voir « objet TÊTE » pour plus de détails.

> Si un objet est stocké dans un pool de stockage cloud et qu'une ou plusieurs copies de cet objet existent également dans la grille, il n'est pas nécessaire de le restaurer en émettant une demande de restauration POST-objet. En revanche, la copie locale peut être récupérée directement à l'aide d'une demande D'OBJET GET.

État de l'objet	Comportement de la restauration POST-objet
L'objet est ingéré dans StorageGRID mais pas encore évalué par ILM ou l'objet ne se trouve pas dans un pool de stockage cloud	`403 Forbidden`, `InvalidObjectState`
Objet dans Cloud Storage Pool, mais pas encore migré vers un état non récupérable	`200 OK` Aucune modification n'est apportée. **Remarque** : avant qu'un objet ne soit transféré à un état non récupérable, vous ne pouvez pas le modifier `expiry-date`.
L'objet a été transféré à un état non récupérable	`202 Accepted` Restaure une copie récupérable de l'objet vers le pool de stockage cloud pendant le nombre de jours spécifié dans le corps de la demande. À la fin de cette période, l'objet est renvoyé à un état non récupérable. Si vous le souhaitez, utilisez le `Tier` élément de demande pour déterminer la durée de la tâche de restauration (`Expedited`, `Standard`, ou `Bulk`). Si vous ne spécifiez pas `Tier`, le `Standard` le niveau est utilisé. **Important** : si un objet a été transféré vers S3 Glacier Deep Archive ou si le pool de stockage cloud utilise le stockage Azure Blob, vous ne pouvez pas le restaurer à l'aide du `Expedited` niveau. L'erreur suivante est renvoyée `403 Forbidden`, `InvalidTier`: `Retrieval option is not supported by this storage class`.

État de l'objet	Comportement de la restauration POST-objet
Objet en cours de restauration à partir d'un état non récupérable	`409 Conflict`, `RestoreAlreadyInProgress`
Objet entièrement restauré dans le pool de stockage cloud	`200 OK` **Remarque :** si un objet a été restauré à un état récupérable, vous pouvez le modifier `expiry-date` En réémettant la demande DE restauration POST Object avec une nouvelle valeur pour `Days`. La date de restauration est mise à jour par rapport à l'heure de la demande.

Informations associées

"Gestion des objets avec ILM"

"Objet TÊTE"

"Opérations S3 suivies dans les journaux d'audit"

PLACER l'objet

Vous pouvez utiliser la demande S3 PUT Object pour ajouter un objet à un compartiment.

Résoudre les conflits

Les demandes contradictoires des clients, telles que deux clients qui écrivent sur la même clé, sont résolues sur une base de « derniers-victoires ». La chronologie de l'évaluation « derniers-victoires » repose sur la date à laquelle le système StorageGRID termine une demande donnée et non sur la date à laquelle les clients S3 commencent une opération.

Taille de l'objet

La taille maximale *recommandée* pour une opération d'objet PUT unique est de 5 Gio (5,368,709,120 octets). Si vos objets sont supérieurs à 5 Gio, utilisez le téléchargement partitionné.

La taille *supportée* maximale pour une opération objet PUT unique est de 5 Tio (5,497,558,138,880 octets). Cependant, l'alerte **S3 PUT Object size trop importante** est déclenchée si vous tentez de télécharger un objet supérieur à 5 Gio.

Taille des métadonnées utilisateur

Amazon S3 limite la taille des métadonnées définies par l'utilisateur au sein de chaque en-tête de requête À 2 Ko. StorageGRID limite les métadonnées utilisateur à 24 Kio. La taille des métadonnées définies par l'utilisateur est mesurée en prenant la somme du nombre d'octets dans le codage UTF-8 de chaque clé et valeur.

Caractères UTF-8 dans les métadonnées utilisateur

Si une requête inclut (non échappé) les valeurs UTF-8 dans le nom de clé ou la valeur des métadonnées définies par l'utilisateur, le comportement StorageGRID n'est pas défini.

StorageGRID n'analyse ni n'interprète pas les caractères UTF-8 qui se sont échappé dans le nom de clé ou la valeur des métadonnées définies par l'utilisateur. Les caractères UTF-8 échappés sont traités comme des

caractères ASCII :

- LES demandes PUT, PUT Object-Copy, GET et HEAD sont satisfaites si les métadonnées définies par l'utilisateur incluent des caractères UTF-8 échappés.
- StorageGRID ne renvoie pas le `x-amz-missing-meta` en-tête si la valeur interprétée du nom ou de la valeur de la clé comprend des caractères non imprimables.

Limites des balises d'objet

Vous pouvez ajouter des balises à de nouveaux objets lorsque vous les téléchargez ou les ajouter à des objets existants. StorageGRID et Amazon S3 prennent en charge jusqu'à 10 balises pour chaque objet. Les balises associées à un objet doivent avoir des clés de balise uniques. Une clé de balise peut comporter jusqu'à 128 caractères Unicode et les valeurs de balise peuvent comporter jusqu'à 256 caractères Unicode. Les clés et les valeurs sont sensibles à la casse

Propriété de l'objet

Dans StorageGRID, tous les objets sont détenus par le compte du propriétaire de compartiment, y compris les objets créés par un compte autre que le propriétaire ou un utilisateur anonyme.

En-têtes de demande pris en charge

Les en-têtes de requête suivants sont pris en charge :

- `Cache-Control`
- `Content-Disposition`
- `Content-Encoding`

  Lorsque vous spécifiez `aws-chunked` pour `Content-Encoding`StorageGRID ne vérifie pas les éléments suivants :

  - StorageGRID ne vérifie pas le `chunk-signature` par rapport aux données de bloc.
  - StorageGRID ne vérifie pas la valeur que vous fournissez pour `x-amz-decoded-content-length` contre l'objet.
- `Content-Language`
- `Content-Length`
- `Content-MD5`
- `Content-Type`
- `Expires`
- `Transfer-Encoding`

  Le codage du transfert haché est pris en charge si `aws-chunked` la signature de charge utile est également utilisée.

- `x-amz-meta-`, suivi d'une paire nom-valeur contenant des métadonnées définies par l'utilisateur.

  Lorsque vous spécifiez la paire nom-valeur pour les métadonnées définies par l'utilisateur, utilisez le format général suivant :

```
x-amz-meta-name: value
```

Si vous souhaitez utiliser l'option **temps de création défini par l'utilisateur** comme heure de référence pour une règle ILM, vous devez utiliser `creation-time` nom des métadonnées enregistrées lors de la création de l'objet. Par exemple :

```
x-amz-meta-creation-time: 1443399726
```

La valeur pour `creation-time` Est évaluée en secondes depuis le 1er janvier 1970.

> Une règle ILM ne peut pas utiliser à la fois une **heure de création définie par l'utilisateur** pour l'heure de référence et les options équilibrées ou strictes pour le comportement d'ingestion. Une erreur est renvoyée lors de la création de la règle ILM.

- `x-amz-tagging`
- En-têtes de requête de verrouillage d'objet S3
  - `x-amz-object-lock-mode`
  - `x-amz-object-lock-retain-until-date`
  - `x-amz-object-lock-legal-hold`

    Si une demande est effectuée sans ces en-têtes, les paramètres de rétention par défaut du compartiment sont utilisés pour calculer le mode de version de l'objet et conserver jusqu'à la date. Voir "Utilisez l'API REST S3 pour configurer le verrouillage objet S3".
- En-têtes de demande SSE :
  - `x-amz-server-side-encryption`
  - `x-amz-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption-customer-key`
  - `x-amz-server-side-encryption-customer-algorithm`

    Voir Demander des en-têtes pour le cryptage côté serveur

En-têtes de requête non pris en charge

Les en-têtes de demande suivants ne sont pas pris en charge :

- Le `x-amz-acl` l'en-tête de demande n'est pas pris en charge.
- Le `x-amz-website-redirect-location` l'en-tête de demande n'est pas pris en charge et renvoie `XNotImplemented`.

Options de classe de stockage

Le `x-amz-storage-class` l'en-tête de demande est pris en charge. Valeur soumise pour `x-amz-storage-class` StorageGRID protège les données d'objet lors de leur ingestion, mais pas le nombre de copies

persistantes de l'objet stockées dans le système StorageGRID (déterminé par ILM).

Si la règle ILM correspondant à un objet ingéré utilise l'option stricte pour le comportement d'ingestion, le `x-amz-storage-class` la barre de coupe n'a aucun effet.

Les valeurs suivantes peuvent être utilisées pour `x-amz-storage-class`:

- `STANDARD` (Valeur par défaut)
  - **Double commit** : si la règle ILM spécifie l'option de double validation pour le comportement d'ingestion, dès qu'un objet est ingéré, une seconde copie de cet objet est créée et distribuée à un autre nœud de stockage (double commit). Une fois la règle ILM évaluée, StorageGRID détermine si ces copies intermédiaires initiales répondent aux instructions de placement de la règle. Si ce n'est pas le cas, de nouvelles copies d'objet peuvent avoir besoin d'être effectuées à différents emplacements et les copies intermédiaires initiales peuvent avoir besoin d'être supprimées.
  - **Balanced** : si la règle ILM spécifie l'option équilibrée et que StorageGRID ne peut pas immédiatement effectuer toutes les copies spécifiées dans la règle, StorageGRID effectue deux copies intermédiaires sur différents nœuds de stockage.

    Si StorageGRID peut immédiatement créer toutes les copies d'objet spécifiées dans la règle ILM (placement synchrone), l' `x-amz-storage-class` la barre de coupe n'a aucun effet.

- `REDUCED_REDUNDANCY`
  - **Double commit** : si la règle ILM spécifie l'option de double validation pour le comportement d'ingestion, StorageGRID crée une copie intermédiaire unique lors de l'ingestion de l'objet (simple commit).
  - **Équilibré** : si la règle ILM spécifie l'option équilibrée, StorageGRID effectue une seule copie intermédiaire uniquement si le système ne peut pas immédiatement effectuer toutes les copies spécifiées dans la règle. Si StorageGRID peut effectuer un placement synchrone, cet en-tête n'a aucun effet. Le `REDUCED_REDUNDANCY` L'option est meilleure lorsque la règle ILM correspondant à l'objet crée une copie répliquée unique. Dans ce cas, utilisez `REDUCED_REDUNDANCY` élimine la création et la suppression inutiles d'une copie d'objet supplémentaire pour chaque opération d'ingestion.

  À l'aide du `REDUCED_REDUNDANCY` cette option n'est pas recommandée dans d'autres cas. `REDUCED_REDUNDANCY` augmente le risque de perte de données d'objet lors de l'ingestion. Vous risquez par exemple de perdre des données si une seule copie est initialement stockée sur un nœud de stockage qui échoue avant l'évaluation du ILM.

> Le fait d'avoir une seule copie répliquée pendant une période donnée présente un risque de perte permanente des données. Si une seule copie répliquée d'un objet existe, cet objet est perdu en cas de défaillance ou d'erreur importante d'un noeud de stockage. De plus, lors des procédures de maintenance telles que les mises à niveau, l'accès à l'objet est temporairement perdu.

Spécification `REDUCED_REDUNDANCY` l'impact sur le nombre de copies créées uniquement lors de l'ingestion d'un objet. Elle n'affecte pas le nombre de copies de l'objet lorsque celui-ci est évalué par la règle ILM active ; le stockage des données ne se produit pas à des niveaux de redondance inférieurs dans le système StorageGRID.

Si vous ingez un objet dans un compartiment avec l'option de verrouillage objet S3 activée, la `REDUCED_REDUNDANCY` l'option est ignorée. Si vous ingez un objet dans un compartiment conforme d'ancienne génération, le `REDUCED_REDUNDANCY` option renvoie une erreur. StorageGRID procède toujours à une récupération à double engagement afin de satisfaire les exigences de conformité.

Demander des en-têtes pour le cryptage côté serveur

Vous pouvez utiliser les en-têtes de requête suivants pour crypter un objet avec un chiffrement côté serveur. Les options SSE et SSE-C sont mutuellement exclusives.

- **SSE**: Utilisez l'en-tête suivant si vous voulez chiffrer l'objet avec une clé unique gérée par StorageGRID.
  - `x-amz-server-side-encryption`
- **SSE-C**: Utilisez les trois en-têtes si vous voulez chiffrer l'objet avec une clé unique que vous fournissez et gérez.
  - `x-amz-server-side-encryption-customer-algorithm`: Spécifiez `AES256`.
  - `x-amz-server-side-encryption-customer-key`: Spécifiez votre clé de cryptage pour le nouvel objet.
  - `x-amz-server-side-encryption-customer-key-MD5`: Spécifiez le résumé MD5 de la clé de chiffrement du nouvel objet.

Les clés de chiffrement que vous fournissez ne sont jamais stockées. Si vous perdez une clé de chiffrement, vous perdez l'objet correspondant. Avant d'utiliser des clés fournies par le client pour sécuriser les données d'objet, consultez les points à prendre en compte à la section "utilisation du chiffrement côté serveur".

Si un objet est chiffré avec SSE ou SSE-C, tous les paramètres de chiffrement au niveau du godet ou de la grille sont ignorés.

Gestion des versions

Si le contrôle de version est activé pour un compartiment, un contrôle unique `versionId` est automatiquement généré pour la version de l'objet stocké. C'est ça `versionId` est également renvoyé dans la réponse en utilisant le `x-amz-version-id` en-tête de réponse.

Si la gestion des versions est suspendue, la version de l'objet est stockée avec un null `versionId` si une version nulle existe déjà, elle sera remplacée.

Calculs de signature pour l'en-tête autorisation

Lorsque vous utilisez le `Authorization` En-tête pour l'authentification des demandes, StorageGRID diffère d'AWS de la manière suivante :

- StorageGRID n'est pas nécessaire `host` en-têtes à inclure dans `CanonicalHeaders`.
- StorageGRID n'est pas nécessaire `Content-Type` à inclure dans `CanonicalHeaders`.
- StorageGRID n'est pas nécessaire `x-amz-*` en-têtes à inclure dans `CanonicalHeaders`.

En règle générale, incluez toujours ces en-têtes dans `CanonicalHeaders` Pour s'assurer qu'ils sont vérifiés, cependant, si vous excluez ces en-têtes, StorageGRID ne renvoie pas d'erreur.

Pour plus de détails, reportez-vous à "Calculs de signature pour l'en-tête d'autorisation : transfert de charge utile dans un seul bloc (signature AWS version 4)".

Informations associées

"Gestion des objets avec ILM"

"Opérations sur les compartiments"

"Opérations S3 suivies dans les journaux d'audit"

"Configuration des connexions client"

PLACER l'objet - Copier

Vous pouvez utiliser la demande S3 PUT Object - copie pour créer une copie d'un objet déjà stocké dans S3. Une opération PUT Object - Copy est la même que l'exécution d'un GET puis D'un PUT.

Résoudre les conflits

Les demandes contradictoires des clients, telles que deux clients qui écrivent sur la même clé, sont résolues sur une base de « derniers-victoires ». La chronologie de l'évaluation « derniers-victoires » repose sur la date à laquelle le système StorageGRID termine une demande donnée et non sur la date à laquelle les clients S3 commencent une opération.

Taille de l'objet

La taille maximale *recommandée* pour une opération d'objet PUT unique est de 5 Gio (5,368,709,120 octets). Si vos objets sont supérieurs à 5 Gio, utilisez le téléchargement partitionné.

La taille *supportée* maximale pour une opération objet PUT unique est de 5 Tio (5,497,558,138,880 octets). Cependant, l'alerte **S3 PUT Object size trop importante** est déclenchée si vous tentez de télécharger un objet supérieur à 5 Gio.

Caractères UTF-8 dans les métadonnées utilisateur

Si une requête inclut (non échappé) les valeurs UTF-8 dans le nom de clé ou la valeur des métadonnées définies par l'utilisateur, le comportement StorageGRID n'est pas défini.

StorageGRID n'analyse ni n'interprète pas les caractères UTF-8 qui se sont échappé dans le nom de clé ou la valeur des métadonnées définies par l'utilisateur. Les caractères UTF-8 échappés sont traités comme des caractères ASCII :

- Les requêtes réussissent si les métadonnées définies par l'utilisateur incluent des caractères UTF-8 échappés.
- StorageGRID ne renvoie pas le `x-amz-missing-meta` en-tête si la valeur interprétée du nom ou de la valeur de la clé comprend des caractères non imprimables.

En-têtes de demande pris en charge

Les en-têtes de requête suivants sont pris en charge :

- `Content-Type`
- `x-amz-copy-source`
- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-none-match`
- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-if-modified-since`
- `x-amz-meta-`, suivi d'une paire nom-valeur contenant des métadonnées définies par l'utilisateur
- `x-amz-metadata-directive`: La valeur par défaut est `COPY`, qui permet de copier l'objet et les métadonnées associées.

  Vous pouvez spécifier `REPLACE` pour remplacer les métadonnées existantes lors de la copie de l'objet ou pour la mise à jour des métadonnées de l'objet.

- `x-amz-storage-class`
- `x-amz-tagging-directive`: La valeur par défaut est `COPY`, qui vous permet de copier l'objet et toutes les balises.

  Vous pouvez spécifier `REPLACE` pour remplacer les balises existantes lors de la copie de l'objet ou pour mettre à jour les balises.

- En-têtes de demande de verrouillage d'objet S3 :
  - `x-amz-object-lock-mode`
  - `x-amz-object-lock-retain-until-date`
  - `x-amz-object-lock-legal-hold`

    Si une demande est effectuée sans ces en-têtes, les paramètres de rétention par défaut du compartiment sont utilisés pour calculer le mode de version de l'objet et conserver jusqu'à la date. Voir "Utilisez l'API REST S3 pour configurer le verrouillage objet S3".

- En-têtes de demande SSE :
  - `x-amz-copy-source-server-side-encryption-customer-algorithm`
  - `x-amz-copy-source-server-side-encryption-customer-key`
  - `x-amz-copy-source-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption`
  - `x-amz-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption-customer-key`
  - `x-amz-server-side-encryption-customer-algorithm`

    Voir Demander des en-têtes pour le cryptage côté serveur

En-têtes de requête non pris en charge

Les en-têtes de demande suivants ne sont pas pris en charge :

- `Cache-Control`
- `Content-Disposition`
- `Content-Encoding`
- `Content-Language`
- `Expires`
- `x-amz-website-redirect-location`

Options de classe de stockage

Le `x-amz-storage-class` L'en-tête de demande est pris en charge et affecte le nombre de copies d'objet créé par StorageGRID si la règle ILM correspondante spécifie le comportement d'ingestion de la double validation ou de l'équilibrage.

- `STANDARD`

  (Valeur par défaut) Spécifie une opération d'ingestion à double validation lorsque la règle ILM utilise l'option de validation double, ou lorsque l'option équilibrée revient à créer des copies intermédiaires.

- `REDUCED_REDUNDANCY`

  Spécifie une opération d'entrée de validation unique lorsque la règle ILM utilise l'option Double allocation ou lorsque l'option équilibrée revient à créer des copies intermédiaires.

> Si vous ingez un objet dans un compartiment avec l'option de verrouillage objet S3 activée, la `REDUCED_REDUNDANCY` l'option est ignorée. Si vous ingez un objet dans un compartiment conforme d'ancienne génération, le `REDUCED_REDUNDANCY` option renvoie une erreur. StorageGRID procède toujours à une récupération à double engagement afin de satisfaire les exigences de conformité.

Utilisation de x-amz-copy-source dans PUT Object - Copy

Si le godet source et la clé, spécifiés dans le `x-amz-copy-source` en-tête diffèrent du compartiment de destination et de la clé, une copie des données de l'objet source est écrite sur la destination.

Si la source et la destination correspondent, et le `x-amz-metadata-directive` l'en-tête est spécifié comme `REPLACE`, les métadonnées de l'objet sont mises à jour avec les valeurs de métadonnées fournies dans la demande. Dans ce cas, StorageGRID ne réingère pas l'objet. Ceci a deux conséquences importantes :

- Vous ne pouvez pas utiliser METTRE objet - Copier pour chiffrer un objet existant ou pour modifier le chiffrement d'un objet existant. Si vous fournissez le `x-amz-server-side-encryption` en-tête ou le `x-amz-server-side-encryption-customer-algorithm` En-tête, StorageGRID rejette la demande et renvoie la requête `XNotImplemented`.
- L'option de comportement d'ingestion spécifiée dans la règle ILM correspondante n'est pas utilisée. Tout changement au placement d'objet déclenché par la mise à jour est apporté lors de l'évaluation de ILM par des processus ILM en arrière-plan normaux.

En d'autres termes, si la règle ILM utilise l'option strict pour le comportement d'ingestion, aucune action n'est entreprise si les placements d'objet requis ne peuvent pas être effectués (par exemple, parce qu'un nouvel emplacement n'est pas disponible). L'objet mis à jour conserve son emplacement actuel jusqu'à ce que le placement requis soit possible.

Demander des en-têtes pour le cryptage côté serveur

Si vous utilisez le chiffrement côté serveur, les en-têtes de requête que vous fournissez dépendent du chiffrement de l'objet source et de l'intention de chiffrer l'objet cible.

- Si l'objet source est chiffré à l'aide d'une clé fournie par le client (SSE-C), vous devez inclure les trois en-têtes suivants dans la demande PUT Object - Copy, afin que l'objet puisse être décrypté puis copié :
  - `x-amz-copy-source-server-side-encryption-customer-algorithm`: Spécifiez `AES256`.
  - `x-amz-copy-source-server-side-encryption-customer-key`: Spécifiez la clé de cryptage que vous avez fournie lors de la création de l'objet source.
  - `x-amz-copy-source-server-side-encryption-customer-key-MD5`: Spécifiez le résumé MD5 que vous avez fourni lors de la création de l'objet source.
- Si vous souhaitez chiffrer l'objet cible (la copie) avec une clé unique que vous fournissez et gérez, incluez les trois en-têtes suivants :
  - `x-amz-server-side-encryption-customer-algorithm`: Spécifiez `AES256`.
  - `x-amz-server-side-encryption-customer-key`: Spécifiez une nouvelle clé de cryptage pour l'objet cible.
  - `x-amz-server-side-encryption-customer-key-MD5`: Spécifiez le résumé MD5 de la nouvelle clé de chiffrement.

> Les clés de chiffrement que vous fournissez ne sont jamais stockées. Si vous perdez une clé de chiffrement, vous perdez l'objet correspondant. Avant d'utiliser des clés fournies par le client pour sécuriser les données d'objet, consultez les points à prendre en compte à la section "utilisation du chiffrement côté serveur".

- Si vous souhaitez chiffrer l'objet cible (la copie) avec une clé unique gérée par StorageGRID (SSE), incluez cet en-tête dans la demande PUT Object - Copy :
  - `x-amz-server-side-encryption`

> Le `server-side-encryption` impossible de mettre à jour la valeur de l'objet. Faites plutôt une copie avec un nouveau `server-side-encryption` valeur à l'aide de `x-amz-metadata-directive`: `REPLACE`.

Gestion des versions

Si le compartiment source est multiversion, vous pouvez utiliser le `x-amz-copy-source` en-tête pour copier la dernière version d'un objet. Pour copier une version spécifique d'un objet, vous devez spécifier explicitement la version à copier à l'aide de l' `versionId` sous-ressource. Si le compartiment de destination est multiversion, la version générée est renvoyée dans le `x-amz-version-id` en-tête de réponse. Si le contrôle de version est suspendu pour le compartiment cible, alors `x-amz-version-id` renvoie une valeur « nulle ».

Informations associées

"Gestion des objets avec ILM"

"Opérations S3 suivies dans les journaux d'audit"

"PLACER l'objet"

SelectObjectContent

Vous pouvez utiliser la requête S3 SelectObjectContent pour filtrer le contenu d'un objet S3 à partir d'une instruction SQL simple.

Pour plus d'informations, reportez-vous au "Documentation AWS pour SelectObjectContent".

Avant de commencer

- Le compte de tenant dispose de l'autorisation S3 Select.
- Vous avez `s3:GetObject` autorisation pour l'objet à interroger.
- L'objet que vous souhaitez interroger doit être dans l'un des formats suivants :
  - **CSV**. Peut être utilisé tel qu'il est ou compressé dans des archives GZIP ou BZIP2.
  - **Parquet**. Exigences supplémentaires pour les objets parquet :
    - S3 Select prend uniquement en charge la compression par colonne à l'aide de GZIP ou de Snappy. S3 Select ne prend pas en charge la compression d'objets entiers pour les objets parquet.
    - S3 Select ne prend pas en charge la sortie parquet. Vous devez spécifier le format de sortie au format CSV ou JSON.
    - La taille maximale du groupe de lignes non compressées est de 512 Mo.
    - Vous devez utiliser les types de données spécifiés dans le schéma de l'objet.
    - Vous ne pouvez pas utiliser de types logiques D'INTERVALLE, de JSON, DE LISTE, DE TEMPS ou d'UUID.
- Votre expression SQL a une longueur maximale de 256 Ko.
- Tout enregistrement dans l'entrée ou les résultats a une longueur maximale de 1 MIB.

> ⓘ L'utilisation de ScanRange n'est pas prise en charge.

Exemple de syntaxe de demande CSV

```
POST /{Key+}?select&select-type=2 HTTP/1.1
Host: Bucket.s3.abc-company.com
x-amz-expected-bucket-owner: ExpectedBucketOwner
<?xml version="1.0" encoding="UTF-8"?>
<SelectObjectContentRequest xmlns="http://s3.amazonaws.com/doc/2006-03-
01/">
   <Expression>string</Expression>
   <ExpressionType>string</ExpressionType>
   <RequestProgress>
      <Enabled>boolean</Enabled>
   </RequestProgress>
   <InputSerialization>
      <CompressionType>GZIP</CompressionType>
      <CSV>
         <AllowQuotedRecordDelimiter>boolean</AllowQuotedRecordDelimiter>
         <Comments>#</Comments>
         <FieldDelimiter>\t</FieldDelimiter>
         <FileHeaderInfo>USE</FileHeaderInfo>
         <QuoteCharacter>'</QuoteCharacter>
         <QuoteEscapeCharacter>\\</QuoteEscapeCharacter>
         <RecordDelimiter>\n</RecordDelimiter>
      </CSV>
   </InputSerialization>
   <OutputSerialization>
      <CSV>
         <FieldDelimiter>string</FieldDelimiter>
         <QuoteCharacter>string</QuoteCharacter>
         <QuoteEscapeCharacter>string</QuoteEscapeCharacter>
         <QuoteFields>string</QuoteFields>
         <RecordDelimiter>string</RecordDelimiter>
      </CSV>
   </OutputSerialization>
   <ScanRange>
      <End>long</End>
      <Start>long</Start>
   </ScanRange>
</SelectObjectContentRequest>
```

Exemple de syntaxe de demande de parquet

```
POST /{Key+}?select&select-type=2 HTTP/1.1
Host: Bucket.s3.abc-company.com
x-amz-expected-bucket-owner: ExpectedBucketOwner
<?xml version="1.0" encoding="UTF-8"?>
<SelectObjectContentRequest xmlns=http://s3.amazonaws.com/doc/2006-03-01/>
   <Expression>string</Expression>
   <ExpressionType>string</ExpressionType>
   <RequestProgress>
      <Enabled>boolean</Enabled>
   </RequestProgress>
   <InputSerialization>
      <CompressionType>GZIP</CompressionType>
      <PARQUET>
      </PARQUET>
   </InputSerialization>
   <OutputSerialization>
      <CSV>
         <FieldDelimiter>string</FieldDelimiter>
         <QuoteCharacter>string</QuoteCharacter>
         <QuoteEscapeCharacter>string</QuoteEscapeCharacter>
         <QuoteFields>string</QuoteFields>
         <RecordDelimiter>string</RecordDelimiter>
      </CSV>
   </OutputSerialization>
   <ScanRange>
      <End>long</End>
      <Start>long</Start>
   </ScanRange>
</SelectObjectContentRequest>
```

Exemple de requête SQL

Cette requête obtient le nom de l'état, 2010 populations, environ 2015 populations et le pourcentage de changement des données de recensement des États-Unis. Les enregistrements du fichier qui ne sont pas des États sont ignorés.

```
SELECT STNAME, CENSUS2010POP, POPESTIMATE2015, CAST((POPESTIMATE2015 -
CENSUS2010POP) AS DECIMAL) / CENSUS2010POP * 100.0 FROM S3Object WHERE
NAME = STNAME
```

Les premières lignes du fichier à interroger, `SUB-EST2020_ALL.csv`, regardez comme ceci:

```
SUMLEV,STATE,COUNTY,PLACE,COUSUB,CONCIT,PRIMGEO_FLAG,FUNCSTAT,NAME,STNAME,
CENSUS2010POP,
ESTIMATESBASE2010,POPESTIMATE2010,POPESTIMATE2011,POPESTIMATE2012,POPESTIM
ATE2013,POPESTIMATE2014,
POPESTIMATE2015,POPESTIMATE2016,POPESTIMATE2017,POPESTIMATE2018,POPESTIMAT
E2019,POPESTIMATE042020,
POPESTIMATE2020
040,01,000,00000,00000,00000,0,A,Alabama,Alabama,4779736,4780118,4785514,4
799642,4816632,4831586,
4843737,4854803,4866824,4877989,4891628,4907965,4920706,4921532
162,01,000,00124,00000,00000,0,A,Abbeville
city,Alabama,2688,2705,2699,2694,2645,2629,2610,2602,
2587,2578,2565,2555,2555,2553
162,01,000,00460,00000,00000,0,A,Adamsville
city,Alabama,4522,4487,4481,4474,4453,4430,4399,4371,
4335,4304,4285,4254,4224,4211
162,01,000,00484,00000,00000,0,A,Addison
town,Alabama,758,754,751,750,745,744,742,734,734,728,
725,723,719,717
```

Exemple d'utilisation d'AWS-CLI (CSV)

```
aws s3api select-object-content --endpoint-url https://10.224.7.44:10443
--no-verify-ssl  --bucket 619c0755-9e38-42e0-a614-05064f74126d --key SUB-
EST2020_ALL.csv --expression-type SQL --input-serialization '{"CSV":
{"FileHeaderInfo": "USE", "Comments": "#", "QuoteEscapeCharacter": "\"",
"RecordDelimiter": "\n", "FieldDelimiter": ",", "QuoteCharacter": "\"",
"AllowQuotedRecordDelimiter": false}, "CompressionType": "NONE"}' --output
-serialization '{"CSV": {"QuoteFields": "ASNEEDED",
"QuoteEscapeCharacter": "#", "RecordDelimiter": "\n", "FieldDelimiter":
",", "QuoteCharacter": "\""}}' --expression "SELECT STNAME, CENSUS2010POP,
POPESTIMATE2015, CAST((POPESTIMATE2015 - CENSUS2010POP) AS DECIMAL) /
CENSUS2010POP * 100.0 FROM S3Object WHERE NAME = STNAME" changes.csv
```

Les premières lignes du fichier de sortie, `changes.csv`, regardez comme ceci:

```
Alabama,4779736,4854803,1.570526070895965802295356898372629785 4
Alaska,710231,738430,3.970398363349389142405780654463125377 5
Arizona,6392017,6832810,6.895992297892824753125656580700583243 1
Arkansas,2915918,2979732,2.188470320495981025529524492801237894 9
California,37253956,38904296,4.429972483996062055798852610444914897 1
Colorado,5029196,5454328,8.453279609703022113276157859029554624 6
```

Exemple d'utilisation de l'interface de ligne de commande AWS (parquet)

```
aws s3api select-object-content  -endpoint-url https://10.224.7.44:10443
--bucket 619c0755-9e38-42e0-a614-05064f74126d --key SUB-
EST2020_ALL.parquet --expression "SELECT STNAME, CENSUS2010POP,
POPESTIMATE2015, CAST((POPESTIMATE2015 - CENSUS2010POP) AS DECIMAL) /
CENSUS2010POP * 100.0 FROM S3Object WHERE NAME = STNAME" --expression-type
'SQL' --input-serialization '{"Parquet":{}}'  --output-serialization
'{"CSV": {}}' changes.csv
```

Les premières lignes du fichier de sortie, change.csv, se ressemblent à ceci :

```
Alabama,4779736,4854803,1.5705260708959658022953568983726297854
Alaska,710231,738430,3.9703983633493891424057806544631253775
Arizona,6392017,6832810,6.8959922978928247531256565807005832431
Arkansas,2915918,2979732,2.1884703204959810255295244928012378949
California,37253956,38904296,4.4299724839960620557988526104449148971
Colorado,5029196,5454328,8.4532796097030221132761578590295546246
```

Opérations pour les téléchargements partitionnés

Cette section décrit comment StorageGRID prend en charge les opérations de téléchargement partitionné.

Les conditions et notes suivantes s'appliquent à toutes les opérations de téléchargement partitionné :

- Vous ne devez pas dépasser 1,000 téléchargements partitionnés simultanés dans un seul compartiment car les résultats des requêtes List Multipart Uploads pour ce compartiment pourraient renvoyer des résultats incomplets.
- StorageGRID fait respecter les limites de taille d'AWS pour les pièces en plusieurs parties. Les clients S3 doivent respecter les consignes suivantes :
  - Chaque partie d'un téléchargement partitionné doit être comprise entre 5 Mio (5,242,880 octets) et 5 Gio (5,368,709,120 octets).
  - La dernière partie peut être inférieure à 5 Mio (5,242,880 octets).
  - En général, la taille des pièces doit être la plus grande possible. Par exemple, utilisez une taille de pièce de 5 Gio pour un objet de 100 Gio. Chaque pièce étant considérée comme un objet unique, l'utilisation de pièces de grande taille réduit la surcharge liée aux métadonnées StorageGRID.
  - Pour les objets de moins de 5 Gio, envisagez l'utilisation de téléchargement non partitionné.
- La gestion des règles ILM est évaluée pour chaque partie d'un objet en plusieurs parties lors de son ingestion et pour l'objet dans son ensemble lorsque le téléchargement partitionné est terminé, si la règle ILM utilise le comportement d'ingestion équilibré ou strict. Vous devez savoir comment cela affecte le positionnement de l'objet et de la pièce :
  - Si le téléchargement partitionné est en cours de modification du ILM, si le téléchargement partitionné et certaines parties de l'objet peuvent ne pas répondre aux exigences ILM actuelles. Toute pièce qui n'est pas placée correctement est mise en file d'attente pour la réévaluation ILM et est déplacée

ultérieurement au bon emplacement.

    - Lors de l'évaluation d'ILM pour une pièce, StorageGRID filtre la taille de la pièce, et non la taille de l'objet. Ainsi, certaines parties d'un objet peuvent être stockées dans des emplacements qui ne respectent pas les exigences de la règle ILM pour l'ensemble de l'objet. Par exemple, si une règle indique que tous les objets de 10 Go ou plus sont stockés dans DC1 alors que tous les objets plus petits sont stockés dans DC2, à l'acquisition chaque partie de 1 Go d'un téléchargement partitionné en 10 parties est stockée dans DC2. Lorsque ILM est évaluée pour l'ensemble de l'objet, toutes les parties de l'objet sont déplacées vers DC1.

- Toutes les opérations de téléchargement partitionné prennent en charge les contrôles de cohérence StorageGRID.
- Si nécessaire, vous pouvez utiliser le cryptage côté serveur avec des téléchargements partitionnés. Pour utiliser SSE (chiffrement côté serveur avec clés gérées par StorageGRID), vous avez accès au `x-amz-server-side-encryption` En-tête de demande dans la demande de téléchargement de pièces multiples uniquement. Pour utiliser SSE-C (chiffrement côté serveur avec clés fournies par le client), vous devez spécifier les trois mêmes en-têtes de demande de clé de chiffrement dans la demande de lancement de Multipart Upload et dans chaque demande de chargement de pièce suivante.

Fonctionnement	Mise en place
Liste des téléchargements partitionnés	Voir "Liste des téléchargements partitionnés"
Lancer le téléchargement de pièces multiples	Voir "Lancer le téléchargement de pièces multiples"
Télécharger la pièce	Voir "Télécharger la pièce"
Télécharger la pièce - Copier	Voir "Télécharger la pièce - Copier"
Chargement de pièces multiples complet	Voir "Chargement de pièces multiples complet"
Abandonner le téléchargement de pièces multiples	Mise en œuvre avec tout le comportement de l'API REST Amazon S3. D'être modifiées sans préavis.
Répertorier les pièces	Mise en œuvre avec tout le comportement de l'API REST Amazon S3. D'être modifiées sans préavis.

Informations associées

- "Contrôles de cohérence"
- "Utilisez le cryptage côté serveur"

Liste des téléchargements partitionnés

L'opération List Multipart Uploads répertorie les téléchargements partitionnés en cours pour un compartiment.

Les paramètres de demande suivants sont pris en charge :

- `encoding-type`

- `key-marker`
- `max-uploads`
- `prefix`
- `upload-id-marker`
- `Host`
- `Date`
- `Authorization`

Gestion des versions

Le téléchargement partitionné est constitué de différentes opérations permettant de lancer le téléchargement, de répertorier les téléchargements, de télécharger des pièces, d'assembler les pièces téléchargées et de terminer le téléchargement. Lorsque l'opération de téléchargement multipart complète est exécutée, c'est-à-dire le point où les objets sont créés (et versionnés le cas échéant).

Lancer le téléchargement de pièces multiples

L'opération Initiate Multipart Upload (CreateMultipartUpload) lance un téléchargement partitionné pour un objet et renvoie un ID de téléchargement.

Le `x-amz-storage-class` l'en-tête de demande est pris en charge. Valeur soumise pour `x-amz-storage-class` StorageGRID protège les données d'objet lors de leur ingestion, mais pas le nombre de copies persistantes de l'objet stockées dans le système StorageGRID (déterminé par ILM).

Si la règle ILM correspondant à un objet ingéré utilise l'option stricte pour le comportement d'ingestion, le `x-amz-storage-class` la barre de coupe n'a aucun effet.

Les valeurs suivantes peuvent être utilisées pour `x-amz-storage-class`:

- `STANDARD` (Valeur par défaut)
  - **Double commit** : si la règle ILM spécifie l'option de double validation pour le comportement d'ingestion, dès qu'un objet est ingéré, une seconde copie de cet objet est créée et distribuée à un autre nœud de stockage (double commit). Une fois la règle ILM évaluée, StorageGRID détermine si ces copies intermédiaires initiales répondent aux instructions de placement de la règle. Si ce n'est pas le cas, de nouvelles copies d'objet peuvent avoir besoin d'être effectuées à différents emplacements et les copies intermédiaires initiales peuvent avoir besoin d'être supprimées.
  - **Balanced** : si la règle ILM spécifie l'option équilibrée et que StorageGRID ne peut pas immédiatement effectuer toutes les copies spécifiées dans la règle, StorageGRID effectue deux copies intermédiaires sur différents nœuds de stockage.

    Si StorageGRID peut immédiatement créer toutes les copies d'objet spécifiées dans la règle ILM (placement synchrone), l' `x-amz-storage-class` la barre de coupe n'a aucun effet.
- `REDUCED_REDUNDANCY`
  - **Double commit** : si la règle ILM spécifie l'option de double validation pour le comportement d'ingestion, StorageGRID crée une copie intermédiaire unique lors de l'ingestion de l'objet (simple commit).

- **Équilibré** : si la règle ILM spécifie l'option équilibrée, StorageGRID effectue une seule copie intermédiaire uniquement si le système ne peut pas immédiatement effectuer toutes les copies spécifiées dans la règle. Si StorageGRID peut effectuer un placement synchrone, cet en-tête n'a aucun effet. Le `REDUCED_REDUNDANCY` L'option est meilleure lorsque la règle ILM correspondant à l'objet crée une copie répliquée unique. Dans ce cas, utilisez `REDUCED_REDUNDANCY` élimine la création et la suppression inutiles d'une copie d'objet supplémentaire pour chaque opération d'ingestion.

  À l'aide du `REDUCED_REDUNDANCY` cette option n'est pas recommandée dans d'autres cas. `REDUCED_REDUNDANCY` augmente le risque de perte de données d'objet lors de l'ingestion. Vous risquez par exemple de perdre des données si une seule copie est initialement stockée sur un nœud de stockage qui échoue avant l'évaluation du ILM.

> Le fait d'avoir une seule copie répliquée pendant une période donnée présente un risque de perte permanente des données. Si une seule copie répliquée d'un objet existe, cet objet est perdu en cas de défaillance ou d'erreur importante d'un noeud de stockage. De plus, lors des procédures de maintenance telles que les mises à niveau, l'accès à l'objet est temporairement perdu.

Spécification `REDUCED_REDUNDANCY` l'impact sur le nombre de copies créées uniquement lors de l'ingestion d'un objet. Elle n'affecte pas le nombre de copies de l'objet lorsque celui-ci est évalué par la règle ILM active ; le stockage des données ne se produit pas à des niveaux de redondance inférieurs dans le système StorageGRID.

> Si vous ingez un objet dans un compartiment avec l'option de verrouillage objet S3 activée, la `REDUCED_REDUNDANCY` l'option est ignorée. Si vous ingez un objet dans un compartiment conforme d'ancienne génération, le `REDUCED_REDUNDANCY` option renvoie une erreur. StorageGRID procède toujours à une récupération à double engagement afin de satisfaire les exigences de conformité.

Les en-têtes de requête suivants sont pris en charge :

- `Content-Type`
- `x-amz-meta-`, suivi d'une paire nom-valeur contenant des métadonnées définies par l'utilisateur

  Lorsque vous spécifiez la paire nom-valeur pour les métadonnées définies par l'utilisateur, utilisez le format général suivant :

```
x-amz-meta-_name_: `value`
```

  Si vous souhaitez utiliser l'option **temps de création défini par l'utilisateur** comme heure de référence pour une règle ILM, vous devez utiliser `creation-time` nom des métadonnées enregistrées lors de la création de l'objet. Par exemple :

```
x-amz-meta-creation-time: 1443399726
```

  La valeur pour `creation-time` Est évaluée en secondes depuis le 1er janvier 1970.

Ajout `creation-time` Comme les métadonnées définies par l'utilisateur n'sont pas autorisées si vous ajoutez un objet à un compartiment pour lequel la conformité héritée est activée. Une erreur sera renvoyée.

- En-têtes de demande de verrouillage d'objet S3 :
  - `x-amz-object-lock-mode`
  - `x-amz-object-lock-retain-until-date`
  - `x-amz-object-lock-legal-hold`

    Si une demande est effectuée sans ces en-têtes, les paramètres de rétention par défaut du compartiment sont utilisés pour calculer la version de l'objet conserver jusqu'à la date.

"Utilisez l'API REST S3 pour configurer le verrouillage objet S3"

- En-têtes de demande SSE :
  - `x-amz-server-side-encryption`
  - `x-amz-server-side-encryption-customer-key-MD5`
  - `x-amz-server-side-encryption-customer-key`
  - `x-amz-server-side-encryption-customer-algorithm`

    Demander des en-têtes pour le cryptage côté serveur

Pour plus d'informations sur la façon dont StorageGRID traite les caractères UTF-8, reportez-vous à la documentation relative à L'objet PUT.

Demander des en-têtes pour le cryptage côté serveur

Vous pouvez utiliser les en-têtes de demande suivants pour crypter un objet partitionné avec un cryptage côté serveur. Les options SSE et SSE-C sont mutuellement exclusives.

- **SSE** : utilisez l'en-tête suivant dans la demande lancer le téléchargement multi-pièces si vous souhaitez crypter l'objet avec une clé unique gérée par StorageGRID. Ne spécifiez pas cet en-tête dans les demandes de chargement de pièce.
  - `x-amz-server-side-encryption`
- **SSE-C** : utilisez les trois en-têtes de la demande de téléchargement multipièces (et dans chaque demande de chargement ultérieure de pièce) si vous souhaitez chiffrer l'objet avec une clé unique que vous fournissez et gérez.
  - `x-amz-server-side-encryption-customer-algorithm`: Spécifiez `AES256`.
  - `x-amz-server-side-encryption-customer-key`: Spécifiez votre clé de cryptage pour le nouvel objet.
  - `x-amz-server-side-encryption-customer-key-MD5`: Spécifiez le résumé MD5 de la clé de chiffrement du nouvel objet.

Les clés de chiffrement que vous fournissez ne sont jamais stockées. Si vous perdez une clé de chiffrement, vous perdez l'objet correspondant. Avant d'utiliser des clés fournies par le client pour sécuriser les données d'objet, consultez les points à prendre en compte à la section "utilisation du chiffrement côté serveur".

En-têtes de requête non pris en charge

L'en-tête de demande suivant n'est pas pris en charge et renvoie `XNotImplemented`

- `x-amz-website-redirect-location`

Gestion des versions

Le téléchargement partitionné est constitué de différentes opérations permettant de lancer le téléchargement, de répertorier les téléchargements, de télécharger des pièces, d'assembler les pièces téléchargées et de terminer le téléchargement. Les objets sont créés (et versionnés le cas échéant) lorsque l'opération de chargement multipièce complète est exécutée.

Informations associées

"Gestion des objets avec ILM"

"PLACER l'objet"

Télécharger la pièce

L'opération de téléchargement de pièce télécharge une pièce dans un téléchargement partitionné pour un objet.

En-têtes de demande pris en charge

Les en-têtes de requête suivants sont pris en charge :

- `Content-Length`
- `Content-MD5`

Demander des en-têtes pour le cryptage côté serveur

Si vous avez spécifié le cryptage SSE-C pour lancer la demande de téléchargement multipièce, vous devez également inclure les en-têtes de requête suivants dans chaque demande de chargement de pièce :

- `x-amz-server-side-encryption-customer-algorithm`: Spécifiez `AES256`.
- `x-amz-server-side-encryption-customer-key`: Spécifiez la même clé de cryptage que celle que vous avez fournie dans la demande de lancement de Multipart Upload.
- `x-amz-server-side-encryption-customer-key-MD5`: Spécifiez le même résumé MD5 que vous avez fourni dans la demande de lancement de Multipart Upload.

Les clés de chiffrement que vous fournissez ne sont jamais stockées. Si vous perdez une clé de chiffrement, vous perdez l'objet correspondant. Avant d'utiliser les clés fournies par le client pour sécuriser les données d'objet, consultez les considérations de la section « utilisation du cryptage côté serveur ».

Gestion des versions

Le téléchargement partitionné est constitué de différentes opérations permettant de lancer le téléchargement, de répertorier les téléchargements, de télécharger des pièces, d'assembler les pièces téléchargées et de terminer le téléchargement. Les objets sont créés (et versionnés le cas échéant) lorsque l'opération de chargement multipièce complète est exécutée.

Informations associées

"Utilisez le cryptage côté serveur"

Télécharger la pièce - Copier

L'opération Télécharger la pièce - Copier télécharge une partie d'un objet en copiant les données d'un objet existant en tant que source de données.

L'opération Télécharger la pièce - copie est implémentée avec tout le comportement de l'API REST Amazon S3. D'être modifiées sans préavis.

Cette requête lit et écrit les données de l'objet spécifiées dans `x-amz-copy-source-range` Dans le système StorageGRID.

Les en-têtes de requête suivants sont pris en charge :

- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-none-match`
- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-if-modified-since`

Demander des en-têtes pour le cryptage côté serveur

Si vous avez spécifié le cryptage SSE-C pour lancer la demande de téléchargement multi-pièces, vous devez également inclure les en-têtes de requête suivants dans chaque pièce de téléchargement - demande de copie :

- `x-amz-server-side-encryption-customer-algorithm`: Spécifiez `AES256`.
- `x-amz-server-side-encryption-customer-key`: Spécifiez la même clé de cryptage que celle que vous avez fournie dans la demande de lancement de Multipart Upload.
- `x-amz-server-side-encryption-customer-key-MD5`: Spécifiez le même résumé MD5 que vous avez fourni dans la demande de lancement de Multipart Upload.

Si l'objet source est chiffré à l'aide d'une clé fournie par le client (SSE-C), vous devez inclure les trois en-têtes suivants dans la demande de copie de pièce de téléchargement, afin que l'objet puisse être décrypté puis copié :

- `x-amz-copy-source-server-side-encryption-customer-algorithm`: Spécifiez `AES256`.
- `x-amz-copy-source-server-side-encryption-customer-key`: Spécifiez la clé de cryptage que vous avez fournie lors de la création de l'objet source.
- `x-amz-copy-source-server-side-encryption-customer-key-MD5`: Spécifiez le résumé MD5 que vous avez fourni lors de la création de l'objet source.

Les clés de chiffrement que vous fournissez ne sont jamais stockées. Si vous perdez une clé de chiffrement, vous perdez l'objet correspondant. Avant d'utiliser les clés fournies par le client pour sécuriser les données d'objet, consultez les considérations de la section « utilisation du cryptage côté serveur ».

Gestion des versions

Le téléchargement partitionné est constitué de différentes opérations permettant de lancer le téléchargement, de répertorier les téléchargements, de télécharger des pièces, d'assembler les pièces téléchargées et de terminer le téléchargement. Les objets sont créés (et versionnés le cas échéant) lorsque l'opération de chargement multipièce complète est exécutée.

Chargement de pièces multiples complet

L'opération complète de téléchargement de pièces multiples termine un téléchargement partitionné d'un objet en assemblant les pièces précédemment téléchargées.

Résoudre les conflits

Les demandes contradictoires des clients, telles que deux clients qui écrivent sur la même clé, sont résolues sur une base de « derniers-victoires ». La chronologie de l'évaluation « derniers-victoires » repose sur la date à laquelle le système StorageGRID termine une demande donnée et non sur la date à laquelle les clients S3 commencent une opération.

En-têtes de demande

Le `x-amz-storage-class` L'en-tête de demande est pris en charge et affecte le nombre de copies d'objet créé par StorageGRID si la règle ILM correspondante spécifie le comportement d'ingestion de la double validation ou de l'équilibrage.

- `STANDARD`

  (Valeur par défaut) Spécifie une opération d'ingestion à double validation lorsque la règle ILM utilise l'option de validation double, ou lorsque l'option équilibrée revient à créer des copies intermédiaires.

- `REDUCED_REDUNDANCY`

  Spécifie une opération d'entrée de validation unique lorsque la règle ILM utilise l'option Double allocation ou lorsque l'option équilibrée revient à créer des copies intermédiaires.

  Si vous ingez un objet dans un compartiment avec l'option de verrouillage objet S3 activée, la `REDUCED_REDUNDANCY` l'option est ignorée. Si vous ingez un objet dans un compartiment conforme d'ancienne génération, le `REDUCED_REDUNDANCY` option renvoie une erreur. StorageGRID procède toujours à une récupération à double engagement afin de satisfaire les exigences de conformité.

Si un téléchargement partitionné n'est pas terminé dans les 15 jours, l'opération est marquée comme inactive et toutes les données associées sont supprimées du système.

Le `ETag` La valeur renvoyée n'est pas une somme MD5 des données, mais suit l'implémentation de l'API Amazon S3 du `ETag` valeur pour les objets en plusieurs parties.

Gestion des versions

Cette opération termine un téléchargement partitionné. Si la gestion des versions est activée pour un compartiment, la version de l'objet est créée une fois le téléchargement partitionné terminé.

Si le contrôle de version est activé pour un compartiment, un contrôle unique `versionId` est automatiquement généré pour la version de l'objet stocké. C'est ça `versionId` est également renvoyé dans la réponse en utilisant le `x-amz-version-id` en-tête de réponse.

Si la gestion des versions est suspendue, la version de l'objet est stockée avec un null `versionId` si une version nulle existe déjà, elle sera remplacée.

> Lorsque le contrôle de version est activé pour un compartiment, le fait de terminer un téléchargement partitionné crée toujours une nouvelle version, même si des téléchargements partitionnés simultanés sont terminés sur la même clé d'objet. Lorsque le contrôle de version n'est pas activé pour un compartiment, il est possible de lancer un téléchargement partitionné et de lancer un autre lancement de téléchargement partitionné et de le terminer d'abord sur la même clé d'objet. Pour les compartiments non versionnés, le téléchargement partitionné de la dernière version est prioritaire.

Échec de la réplication, de la notification ou de la notification des métadonnées

Si le compartiment dans lequel le téléchargement partitionné est configuré pour un service de plateforme, le téléchargement partitionné réussit même si l'action de réplication ou de notification associée échoue.

Dans ce cas, une alarme est déclenchée dans le gestionnaire de grille sur Total Events (SMTT). Le message « échec de publication des notifications pour la clé nom-zone » s'affiche pour le dernier objet dont la notification a échoué. (Pour afficher ce message, sélectionnez **NOEUDS** > ***noeud de stockage*** > **événements**. Afficher le dernier événement en haut du tableau.) Les messages d'événement sont également répertoriés dans le `/var/local/log/bycast-err.log`.

Un locataire peut déclencher la réplication ou la notification d'échec en mettant à jour les métadonnées ou les balises de l'objet. Un locataire peut soumettre à nouveau les valeurs existantes afin d'éviter toute modification non souhaitée.

Informations associées

"Gestion des objets avec ILM"

Réponses d'erreur

Le système StorageGRID prend en charge toutes les réponses d'erreur de l'API REST S3 standard qui s'appliquent. En outre, l'implémentation de StorageGRID ajoute plusieurs réponses personnalisées.

Codes d'erreur de l'API S3 pris en charge

Nom	Statut HTTP
AccessDenied	403 interdit
BadDigest	400 demande erronée

Nom	Statut HTTP
BucketAlreadyExists	409 conflit
BucketNotEmpty	409 conflit
Corps entier	400 demande erronée
Erreur interne	500 erreur interne du serveur
InvalidAccessKeyId	403 interdit
Invalides	400 demande erronée
InvalidBucketName	400 demande erronée
InvalidBucketState	409 conflit
InvalidDigest	400 demande erronée
InvalidEncryptionAlgorithmError	400 demande erronée
Invalidpart	400 demande erronée
Ordre de pièce InvalidPartOrder	400 demande erronée
InvalidRange	416 Plage demandée non satisfiable
InvalidRequest	400 demande erronée
InvalidStorageClass	400 demande erronée
InvalidTag	400 demande erronée
URI non valide	400 demande erronée
KeyToolong	400 demande erronée
MalformedXML	400 demande erronée
MetadaTooLarge	400 demande erronée
MethodNotAlldue	405 méthode non autorisée
MissingContentLength	411 longueur requise

Nom	Statut HTTP
Erreur MissingestBodyError	400 demande erronée
En-tête MissinécuritéSent	400 demande erronée
NoSuchBucket	404 introuvable
NoSuchKey	404 introuvable
NoSuchUpload	404 introuvable
Note d'implémentation	501 non mis en œuvre
NoSuchBucketPolicy	404 introuvable
ObjectLockNotConfigurationError	404 introuvable
Pré-conditionFailed	412 Echec de la condition préalable
RequestTimeTooSkewed	403 interdit
Disponibilité des services	503 Service indisponible
SignatureDoesNotMatch	403 interdit
TooManyseaux	400 demande erronée
UserKeyMustBeSpecified	400 demande erronée

Codes d'erreur personnalisés StorageGRID

Nom	Description	Statut HTTP
XBuckeLifecycleNotAlldue	La configuration du cycle de vie des compartiments n'est pas autorisée dans un compartiment conforme aux anciennes	400 demande erronée
XBuckePolicyParseException	Impossible d'analyser la politique de compartiment JSON.	400 demande erronée
XComplanceConflitt	Opération refusée en raison des paramètres de conformité hérités.	403 interdit

Nom	Description	Statut HTTP
XComplanceReduceRAIDForbidden	La réduction de la redondance est interdite dans le compartiment conforme aux réglementations existantes	400 demande erronée
XMaxBucketPolicyLengthExcediédé	Votre politique dépasse la longueur maximale autorisée pour la règle de gestion des compartiments.	400 demande erronée
XMissingInternalRequestHeader	En-tête d'une demande interne manquant.	400 demande erronée
XNoSuchBucketCompliance	La conformité héritée n'est pas activée dans le compartiment spécifié.	404 introuvable
XNotAcceptable	La demande contient un ou plusieurs en-têtes Accept qui n'ont pas pu être satisfaits.	406 non acceptable
XNotImplementation	La demande que vous avez fournie implique une fonctionnalité qui n'est pas implémentée.	501 non mis en œuvre

Requêtes StorageGRID S3

OPTIMISEZ la cohérence des compartiments

La demande D'obtention de cohérence de godet vous permet de déterminer le niveau de cohérence appliqué à un compartiment particulier.

Les contrôles de cohérence par défaut garantissent la lecture après écriture des nouveaux objets.

Pour effectuer cette opération, vous disposez de l'autorisation s3:GetBucketConsistency, ou d'un compte root.

Exemple de demande

```
GET /bucket?x-ntap-sg-consistency HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Réponse

Dans le XML de réponse, `<Consistency>` renvoie l'une des valeurs suivantes :

Contrôle de cohérence	Description
tous	Tous les nœuds reçoivent les données immédiatement, sinon la requête échoue.
forte croissance mondiale	Garantit une cohérence de lecture après écriture pour toutes les demandes client sur tous les sites.
site fort	Garantit la cohérence de lecture après écriture pour toutes les demandes client dans un site.
lecture-après-nouvelle-écriture	(Valeur par défaut) assure la cohérence en lecture après écriture des nouveaux objets et la cohérence des mises à jour des objets. Offre une haute disponibilité et une protection des données garanties. Recommandé dans la plupart des cas.
disponibilité	Assure la cohérence pour les nouveaux objets et les mises à jour d'objets. Pour les compartiments S3, utilisez uniquement si nécessaire (par exemple, pour un compartiment qui contient des valeurs de journal rarement lues ou pour les opérations HEAD ou GET sur des clés qui n'existent pas). Non pris en charge pour les compartiments FabricPool S3.

Exemple de réponse

```
HTTP/1.1 200 OK
Date: Fri, 18 Sep 2020 01:02:18 GMT
Connection: CLOSE
Server: StorageGRID/11.5.0
x-amz-request-id: 12345
Content-Length: 127
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<Consistency xmlns="http://s3.storagegrid.com/doc/2015-02-01/">read-after-new-write</Consistency>
```

Informations associées

"Contrôles de cohérence"

PRÉSERVER la cohérence du godet

La demande de cohérence PUT bucket permet de spécifier le niveau de cohérence à appliquer aux opérations effectuées dans un compartiment.

Les contrôles de cohérence par défaut garantissent la lecture après écriture des nouveaux objets.

Avant de commencer

Vous disposez de l'autorisation s3:PutBuckeConsistency, ou soyez root de compte, pour effectuer cette opération.

Demande

Le `x-ntap-sg-consistency` le paramètre doit contenir l'une des valeurs suivantes :

Contrôle de cohérence	Description
tous	Tous les nœuds reçoivent les données immédiatement, sinon la requête échoue.
forte croissance mondiale	Garantit une cohérence de lecture après écriture pour toutes les demandes client sur tous les sites.
site fort	Garantit la cohérence de lecture après écriture pour toutes les demandes client dans un site.
lecture-après-nouvelle-écriture	(Valeur par défaut) assure la cohérence en lecture après écriture des nouveaux objets et la cohérence des mises à jour des objets. Offre une haute disponibilité et une protection des données garanties. Recommandé dans la plupart des cas.
disponibilité	Assure la cohérence pour les nouveaux objets et les mises à jour d'objets. Pour les compartiments S3, utilisez uniquement si nécessaire (par exemple, pour un compartiment qui contient des valeurs de journal rarement lues ou pour les opérations HEAD ou GET sur des clés qui n'existent pas). Non pris en charge pour les compartiments FabricPool S3.

Remarque: en général, vous devez utiliser la valeur de contrôle de cohérence "entre les nouvelles écritures". Si les demandes ne fonctionnent pas correctement, modifiez le comportement du client d'application si possible. Ou configurez le client afin de spécifier le contrôle de cohérence pour chaque requête d'API. Réglez le contrôle de cohérence au niveau du godet uniquement en dernier recours.

Exemple de demande

```
PUT /bucket?x-ntap-sg-consistency=strong-global HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Informations associées

"Contrôles de cohérence"

HEURE du dernier accès au compartiment

La demande D'heure de dernier accès À GET Bucket vous permet de déterminer si les dernières mises à jour de temps d'accès sont activées ou désactivées pour les

compartiments individuels.

Vous disposez de l'autorisation s3:GetBucketLastAccessTime, ou d'un compte root, pour effectuer cette opération.

Exemple de demande

```
GET /bucket?x-ntap-sg-lastaccesstime HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Exemple de réponse

Cet exemple montre que les mises à jour du temps de dernier accès sont activées pour le compartiment.

```
HTTP/1.1 200 OK
Date: Sat, 29 Nov 2015 01:02:18 GMT
Connection: CLOSE
Server: StorageGRID/10.3.0
x-amz-request-id: 12345
Content-Length: 127
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<LastAccessTime xmlns="http://s3.storagegrid.com/doc/2015-02-01/">enabled
</LastAccessTime>
```

METTRE l'heure du dernier accès au compartiment

La demande d'heure de dernier accès AU compartiment PERMET d'activer ou de désactiver les mises à jour des temps de dernier accès pour chaque compartiment. La désactivation des mises à jour du temps d'accès précédent améliore les performances. Il s'agit du paramètre par défaut pour tous les compartiments créés avec la version 10.3.0, ou ultérieure.

Pour terminer cette opération, vous disposez de l'autorisation s3:PutBuckLastAccessTime pour un compartiment, ou etre root pour un compte.

> À partir de StorageGRID version 10.3, les mises à jour de l'heure du dernier accès sont désactivées par défaut pour tous les nouveaux compartiments. Si des compartiments ont été créés à l'aide d'une version antérieure de StorageGRID et que vous souhaitez faire correspondre le nouveau comportement par défaut, vous devez désactiver explicitement les mises à jour de la dernière heure d'accès pour chacune de ces rubriques précédentes. Vous pouvez activer ou désactiver les mises à jour de l'heure du dernier accès à l'aide de la demande PUT Bucket Last Access Time, de la case **S3** > **Bucket** > **change Last Access Setting** dans le gestionnaire de locataires ou de l'API de gestion des locataires.

Si les dernières mises à jour de temps d'accès sont désactivées pour un compartiment, les opérations suivantes sont appliquées sur le compartiment :

- LES requêtes GET Object, GET Object ACL, GET Object Tagging et HEAD Object ne mettent pas à jour l'heure du dernier accès. L'objet n'est pas ajouté aux files d'attente pour l'évaluation de la gestion du cycle de vie des informations (ILM).
- PUT Object : les demandes de copie et DE BALISAGE d'objets QUI mettent à jour uniquement les métadonnées mettent également à jour l'heure du dernier accès. L'objet est ajouté aux files d'attente pour l'évaluation ILM.
- Si les mises à jour de l'heure du dernier accès sont désactivées pour le compartiment source, PUT Object - Copy Requests ne mettent pas à jour l'heure du dernier accès pour le compartiment source. L'objet copié n'est pas ajouté aux files d'attente pour l'évaluation ILM du compartiment source. Cependant, pour la destination, PLACER l'objet - demandes de copie toujours mettre à jour l'heure du dernier accès. La copie de l'objet est ajoutée aux files d'attente pour l'évaluation ILM.
- Terminer les demandes de téléchargement de pièces multiples mises à jour de l'heure de dernier accès. L'objet terminé est ajouté aux files d'attente pour l'évaluation ILM.

Exemples de demandes

Cet exemple permet d'activer le temps du dernier accès pour un compartiment.

```
PUT /bucket?x-ntap-sg-lastaccesstime=enabled HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Cet exemple désactive l'heure du dernier accès pour un compartiment.

```
PUT /bucket?x-ntap-sg-lastaccesstime=disabled HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Informations associées

"Utilisez un compte de locataire"

SUPPRIMEZ la configuration de notification des métadonnées de compartiment

La demande de configuration DE notification DE métadonnées DELETE Bucket vous permet de désactiver le service d'intégration de recherche pour les compartiments individuels en supprimant le XML de configuration.

Pour effectuer cette opération, vous disposez de l'autorisation s3:DeleteBucketMetadanotification pour un compartiment, ou être un compte root.

Exemple de demande

Cet exemple montre la désactivation du service d'intégration de recherche pour un compartiment.

```
DELETE /test1?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

CONFIGURATION DES notifications de métadonnées de compartiment

La demande de configuration DE notification DE métadonnées GET Bucket vous permet de récupérer le XML de configuration utilisé pour configurer l'intégration de la recherche pour chaque compartiment.

Pour terminer cette opération, vous disposez de l'autorisation s3:GetBuckeMetadatanotification, ou d'un compte root.

Exemple de demande

Cette demande récupère la configuration de notification des métadonnées pour le compartiment nommé `bucket`.

```
GET /bucket?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Réponse

L'organe de réponse inclut la configuration de notification des métadonnées pour le compartiment. La configuration de notification des métadonnées vous permet de déterminer la configuration du compartiment pour l'intégration de la recherche. En d'autres termes, il vous permet de déterminer les objets à indexer et à quels terminaux leurs métadonnées d'objet sont envoyées.

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>rule-status</Status>
        <Prefix>key-prefix</Prefix>
        <Destination>
           <Urn>arn:aws:es:_region:account-
ID_:domain/_mydomain/myindex/mytype_</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Rule-2</ID>
         ...
    </Rule>
     ...
</MetadataNotificationConfiguration>
```

Chaque configuration de notification de métadonnées comprend une ou plusieurs règles. Chaque règle indique les objets qu'elle s'applique ainsi que la destination à laquelle StorageGRID doit envoyer les métadonnées d'objet. Les destinations doivent être spécifiées à l'aide de l'URN d'un terminal StorageGRID.

Nom	Description	Obligatoire
Configuration de la MetadaNotificationConfiguration	Balise de conteneur pour les règles utilisées pour spécifier les objets et la destination des notifications de métadonnées. Contient un ou plusieurs éléments de règle.	Oui.
Règle	Balise de conteneur d'une règle qui identifie les objets dont les métadonnées doivent être ajoutées à un index spécifié. Les règles avec des préfixes qui se chevauchent sont rejetées. Inclus dans l'élément MetadaNotificationConfiguration.	Oui.
ID	Identifiant unique de la règle. Inclus dans l'élément règle.	Non
État	L'état peut être « activé » ou « désactivé ». Aucune action n'est prise pour les règles désactivées. Inclus dans l'élément règle.	Oui.

Nom	Description	Obligatoire
Préfixe	Les objets qui correspondent au préfixe sont affectés par la règle et leurs métadonnées sont envoyées à la destination spécifiée. Pour faire correspondre tous les objets, spécifiez un préfixe vide. Inclus dans l'élément règle.	Oui.
Destination	Balise de conteneur pour la destination d'une règle. Inclus dans l'élément règle.	Oui.
Urne	URN de la destination où les métadonnées d'objet sont envoyées. Doit être l'URN d'un terminal StorageGRID avec les propriétés suivantes : • `es` doit être le troisième élément. • L'URN doit se terminer par l'index et le type où les métadonnées sont stockées, sous la forme `domain-name/myindex/mytype`. Les terminaux sont configurés à l'aide du Gestionnaire de locataires ou de l'API de gestion des locataires. Ils se présentent sous la forme suivante : • `arn:aws:es:_region:account-ID_:domain/mydomain/myindex/mytype` • `urn:mysite:es:::mydomain/myindex/mytype` Le noeud final doit être configuré avant la soumission du XML de configuration, ou la configuration échouera avec une erreur 404. L'urne est incluse dans l'élément destination.	Oui.

Exemple de réponse

XML inclus entre le `<MetadataNotificationConfiguration></MetadataNotificationConfiguration>` les balises indiquent comment l'intégration avec un terminal d'intégration de la recherche est configurée pour le compartiment. Dans cet exemple, les métadonnées d'objet sont envoyées à un index Elasticsearch nommé `current` et le type nommé `2017` Hébergé dans un domaine AWS nommé `records`.

```
HTTP/1.1 200 OK
Date: Thu, 20 Jul 2017 18:24:05 GMT
Connection: KEEP-ALIVE
Server: StorageGRID/11.0.0
x-amz-request-id: 3832973499
Content-Length: 264
Content-Type: application/xml

<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>Enabled</Status>
        <Prefix>2017</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-east-
1:3333333:domain/records/current/2017</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

Informations associées

"Utilisez un compte de locataire"

CONFIGURATION de notification des métadonnées de compartiment

La demande de configuration DE notification DE métadonnées PUT compartiments vous permet d'activer le service d'intégration de la recherche pour chaque compartiment. Le XML de configuration de notification de métadonnées que vous fournissez dans le corps de la requête spécifie les objets dont les métadonnées sont envoyées à l'index de recherche de destination.

Pour effectuer cette opération, vous disposez de l'autorisation s3:PutBuckeMetadanotification pour un compartiment ou être un compte root.

Demande

La demande doit inclure la configuration de notification de métadonnées dans l'organisme de demande. Chaque configuration de notification de métadonnées comprend une ou plusieurs règles. Chaque règle spécifie les objets à lesquels elle s'applique, ainsi que la destination vers laquelle StorageGRID doit envoyer les métadonnées d'objet.

Les objets peuvent être filtrés sur le préfixe du nom de l'objet. Par exemple, vous pouvez envoyer les métadonnées pour les objets avec le préfixe `/images` à une destination et à des objets avec le préfixe `/videos` à un autre.

Les configurations avec des préfixes qui se chevauchent ne sont pas valides et sont rejetées lorsqu'elles sont soumises. Par exemple, une configuration comprenant une règle pour les objets avec le préfixe `test` et une seconde règle pour les objets avec le préfixe `test2` ne serait pas autorisé.

Les destinations doivent être spécifiées à l'aide de l'URN d'un terminal StorageGRID. Le noeud final doit exister lorsque la configuration de notification de métadonnées est soumise, ou que la demande échoue en tant que `400 Bad Request`. Le message d'erreur indique : `Unable to save the metadata notification (search) policy. The specified endpoint URN does not exist: URN`.

```
<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>rule-status</Status>
        <Prefix>key-prefix</Prefix>
        <Destination>
           <Urn>arn:aws:es:region:account-
ID:domain/mydomain/myindex/mytype</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Rule-2</ID>
         ...
    </Rule>
     ...
</MetadataNotificationConfiguration>
```

Le tableau décrit les éléments du XML de configuration de notification des métadonnées.

Nom	Description	Obligatoire
Configuration de la MetadaNotificationConfiguration	Balise de conteneur pour les règles utilisées pour spécifier les objets et la destination des notifications de métadonnées. Contient un ou plusieurs éléments de règle.	Oui.
Règle	Balise de conteneur d'une règle qui identifie les objets dont les métadonnées doivent être ajoutées à un index spécifié. Les règles avec des préfixes qui se chevauchent sont rejetées. Inclus dans l'élément MetadaNotificationConfiguration.	Oui.
ID	Identifiant unique de la règle. Inclus dans l'élément règle.	Non

Nom	Description	Obligatoire
État	L'état peut être « activé » ou « désactivé ». Aucune action n'est prise pour les règles désactivées. Inclus dans l'élément règle.	Oui.
Préfixe	Les objets qui correspondent au préfixe sont affectés par la règle et leurs métadonnées sont envoyées à la destination spécifiée. Pour faire correspondre tous les objets, spécifiez un préfixe vide. Inclus dans l'élément règle.	Oui.
Destination	Balise de conteneur pour la destination d'une règle. Inclus dans l'élément règle.	Oui.
Urne	URN de la destination où les métadonnées d'objet sont envoyées. Doit être l'URN d'un terminal StorageGRID avec les propriétés suivantes : • `es` doit être le troisième élément. • L'URN doit se terminer par l'index et le type où les métadonnées sont stockées, sous la forme `domain-name/myindex/mytype`. Les terminaux sont configurés à l'aide du Gestionnaire de locataires ou de l'API de gestion des locataires. Ils se présentent sous la forme suivante : • `arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype` • `urn:mysite:es:::mydomain/myindex/mytype` Le noeud final doit être configuré avant la soumission du XML de configuration, ou la configuration échouera avec une erreur 404. L'urne est incluse dans l'élément destination.	Oui.

Exemples de demandes

Cet exemple montre l'activation de l'intégration de la recherche pour un compartiment. Dans cet exemple, les métadonnées d'objet de tous les objets sont envoyées vers la même destination.

```
PUT /test1?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host

<MetadataNotificationConfiguration>
    <Rule>
        <ID>Rule-1</ID>
        <Status>Enabled</Status>
        <Prefix></Prefix>
        <Destination>
           <Urn>urn:sgws:es:::sgws-notifications/test1/all</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

Dans cet exemple, les métadonnées d'objet pour les objets qui correspondent au préfixe `/images` est envoyée à une destination, tandis que les métadonnées d'objet correspondent au préfixe `/videos` est envoyé à une seconde destination.

```
PUT /graphics?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host

<MetadataNotificationConfiguration>
    <Rule>
        <ID>Images-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/images</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-east-1:3333333:domain/es-
domain/graphics/imagetype</Urn>
        </Destination>
    </Rule>
    <Rule>
        <ID>Videos-rule</ID>
        <Status>Enabled</Status>
        <Prefix>/videos</Prefix>
        <Destination>
           <Urn>arn:aws:es:us-west-1:22222222:domain/es-
domain/graphics/videotype</Urn>
        </Destination>
    </Rule>
</MetadataNotificationConfiguration>
```

JSON généré par le service d'intégration de la recherche

Lorsque vous activez le service d'intégration de la recherche pour un compartiment, un document JSON est généré et envoyé au terminal de destination à chaque ajout, mise à jour ou suppression de métadonnées d'objet.

Cet exemple montre un exemple de fichier JSON qui peut être généré lorsqu'un objet doté de la clé est associé `SGWS/Tagging.txt` est créé dans un compartiment nommé `test`. Le `test` le compartiment n'est pas multiversion `versionId` l'étiquette est vide.

```
{
  "bucket": "test",
  "key": "SGWS/Tagging.txt",
  "versionId": "",
  "accountId": "86928401983529626822",
  "size": 38,
  "md5": "3d6c7634a85436eee06d43415012855",
  "region":"us-east-1"
  "metadata": {
    "age": "25"
  },
  "tags": {
    "color": "yellow"
  }
}
```

Métadonnées d'objet incluses dans les notifications de métadonnées

Le tableau répertorie tous les champs inclus dans le document JSON qui est envoyé au noeud final de destination lorsque l'intégration de la recherche est activée.

Le nom du document inclut le nom du compartiment, le nom de l'objet et l'ID de version, le cas échéant.

Type	Nom de l'élément	Description
Informations sur les compartiments et les objets	godet	Nom du compartiment
Informations sur les compartiments et les objets	clé	Nom de clé d'objet
Informations sur les compartiments et les objets	ID de version	Version d'objet, pour les objets dans les compartiments multiversion
Informations sur les compartiments et les objets	région	Zone de godet, par exemple `us-east-1`
Métadonnées de système	taille	Taille de l'objet (en octets) visible par un client HTTP
Métadonnées de système	md5	Hachage d'objets
Métadonnées d'utilisateur	les métadonnées *`key:value`*	Toutes les métadonnées utilisateur pour l'objet, comme paires de clé-valeur

Type	Nom de l'élément	Description
Étiquettes	balises *key:value*	Toutes les balises d'objet définies pour l'objet, en tant que paires clé-valeur

Pour les balises et les métadonnées d'utilisateur, StorageGRID transmet des dates et des chiffres à Elasticsearch en tant que chaînes ou notifications d'événement S3. Pour configurer Elasticsearch afin d'interpréter ces chaînes comme des dates ou des chiffres, suivez les instructions Elasticsearch pour un mappage dynamique des champs et un mappage des formats de date. Vous devez activer les mappages de champs dynamiques sur l'index avant de configurer le service d'intégration de la recherche. Une fois qu'un document est indexé, vous ne pouvez pas modifier les types de champ du document dans l'index.

Informations associées

"Utilisez un compte de locataire"

DEMANDE d'utilisation du stockage

La demande GET Storage usage vous indique la quantité totale de stockage utilisée par un compte et pour chaque compartiment associé au compte.

Le volume de stockage utilisé par un compte et ses compartiments peut être obtenu à l'aide d'une demande GET Service modifiée avec le `x-ntap-sg-usage` paramètre de requête. L'utilisation du stockage par compartiment est suivie séparément des demandes DE PUT et DELETE traitées par le système. Il peut y avoir un certain délai avant que les valeurs d'utilisation correspondent aux valeurs attendues en fonction du traitement des demandes, en particulier si le système est soumis à une charge importante.

Par défaut, StorageGRID tente de récupérer les informations d'utilisation à l'aide d'une cohérence globale forte. S'il est impossible d'obtenir une cohérence globale élevée, StorageGRID tente de récupérer les informations relatives à l'utilisation de façon cohérente sur les sites.

Vous disposez de l'autorisation s3:ListAllMyseaux, ou soyez root de compte, pour effectuer cette opération.

Exemple de demande

```
GET /?x-ntap-sg-usage HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Exemple de réponse

Cet exemple montre un compte qui contient quatre objets et 12 octets de données dans deux compartiments. Chaque compartiment contient deux objets et six octets de données.

```
HTTP/1.1 200 OK
Date: Sat, 29 Nov 2015 00:49:05 GMT
Connection: KEEP-ALIVE
Server: StorageGRID/10.2.0
x-amz-request-id: 727237123
Content-Length: 427
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<UsageResult xmlns="http://s3.storagegrid.com/doc/2015-02-01">
<CalculationTime>2014-11-19T05:30:11.000000Z</CalculationTime>
<ObjectCount>4</ObjectCount>
<DataBytes>12</DataBytes>
<Buckets>
<Bucket>
<Name>bucket1</Name>
<ObjectCount>2</ObjectCount>
<DataBytes>6</DataBytes>
</Bucket>
<Bucket>
<Name>bucket2</Name>
<ObjectCount>2</ObjectCount>
<DataBytes>6</DataBytes>
</Bucket>
</Buckets>
</UsageResult>
```

Gestion des versions

Chaque version d'objet stockée contribuera à la `ObjectCount` et `DataBytes` valeurs dans la réponse. Les marqueurs de suppression ne sont pas ajoutés au `ObjectCount` total.

Informations associées

"Contrôles de cohérence"

Demandes de compartiment obsolètes pour la conformité des anciennes

Vous devrez peut-être utiliser l'API REST StorageGRID S3 pour gérer les compartiments qui ont été créés à l'aide de la fonctionnalité de conformité héritée.

Fonction de conformité obsolète

La fonctionnalité de conformité StorageGRID disponible dans les versions précédentes d'StorageGRID est obsolète et a été remplacée par le verrouillage d'objet S3.

Si vous avez précédemment activé le paramètre de conformité globale, le paramètre de verrouillage d'objet S3 global est activé dans StorageGRID 11.6. Vous ne pouvez plus créer de compartiments avec la conformité

activée. Toutefois, si nécessaire, vous pouvez utiliser l'API REST StorageGRID S3 pour gérer tous les compartiments conformes existants.

- "Utilisez l'API REST S3 pour configurer le verrouillage objet S3"
- "Gestion des objets avec ILM"
- "Base de connaissances NetApp : comment gérer des compartiments conformes aux ancienne génération dans StorageGRID 11.5"

Demandes de conformité obsolètes :

- "Obsolète - METTRE les modifications de la demande de godet à des fins de conformité"

  L'élément XML SGCompliance est obsolète. Auparavant, vous pouviez inclure cet élément personnalisé StorageGRID dans le corps de demande XML facultatif de requêtes Put Bucket pour créer un compartiment conforme.

- "Obsolète : OBTENEZ la conformité des compartiments"

  La demande DE conformité DE GET Bucket est obsolète. Cependant, vous pouvez continuer à utiliser cette demande pour déterminer les paramètres de conformité actuellement en vigueur pour un compartiment compatible existant.

- "Obsolète : conformité DES compartiments PUT"

  La demande de conformité PUT Bucket est obsolète. Cependant, vous pouvez continuer à utiliser cette demande pour modifier les paramètres de conformité d'un compartiment conforme existant. Par exemple, vous pouvez placer un compartiment existant en attente légale ou augmenter sa période de conservation.

Obsolète : METTEZ les modifications de la demande de compartiment à des fins de conformité

L'élément XML SGCompliance est obsolète. Auparavant, vous pouviez inclure cet élément personnalisé StorageGRID dans le corps de demande XML facultatif de requêtes Put Bucket pour créer un compartiment conforme.

> La fonctionnalité de conformité StorageGRID disponible dans les versions précédentes d'StorageGRID est obsolète et a été remplacée par le verrouillage d'objet S3.

"Utilisez l'API REST S3 pour configurer le verrouillage objet S3"

"Gestion des objets avec ILM"

"Base de connaissances NetApp : comment gérer des compartiments conformes aux ancienne génération dans StorageGRID 11.5"

Vous ne pouvez plus créer de compartiments avec la fonctionnalité conformité activée. Le message d'erreur suivant s'affiche si vous tentez d'utiliser les modifications de demande DE MISE en godet pour la conformité afin de créer un nouveau compartiment conforme :

```
The Compliance feature is deprecated.
Contact your StorageGRID administrator if you need to create new Compliant
buckets.
```

Obsolète : RÉCUPÉRER la demande de conformité du compartiment

La demande DE conformité DE GET Bucket est obsolète. Cependant, vous pouvez continuer à utiliser cette demande pour déterminer les paramètres de conformité actuellement en vigueur pour un compartiment compatible existant.

> La fonctionnalité de conformité StorageGRID disponible dans les versions précédentes d'StorageGRID est obsolète et a été remplacée par le verrouillage d'objet S3.

"Utilisez l'API REST S3 pour configurer le verrouillage objet S3"

"Gestion des objets avec ILM"

"Base de connaissances NetApp : comment gérer des compartiments conformes aux ancienne génération dans StorageGRID 11.5"

Vous disposez de l'autorisation s3:GetBucketCompliance, ou d'un compte root, pour effectuer cette opération.

Exemple de demande

Cet exemple de demande vous permet de déterminer les paramètres de conformité pour le compartiment nommé `mybucket`.

```
GET /mybucket/?x-ntap-sg-compliance HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Exemple de réponse

Dans le XML de réponse, `<SGCompliance>` le répertorie les paramètres de conformité utilisés pour le compartiment. Cet exemple de réponse montre les paramètres de conformité d'un compartiment dans lequel chaque objet sera conservé pendant un an (525,600 minutes), à partir de l'ingestion de l'objet dans la grille. Il n'y a actuellement aucune retenue légale sur ce godet. Chaque objet sera automatiquement supprimé après un an.

```
HTTP/1.1 200 OK
Date: date
Connection: connection
Server: StorageGRID/11.1.0
x-amz-request-id: request ID
Content-Length: length
Content-Type: application/xml

<SGCompliance>
  <RetentionPeriodMinutes>525600</RetentionPeriodMinutes>
  <LegalHold>false</LegalHold>
  <AutoDelete>true</AutoDelete>
</SGCompliance>
```

Nom	Description
RetentionPeriodMinutes	Durée de conservation des objets ajoutés à ce compartiment, en minutes. La période de conservation commence lorsque l'objet est ingéré dans la grille.
LegalHold	• Vrai : ce compartiment est actuellement en attente légale. Les objets de ce compartiment ne peuvent pas être supprimés tant que la conservation légale n'est pas levée, même si leur période de conservation a expiré. • Faux : ce godet n'est pas actuellement en attente légale. Les objets de ce compartiment peuvent être supprimés à la fin de leur période de conservation.
Suppression automatique	• Vrai : les objets de ce compartiment sont automatiquement supprimés lors de leur expiration, à moins que le compartiment ne soit soumis à une obligation légale. • FALSE : les objets de ce compartiment ne sont pas supprimés automatiquement lorsque la période de conservation expire. Vous devez supprimer ces objets manuellement si vous devez les supprimer.

Réponses d'erreur

Si le compartiment n'a pas été créé pour être conforme, le code d'état HTTP de la réponse est `404 Not Found`, Avec un code d'erreur S3 de `XNoSuchBucketCompliance`.

Obsolète : PUT Bucket Compliance request

La demande de conformité PUT Bucket est obsolète. Cependant, vous pouvez continuer à utiliser cette demande pour modifier les paramètres de conformité d'un compartiment conforme existant. Par exemple, vous pouvez placer un compartiment existant en attente légale ou augmenter sa période de conservation.

La fonctionnalité de conformité StorageGRID disponible dans les versions précédentes d'StorageGRID est obsolète et a été remplacée par le verrouillage d'objet S3.

"Utilisez l'API REST S3 pour configurer le verrouillage objet S3"

"Gestion des objets avec ILM"

"Base de connaissances NetApp : comment gérer des compartiments conformes aux ancienne génération dans StorageGRID 11.5"

Vous disposez de l'autorisation s3:PutBuckeCompliance, ou d'un compte root, pour effectuer cette opération.

Vous devez spécifier une valeur pour chaque champ des paramètres de conformité lors de l'émission d'une demande de conformité PUT Bucket.

Exemple de demande

Cet exemple de demande modifie les paramètres de conformité du compartiment nommé `mybucket`. Dans cet exemple, objets dans `mybucket` sera maintenant conservé pendant deux ans (1,051,200 minutes) au lieu d'un an, à partir de l'ingestion de l'objet dans le grid. Il n'y a pas de retenue légale sur ce godet. Chaque objet sera automatiquement supprimé après deux ans.

```
PUT /mybucket/?x-ntap-sg-compliance HTTP/1.1
Date: date
Authorization: authorization name
Host: host
Content-Length: 152

<SGCompliance>
  <RetentionPeriodMinutes>1051200</RetentionPeriodMinutes>
  <LegalHold>false</LegalHold>
  <AutoDelete>true</AutoDelete>
</SGCompliance>
```

Nom	Description
RetentionPeriodMinutes	Durée de conservation des objets ajoutés à ce compartiment, en minutes. La période de conservation commence lorsque l'objet est ingéré dans la grille. **Important** lorsque vous spécifiez une nouvelle valeur pour RetentionPeriodMinutes, vous devez spécifier une valeur égale ou supérieure à la période de rétention actuelle du compartiment. Une fois la période de rétention du compartiment définie, vous ne pouvez pas la réduire ; vous pouvez uniquement l'augmenter.

Nom	Description
LegalHold	• Vrai : ce compartiment est actuellement en attente légale. Les objets de ce compartiment ne peuvent pas être supprimés tant que la conservation légale n'est pas levée, même si leur période de conservation a expiré. • Faux : ce godet n'est pas actuellement en attente légale. Les objets de ce compartiment peuvent être supprimés à la fin de leur période de conservation.
Suppression automatique	• Vrai : les objets de ce compartiment sont automatiquement supprimés lors de leur expiration, à moins que le compartiment ne soit soumis à une obligation légale. • FALSE : les objets de ce compartiment ne sont pas supprimés automatiquement lorsque la période de conservation expire. Vous devez supprimer ces objets manuellement si vous devez les supprimer.

Niveau de cohérence des paramètres de conformité

Lorsque vous mettez à jour les paramètres de conformité d'un compartiment S3 avec une demande DE conformité PUT bucket, StorageGRID tente de mettre à jour les métadonnées du compartiment dans la grille. Par défaut, StorageGRID utilise le niveau de cohérence **Strong-global** pour garantir que tous les sites de data Center et tous les nœuds de stockage contenant des métadonnées de compartiment sont cohérents en lecture après écriture pour les paramètres de conformité modifiés.

Si StorageGRID ne parvient pas à atteindre le niveau de cohérence **strong-global** car un site de data Center ou plusieurs nœuds de stockage sur un site sont indisponibles, le code d'état HTTP de la réponse est `503 Service Unavailable.`

Si vous recevez cette réponse, vous devez contacter l'administrateur du grid pour vous assurer que les services de stockage requis sont disponibles dans les plus brefs délais. Si l'administrateur de la grille ne parvient pas à mettre suffisamment de nœuds de stockage sur chaque site, le support technique vous demandera peut-être de relancer la demande échouée en forçant le niveau de cohérence **site fort**.

> Ne forcez jamais le niveau de cohérence **site fort** pour la conformité DU godet DE MISE à moins que vous n'ayez été invité à le faire par le support technique et à moins que vous compreniez les conséquences possibles de l'utilisation de ce niveau.

Lorsque le niveau de cohérence est réduit à **strong-site**, StorageGRID garantit que les paramètres de conformité mis à jour auront une cohérence lecture-après-écriture uniquement pour les requêtes client au sein d'un site. Il est donc possible que le système StorageGRID dispose de plusieurs paramètres incohérents pour ce compartiment jusqu'à ce que tous les sites et nœuds de stockage soient disponibles. Les paramètres incohérents peuvent entraîner un comportement inattendu et indésirable. Par exemple, si vous placez un compartiment sous une obligation légale et que vous forcez un niveau de cohérence inférieur, les paramètres de conformité précédents du compartiment (c'est-à-dire la conservation légale) peuvent continuer à être en vigueur sur certains sites de data Center. Par conséquent, les objets qui, selon vous, sont en attente légale peuvent être supprimés à l'expiration de leur période de conservation, soit par l'utilisateur, soit par AutoDelete, si cette option est activée.

Pour forcer l'utilisation du niveau de cohérence **site fort**, réémettez la demande de conformité Put et incluez le `Consistency-Control` En-tête de requête HTTP, comme suit :

```
PUT /mybucket/?x-ntap-sg-compliance HTTP/1.1
Consistency-Control: strong-site
```

Réponses d'erreur

- Si le compartiment n'a pas été créé pour être conforme, le code d'état HTTP de la réponse est `404 Not Found`.
- Si `RetentionPeriodMinutes` Dans la demande est inférieure à la période de conservation actuelle du compartiment, le code d'état HTTP est `400 Bad Request`.

Informations associées

"Obsolète : METTEZ les modifications de la demande de compartiment à des fins de conformité"

Règles d'accès au compartiment et au groupe

Utilisez les règles d'accès au compartiment et au groupe

StorageGRID utilise le langage de règles Amazon Web Services (AWS) pour permettre aux locataires S3 de contrôler l'accès aux compartiments et aux objets dans ces compartiments. Le système StorageGRID implémente un sous-ensemble du langage de règles de l'API REST S3. Les règles d'accès de l'API S3 sont écrites au format JSON.

Présentation de la stratégie d'accès

Il existe deux types de politiques d'accès pris en charge par StorageGRID.

- **Les règles de compartiment**, qui sont configurées à l'aide de la stratégie DE compartiment, DE LA règle DE compartiment PUT et DES opérations de L'API S3 de la politique de compartiment. Les règles de compartiment sont liées aux compartiments. Elles sont donc configurées de façon à contrôler l'accès des utilisateurs du compte du propriétaire du compartiment ou d'autres comptes au compartiment et aux objets. Une politique de compartiment s'applique à un seul compartiment et peut-être à plusieurs groupes.
- **Stratégies de groupe**, qui sont configurées à l'aide du Gestionnaire de locataires ou de l'API de gestion des locataires. Les stratégies de groupe sont associées à un groupe du compte, de sorte qu'elles sont configurées de manière à permettre à ce groupe d'accéder à des ressources spécifiques appartenant à ce compte. Une stratégie de groupe s'applique à un seul groupe et peut-être plusieurs compartiments.

> ⓘ La priorité est la même entre les politiques de groupe et de compartiment.

Les règles de compartiment et de groupe StorageGRID respectent une grammaire spécifique définie par Amazon. À l'intérieur de chaque règle se trouve un ensemble d'énoncés de politique, et chaque instruction contient les éléments suivants :

- ID de déclaration (ID) (facultatif)
- Effet
- Principal/notPrincipal
- Ressource/NotResource
- Action/NotAction

- Condition (en option)

Les instructions de règles sont créées à l'aide de cette structure pour spécifier les autorisations : accorder <effet> pour autoriser/refuser <principal> d'exécuter <action> sur <ressource> lorsque <condition> s'applique.

Chaque élément de règle est utilisé pour une fonction spécifique :

Elément	Description
SID	L'élément Sid est facultatif. Le SID n'est destiné qu'à la description de l'utilisateur. Il est stocké mais non interprété par le système StorageGRID.
Effet	Utilisez l'élément d'effet pour déterminer si les opérations spécifiées sont autorisées ou refusées. Vous devez identifier les opérations que vous autorisez (ou refusez) les compartiments ou les objets à l'aide des mots clés action Element pris en charge.
Principal/notPrincipal	Vous pouvez autoriser les utilisateurs, groupes et comptes à accéder à des ressources spécifiques et à effectuer des actions spécifiques. Si aucune signature S3 n'est incluse dans la demande, l'accès anonyme est autorisé en spécifiant le caractère générique (*) comme principal. Par défaut, seul le root du compte peut accéder aux ressources qui lui sont propres. Il vous suffit de spécifier l'élément principal dans une stratégie de rubrique. Pour les stratégies de groupe, le groupe auquel la stratégie est associée est l'élément principal implicite.
Ressource/NotResource	L'élément ressource identifie les compartiments et les objets. Vous pouvez autoriser ou refuser des autorisations pour les compartiments et les objets en utilisant le nom de ressource Amazon (ARN) pour identifier la ressource.
Action/NotAction	Les éléments action et effet sont les deux composants des autorisations. Lorsqu'un groupe demande une ressource, l'accès à la ressource est accordé ou refusé. L'accès est refusé sauf si vous attribuez des autorisations spécifiques, mais vous pouvez utiliser le refus explicite pour remplacer une autorisation accordée par une autre stratégie.
Condition	L'élément condition est facultatif. Les conditions vous permettent de créer des expressions pour déterminer quand une stratégie doit être appliquée.

Dans l'élément action, vous pouvez utiliser le caractère générique (*) pour spécifier toutes les opérations ou un sous-ensemble d'opérations. Par exemple, cette action correspond à des autorisations telles que s3:GetObject, s3:PutObject et s3:DeleteObject.

```
s3:*Object
```

Dans l'élément ressource, vous pouvez utiliser les caractères génériques (*) et (?). Alors que l'astérisque (*) correspond à 0 caractères ou plus, le point d'interrogation (?) correspond à n'importe quel caractère.

Dans l'élément principal, les caractères génériques ne sont pas pris en charge, sauf pour définir l'accès anonyme, qui accorde l'autorisation à tout le monde. Par exemple, vous définissez le caractère générique (*) comme valeur principale.

```
"Principal":"*"
```

Dans l'exemple suivant, l'instruction utilise les éléments effet, principal, action et ressource. Cet exemple montre une instruction de stratégie de compartiment complète qui utilise l'effet « Autoriser » pour donner les responsables, le groupe admin `federated-group/admin` et le groupe financier `federated-group/finance`, Autorisations d'exécution de l'action `s3:ListBucket` sur le compartiment nommé `mybucket` Et l'action `s3:GetObject` sur tous les objets à l'intérieur de ce godet.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::27233906934684427525:federated-group/admin",
          "arn:aws:iam::27233906934684427525:federated-group/finance"
        ]
      },
      "Action": [
        "s3:ListBucket",
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:iam:s3:::mybucket",
        "arn:aws:iam:s3:::mybucket/*"
      ]
    }
  ]
}
```

La stratégie de compartiment a une taille limite de 20,480 octets et la stratégie de groupe a une taille limite de 5,120 octets.

Paramètres de contrôle de cohérence des règles

Par défaut, toutes les mises à jour apportées aux stratégies de groupe sont cohérentes. Une fois la stratégie de groupe cohérente, les modifications peuvent prendre 15 minutes supplémentaires à appliquer en raison de la mise en cache des règles. Par défaut, toutes les mises à jour effectuées sur les règles de compartiment sont également cohérentes en définitive.

Si nécessaire, vous pouvez modifier les garanties de cohérence pour les mises à jour des règles de

compartiment. Par exemple, il peut être intéressant de vouloir modifier cette règle afin qu'elle devienne effective dès que possible pour des raisons de sécurité.

Dans ce cas, vous pouvez définir le `Consistency-Control` L'en-tête de la demande de stratégie PUT Bucket ou vous pouvez utiliser la demande DE cohérence PUT Bucket. Lorsque vous modifiez le contrôle de cohérence pour cette demande, vous devez utiliser la valeur **All**, qui fournit la garantie la plus élevée de cohérence de lecture après écriture. Si vous spécifiez une autre valeur de contrôle de cohérence dans un en-tête pour la demande DE cohérence PUT Bucket, la demande sera rejetée. Si vous spécifiez une autre valeur pour une demande de stratégie PUT Bucket, la valeur sera ignorée. Une fois la règle de compartiment cohérente, les modifications peuvent prendre 8 secondes supplémentaires pour effet, grâce à la mise en cache des règles.

> Si vous définissez le niveau de cohérence sur **All** pour forcer une nouvelle stratégie de godet à devenir efficace plus tôt, veillez à remettre le contrôle au niveau du godet à sa valeur d'origine lorsque vous avez terminé. Sinon, toutes les futures demandes de rubrique utiliseront le paramètre **tous**.

Utilisez ARN dans les énoncés de politique

Dans les instructions de politique, le ARN est utilisé dans les éléments principal et ressource.

- Utilisez cette syntaxe pour spécifier la ressource S3 ARN :

```
arn:aws:s3:::bucket-name
arn:aws:s3:::bucket-name/object_key
```

- Utilisez cette syntaxe pour spécifier la ressource d'identité ARN (utilisateurs et groupes) :

```
arn:aws:iam::account_id:root
arn:aws:iam::account_id:user/user_name
arn:aws:iam::account_id:group/group_name
arn:aws:iam::account_id:federated-user/user_name
arn:aws:iam::account_id:federated-group/group_name
```

Autres considérations :

- Vous pouvez utiliser l'astérisque (*) comme caractère générique pour correspondre à zéro ou plus de caractères dans la clé d'objet.
- Les caractères internationaux, qui peuvent être spécifiés dans la clé d'objet, doivent être codés à l'aide de JSON UTF-8 ou de séquences d'échappement JSON \u. Le codage pourcentage n'est pas pris en charge.

  "Syntaxe RFC 2141 URN"

  Le corps de requête HTTP pour l'opération de stratégie PUT Bucket doit être codé avec charset=UTF-8.

Spécifiez les ressources dans une stratégie

Dans les instructions de stratégie, vous pouvez utiliser l'élément ressource pour spécifier le compartiment ou l'objet pour lequel les autorisations sont autorisées ou refusées.

- Chaque instruction de stratégie nécessite un élément ressource. Dans une politique, les ressources sont signalées par l'élément `Resource`, ou alternativement, `NotResource` pour exclusion.
- Vous spécifiez des ressources avec une ressource S3 ARN. Par exemple :

```
"Resource": "arn:aws:s3:::mybucket/*"
```

- Vous pouvez également utiliser des variables de règles à l'intérieur de la clé d'objet. Par exemple :

```
"Resource": "arn:aws:s3:::mybucket/home/${aws:username}/*"
```

- La valeur de ressource peut spécifier un compartiment qui n'existe pas encore lorsqu'une stratégie de groupe est créée.

Spécifiez les entités de gestion dans une stratégie

Utilisez l'élément principal pour identifier l'utilisateur, le groupe ou le compte locataire qui est autorisé/refusé l'accès à la ressource par l'instruction de stratégie.

- Chaque énoncé de politique dans une politique de rubrique doit inclure un élément principal. Les énoncés de politique dans une stratégie de groupe n'ont pas besoin de l'élément principal car le groupe est considéré comme le principal.
- Dans une politique, les principes sont indiqués par l'élément « principal » ou « notprincipal » pour exclusion.
- Les identités basées sur les comptes doivent être spécifiées à l'aide d'un ID ou d'un ARN :

```
"Principal": { "AWS": "account_id"}
"Principal": { "AWS": "identity_arn" }
```

- Dans cet exemple, le compte locataire utilise l'ID 27233906934684427525, qui inclut le compte root et tous les utilisateurs du compte :

```
 "Principal": { "AWS": "27233906934684427525" }
```

- Vous pouvez spécifier uniquement la racine du compte :

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:root" }
```

- Vous pouvez spécifier un utilisateur fédéré spécifique (« Alex ») :

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-
user/Alex" }
```

- Vous pouvez spécifier un groupe fédéré spécifique (« gestionnaires ») :

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-
group/Managers"  }
```

- Vous pouvez spécifier un principal anonyme :

```
"Principal": "*"
```

- Pour éviter toute ambiguïté, vous pouvez utiliser l'UUID de l'utilisateur au lieu du nom d'utilisateur :

```
arn:aws:iam::27233906934684427525:user-uuid/de305d54-75b4-431b-adb2-
eb6b9e546013
```

  Par exemple, supposons que Alex quitte l'entreprise et le nom d'utilisateur `Alex` est supprimé. Si un nouveau Alex rejoint l'organisation et est affecté de la même façon `Alex` nom d'utilisateur, le nouvel utilisateur peut hériter involontairement des autorisations accordées à l'utilisateur d'origine.

- La valeur principale peut spécifier un nom de groupe/utilisateur qui n'existe pas encore lors de la création d'une stratégie de compartiment.

Spécifiez les autorisations dans une stratégie

Dans une stratégie, l'élément action est utilisé pour autoriser/refuser des autorisations à une ressource. Il existe un ensemble d'autorisations que vous pouvez spécifier dans une stratégie, qui sont désignées par l'élément « action » ou par « NotAction » pour exclusion. Chacun de ces éléments est associé à des opérations spécifiques d'API REST S3.

Le tableau répertorie les autorisations qui s'appliquent aux compartiments et aux autorisations qui s'appliquent aux objets.

> Amazon S3 utilise désormais l'autorisation s3:PutReplicationConfiguration pour les opérations de réplication de compartiments PUT et DELETE. StorageGRID utilise des autorisations distinctes pour chaque action, qui correspond à la spécification Amazon S3 d'origine.

> Une SUPPRESSION est effectuée lorsqu'un PUT est utilisé pour remplacer une valeur existante.

Autorisations qui s'appliquent aux compartiments

Autorisations	OPÉRATIONS DES API REST S3	Personnalisée pour StorageGRID
s3:CreateBucket	PLACER le godet	
s3:DeleteBucket	SUPPRIMER le compartiment	

Autorisations	OPÉRATIONS DES API REST S3	Personnalisée pour StorageGRID
s3:DeleteBuckeMetadatanotification	SUPPRIMEZ la configuration de notification des métadonnées de compartiment	Oui.
s3:DeleteBucketPolicy	SUPPRIMER la règle de compartiment	
s3:DeleteReplicationConfiguration	SUPPRIMER la réplication du compartiment	Oui, séparer les autorisations pour PUT et DELETE*
s3:GetBucketAcl	OBTENIR l'ACL du compartiment	
s3:GetBuckeCompliance	GARANTIR la conformité des compartiments (obsolète)	Oui.
s3:persistance GetBucketConsistency	OPTIMISEZ la cohérence des compartiments	Oui.
s3:GetBucketCORS	OBTENIR les godets	
s3:GetEncryptionConfiguration	CHIFFREMENT des compartiments	
s3:GetBucketLastAccessTime	HEURE du dernier accès au compartiment	Oui.
s3:GetBucketLocation	ACCÉDER à l'emplacement du compartiment	
s3:GetBucketMetadatanotification	CONFIGURATION DES notifications de métadonnées de compartiment	Oui.
s3:GetBuckenotification	GET Bucket notification	
s3:GetBuckeObjectLockConfiguration	OBTENIR la configuration de verrouillage d'objet	
s3:GetBucketPolicy	GET Bucket policy	
s3:GetBucketTagging	GET Bucket tagging	
s3:GetBucketVersioning	GESTION des versions des compartiments	
s3:GetLifecyclConfiguration	OPTIMISEZ le cycle de vie des compartiments	

Autorisations	OPÉRATIONS DES API REST S3	Personnalisée pour StorageGRID
s3:GetReplicationTM	RÉPLICATION des compartiments	
s3:ListAllMyseaux	• ACCÉDER au service • DÉCOUVREZ l'utilisation du stockage	Oui, pour BÉNÉFICIER DE l'utilisation DU stockage
s3:ListBucket	• OBTENIR le compartiment (liste d'objets) • Godet DE TÊTE • Restauration POST-objet	
s3:ListBuckMultipartUploads	• Liste des téléchargements partitionnés • Restauration POST-objet	
s3:ListBuckeVersions	OBTENIR les versions de compartiment	
s3:PutBuckeCompliance	MISE en conformité des compartiments (obsolète)	Oui.
s3:persistance de PutBuckeConsistency	PRÉSERVER la cohérence du godet	Oui.
s3:PutBuckeCORS	• SUPPRIMER les godets† • PLACEZ les godets	
s3:PutEncryptionConfiguration	• SUPPRIMER le chiffrement du compartiment • PUT Bucket Encryption	
s3:PutBuckeLastAccessTime	METTRE l'heure du dernier accès au compartiment	Oui.
s3:PutBuckeMetadanotification	CONFIGURATION de notification des métadonnées de compartiment	Oui.
s3:PutBuckenotification	PUT Bucket notification	

Autorisations	OPÉRATIONS DES API REST S3	Personnalisée pour StorageGRID
s3:PutBuckObjectLockConfiguration	• PLACEZ le godet avec le `x-amz-bucket-object-lock-enabled: true` En-tête de demande (nécessite également l'autorisation s3:CreateBucket) • CONFIGURATION du verrouillage de l'objet	
s3:PutBuckePolicy	PUT Bucket policy	
s3:PutBuckeTagging	• SUPPRIMER le marquage du compartiment† • PUT Bucket tagging	
s3:PutBuckeVersioning	GESTION des versions du compartiment	
s3:PutLifecyclConfiguration	• SUPPRIMER le cycle de vie du godet† • CYCLE de vie des compartiments	
s3:PutReplicationTM	RÉPLICATION des compartiments	Oui, séparer les autorisations pour PUT et DELETE*

Autorisations qui s'appliquent aux objets

Autorisations	OPÉRATIONS DES API REST S3	Personnalisée pour StorageGRID
s3:AbortMultipartUpload	• Abandonner le téléchargement de pièces multiples • Restauration POST-objet	
s3:BipassGovernanceRetention	• SUPPRIMER l'objet • SUPPRIMER plusieurs objets • CONSERVATION des objets	
s3:DeleteObject	• SUPPRIMER l'objet • SUPPRIMER plusieurs objets • Restauration POST-objet	
s3:DeleteObjectTagging	SUPPRIMER le balisage d'objets	

Autorisations	OPÉRATIONS DES API REST S3	Personnalisée pour StorageGRID
s3:DeleteObjectVersionTagging	SUPPRIMER le balisage d'objets (une version spécifique de l'objet)	
s3:DeleteObjectVersion	SUPPRIMER l'objet (une version spécifique de l'objet)	
s3:GetObject	• OBTENIR l'objet • Objet TÊTE • Restauration POST-objet • SÉLECTIONNEZ contenu de l'objet	
s3:GetObjectAcl	OBTENIR l'ACL d'objet	
s3:GetObjectLegalHold	OBTENIR la mise en attente légale de l'objet	
s3:GetObjectRetention	OBTENIR la conservation des objets	
s3:GetObjectTagging	OBTENIR le balisage d'objets	
s3:GetObjectVersionTagging	OBTENIR le balisage d'objets (une version spécifique de l'objet)	
s3:GetObjectVersion	OBTENIR objet (une version spécifique de l'objet)	
s3:ListMultipartUploadParts	Répertorier les pièces, POST-restauration d'objet	
s3:PutObject	• PLACER l'objet • PLACER l'objet - Copier • Restauration POST-objet • Lancer le téléchargement de pièces multiples • Chargement de pièces multiples complet • Télécharger la pièce • Télécharger la pièce - Copier	
s3:PutObjectLegalHold	METTRE l'objet en attente légale	

Autorisations	OPÉRATIONS DES API REST S3	Personnalisée pour StorageGRID
s3:PutObjectRetention	CONSERVATION des objets	
s3:PutObjectTagging	PLACER le balisage d'objets	
s3:PutObjectVersionTagging	PUT Object Tagging (une version spécifique de l'objet)	
s3:PutOverwriteObject	• PLACER l'objet • PLACER l'objet - Copier • PUT Object tagging • SUPPRIMER le balisage d'objets • Chargement de pièces multiples complet	Oui.
s3:RestoreObject	Restauration POST-objet	

Utiliser l'autorisation PutOverwriteObject

L'autorisation s3:PutOverwriteObject est une autorisation StorageGRID personnalisée qui s'applique aux opérations qui créent ou mettent à jour des objets. Le paramètre de cette autorisation détermine si le client peut remplacer les données d'un objet, les métadonnées définies par l'utilisateur ou le balisage d'objets S3.

Les paramètres possibles pour cette autorisation sont les suivants :

- **Autoriser** : le client peut écraser un objet. Il s'agit du paramètre par défaut.
- **Deny** : le client ne peut pas écraser un objet. Lorsque cette option est définie sur Deny, l'autorisation PutOverwriteObject fonctionne comme suit :
  - Si un objet existant se trouve sur le même chemin :
    - Les données de l'objet, les métadonnées définies par l'utilisateur ou le balisage d'objets S3 ne peuvent pas être remplacés.
    - Toutes les opérations d'entrée en cours sont annulées et une erreur est renvoyée.
    - Si la gestion des versions S3 est activée, le paramètre Deny empêche les opérations PUT Object tagging ou DELETE Object tagging de modifier le TagSet d'un objet et ses versions non actuelles.
  - Si aucun objet existant n'est trouvé, cette autorisation n'a aucun effet.
- Lorsque cette autorisation n'est pas présente, l'effet est le même que si autorisation a été définie.

> Si la règle S3 actuelle autorise l'écrasement et que l'autorisation PutOverwriteObject est définie sur refuser, le client ne peut pas écraser les données d'un objet, les métadonnées définies par l'utilisateur ou le balisage d'objet. En outre, si la case **empêcher la modification du client** est cochée (**CONFIGURATION** > **Paramètres de sécurité** > **réseau et objets**), ce paramètre remplace le paramètre de l'autorisation PutOverwriteObject.

Spécifiez les conditions dans une stratégie

Les conditions définissent le moment où une police sera en vigueur. Les conditions sont constituées d'opérateurs et de paires de clé-valeur.

Les conditions utilisent des paires de clé-valeur pour l'évaluation. Un élément condition peut contenir plusieurs conditions, et chaque condition peut contenir plusieurs paires clé-valeur. Le bloc condition utilise le format suivant :

```
Condition: {
     condition_type: {
          condition_key: condition_values
```

Dans l'exemple suivant, la condition ipaddress utilise la clé condition SourceIp.

```
"Condition": {
    "IpAddress": {
      "aws:SourceIp": "54.240.143.0/24"
        ...
},
        ...
```

Opérateurs de condition pris en charge

Les opérateurs de condition sont classés comme suit :

- Chaîne
- Valeur numérique
- Booléen
- Adresse IP
- Vérification nulle

Opérateurs de condition	Description
Equals à jambes de chaîne	Compare une clé à une valeur de chaîne en fonction de la correspondance exacte (sensible à la casse).
Equals stringNotEquals	Compare une clé à une valeur de chaîne basée sur la correspondance niée (sensible à la casse).
StringEqualisIgnoreCase	Compare une clé à une valeur de chaîne basée sur la correspondance exacte (ignore case).
StringNotEqualisIgnoreCase	Compare une clé à une valeur de chaîne basée sur la correspondance nérée (ignore le cas).

Opérateurs de condition	Description
StringLike	Compare une clé à une valeur de chaîne en fonction de la correspondance exacte (sensible à la casse). Peut inclure * et ? caractères génériques.
StringNotLike	Compare une clé à une valeur de chaîne basée sur la correspondance niée (sensible à la casse). Peut inclure * et ? caractères génériques.
Valeurs numériques	Compare une touche à une valeur numérique en fonction de la correspondance exacte.
NumericNotEquals	Compare une touche à une valeur numérique basée sur la correspondance annulée.
NumericGreaterThan	Compare une clé à une valeur numérique basée sur la comparaison « supérieure à ».
NumericGreaterThanEquals	Compare une clé à une valeur numérique basée sur la comparaison « supérieure ou égale ».
NumericLessThan	Compare une clé à une valeur numérique basée sur la comparaison « moins que ».
NumericLessThanEquals	Compare une clé à une valeur numérique basée sur la comparaison « inférieure à ou égale ».
BOOL	Compare une clé à une valeur booléenne basée sur la correspondance « vrai ou faux ».
Adresse IP	Compare une clé à une adresse IP ou une plage d’adresses IP.
Adresse de la note	Compare une clé à une adresse IP ou une plage d’adresses IP basée sur la correspondance annulée.
Nul	Vérifie si une clé condition est présente dans le contexte de demande actuel.

Touches de condition prises en charge

Catégorie	Touches de condition applicables	Description
Opérateurs IP	aws:SourceIp	Compare à l'adresse IP à partir de laquelle la demande a été envoyée. Peuvent être utilisées pour les opérations de compartiment ou d'objet. **Remarque :** si la requête S3 a été envoyée via le service Load Balancer sur les nœuds Admin et les passerelles, cela se compare à l'adresse IP en amont du service Load Balancer. **Remarque** : si un équilibreur de charge tiers non transparent est utilisé, il sera comparé à l'adresse IP de cet équilibreur de charge. Toutes `X-Forwarded-For` l'en-tête sera ignoré car sa validité ne peut pas être établie.
Ressource/identité	aws:nom d'utilisateur	Compare le nom d'utilisateur de l'expéditeur à partir duquel la demande a été envoyée. Peuvent être utilisées pour les opérations de compartiment ou d'objet.
s3:ListBucket et s3:permissions ListBuckeVersions	s3:délimiteur	Compare avec le paramètre de délimiteur spécifié dans une demande GET Bucket ou GET Bucket Object versions.
s3:ListBucket et s3:permissions ListBuckeVersions	s3:touches max	Compare au paramètre max-keys spécifié dans une demande GET Bucket ou GET Bucket Object versions.
s3:ListBucket et s3:permissions ListBuckeVersions	s3:préfixe	Compare au paramètre de préfixe spécifié dans une demande GET Bucket ou GET Bucket Object versions.
s3:PutObject	s3 :conservation des jours restants avec un verrouillage objet	Compare à la date de conservation spécifiée dans le `x-amz-object-lock-retain-until-date` demander l'en-tête ou calculé à partir de la période de rétention par défaut du compartiment pour s'assurer que ces valeurs se situent dans la plage autorisée pour les demandes suivantes : • PLACER l'objet • PLACER l'objet - Copier • Lancer le téléchargement de pièces multiples

Catégorie	Touches de condition applicables	Description
s3:PutObjectRetention	s3 :conservation des jours restants avec un verrouillage objet	Compare à la date de conservation spécifiée dans la demande DE conservation D'objet PUT pour s'assurer qu'elle se trouve dans la plage autorisée.

Spécifiez les variables d'une règle

Vous pouvez utiliser des variables dans les règles pour remplir les informations relatives aux règles lorsqu'elles sont disponibles. Vous pouvez utiliser des variables de règle dans le `Resource` comparaisons d'éléments et de chaînes dans `Condition` elément.

Dans cet exemple, la variable `${aws:username}` Fait partie de l'élément ressource :

```
"Resource": "arn:aws:s3:::bucket-name/home/${aws:username}/*"
```

Dans cet exemple, la variable `${aws:username}` fait partie de la valeur de condition dans le bloc condition :

```
"Condition": {
    "StringLike": {
      "s3:prefix": "${aws:username}/*"
        ...
},
        ...
```

Variable	Description
`${aws:SourceIp}`	Utilise la touche SourceIp comme variable fournie.
`${aws:username}`	Utilise la clé de nom d'utilisateur comme variable fournie.
`${s3:prefix}`	Utilise la clé de préfixe spécifique au service comme variable fournie.
`${s3:max-keys}`	Utilise la touche max-keys spécifique au service comme variable fournie.
`${*}`	Caractère spécial. Utilise le caractère comme caractère littéral *.
`${?}`	Caractère spécial. Utilise le caractère comme littéral ? caractère.
`${$}`	Caractère spécial. Utilise le caractère comme caractère littéral $.

Créez des règles nécessitant une gestion spéciale

Parfois, une politique peut accorder des autorisations dangereuses pour la sécurité ou dangereuses pour les opérations continues, telles que le verrouillage de l'utilisateur racine du compte. L'implémentation de l'API REST StorageGRID S3 est moins restrictive lors de la validation des règles qu'Amazon, mais tout aussi stricte lors de l'évaluation des règles.

Description de la politique	Type de règle	Comportement Amazon	Comportement de StorageGRID
Refusez vous-même toutes les autorisations sur le compte racine	Godet	Valide et appliquée, mais le compte utilisateur root conserve les autorisations nécessaires pour toutes les opérations des règles de compartiment S3	Identique
Refusez vous-même les autorisations d'accès à l'utilisateur/au groupe	Groupe	Valide et appliquée	Identique
Autoriser un groupe de comptes étrangers toute autorisation	Godet	Principal non valide	Valide, mais les autorisations pour toutes les opérations de stratégie de compartiment S3 renvoient une erreur 405 méthode non autorisée lorsque cela est autorisé par une règle
Autoriser un utilisateur ou une racine de compte étranger à accorder toute autorisation	Godet	Valide, mais les autorisations pour toutes les opérations de stratégie de compartiment S3 renvoient une erreur 405 méthode non autorisée lorsque cela est autorisé par une règle	Identique
Autoriser tout le monde à autoriser toutes les actions	Godet	Valide, mais les autorisations pour toutes les opérations de politique de compartiment S3 renvoient une erreur 405 méthode non autorisée pour la racine du compte étranger et les utilisateurs	Identique
Refuser les autorisations de tous pour toutes les actions	Godet	Valide et appliquée, mais le compte utilisateur root conserve les autorisations nécessaires pour toutes les opérations des règles de compartiment S3	Identique

Description de la politique	Type de règle	Comportement Amazon	Comportement de StorageGRID
Le principal est un utilisateur ou un groupe inexistant	Godet	Principal non valide	Valide
La ressource est un compartiment S3 inexistant	Groupe	Valide	Identique
Principal est un groupe local	Godet	Principal non valide	Valide
La police accorde à un compte non propriétaire (y compris les comptes anonymes) des autorisations pour METTRE des objets	Godet	Valide. Les objets sont détenus par le compte de créateur et la stratégie de compartiment ne s'applique pas. Le compte créateur doit accorder des autorisations d'accès à l'objet à l'aide des listes de contrôle d'accès d'objet.	Valide. Les objets sont la propriété du compte du propriétaire du compartiment. La politique de compartiment s'applique.

Protection WORM (Write-once, Read-many)

Vous pouvez créer des compartiments WORM (Write-once, Read-many) pour protéger les données, les métadonnées d'objet définies par l'utilisateur et le balisage d'objets S3. Vous configurez les compartiments WORM pour permettre la création de nouveaux objets et empêcher les écrasements ou la suppression de contenu existant. Utilisez l'une des approches décrites ici.

Pour vous assurer que les écrasements sont toujours refusés, vous pouvez :

- Dans le Gestionnaire de grille, accédez à **CONFIGURATION** > **sécurité** > **Paramètres de sécurité** > **réseau et objets**, puis cochez la case **empêcher la modification du client**.
- Appliquez les règles suivantes et les règles S3 :
  - Ajoutez une opération DE REFUS PutOverwriteObject à la règle S3.
  - Ajoutez une opération DE REFUS DeleteObject à la règle S3.
  - Ajouter une opération D'AUTORISATION PLACER l'objet à la règle S3.

> La définition de DeleteObject sur DENY dans une politique S3 n'empêche pas ILM de supprimer des objets lorsqu'une règle telle que « zéro copie après 30 jours » existe.

> Même lorsque toutes ces règles et politiques sont appliquées, elles ne protègent pas contre les écritures simultanées (voir situation A). Ils protègent contre les écrasements séquentiels terminés (voir situation B).

Situation A: Écritures simultanées (non protégées contre)

```
/mybucket/important.doc
PUT#1 ---> OK
PUT#2 -------> OK
```

Situation B: Remplacements séquentiels terminés (protégés contre)

```
/mybucket/important.doc
PUT#1 -------> PUT#2 ---X (denied)
```

Informations associées

- "Gestion des objets par les règles StorageGRID ILM"
- "Exemples de politiques de compartiments"
- "Exemples de stratégies de groupe"
- "Gestion des objets avec ILM"
- "Utilisez un compte de locataire"

Exemples de politiques de compartiments

Utilisez les exemples de cette section pour créer des règles d'accès StorageGRID pour les compartiments.

Les politiques de compartiment spécifient les autorisations d'accès pour le compartiment à lequel la politique est attachée. Les règles de compartiment sont configurées à l'aide de l'API S3 PutBuckPolicy. Voir "Opérations sur les compartiments".

Il est possible de configurer une politique de compartiment à l'aide de l'interface de ligne de commandes AWS, comme indiqué dans la commande suivante :

```
> aws s3api put-bucket-policy --bucket examplebucket --policy
file://policy.json
```

Exemple : autoriser tout le monde à accéder en lecture seule à un compartiment

Dans cet exemple, tout le monde, y compris anonyme, est autorisé à lister les objets dans le compartiment et à effectuer des opérations get Object sur tous les objets du compartiment. Toutes les autres opérations seront refusées. Notez que cette politique peut ne pas être particulièrement utile, car personne, à l'exception de la racine du compte, ne peut écrire dans le compartiment.

```
{
  "Statement": [
    {
      "Sid": "AllowEveryoneReadOnlyAccess",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [ "s3:GetObject", "s3:ListBucket" ],
      "Resource":
["arn:aws:s3:::examplebucket","arn:aws:s3:::examplebucket/*"]
    }
  ]
}
```

Exemple : autoriser l'accès complet de tous les utilisateurs d'un compte et permettre à chacun d'un autre compte d'accéder en lecture seule à un compartiment

Dans cet exemple, tout le monde d'un compte spécifié peut accéder intégralement à un compartiment, tandis que les utilisateurs d'un autre compte spécifié ne sont autorisés qu'à répertorier le compartiment et effectuer des opérations GetObject sur les objets du compartiment en commençant par le `shared/` préfixe de clé d'objet.

> Dans StorageGRID, les objets créés par un compte autre que le propriétaire (y compris les comptes anonymes) sont détenus par le compte du propriétaire du compartiment. La politique de compartiment s'applique à ces objets.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "95390887230002558202"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "31181711887329436680"
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::examplebucket/shared/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "31181711887329436680"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::examplebucket",
      "Condition": {
        "StringLike": {
          "s3:prefix": "shared/*"
        }
      }
    }
  ]
}
```

Exemple : autoriser tout le monde à accéder en lecture seule à un compartiment et à accéder entièrement au groupe spécifié

Dans cet exemple, tout le monde, y compris anonyme, est autorisé à répertorier le compartiment et à effectuer des opérations GET Object sur tous les objets du compartiment, tandis que seuls les utilisateurs appartenant au groupe `Marketing` le compte spécifié est autorisé à accéder pleinement.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/Marketing"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": ["s3:ListBucket","s3:GetObject"],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    }
  ]
}
```

Exemple : autoriser tout le monde à lire et à écrire l'accès à un compartiment si le client se trouve dans la plage IP

Dans cet exemple, tout le monde, y compris anonyme, est autorisé à répertorier le compartiment et à effectuer toutes les opérations objet sur tous les objets du compartiment, à condition que les demandes proviennent d'une plage IP spécifiée (54.240.143.0 à 54.240.143.255, sauf 54.240.143.188). Toutes les autres opérations seront refusées et toutes les demandes en dehors de la plage IP seront refusées.

```
{
  "Statement": [
    {
      "Sid": "AllowEveryoneReadWriteAccessIfInSourceIpRange",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [ "s3:*Object", "s3:ListBucket" ],
      "Resource":
["arn:aws:s3:::examplebucket","arn:aws:s3:::examplebucket/*"],
      "Condition": {
        "IpAddress": {"aws:SourceIp": "54.240.143.0/24"},
        "NotIpAddress": {"aws:SourceIp": "54.240.143.188"}
      }
    }
  ]
}
```

Exemple : autoriser un accès complet à un compartiment exclusivement par un utilisateur fédéré spécifié

Dans cet exemple, l'utilisateur fédéré Alex est autorisé à accéder pleinement au `examplebucket` le godet et ses objets. Tous les autres utilisateurs, y compris « root », sont explicitement refusés à toutes les opérations. Notez toutefois que « root » n'est jamais refusé les autorisations de mettre/obtenir/DeleteBuckePolicy.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-user/Alex"
      },
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Deny",
      "NotPrincipal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-user/Alex"
      },
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    }
  ]
}
```

Exemple : autorisation PutOverwriteObject

Dans cet exemple, le `Deny` Effet pour PutOverwriteObject et DeleteObject garantit que personne ne peut écraser ou supprimer les données de l'objet, les métadonnées définies par l'utilisateur et le balisage d'objets S3.

```
{
  "Statement": [
    {
      "Effect": "Deny",
      "Principal": "*",
      "Action": [
        "s3:PutOverwriteObject",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion"
      ],
      "Resource": "arn:aws:s3:::wormbucket/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/SomeGroup"

},
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::wormbucket"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/SomeGroup"

},
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::wormbucket/*"
    }
  ]
}
```

Exemples de stratégies de groupe

Utilisez les exemples de cette section pour créer des stratégies d'accès StorageGRID pour les groupes.

Les stratégies de groupe spécifient les autorisations d'accès pour le groupe auquel la stratégie est associée. Il n'y a pas de `Principal` élément de la règle car il est implicite. Les règles de groupe sont configurées à l'aide du Gestionnaire de locataires ou de l'API.

Exemple : définissez la stratégie de groupe à l'aide du Gestionnaire de locataires

Lorsque vous ajoutez ou modifiez un groupe dans le Gestionnaire de locataires, vous pouvez sélectionner une stratégie de groupe pour déterminer les autorisations d'accès S3 dont les membres de ce groupe auront accès. Voir "Créez des groupes pour un locataire S3".

- **Pas d'accès S3** : option par défaut. Les utilisateurs de ce groupe n'ont pas accès aux ressources S3, sauf si l'accès est accordé avec une règle de compartiment. Si vous sélectionnez cette option, seul l'utilisateur root peut accéder aux ressources S3 par défaut.
- **Accès en lecture seule** : les utilisateurs de ce groupe ont accès en lecture seule aux ressources S3. Par exemple, les utilisateurs de ce groupe peuvent afficher la liste des objets et lire les données d'objet, les métadonnées et les balises. Lorsque vous sélectionnez cette option, la chaîne JSON pour une stratégie de groupe en lecture seule s'affiche dans la zone de texte. Vous ne pouvez pas modifier cette chaîne.
- **Accès complet** : les utilisateurs de ce groupe ont accès aux ressources S3, y compris aux compartiments. Lorsque vous sélectionnez cette option, la chaîne JSON pour une stratégie de groupe à accès complet s'affiche dans la zone de texte. Vous ne pouvez pas modifier cette chaîne.
- **Atténuation des ransomware** : cet exemple de politique s'applique à tous les compartiments pour ce locataire. Les utilisateurs de ce groupe peuvent effectuer des actions courantes, mais ne peuvent pas supprimer définitivement des objets des compartiments pour lesquels la gestion des versions d'objet est activée.

  Les utilisateurs du Gestionnaire de locataires disposant de l'autorisation gérer tous les compartiments peuvent remplacer cette stratégie de groupe. Limitez l'autorisation gérer tous les compartiments aux utilisateurs de confiance et utilisez l'authentification multifacteur (MFA), le cas échéant.

- **Custom** : les utilisateurs du groupe disposent des autorisations que vous spécifiez dans la zone de texte.

Exemple : autoriser l'accès complet du groupe à toutes les rubriques

Dans cet exemple, tous les membres du groupe sont autorisés à accéder à tous les compartiments appartenant au compte du locataire, sauf s'ils sont explicitement refusés par la politique de compartiment.

```
{
  "Statement": [
    {
      "Action": "s3:*",
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::*"
    }
  ]
}
```

Exemple : autoriser l'accès en lecture seule du groupe à tous les compartiments

Dans cet exemple, tous les membres du groupe ont un accès en lecture seule aux ressources S3, à moins qu'ils ne soient explicitement refusés par la règle de compartiment. Par exemple, les utilisateurs de ce groupe peuvent afficher la liste des objets et lire les données d'objet, les métadonnées et les balises.

```
{
  "Statement": [
    {
      "Sid": "AllowGroupReadOnlyAccess",
      "Effect": "Allow",
      "Action": [
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:GetObject",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionTagging"
      ],
      "Resource": "arn:aws:s3:::*"
    }
  ]
}
```

Exemple : permettre aux membres du groupe d'accéder pleinement à leur « dossier » uniquement dans un compartiment

Dans cet exemple, les membres du groupe ne sont autorisés qu'à répertorier et accéder à leur dossier spécifique (préfixe de clé) dans le compartiment spécifié. Notez que les autorisations d'accès à partir d'autres stratégies de groupes et de la règle de compartiment doivent être prises en compte lors de la détermination de la confidentialité de ces dossiers.

```
{
  "Statement": [
    {
      "Sid": "AllowListBucketOfASpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::department-bucket",
      "Condition": {
        "StringLike": {
          "s3:prefix": "${aws:username}/*"
        }
      }
    },
    {
      "Sid": "AllowUserSpecificActionsOnlyInTheSpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3:*Object",
      "Resource": "arn:aws:s3:::department-bucket/${aws:username}/*"
    }
  ]
}
```

Configuration de la sécurité pour l'API REST

Il est recommandé de passer en revue les mesures de sécurité mises en œuvre pour l'API REST et de comprendre comment sécuriser votre système.

Comment StorageGRID assure la sécurité pour l'API REST

Vous devez comprendre comment le système StorageGRID implémente la sécurité, l'authentification et l'autorisation pour l'API REST.

StorageGRID utilise les mesures de sécurité suivantes.

- Les communications client avec le service Load Balancer utilisent HTTPS si HTTPS est configuré pour le noeud final Load Balancer.

  Lorsque vous configurez un point final d'équilibreur de charge, HTTP peut éventuellement être activé. Par exemple, vous pouvez utiliser HTTP à des fins de test ou autres que la production. Pour plus d'informations, reportez-vous aux instructions d'administration de StorageGRID.

- Par défaut, StorageGRID utilise HTTPS pour les communications client avec les nœuds de stockage.

  HTTP peut éventuellement être activé pour ces connexions. Par exemple, vous pouvez utiliser HTTP à des fins de test ou autres que la production. Pour plus d'informations, reportez-vous aux instructions d'administration de StorageGRID.

- Les communications entre StorageGRID et le client sont chiffrées à l'aide de TLS.

- Les communications entre le service Load Balancer et les nœuds de stockage dans la grille sont cryptées que le terminal de l'équilibreur de charge soit configuré pour accepter les connexions HTTP ou HTTPS.
- Les clients doivent fournir des en-têtes d'authentification HTTP à StorageGRID pour effectuer des opérations d'API REST.

Certificats de sécurité et applications client

Les clients peuvent se connecter au service Load Balancer sur les nœuds de passerelle ou les nœuds d'administration, directement aux nœuds de stockage.

Dans tous les cas, les applications client peuvent établir des connexions TLS à l'aide d'un certificat de serveur personnalisé chargé par l'administrateur de la grille ou d'un certificat généré par le système StorageGRID :

- Lorsque les applications client se connectent au service Load Balancer, elles le font à l'aide du certificat configuré pour le noeud final de l'équilibreur de charge spécifique utilisé pour établir la connexion. Chaque noeud final possède son propre certificat, qui est soit un certificat de serveur personnalisé chargé par l'administrateur de la grille, soit un certificat que l'administrateur de la grille a généré dans StorageGRID lors de la configuration du noeud final.
- Lorsque les applications client se connectent directement à un nœud de stockage, elles utilisent les certificats de serveur générés par le système qui ont été générés pour les nœuds de stockage lors de l'installation du système StorageGRID (qui sont signés par l'autorité de certification du système), ou un seul certificat de serveur personnalisé fourni pour la grille par un administrateur de grille.

Les clients doivent être configurés pour approuver l'autorité de certification qui a signé le certificat qu'ils utilisent pour établir des connexions TLS.

Pour plus d'informations sur la configuration des terminaux d'équilibrage de charge et sur l'ajout d'un certificat de serveur personnalisé unique pour les connexions TLS directement aux nœuds de stockage, reportez-vous aux instructions relatives à l'administration de StorageGRID.

Récapitulatif

Le tableau suivant montre comment les problèmes de sécurité sont implémentés dans les API REST S3 et Swift :

Problème de sécurité	Implémentation pour l'API REST
Sécurité de la connexion	TLS
Authentification du serveur	Certificat de serveur X.509 signé par l'autorité de certification du système ou certificat de serveur personnalisé fourni par l'administrateur
Authentification client	• S3 : compte S3 (ID de clé d'accès et clé d'accès secrète) • SWIFT : compte Swift (nom d'utilisateur et mot de passe)
Autorisation du client	• S3 : propriété des compartiments et toutes les règles de contrôle d'accès applicables • SWIFT : accès aux rôles d'administrateur

Informations associées

"Administrer StorageGRID"

Algorithmes de hachage et de cryptage pris en charge pour les bibliothèques TLS

Le système StorageGRID prend en charge un ensemble limité de suites de chiffrement que les applications clientes peuvent utiliser lors de l'établissement d'une session TLS (transport Layer Security). Pour configurer les chiffrements, accédez à **CONFIGURATION** > **sécurité** > **Paramètres de sécurité** et sélectionnez **règles TLS et SSH**.

Versions supportées de TLS

StorageGRID supporte TLS 1.2 et TLS 1.3.

SSLv3 et TLS 1.1 (ou versions antérieures) ne sont plus pris en charge.

Informations associées

"Configurez les comptes et les connexions des locataires"

Surveiller et auditer les opérations

Contrôler les taux d'entrée et de récupération des objets

Vous pouvez surveiller les taux d'entrée et de récupération des objets, ainsi que les mesures relatives au nombre d'objets, aux requêtes et à la vérification. Vous pouvez afficher le nombre de tentatives de lecture, d'écriture et de modification d'objets du système StorageGRID ayant échoué et réussies par les applications client.

Étapes

1. Connectez-vous au Grid Manager à l'aide d'un "navigateur web pris en charge".
2. Sur le tableau de bord, sélectionnez **Performance** > **S3 Operations** ou **Performance** > **Swift Operations**.

   Cette section récapitule le nombre d'opérations client effectuées par votre système StorageGRID. La moyenne des débits de protocole est calculée au cours des deux dernières minutes.

3. Sélectionnez **NOEUDS**.
4. Dans la page d'accueil noeuds (niveau de déploiement), cliquez sur l'onglet **Load Balancer**.

   Les graphiques présentent les tendances de tout le trafic client dirigé vers les terminaux d'équilibreur de charge dans la grille. Vous pouvez sélectionner un intervalle de temps en heures, jours, semaines, mois ou années, vous pouvez également appliquer un intervalle personnalisé.

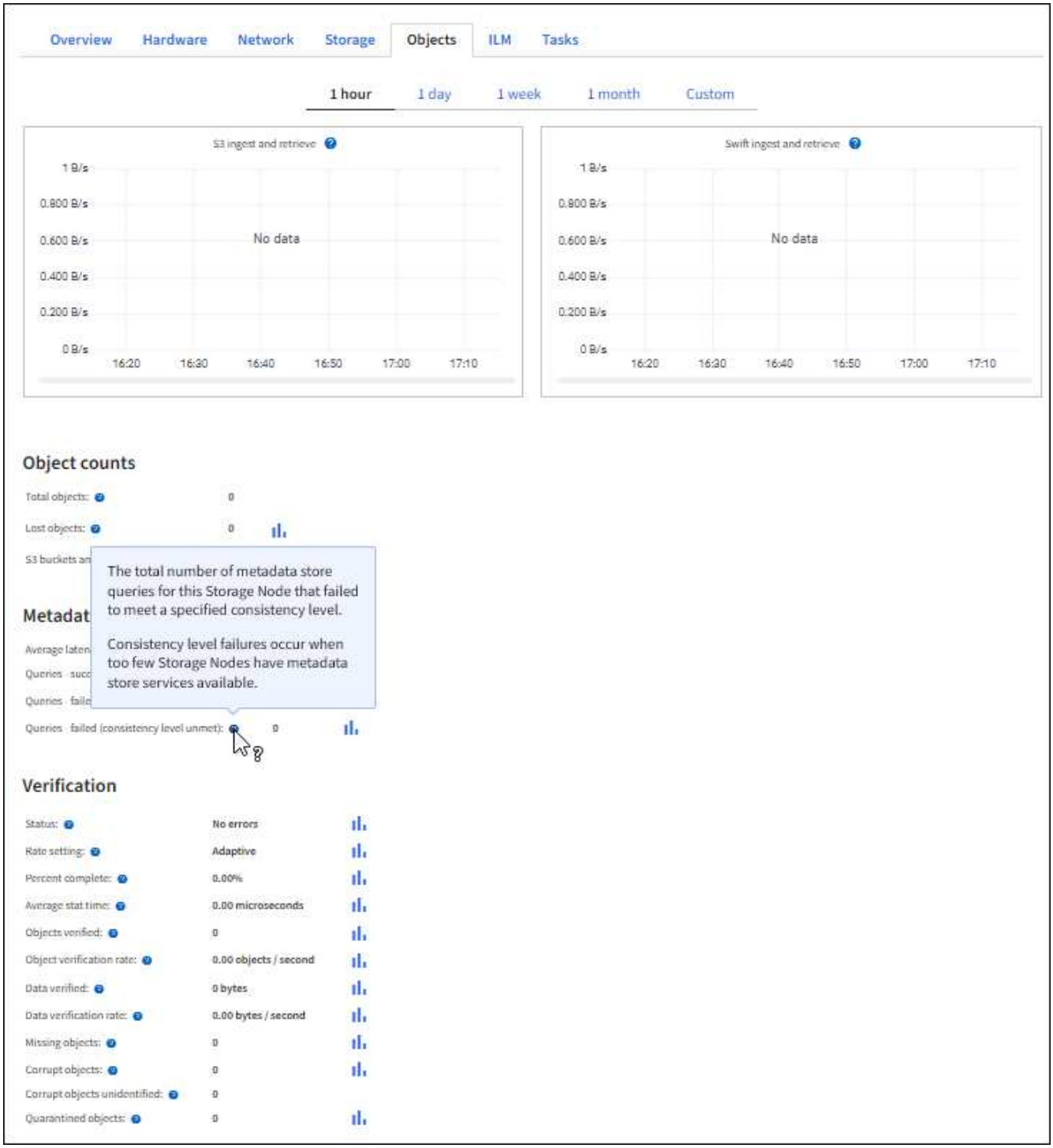
5. Dans la page d'accueil noeuds (niveau de déploiement), cliquez sur l'onglet **objets**.

   Le graphique montre les taux d'entrée et de récupération de l'intégralité de votre système StorageGRID en octets par seconde et en octets totaux. Vous pouvez sélectionner un intervalle de temps en heures, jours, semaines, mois ou années, vous pouvez également appliquer un intervalle personnalisé.

6. Pour afficher les informations relatives à un noeud de stockage particulier, sélectionnez-le dans la liste de gauche, puis cliquez sur l'onglet **objets**.

   Le tableau affiche les taux d'entrée et de récupération de l'objet pour ce nœud de stockage. L'onglet inclut également des mesures pour le nombre d'objets, les requêtes et la vérification. Vous pouvez cliquer sur les

étiquettes pour afficher les définitions de ces mesures.



7. Si vous voulez encore plus de détails :
   a. Sélectionnez **SUPPORT** > **Outils** > **topologie de grille**.
   b. Sélectionnez ***site*** > **Présentation** > **main**.

      La section opérations d'API affiche un récapitulatif des informations sur l'ensemble de la grille.

   c. Sélectionnez ***Storage Node*** > **LDR** > ***client application*** > **Présentation** > **main**

      La section opérations affiche un récapitulatif des informations sur le nœud de stockage sélectionné.

Examiner les journaux d'audit

Les messages d'audit sont générés par les services StorageGRID et stockés dans des fichiers journaux texte. Des messages d'audit spécifiques aux API dans les journaux d'audit fournissent des données stratégiques de sécurité, d'exploitation et de surveillance des performances qui vous aideront à évaluer l'état de votre système.

Avant de commencer

- Vous disposez d'autorisations d'accès spécifiques.
- Vous avez le `Passwords.txt` fichier.
- Vous connaissez l'adresse IP d'un nœud d'administration.

Description de la tâche

Le fichier journal d'audit actif est nommé `audit.log`, Et il est stocké sur des nœuds d'administration.

Une fois par jour, le fichier audit.log actif est enregistré, et un nouveau `audit.log` le fichier est démarré. Le nom du fichier enregistré indique quand il a été enregistré, au format *`yyyy-mm-dd.txt`*.

Après un jour, le fichier enregistré est compressé et renommé, au format *`yyyy-mm-dd.txt.gz`*, qui conserve la date originale.

Cet exemple montre l'actif `audit.log` fichier du jour précédent (`2018-04-15.txt`), et le fichier compressé pour la veille (`2018-04-14.txt.gz`).

```
audit.log
2018-04-15.txt
2018-04-14.txt.gz
```

Étapes

1. Connectez-vous à un nœud d'administration :
   a. Saisissez la commande suivante : `ssh admin@primary_Admin_Node_IP`
   b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
   c. Entrez la commande suivante pour passer à la racine : `su -`
   d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

      Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

2. Accédez au répertoire contenant les fichiers journaux d'audit :

   ```
   cd /var/local/audit/export
   ```

3. Afficher le fichier journal d'audit actuel ou enregistré, selon les besoins.

Opérations S3 suivies dans les journaux d'audit

Plusieurs opérations de compartiment et les opérations d'objets sont suivies dans les journaux d'audit de StorageGRID.

Les opérations des compartiments sont suivies dans les journaux d'audit

- SUPPRIMER le compartiment
- SUPPRIMER le balisage du compartiment
- SUPPRIMER plusieurs objets
- OBTENIR le compartiment (liste d'objets)
- OBTENIR les versions d'objet de compartiment
- GET Bucket tagging
- Godet DE TÊTE
- PLACER le godet
- METTEZ le godet en conformité
- PUT Bucket tagging
- GESTION des versions du compartiment

Opérations d'objet suivies dans les journaux d'audit

- Chargement de pièces multiples complet
- Télécharger la pièce (lorsque la règle ILM utilise les comportements d'ingestion équilibrés ou stricts)
- Télécharger la pièce - Copier (lorsque la règle ILM utilise les comportements d'ingestion équilibrés ou stricts)
- SUPPRIMER l'objet
- OBTENIR l'objet
- Objet TÊTE
- Restauration POST-objet
- PLACER l'objet
- PLACER l'objet - Copier

Informations associées

"Opérations sur les compartiments"

"Opérations sur les objets"

Avantages des connexions HTTP actives, inactives et simultanées

La configuration des connexions HTTP peut avoir un impact sur les performances du système StorageGRID. Les configurations varient selon que la connexion HTTP est active ou inactive ou si vous avez simultanément plusieurs connexions.

Vous pouvez identifier les avantages en termes de performances pour les types de connexions HTTP suivants :

- Connexions HTTP inactives
- Connexions HTTP actives
- Connexions HTTP simultanées

Avantages de maintenir les connexions HTTP inactives ouvertes

Vous devez maintenir les connexions HTTP ouvertes même lorsque les applications client sont inactives pour permettre aux applications client d'effectuer les transactions suivantes sur la connexion ouverte. En fonction des mesures du système et de l'expérience d'intégration, vous devez garder une connexion HTTP inactive ouverte pendant 10 minutes maximum. StorageGRID peut fermer automatiquement une connexion HTTP qui reste ouverte et inactive pendant plus de 10 minutes.

Les connexions HTTP ouvertes et inactives offrent les avantages suivants :

- Réduction de la latence entre le moment où le système StorageGRID détermine qu'il doit effectuer une transaction HTTP et le moment où le système StorageGRID peut effectuer la transaction

  La réduction de la latence constitue l'avantage principal, notamment pour la durée nécessaire à l'établissement des connexions TCP/IP et TLS.

- Augmentation de la vitesse de transfert des données en amorçant l'algorithme TCP/IP à démarrage lent avec des transferts effectués précédemment
- Notification instantanée de plusieurs classes de conditions de défaillance qui interrompent la connectivité entre l'application cliente et le système StorageGRID

Déterminer la durée d'ouverture d'une connexion inactive est un compromis entre les avantages du démarrage lent associés à la connexion existante et l'affectation idéale de la connexion aux ressources système internes.

Avantages des connexions HTTP actives

Pour les connexions directes aux nœuds de stockage, vous devez limiter la durée d'une connexion HTTP active à un maximum de 10 minutes, même si la connexion HTTP effectue des transactions en continu.

La détermination de la durée maximale pendant laquelle une connexion doit être maintenue ouverte est un compromis entre les avantages de la persistance de connexion et l'allocation idéale de la connexion aux ressources système internes.

Pour les connexions client aux nœuds de stockage, la limitation des connexions HTTP actives offre les avantages suivants :

- Équilibrage optimal de la charge sur l'ensemble du système StorageGRID.

  Avec le temps, une connexion HTTP pourrait ne plus être optimale au fur et à mesure que les besoins en équilibrage de la charge évoluent. Le système réalise son meilleur équilibrage de charge lorsque les applications client établissent une connexion HTTP distincte pour chaque transaction, mais cela annule les gains les plus importants associés aux connexions persistantes.

- Permet aux applications clientes de diriger des transactions HTTP vers des services LDR qui ont de l'espace disponible.
- Permet de démarrer les procédures de maintenance.

  Certaines procédures de maintenance ne démarrent qu'une fois toutes les connexions HTTP en cours terminées.

Pour les connexions client au service Load Balancer, limiter la durée des connexions ouvertes peut être utile pour permettre le démarrage rapide de certaines procédures de maintenance. Si la durée des connexions client n'est pas limitée, l'arrêt automatique des connexions actives peut prendre plusieurs minutes.

Avantages des connexions HTTP simultanées

Vous devez maintenir plusieurs connexions TCP/IP ouvertes au système StorageGRID pour permettre le parallélisme, ce qui augmente les performances. Le nombre optimal de connexions parallèles dépend de divers facteurs.

Les connexions HTTP simultanées offrent les avantages suivants :

- Latence réduite

  Les transactions peuvent commencer immédiatement au lieu d'attendre que d'autres transactions soient effectuées.

- Rendement accru

  Le système StorageGRID peut effectuer des transactions parallèles et augmenter le débit des transactions globales.

Les applications client doivent établir plusieurs connexions HTTP. Lorsqu'une application client doit effectuer une transaction, elle peut sélectionner et utiliser immédiatement toute connexion établie qui ne traite pas actuellement une transaction.

Le débit maximal de chaque topologie de chaque système StorageGRID est différent pour les transactions et les connexions simultanées, avant que les performances ne commencent à se dégrader. Le pic de débit dépend de facteurs tels que les ressources informatiques, les ressources réseau, les ressources de stockage et les liaisons WAN. Des facteurs sont également pris en charge par le nombre de serveurs et de services, ainsi que par le nombre d'applications prises en charge par le système StorageGRID.

Les systèmes StorageGRID prennent souvent en charge plusieurs applications client. Vous devez garder cela à l'esprit lorsque vous déterminez le nombre maximal de connexions simultanées utilisées par une application client. Si l'application client se compose de plusieurs entités logicielles qui établissent chacune des connexions avec le système StorageGRID, vous devez ajouter toutes les connexions entre les entités. Vous devrez peut-être régler le nombre maximal de connexions simultanées dans les situations suivantes :

- La topologie du système StorageGRID affecte le nombre maximal de transactions et de connexions simultanées pris en charge par le système.
- Les applications client qui interagissent avec le système StorageGRID sur un réseau avec une bande passante limitée peuvent être contraintes de réduire le niveau de simultanéité pour s'assurer que les transactions individuelles sont effectuées dans un délai raisonnable.
- Lorsque de nombreuses applications client partagent le système StorageGRID, il peut être nécessaire de réduire le degré de simultanéité pour ne pas dépasser les limites du système.

Séparation des pools de connexions HTTP pour les opérations de lecture et d'écriture

Vous pouvez utiliser des pools séparés de connexions HTTP pour les opérations en lecture et écriture, et contrôler la proportion que vous souhaitez utiliser pour chacun d'eux. Le recours à des pools séparés de connexions HTTP vous permet de contrôler les transactions et d'équilibrer la charge plus efficacement.

Les applications client peuvent créer des chargements qui sont dominants par la récupération (lecture) ou dominants par le stockage (écriture). Grâce à des pools séparés de connexions HTTP pour les transactions en lecture et écriture, vous pouvez ajuster la quantité de chaque pool à dédier pour les transactions en lecture ou en écriture.

Utiliser l'API REST de Swift (obsolète)

Utilisez l'API REST de Swift : présentation

Les applications client peuvent utiliser l'API OpenStack Swift pour interagir avec le système StorageGRID.

> La prise en charge des applications du client Swift a été obsolète et sera supprimée dans une prochaine version.

StorageGRID prend en charge les versions spécifiques suivantes de Swift et HTTP.

Élément	Version
Spécification SWIFT	OpenStack Swift Object Storage API v1 depuis novembre 2015
HTTP	1.1 pour plus d'informations sur HTTP, consultez le document HTTP/1.1 (RFC 7230-35). **Remarque**: StorageGRID ne prend pas en charge HTTP/1.1 pipeline.

Informations associées

"OpenStack : API de stockage objet"

Historique de la prise en charge de l'API Swift dans StorageGRID

Notez que des modifications ont été apportées à la prise en charge du système StorageGRID pour l'API REST Swift.

Relâchez	Commentaires
11.7	La prise en charge des applications du client Swift a été obsolète et sera supprimée dans une prochaine version.
11.6	Modifications éditoriales mineures.
11.5	Suppression du contrôle de cohérence faible Le niveau de cohérence disponible sera utilisé à la place.
11.4	Ajout de la prise en charge de TLS 1.3. Ajout d'une description de l'interrelation entre ILM et paramètre de cohérence.

Relâchez	Commentaires
11.3	Les opérations PUT mises à jour décrivent l'impact des règles ILM qui utilisent le placement synchrone à l'ingestion (options équilibrées et strictes pour le comportement d'ingestion). Ajout d'une description des connexions client qui utilisent des noeuds finaux d'équilibreur de charge ou des groupes de haute disponibilité. Les chiffrements TLS 1.1 ne sont plus pris en charge.
11.2	Modifications rédactionnelles mineures apportées au document
11.1	Ajout de la prise en charge de l'utilisation des connexions client HTTP pour Swift aux nœuds de la grille. Mise à jour des définitions des contrôles de cohérence.
11.0	Ajout de la prise en charge de 1,000 conteneurs pour chaque compte locataire.
10.3	Mises à jour administratives et corrections du document. Suppression des sections pour la configuration des certificats de serveur personnalisés.
10.2	Prise en charge initiale de l'API Swift par le système StorageGRID. La version actuellement prise en charge est l'API de stockage objet OpenStack Swift v1.

Comment StorageGRID implémente l'API REST Swift

Une application client peut utiliser les appels de l'API REST Swift pour se connecter aux nœuds de stockage et aux nœuds de passerelle afin de créer des conteneurs et de stocker et récupérer des objets. Les applications orientées services développées pour OpenStack Swift peuvent ainsi se connecter au stockage objet sur site fourni par le système StorageGRID.

Gestion des objets Swift

À l'entrée des objets Swift dans le système StorageGRID, ils sont gérés par les règles de gestion du cycle de vie des informations de la politique ILM active du système. Le "Règles ILM" et "Politique ILM" Création et distribution de copies des données d'objet par StorageGRID et gestion de ces copies au fil du temps Par exemple, une règle ILM peut s'appliquer aux objets de conteneurs Swift spécifiques et peut spécifier que plusieurs copies d'objets seront enregistrées dans plusieurs data centers pendant un certain nombre d'années.

Contactez votre consultant en services professionnels NetApp ou votre administrateur StorageGRID si vous avez besoin de comprendre en quoi les règles et règles ILM de la grille affecteront les objets de votre compte de locataire Swift.

Requêtes des clients en conflit

Les demandes contradictoires des clients, telles que deux clients qui écrivent sur la même clé, sont résolues sur une base de « derniers-victoires ». Le moment auquel l'évaluation « derniers-victoires » est basé sur la date à laquelle le système StorageGRID remplit une demande donnée et non sur la date à laquelle les clients Swift entament une opération.

Garanties et contrôles de cohérence

Par défaut, StorageGRID fournit une cohérence de lecture après écriture pour les objets nouvellement créés et une cohérence éventuelle pour les mises à jour et les OPÉRATIONS HEAD d'objet. Toutes "OBTENEZ" suite à une exécution réussie "EN" pourra lire les données nouvellement écrites. Les écrasements d'objets existants, les mises à jour de métadonnées et les suppressions sont cohérents. La propagation des écrasements ne prend généralement que quelques secondes ou minutes, mais peut prendre jusqu'à 15 jours.

StorageGRID vous permet également de contrôler la cohérence par conteneur. Les contrôles de cohérence assurent un équilibre entre la disponibilité des objets et la cohérence de ces objets entre plusieurs nœuds et sites de stockage, selon les exigences de votre application.

Recommandations pour l'implémentation de l'API REST Swift

Suivez ces recommandations lors de la mise en œuvre de l'API REST Swift pour une utilisation avec StorageGRID.

Recommandations pour les têtes à des objets inexistants

Si votre application vérifie régulièrement si un objet existe dans un chemin où vous ne vous attendez pas à ce que l'objet existe réellement, vous devez utiliser le contrôle de cohérence « disponible ». Par exemple, vous devez utiliser le contrôle de cohérence « disponible » si votre application effectue une opération DE TÊTE à un emplacement avant d'effectuer une opération DE MISE à cet emplacement.

Sinon, si l'opération HEAD ne trouve pas l'objet, vous pouvez recevoir un nombre élevé de 500 erreurs de serveur interne si un ou plusieurs nœuds de stockage ne sont pas disponibles.

Vous pouvez définir le contrôle de cohérence « disponible » pour chaque conteneur à l'aide du "REQUÊTE de cohérence du conteneur". Le contrôle de cohérence « disponible » est défini pour chaque conteneur utilisant le "DEMANDE DE cohérence du conteneur".

Recommandations pour les noms d'objet

Pour les conteneurs créés dans StorageGRID 11.4 ou version ultérieure, il n'est plus nécessaire de limiter les noms d'objet afin de respecter les bonnes pratiques de performance. Par exemple, vous pouvez maintenant utiliser des valeurs aléatoires pour les quatre premiers caractères des noms d'objets.

Pour les conteneurs créés dans des versions antérieures à StorageGRID 11.4, suivez ces recommandations pour les noms d'objet :

- Vous ne devez pas utiliser de valeurs aléatoires comme les quatre premiers caractères des noms d'objets. Cela contraste avec l'ancienne recommandation AWS pour les préfixes de noms. Au lieu de cela, vous devez utiliser des préfixes non aléatoires et non uniques, tels que `image`.
- Si vous suivez l'ancienne recommandation AWS pour utiliser des caractères aléatoires et uniques dans les préfixes de noms, vous devez préfixer les noms d'objets avec un nom de répertoire. C'est-à-dire, utilisez le format suivant :

  ```
  mycontainer/mydir/f8e3-image3132.jpg
  ```

  Au lieu de ce format :

```
mycontainer/f8e3-image3132.jpg
```

Recommandations pour « plages de lectures »

Si le "option globale pour compresser les objets stockés" Est activé, les applications clientes Swift doivent éviter d'effectuer des opérations GET Object qui spécifient une plage d'octets à renvoyer. Ces opérations de « lecture à plage » sont inefficaces, car StorageGRID doit décompresser efficacement les objets pour accéder aux octets demandés. LES opérations GET Object qui demandent une petite plage d'octets provenant d'un objet très volumineux sont particulièrement inefficaces. Par exemple, il est très inefficace de lire une plage de 10 Mo à partir d'un objet compressé de 50 Go.

Si les plages sont lues à partir d'objets compressés, les demandes client peuvent être en attente.

> ⓘ Si vous devez compresser des objets et que votre application client doit utiliser des lectures de plage, augmentez le délai de lecture de l'application.

Configurez les comptes et les connexions des locataires

Pour configurer StorageGRID pour accepter les connexions à partir des applications client, vous devez créer un ou plusieurs comptes de tenant et configurer les connexions.

Créez et configurez des comptes de locataire Swift

Un compte de locataire Swift est requis pour que les clients de l'API Swift puissent stocker et récupérer des objets sur StorageGRID. Chaque compte de locataire possède son propre ID de compte, groupes et utilisateurs, ainsi que des conteneurs et des objets.

Les comptes de locataires Swift sont créés par un administrateur StorageGRID GRID à l'aide de Grid Manager ou de l'API de gestion du grid.

Quand "Création d'un compte de locataire Swift", l'administrateur de la grille spécifie les informations suivantes :

- "Nom d'affichage du locataire" (L'ID de compte du locataire est attribué automatiquement et ne peut pas être modifié)
- En option, un "quota de stockage pour le compte locataire" — le nombre maximal de gigaoctets, de téraoctets ou de pétaoctets disponibles pour les objets du locataire. Le quota de stockage d'un locataire représente une quantité logique (taille d'objet), et non une quantité physique (taille sur disque).
- Si "Authentification unique (SSO)" N'est pas utilisé pour le système StorageGRID, que le compte de locataire utilise son propre référentiel d'identité ou partage le référentiel d'identité de la grille, ainsi que le mot de passe initial pour l'utilisateur root local du locataire.
- Si SSO est activé, quel groupe fédéré dispose de l'autorisation d'accès racine pour configurer le compte de locataire.

Après la création d'un compte de locataire Swift, les utilisateurs disposant de l'autorisation d'accès racine peuvent accéder au gestionnaire de locataires pour effectuer des tâches telles que :

- Configuration de la fédération des identités (sauf si le référentiel d'identité est partagé avec la grille) et création de groupes et d'utilisateurs locaux

- Contrôle de l'utilisation du stockage

> Les utilisateurs Swift doivent disposer de l'autorisation d'accès racine à "Accédez au gestionnaire de locataires". Toutefois, l'autorisation d'accès racine ne permet pas aux utilisateurs de s'authentifier auprès de l'API REST Swift pour créer des conteneurs et ingérer des objets. Les utilisateurs doivent disposer de l'autorisation Administrateur Swift pour s'authentifier dans l'API REST de Swift.

Configuration des connexions client

Un administrateur du grid fait des choix de configuration qui affectent la manière dont les clients Swift se connectent à StorageGRID pour stocker et récupérer les données. Les informations spécifiques dont vous avez besoin pour établir une connexion dépendent de la configuration choisie.

Les applications client peuvent stocker ou récupérer des objets en se connectant au service Load Balancer sur des nœuds d'administration ou des nœuds de passerelle, ou éventuellement l'adresse IP virtuelle d'un groupe haute disponibilité de nœuds d'administration ou de nœuds de passerelle.

> Toutes les applications qui dépendent de StorageGRID pour l'équilibrage de la charge doivent se connecter à l'aide du service Load Balancer.

- Des nœuds de stockage, avec ou sans équilibreur de charge externe

Lors de la configuration de StorageGRID, un administrateur de la grille peut utiliser le gestionnaire de grille ou l'API de gestion de grille pour effectuer les étapes suivantes, qui sont toutes facultatives :

1. Configurez les noeuds finaux pour le service Load Balancer.

   Vous devez configurer les noeuds finaux pour utiliser le service Load Balancer. Le service Load Balancer sur les nœuds d'administration ou de passerelle distribue les connexions réseau entrantes des applications client aux nœuds de stockage. Lors de la création d'un terminal d'équilibrage de charge, l'administrateur StorageGRID spécifie un numéro de port, si le terminal accepte les connexions HTTP ou HTTPS, le type de client (S3 ou Swift) qui utilisera le terminal ainsi que le certificat à utiliser pour les connexions HTTPS (le cas échéant). SWIFT les prend en charge "types de points finaux".

2. Configurer des réseaux clients non fiables.

   Si un administrateur StorageGRID configure le réseau client d'un nœud pour qu'il ne soit pas fiable, le nœud accepte uniquement les connexions entrantes sur le réseau client sur les ports explicitement configurés en tant que noeuds finaux d'équilibreur de charge.

3. Configurez les groupes haute disponibilité.

   Si l'administrateur crée un groupe haute disponibilité, les interfaces réseau de plusieurs nœuds d'administration ou nœuds de passerelle sont placées dans une configuration de sauvegarde active/active. Les connexions client sont établies à l'aide de l'adresse IP virtuelle du groupe haute disponibilité.

Voir "Options de configuration pour les groupes haute disponibilité" pour en savoir plus.

Résumé : adresses IP et ports pour les connexions client

Les applications client se connectent à StorageGRID en utilisant l'adresse IP d'un nœud de grid et le numéro de port d'un service sur ce nœud. Si des groupes de haute disponibilité sont configurés, les applications client peuvent se connecter en utilisant l'adresse IP virtuelle du groupe de haute disponibilité.

Informations requises pour établir des connexions client

Le tableau récapitule les différentes façons dont les clients peuvent se connecter à StorageGRID ainsi que les adresses IP et les ports utilisés pour chaque type de connexion. Voir "Adresses IP et ports pour les connexions client" Ou contactez votre administrateur StorageGRID pour plus d'informations.

Là où la connexion est établie	Service auquel le client se connecte	Adresse IP	Port
Groupe HAUTE DISPONIBILITÉ	Équilibreur de charge	Adresse IP virtuelle d'un groupe haute disponibilité	• Port du terminal de l'équilibreur de charge
Nœud d'administration	Équilibreur de charge	Adresse IP du nœud d'administration	• Port du terminal de l'équilibreur de charge
Nœud de passerelle	Équilibreur de charge	Adresse IP du nœud de passerelle	• Port du terminal de l'équilibreur de charge
Nœud de stockage	LDR	Adresse IP du nœud de stockage	Ports Swift par défaut : • HTTPS: 18083 • HTTP : 18085

Exemple

Pour connecter un client Swift au point de terminaison Load Balancer d'un groupe HA de nœuds de passerelle, utilisez une URL structurée comme indiqué ci-dessous :

- `https://VIP-of-HA-group:LB-endpoint-port`

Par exemple, si l'adresse IP virtuelle du groupe HA est 192.0.2.6 et que le numéro de port d'un noeud final Swift Load Balancer est 10444, un client Swift peut utiliser l'URL suivante pour se connecter à StorageGRID :

- `https://192.0.2.6:10444`

Il est possible de configurer un nom DNS pour l'adresse IP que les clients utilisent pour se connecter à StorageGRID. Contactez votre administrateur réseau local.

Choisissez d'utiliser des connexions HTTPS ou HTTP

Lorsque les connexions client sont effectuées à l'aide d'un noeud final Load Balancer, les connexions doivent être effectuées à l'aide du protocole (HTTP ou HTTPS) spécifié pour ce noeud final. Pour utiliser HTTP pour les connexions client aux nœuds de stockage, vous devez activer son utilisation.

Par défaut, lorsque les applications client se connectent aux nœuds de stockage, elles doivent utiliser le protocole HTTPS chiffré pour toutes les connexions. Vous pouvez éventuellement activer des connexions HTTP moins sécurisées en sélectionnant le "Activez HTTP pour les connexions de nœud de stockage" Dans Grid Manager. Par exemple, une application client peut utiliser HTTP lors du test de la connexion à un noeud de stockage dans un environnement non-production.

> Soyez prudent lorsque vous activez HTTP pour une grille de production car les requêtes et les réponses seront envoyées sans cryptage.

Si l'option **Activer HTTP pour les connexions de nœud de stockage** est sélectionnée, les clients doivent utiliser des ports HTTP différents de ceux utilisés pour HTTPS.

Testez votre connexion dans la configuration de l'API Swift

Vous pouvez utiliser l'interface de ligne de commandes Swift pour tester votre connexion au système StorageGRID et vérifier que vous pouvez lire et écrire des objets sur le système.

Avant de commencer

- Vous devez avoir téléchargé et installé python-swaftclient, le client de ligne de commande Swift.

  "SwiftStack: python-swftclient"

- Vous devez disposer d'un compte de locataire Swift dans le système StorageGRID.

Description de la tâche

Si vous n'avez pas configuré la sécurité, vous devez ajouter le `--insecure` marquer pour chacune de ces commandes.

Étapes

1. Interrogez l'URL d'information pour votre déploiement StorageGRID Swift :

   ```
   swift
   -U <Tenant_Account_ID:Account_User_Name>
   -K <User_Password>
   -A https://<FQDN | IP>:<Port>/info
   capabilities
   ```

   Cela suffit pour tester le fonctionnement de votre déploiement Swift. Pour tester davantage la configuration des comptes en stockant un objet, passez aux étapes supplémentaires.

2. Placer un objet dans le conteneur :

   ```
   touch test_object
   swift
   -U <Tenant_Account_ID:Account_User_Name>
   -K <User_Password>
   -A https://<FQDN | IP>:<Port>/auth/v1.0
   upload test_container test_object
   --object-name test_object
   ```

3. Procurez-vous le conteneur pour vérifier l'objet :

```
swift
-U <Tenant_Account_ID:Account_User_Name>
-K <User_Password>
-A https://<FQDN | IP>:<Port>/auth/v1.0
list test_container
```

4. Supprimez l'objet :

```
swift
-U <Tenant_Account_ID:Account_User_Name>
-K <User_Password>
-A https://<FQDN | IP>:<Port>/auth/v1.0
delete test_container test_object
```

5. Supprimez le conteneur :

```
swift
-U `<_Tenant_Account_ID:Account_User_Name_>`
-K `<_User_Password_>`
-A `\https://<_FQDN_ | _IP_>:<_Port_>/auth/v1.0'
delete test_container
```

Informations associées

"Créez et configurez des comptes de locataire Swift"

"Configuration de la sécurité pour l'API REST"

Opérations prises en charge par l'API REST Swift

Le système StorageGRID prend en charge la plupart des opérations dans l'API OpenStack Swift. Avant d'intégrer des clients de l'API REST Swift avec StorageGRID, consultez les informations d'implémentation pour les opérations des comptes, des conteneurs et des objets.

Opérations prises en charge par StorageGRID

Les opérations de l'API Swift suivantes sont prises en charge :

- "Opérations sur le compte"
- "Opérations sur les conteneurs"
- "Opérations sur l'objet"

En-têtes de réponse courants pour toutes les opérations

Le système StorageGRID implémente toutes les en-têtes courants pour les opérations prises en charge, comme défini par l'API de stockage objet OpenStack Swift v1.

Informations associées

"OpenStack : API de stockage objet"

Terminaux API Swift pris en charge

StorageGRID prend en charge les points de terminaison de l'API Swift suivants : l'URL info, l'URL d'authentification et l'URL de stockage.

URL info

Vous pouvez déterminer les capacités et les limites de l'implémentation de StorageGRID Swift en émettant une demande GET à l'URL de base Swift avec le chemin /info.

```
https://FQDN | Node IP:Swift Port/info/
```

Dans la demande :

- *FQDN* est le nom de domaine complet.
- *Node IP* Est l'adresse IP du nœud de stockage ou du nœud de passerelle sur le réseau StorageGRID.
- *Swift Port* Est le numéro de port utilisé pour les connexions API Swift sur le nœud de stockage ou le nœud de passerelle.

Par exemple, l'URL d'information suivante demande des informations à un noeud de stockage avec l'adresse IP 10.99.106.103 et le port 18083.

```
https://10.99.106.103:18083/info/
```

La réponse inclut les fonctionnalités de l'implémentation Swift sous forme de dictionnaire JSON. Un outil client peut analyser la réponse JSON pour déterminer les fonctionnalités de l'implémentation et les utiliser comme contraintes pour les opérations de stockage ultérieures.

La mise en œuvre de StorageGRID de Swift permet un accès non authentifié à l'URL info.

URL d'authentification

Un client peut utiliser l'URL d'authentification Swift pour s'authentifier en tant qu'utilisateur de compte de locataire.

```
https://FQDN | Node IP:Swift Port/auth/v1.0/
```

Vous devez fournir l'ID de compte de tenant, le nom d'utilisateur et le mot de passe comme paramètres dans le `X-Auth-User` et `X-Auth-Key` en-têtes de demande, comme suit :

```
X-Auth-User: Tenant_Account_ID:Username

X-Auth-Key: Password
```

Dans les en-têtes de demande :

- *Tenant_Account_ID* Est l'ID de compte attribué par StorageGRID lors de la création du locataire Swift. Il s'agit du même ID de compte de locataire que celui utilisé sur la page de connexion du Gestionnaire de locataires.
- *Username* Est le nom d'un utilisateur locataire qui a été créé dans le Gestionnaire de tenant. Cet utilisateur doit appartenir à un groupe disposant de l'autorisation Administrateur Swift. L'utilisateur root du locataire ne peut pas être configuré pour utiliser l'API REST Swift.

  Si la fédération des identités est activée pour le compte de tenant, indiquez le nom d'utilisateur et le mot de passe de l'utilisateur fédéré à partir du serveur LDAP. Vous pouvez également indiquer le nom de domaine de l'utilisateur LDAP. Par exemple :

  `X-Auth-User: Tenant_Account_ID:Username@Domain_Name`

- *Password* est le mot de passe de l'utilisateur tenant. Les mots de passe utilisateur sont créés et gérés dans le Gestionnaire de locataires.

La réponse à une demande d'authentification réussie renvoie une URL de stockage et un jeton d'authentification, comme suit :

`X-Storage-Url: https://FQDN | Node_IP:Swift_Port/v1/Tenant_Account_ID`

`X-Auth-Token: token`

`X-Storage-Token: token`

Par défaut, le jeton est valide pendant 24 heures à compter de l'heure de génération.

Des jetons sont générés pour un compte de locataire spécifique. Un jeton valide pour un compte n'autorise pas un utilisateur à accéder à un autre compte.

URL du stockage

Une application client peut émettre des appels de l'API REST Swift pour exécuter des opérations de compte, conteneur et objet prises en charge sur un nœud de passerelle ou un nœud de stockage. Les demandes de stockage sont adressées à l'URL de stockage renvoyée dans la réponse d'authentification. La demande doit également inclure l'en-tête X-Auth-Token et la valeur renvoyée par la demande d'autorisation.

`https://FQDN | IP:Swift_Port/v1/Tenant_Account_ID`

`[/container][/object]`

`X-Auth-Token: token`

Certains en-têtes de réponse de stockage contenant des statistiques d'utilisation peuvent ne pas refléter les chiffres précis des objets récemment modifiés. L'affichage des nombres précis dans ces en-têtes peut prendre quelques minutes.

Les en-têtes de réponse suivants pour les opérations de compte et de conteneur sont des exemples de ceux qui contiennent des statistiques d'utilisation :

- `X-Account-Bytes-Used`
- `X-Account-Object-Count`

- `X-Container-Bytes-Used`
- `X-Container-Object-Count`

Informations associées

"Configurez les comptes et les connexions des locataires"

"Opérations sur le compte"

"Opérations sur les conteneurs"

"Opérations sur l'objet"

Opérations sur le compte

Les opérations de l'API Swift suivantes sont effectuées sur les comptes.

OBTENIR un compte

Cette opération récupère la liste de conteneurs associée aux statistiques d'utilisation du compte et du compte.

Le paramètre de demande suivant est requis :

- `Account`

L'en-tête de demande suivant est requis :

- `X-Auth-Token`

Les paramètres de requête pris en charge suivants sont facultatifs :

- `Delimiter`
- `End_marker`
- `Format`
- `Limit`
- `Marker`
- `Prefix`

Une exécution réussie renvoie les en-têtes suivants avec une réponse « HTTP/1.1 204 aucun contenu » si le compte est trouvé et qu'aucun conteneur n'est vide, ou une réponse « HTTP/1.1 200 OK » si le compte est trouvé et que la liste de conteneurs n'est pas vide :

- `Accept-Ranges`
- `Content-Length`
- `Content-Type`
- `Date`
- `X-Account-Bytes-Used`
- `X-Account-Container-Count`

- `X-Account-Object-Count`
- `X-Timestamp`
- `X-Trans-Id`

Compte PRINCIPAL

Cette opération récupère les informations et les statistiques du compte à partir d'un compte Swift.

Le paramètre de demande suivant est requis :

- `Account`

L'en-tête de demande suivant est requis :

- `X-Auth-Token`

Une exécution réussie renvoie les en-têtes suivants avec une réponse « HTTP/1.1 204 No Content » :

- `Accept-Ranges`
- `Content-Length`
- `Date`
- `X-Account-Bytes-Used`
- `X-Account-Container-Count`
- `X-Account-Object-Count`
- `X-Timestamp`
- `X-Trans-Id`

Informations associées

"Surveiller et auditer les opérations"

Opérations sur les conteneurs

StorageGRID prend en charge un maximum de 1,000 conteneurs par compte Swift. Les opérations d'API Swift suivantes sont effectuées sur les conteneurs.

SUPPRIMER le conteneur

Cette opération supprime un conteneur vide d'un compte Swift dans un système StorageGRID.

Les paramètres de demande suivants sont requis :

- `Account`
- `Container`

L'en-tête de demande suivant est requis :

- `X-Auth-Token`

Une exécution réussie renvoie les en-têtes suivants avec une réponse "HTTP/1.1 204 No Content" :

- `Content-Length`
- `Content-Type`
- `Date`
- `X-Trans-Id`

CONTENEUR

Cette opération récupère la liste d'objets associée au conteneur, ainsi que les statistiques et métadonnées de conteneur dans un système StorageGRID.

Les paramètres de demande suivants sont requis :

- `Account`
- `Container`

L'en-tête de demande suivant est requis :

- `X-Auth-Token`

Les paramètres de requête pris en charge suivants sont facultatifs :

- `Delimiter`
- `End_marker`
- `Format`
- `Limit`
- `Marker`
- `Path`
- `Prefix`

Une exécution réussie renvoie les en-têtes suivants avec une réponse « HTTP/1.1 200 Success » ou « HTTP/1.1 204 No Content » :

- `Accept-Ranges`
- `Content-Length`
- `Content-Type`
- `Date`
- `X-Container-Bytes-Used`
- `X-Container-Object-Count`
- `X-Timestamp`
- `X-Trans-Id`

Conteneur DE TÊTE

Cette opération récupère les statistiques du conteneur et les métadonnées d'un système StorageGRID.

Les paramètres de demande suivants sont requis :

- `Account`
- `Container`

L'en-tête de demande suivant est requis :

- `X-Auth-Token`

Une exécution réussie renvoie les en-têtes suivants avec une réponse "HTTP/1.1 204 No Content" :

- `Accept-Ranges`
- `Content-Length`
- `Date`
- `X-Container-Bytes-Used`
- `X-Container-Object-Count`
- `X-Timestamp`
- `X-Trans-Id`

PLACER le conteneur

Cette opération crée un conteneur pour un compte dans un système StorageGRID.

Les paramètres de demande suivants sont requis :

- `Account`
- `Container`

L'en-tête de demande suivant est requis :

- `X-Auth-Token`

Une exécution réussie renvoie les en-têtes suivants avec une réponse « HTTP/1.1 201 created » ou « HTTP/1.1 202 Accepted » (si le conteneur existe déjà sous ce compte) :

- `Content-Length`
- `Date`
- `X-Timestamp`
- `X-Trans-Id`

Un nom de conteneur doit être unique dans le namespace StorageGRID. Si le conteneur existe sous un autre compte, l'en-tête suivant est renvoyé : « HTTP/1.1 409 Conflict ».

Informations associées

"Surveiller et auditer les opérations"

Opérations sur l'objet

Les opérations suivantes de l'API Swift sont effectuées sur des objets. Ces opérations peuvent être suivies dans "Journal d'audit StorageGRID".

SUPPRIMER l'objet

Cette opération supprime le contenu et les métadonnées d'un objet du système StorageGRID.

Les paramètres de demande suivants sont requis :

- `Account`
- `Container`
- `Object`

L'en-tête de demande suivant est requis :

- `X-Auth-Token`

Une exécution réussie renvoie les en-têtes de réponse suivants avec un `HTTP/1.1 204 No Content` réponse :

- `Content-Length`
- `Content-Type`
- `Date`
- `X-Trans-Id`

Lors du traitement d'une requête DE SUPPRESSION d'objet, StorageGRID tente de supprimer immédiatement toutes les copies de l'objet des emplacements stockés. En cas de succès, StorageGRID renvoie immédiatement une réponse au client. Si toutes les copies ne peuvent pas être supprimées dans les 30 secondes (par exemple, parce qu'un emplacement est temporairement indisponible), StorageGRID met les copies en file d'attente pour suppression et indique que le client a réussi.

Pour plus d'informations, voir "Comment supprimer les objets".

OBJET GET

Cette opération récupère le contenu de l'objet et obtient ses métadonnées depuis un système StorageGRID.

Les paramètres de demande suivants sont requis :

- `Account`
- `Container`
- `Object`

L'en-tête de demande suivant est requis :

- `X-Auth-Token`

Les en-têtes de demande suivants sont facultatifs :

- `Accept-Encoding`
- `If-Match`
- `If-Modified-Since`
- `If-None-Match`
- `If-Unmodified-Since`
- `Range`

Une exécution réussie renvoie les en-têtes suivants avec un `HTTP/1.1 200 OK` réponse :

- `Accept-Ranges`
- `Content-Disposition`, retourné seulement si `Content-Disposition` les métadonnées ont été définies
- `Content-Encoding`, retourné seulement si `Content-Encoding` les métadonnées ont été définies
- `Content-Length`
- `Content-Type`
- `Date`
- `ETag`
- `Last-Modified`
- `X-Timestamp`
- `X-Trans-Id`

Objet TÊTE

Cette opération récupère les métadonnées et les propriétés d'un objet ingéré à partir d'un système StorageGRID.

Les paramètres de demande suivants sont requis :

- `Account`
- `Container`
- `Object`

L'en-tête de demande suivant est requis :

- `X-Auth-Token`

Une exécution réussie renvoie les en-têtes suivants avec une réponse "HTTP/1.1 200 OK" :

- `Accept-Ranges`
- `Content-Disposition`, retourné seulement si `Content-Disposition` les métadonnées ont été définies

- `Content-Encoding`, retourné seulement si `Content-Encoding` les métadonnées ont été définies
- `Content-Length`
- `Content-Type`
- `Date`
- `ETag`
- `Last-Modified`
- `X-Timestamp`
- `X-Trans-Id`

PLACER l'objet

Cette opération crée un nouvel objet avec des données et des métadonnées, ou remplace un objet existant par des données et des métadonnées dans un système StorageGRID.

StorageGRID prend en charge les objets jusqu'à 5 Tio (5,497,558,138,880 octets).

> Les demandes contradictoires des clients, telles que deux clients qui écrivent sur la même clé, sont résolues sur une base de « derniers-victoires ». Le moment auquel l'évaluation « derniers-victoires » est basé sur la date à laquelle le système StorageGRID remplit une demande donnée et non sur la date à laquelle les clients Swift entament une opération.

Les paramètres de demande suivants sont requis :

- `Account`
- `Container`
- `Object`

L'en-tête de demande suivant est requis :

- `X-Auth-Token`

Les en-têtes de demande suivants sont facultatifs :

- `Content-Disposition`
- `Content-Encoding`

  Ne pas utiliser de moucheté `Content-Encoding` Si la règle ILM appliquée à un objet filtre les objets en fonction de leur taille et utilise le placement synchrone à l'ingestion (options équilibrées ou strictes pour le comportement d'ingestion).

- `Transfer-Encoding`

  N'utilisez pas de compression ou de déboucheté `Transfer-Encoding` Si la règle ILM appliquée à un objet filtre les objets en fonction de leur taille et utilise le placement synchrone à l'ingestion (options équilibrées ou strictes pour le comportement d'ingestion).

- `Content-Length`

Si une règle ILM filtre les objets par taille et utilise le placement synchrone lors de l'ingestion, vous devez spécifier `Content-Length`.

> Si vous ne suivez pas ces directives pour `Content-Encoding`, `Transfer-Encoding`, et `Content-Length`, StorageGRID doit enregistrer l'objet avant de déterminer la taille de l'objet et d'appliquer la règle ILM. En d'autres termes, StorageGRID doit créer par défaut des copies intermédiaires d'un objet à l'entrée. C'est-à-dire que StorageGRID doit utiliser l'option de double validation pour le comportement d'ingestion.

Pour plus d'informations sur le placement synchrone et les règles ILM, voir "Options de protection des données pour l'ingestion".

- `Content-Type`
- `ETag`
- `X-Object-Meta-<name\>` (métadonnées liées aux objets)

  Si vous souhaitez utiliser l'option **temps de création défini par l'utilisateur** comme heure de référence pour une règle ILM, vous devez stocker la valeur dans un en-tête défini par l'utilisateur nommé `X-Object-Meta-Creation-Time`. Par exemple :

  ```
  X-Object-Meta-Creation-Time: 1443399726
  ```

  Ce champ est évalué en secondes depuis le 1er janvier 1970.

- `X-Storage-Class: reduced_redundancy`

  Cet en-tête affecte le nombre de copies d'objet créées par StorageGRID si la règle ILM correspondant à l'objet ingéré spécifie le comportement d'ingestion de la double validation ou de l'équilibrage.

  - **Double commit** : si la règle ILM spécifie l'option de double validation pour le comportement d'ingestion, StorageGRID crée une copie intermédiaire unique lors de l'ingestion de l'objet (simple commit).
  - **Équilibré** : si la règle ILM spécifie l'option équilibrée, StorageGRID effectue une seule copie intermédiaire uniquement si le système ne peut pas immédiatement effectuer toutes les copies spécifiées dans la règle. Si StorageGRID peut effectuer un placement synchrone, cet en-tête n'a aucun effet.

    Le `reduced_redundancy` L'en-tête est le plus utilisé lorsque la règle ILM correspondant à l'objet crée une copie répliquée unique. Dans ce cas, utilisez `reduced_redundancy` élimine la création et la suppression inutiles d'une copie d'objet supplémentaire pour chaque opération d'ingestion.

    À l'aide du `reduced_redundancy` l'en-tête n'est pas recommandé dans d'autres cas, car il augmente le risque de perte de données d'objet lors de l'ingestion. Vous risquez par exemple de perdre des données si une seule copie est initialement stockée sur un nœud de stockage qui échoue avant l'évaluation du ILM.

Le fait d'avoir une seule copie répliquée pendant une période donnée présente un risque de perte permanente des données. Si une seule copie répliquée d'un objet existe, cet objet est perdu en cas de défaillance ou d'erreur importante d'un noeud de stockage. De plus, lors des procédures de maintenance telles que les mises à niveau, l'accès à l'objet est temporairement perdu.

Notez que la spécification `reduced_redundancy` l'impact sur le nombre de copies créées uniquement lors de l'ingestion d'un objet. Elle n'affecte pas le nombre de copies de l'objet lorsque celui-ci est évalué par la règle ILM active et n'entraîne pas le stockage des données avec des niveaux de redondance inférieurs dans le système StorageGRID.

Une exécution réussie renvoie les en-têtes suivants avec une réponse "HTTP/1.1 201 created" :

- `Content-Length`
- `Content-Type`
- `Date`
- `ETag`
- `Last-Modified`
- `X-Trans-Id`

Demande D'OPTIONS

La demande D'OPTIONS vérifie la disponibilité d'un service Swift individuel. La demande D'OPTIONS est traitée par le nœud de stockage ou le nœud passerelle spécifié dans l'URL.

Méthode DES OPTIONS

Par exemple, les applications client peuvent émettre une demande D'OPTIONS vers le port Swift sur un nœud de stockage, sans fournir d'informations d'authentification Swift, pour déterminer si le nœud de stockage est disponible. Vous pouvez utiliser cette requête pour la surveillance ou permettre aux équilibreurs de charge externes d'identifier lorsqu'un nœud de stockage est arrêté.

Lorsqu'elle est utilisée avec l'URL info ou l'URL de stockage, la méthode OPTIONS renvoie une liste de verbes pris en charge pour l'URL donnée (par exemple, HEAD, GET, OPTIONS et PUT). La méthode D'OPTIONS ne peut pas être utilisée avec l'URL d'authentification.

Le paramètre de demande suivant est requis :

- `Account`

Les paramètres de demande suivants sont facultatifs :

- `Container`
- `Object`

Une exécution réussie renvoie les en-têtes suivants avec une réponse « HTTP/1.1 204 No Content ». La demande D'OPTIONS à l'URL de stockage ne nécessite pas que la cible existe.

- `Allow` (Une liste de verbes pris en charge pour l'URL donnée, par exemple, HEAD, GET, OPTIONS, Et PUT)
- `Content-Length`
- `Content-Type`
- `Date`
- `X-Trans-Id`

Informations associées

"Terminaux API Swift pris en charge"

Réponse aux erreurs des opérations de l'API Swift

La compréhension des réponses d'erreur possibles peut vous aider à résoudre les problèmes.

Les codes d'état HTTP suivants peuvent être renvoyés lorsque des erreurs se produisent au cours d'une opération :

Nom de l'erreur Swift	Statut HTTP
AccountNameToolong, ContainerNameToolong, HeaderTooBig, InvalidContainerName, InvalidRequest, InvalidURI, MetadaNameToolong, MetadaValueTooBig, MissingSecurityHeader, ObjectNameToolong, TooManyContainers, TooManyMetadaItems, TotalMetadaTooLarge	400 demande erronée
AccessDenied	403 interdit
ContainerNotEmpty, ContainerAlreadyExists	409 conflit
Erreur interne	500 erreur interne du serveur
InvalidRange	416 Plage demandée non satisfiable
MethodNotAlldue	405 méthode non autorisée
MissingContentLength	411 longueur requise
NOTFOUND	404 introuvable
Note d'implémentation	501 non mis en œuvre
Pré-conditionFailed	412 Echec de la condition préalable
ResourceNotFound	404 introuvable

Nom de l'erreur Swift	Statut HTTP
Non autorisé	401 non autorisé
Entité intraitableEntity	422 entité impossible à traiter

Opérations de l'API REST StorageGRID Swift

Des opérations sont ajoutées à l'API REST Swift qui sont spécifiques au système StorageGRID.

DEMANDE DE cohérence du conteneur

"Contrôles de cohérence" Équilibre entre disponibilité des objets et cohérence entre ces objets sur différents nœuds et sites de stockage. La demande DE cohérence DU conteneur GET vous permet de déterminer le niveau de cohérence appliqué à un conteneur particulier.

Demande

En-tête HTTP de demande	Description
X-Auth-Token	Spécifie le jeton d'authentification Swift pour le compte à utiliser pour la demande.
x-ntap-sg-cohérence	Spécifie le type de demande, où `true` = COHÉRENCE GARANTIE entre les conteneurs, et `false` = CONTENEUR GET.
Hôte	Nom d'hôte auquel la demande est dirigée.

Exemple de demande

```
GET /v1/28544923908243208806/Swift container
X-Auth-Token: SGRD_3a877009a2d24cb1801587bfa9050f29
x-ntap-sg-consistency: true
Host: test.com
```

Réponse

En-tête HTTP de réponse	Description
Date	La date et l'heure de la réponse.
Connexion	Indique si la connexion au serveur est ouverte ou fermée.
X-Trans-ID	Identifiant de transaction unique pour la demande.

En-tête HTTP de réponse	Description
Longueur-contenu	Longueur du corps de réponse.
x-ntap-sg-cohérence	Niveau de contrôle de cohérence appliqué au conteneur. Les valeurs suivantes sont prises en charge : **Tous** : tous les nœuds reçoivent les données immédiatement ou la demande échouera. **Forte-global**: Garantit la cohérence lecture-après-écriture pour toutes les demandes client sur tous les sites. **Site fort** : garantit la cohérence de lecture après écriture pour toutes les demandes de clients au sein d'un site. **Read-after-New-write**: (Par défaut) fournit la cohérence lecture-après-écriture pour les nouveaux objets et éventuellement la cohérence pour les mises à jour d'objets. Offre une haute disponibilité et une protection des données garanties. Recommandé dans la plupart des cas. **Disponible** : assure la cohérence finale pour les nouveaux objets et les mises à jour d'objets. Pour les compartiments S3, utilisez uniquement si nécessaire (par exemple, pour un compartiment qui contient des valeurs de journal rarement lues ou pour les opérations HEAD ou GET sur des clés qui n'existent pas). Non pris en charge pour les compartiments FabricPool S3.

Exemple de réponse

```
HTTP/1.1 204 No Content
Date: Sat, 29 Nov 2015 01:02:18 GMT
Connection: CLOSE
X-Trans-Id: 1936575373
Content-Length: 0
x-ntap-sg-consistency: strong-site
```

REQUÊTE de cohérence du conteneur

La demande DE cohérence PUT dans le conteneur vous permet de spécifier le niveau de cohérence à appliquer aux opérations effectuées dans un conteneur. Par défaut, les nouveaux conteneurs sont créés à l'aide du niveau de cohérence « read-after-New-write ».

Demande

En-tête HTTP de demande	Description
X-Auth-Token	Jeton d'authentification Swift pour le compte à utiliser pour la demande.

En-tête HTTP de demande	Description
x-ntap-sg-cohérence	Niveau de contrôle de cohérence à appliquer aux opérations sur le conteneur. Les valeurs suivantes sont prises en charge : **Tous** : tous les nœuds reçoivent les données immédiatement ou la demande échouera. **Forte-global**: Garantit la cohérence lecture-après-écriture pour toutes les demandes client sur tous les sites. **Site fort** : garantit la cohérence de lecture après écriture pour toutes les demandes de clients au sein d'un site. **Read-after-New-write**: (Par défaut) fournit la cohérence lecture-après-écriture pour les nouveaux objets et éventuellement la cohérence pour les mises à jour d'objets. Offre une haute disponibilité et une protection des données garanties. Recommandé dans la plupart des cas. **Disponible** : assure la cohérence finale pour les nouveaux objets et les mises à jour d'objets. Pour les compartiments S3, utilisez uniquement si nécessaire (par exemple, pour un compartiment qui contient des valeurs de journal rarement lues ou pour les opérations HEAD ou GET sur des clés qui n'existent pas). Non pris en charge pour les compartiments FabricPool S3.
`Host`	Nom d'hôte auquel la demande est dirigée.

Interaction des contrôles de cohérence et des règles ILM pour la protection des données

À la fois de votre choix "contrôle de la cohérence" De plus, votre règle ILM affecte la façon dont les objets sont protégés. Ces paramètres peuvent interagir.

Par exemple, le contrôle de cohérence utilisé lorsqu'un objet est stocké affecte le placement initial des métadonnées d'objet, tandis que l' "comportement d'ingestion" Cette case à cocher affecte le placement initial des copies d'objet. Étant donné que StorageGRID nécessite l'accès aux métadonnées d'un objet et à ses données pour répondre aux demandes client, la sélection de niveaux de protection correspondant au niveau de cohérence et au comportement d'ingestion permet d'améliorer la protection des données initiale et de mieux prévoir les réponses du système.

Exemple d'interaction du contrôle de cohérence et de la règle ILM

Supposons que vous disposez d'une grille à deux sites avec la règle ILM suivante et le paramètre de niveau de cohérence suivant :

- **Règle ILM** : créez deux copies d'objet, une sur le site local et une sur un site distant. Le comportement d'entrée strict est sélectionné.
- **Niveau de cohérence**: "Sept-global" (les métadonnées d'objet sont immédiatement distribuées à tous les sites).

Lorsqu'un client stocke un objet dans la grille, StorageGRID effectue à la fois des copies d'objet et distribue les métadonnées aux deux sites avant de rétablir la réussite du client.

L’objet est entièrement protégé contre la perte au moment du message d’ingestion. Par exemple, si le site local est perdu peu de temps après l’ingestion, des copies des données de l’objet et des métadonnées de l’objet existent toujours sur le site distant. L’objet est entièrement récupérable.

Si vous utilisez à la place la même règle ILM et le niveau de cohérence "sept-site", le client peut recevoir un message de réussite après la réplication des données d’objet vers le site distant, mais avant que les métadonnées d’objet ne soient distribuées sur ce site. Dans ce cas, le niveau de protection des métadonnées d’objet ne correspond pas au niveau de protection des données d’objet. Si le site local est perdu peu de temps après l’ingestion, les métadonnées d’objet sont perdues. Impossible de récupérer l’objet.

L’interdépendance entre les niveaux de cohérence et les règles ILM peut être complexe. Contactez NetApp si vous avez besoin d’aide.

Exemple de demande

```
PUT /v1/28544923908243208806/_Swift container_
X-Auth-Token: SGRD_3a877009a2d24cb1801587bfa9050f29
x-ntap-sg-consistency: strong-site
Host: test.com
```

Réponse

En-tête HTTP de réponse	Description
`Date`	La date et l’heure de la réponse.
`Connection`	Indique si la connexion au serveur est ouverte ou fermée.
`X-Trans-Id`	Identifiant de transaction unique pour la demande.
`Content-Length`	Longueur du corps de réponse.

Exemple de réponse

```
HTTP/1.1 204 No Content
Date: Sat, 29 Nov 2015 01:02:18 GMT
Connection: CLOSE
X-Trans-Id: 1936575373
Content-Length: 0
```

Configuration de la sécurité pour l’API REST

Il est recommandé de passer en revue les mesures de sécurité mises en œuvre pour l’API REST et de comprendre comment sécuriser votre système.

Comment StorageGRID assure la sécurité pour l'API REST

Vous devez comprendre comment le système StorageGRID implémente la sécurité, l'authentification et l'autorisation pour l'API REST.

StorageGRID utilise les mesures de sécurité suivantes.

- Les communications client avec le service Load Balancer utilisent HTTPS si HTTPS est configuré pour le noeud final Load Balancer.

  Lorsque vous "configurez un terminal d'équilibrage de charge", HTTP peut être activé en option. Par exemple, vous pouvez utiliser HTTP à des fins de test ou autres que la production.

- Par défaut, StorageGRID utilise HTTPS pour les communications client avec les nœuds de stockage.

  En option, "Activez HTTP pour ces connexions". Par exemple, vous pouvez utiliser HTTP à des fins de test ou autres que la production.

- Les communications entre StorageGRID et le client sont chiffrées à l'aide de TLS.
- Les communications entre le service Load Balancer et les nœuds de stockage dans la grille sont cryptées que le terminal de l'équilibreur de charge soit configuré pour accepter les connexions HTTP ou HTTPS.
- Les clients doivent fournir des en-têtes d'authentification HTTP à StorageGRID pour effectuer des opérations d'API REST.

Certificats de sécurité et applications client

Les clients peuvent se connecter au service Load Balancer sur les nœuds de passerelle ou les nœuds d'administration, directement aux nœuds de stockage.

Dans tous les cas, les applications client peuvent établir des connexions TLS à l'aide d'un certificat de serveur personnalisé chargé par l'administrateur de la grille ou d'un certificat généré par le système StorageGRID :

- Lorsque les applications client se connectent au service Load Balancer, elles le font à l'aide du certificat configuré pour le noeud final de l'équilibreur de charge spécifique utilisé pour établir la connexion. Chaque noeud final possède son propre certificat, qui est soit un certificat de serveur personnalisé chargé par l'administrateur de la grille, soit un certificat que l'administrateur de la grille a généré dans StorageGRID lors de la configuration du noeud final.
- Lorsque les applications client se connectent directement à un nœud de stockage, elles utilisent les certificats de serveur générés par le système qui ont été générés pour les nœuds de stockage lors de l'installation du système StorageGRID (qui sont signés par l'autorité de certification du système), ou un seul certificat de serveur personnalisé fourni pour la grille par un administrateur de grille.

Les clients doivent être configurés pour approuver l'autorité de certification qui a signé le certificat qu'ils utilisent pour établir des connexions TLS.

Voir "configuration des terminaux d'équilibrage de charge" et "ajout d'un seul certificat de serveur personnalisé" Pour les connexions TLS directement aux nœuds de stockage.

Récapitulatif

Le tableau suivant montre comment les problèmes de sécurité sont implémentés dans les API REST S3 et Swift :

Problème de sécurité	Implémentation pour l'API REST
Sécurité de la connexion	TLS
Authentification du serveur	Certificat de serveur X.509 signé par l'autorité de certification du système ou certificat de serveur personnalisé fourni par l'administrateur
Authentification client	• S3 : compte S3 (ID de clé d'accès et clé d'accès secrète) • SWIFT : compte Swift (nom d'utilisateur et mot de passe)
Autorisation du client	• S3 : propriété des compartiments et toutes les règles de contrôle d'accès applicables • SWIFT : accès aux rôles d'administrateur

Algorithmes de hachage et de cryptage pris en charge pour les bibliothèques TLS

Le système StorageGRID prend en charge un ensemble limité de suites de chiffrement que les applications clientes peuvent utiliser lors de l'établissement d'une session TLS (transport Layer Security). Pour configurer les chiffrements, accédez à **CONFIGURATION** > **sécurité** > **Paramètres de sécurité** et sélectionnez **règles TLS et SSH**.

Versions supportées de TLS

StorageGRID supporte TLS 1.2 et TLS 1.3.

SSLv3 et TLS 1.1 (ou versions antérieures) ne sont plus pris en charge.

Informations associées

"Configurez les comptes et les connexions des locataires"

Surveiller et auditer les opérations

Vous pouvez surveiller les charges de travail et l'efficacité des opérations client en visualisant les tendances de transaction pour l'ensemble du grid ou pour des nœuds spécifiques. Vous pouvez utiliser des messages d'audit pour surveiller les opérations et les transactions des clients.

Contrôler les taux d'entrée et de récupération des objets

Vous pouvez surveiller les taux d'entrée et de récupération des objets, ainsi que les mesures relatives au nombre d'objets, aux requêtes et à la vérification. Vous pouvez afficher le nombre de tentatives de lecture, d'écriture et de modification d'objets du système StorageGRID ayant échoué et réussies par les applications client.

Étapes

1. Connectez-vous au Grid Manager à l'aide d'un "navigateur web pris en charge".

2. Sur le tableau de bord, sélectionnez **Performance** > **S3 Operations** ou **Performance** > **Swift Operations**.

   Cette section récapitule le nombre d'opérations client effectuées par votre système StorageGRID. La moyenne des débits de protocole est calculée au cours des deux dernières minutes.

3. Sélectionnez **NOEUDS**.
4. Dans la page d'accueil noeuds (niveau de déploiement), cliquez sur l'onglet **Load Balancer**.

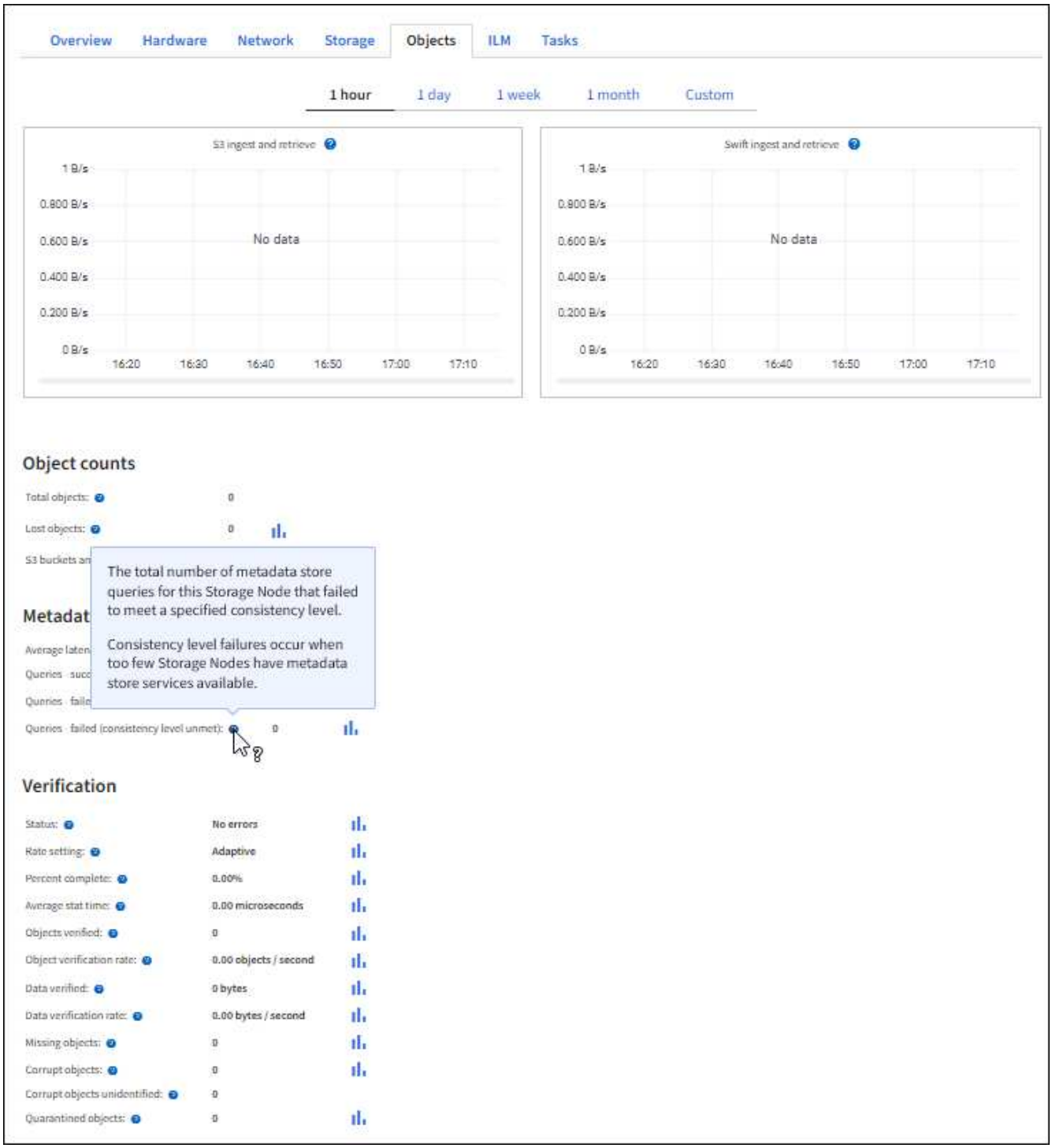
   Les graphiques présentent les tendances de tout le trafic client dirigé vers les terminaux d'équilibreur de charge dans la grille. Vous pouvez sélectionner un intervalle de temps en heures, jours, semaines, mois ou années, vous pouvez également appliquer un intervalle personnalisé.

5. Dans la page d'accueil noeuds (niveau de déploiement), cliquez sur l'onglet **objets**.

   Le graphique montre les taux d'entrée et de récupération de l'intégralité de votre système StorageGRID en octets par seconde et en octets totaux. Vous pouvez sélectionner un intervalle de temps en heures, jours, semaines, mois ou années, vous pouvez également appliquer un intervalle personnalisé.

6. Pour afficher les informations relatives à un noeud de stockage particulier, sélectionnez-le dans la liste de gauche, puis cliquez sur l'onglet **objets**.

   Le tableau affiche les taux d'entrée et de récupération de l'objet pour ce nœud de stockage. L'onglet inclut également des mesures pour le nombre d'objets, les requêtes et la vérification. Vous pouvez cliquer sur les étiquettes pour afficher les définitions de ces mesures.



7. Si vous voulez encore plus de détails :
   a. Sélectionnez **SUPPORT** > **Outils** > **topologie de grille**.
   b. Sélectionnez ***site*** > **Présentation** > **main**.

      La section opérations d'API affiche un récapitulatif des informations sur l'ensemble de la grille.

   c. Sélectionnez ***Storage Node*** > **LDR** > ***client application*** > **Présentation** > **main**

      La section opérations affiche un récapitulatif des informations sur le nœud de stockage sélectionné.

Examiner les journaux d'audit

Les messages d'audit sont générés par les services StorageGRID et stockés dans des fichiers journaux texte. Des messages d'audit spécifiques aux API dans les journaux d'audit fournissent des données stratégiques de sécurité, d'exploitation et de surveillance des performances qui vous aideront à évaluer l'état de votre système.

Avant de commencer

- Vous devez disposer d'autorisations d'accès spécifiques.
- Vous devez avoir le `Passwords.txt` fichier.
- Vous devez connaître l'adresse IP d'un nœud d'administration.

Description de la tâche

Le "fichier journal d'audit actif" est nommé `audit.log`, Et il est stocké sur des nœuds d'administration.

Une fois par jour, le fichier audit.log actif est enregistré et un nouveau fichier audit.log est lancé. Le nom du fichier enregistré indique quand il a été enregistré, au format `yyyy-mm-dd.txt`.

Après un jour, le fichier enregistré est compressé et renommé, au format `yyyy-mm-dd.txt.gz`, qui conserve la date originale.

Cet exemple montre le fichier audit.log actif, le fichier de la veille (2018-04-15.txt) et le fichier compressé de la veille (`2018-04-14.txt.gz`).

```
audit.log
2018-04-15.txt
2018-04-14.txt.gz
```

Étapes

1. Connectez-vous à un nœud d'administration :
   a. Saisissez la commande suivante : `ssh admin@primary_Admin_Node_IP`
   b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
   c. Entrez la commande suivante pour passer à la racine : `su -`
   d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

   Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.
2. Accédez au répertoire contenant les fichiers journaux d'audit :`cd /var/local/audit/export`
3. Afficher le fichier journal d'audit actuel ou enregistré, selon les besoins.

Les opérations Swift sont suivies dans les journaux d'audit

Toutes les opérations de SUPPRESSION de stockage, D'OBTENTION, DE TÊTE, DE POST et DE PUT réussies sont suivies dans le "Journal d'audit StorageGRID". Les échecs ne sont pas consignés, ni les demandes d'informations, d'authentification ou D'OPTIONS.

Les informations sont suivies pour les opérations Swift suivantes.

Opérations sur le compte

- "OBTENIR un compte"
- "Compte PRINCIPAL"

Opérations sur les conteneurs

- "SUPPRIMER le conteneur"
- "CONTENEUR"
- "Conteneur DE TÊTE"
- "PLACER le conteneur"

Opérations sur l’objet

- "SUPPRIMER l’objet"
- "OBJET GET"
- "Objet TÊTE"
- "PLACER l’objet"

Surveiller et résoudre les problèmes

Surveiller le système StorageGRID

Surveillance d'un système StorageGRID : présentation

Suivez ces instructions pour surveiller un système StorageGRID et évaluer les problèmes susceptibles de se produire.

Ces instructions décrivent comment utiliser le Gestionnaire de grille pour surveiller un système StorageGRID. Vous apprendrez quelles informations vous devez surveiller régulièrement, comment gérer les alertes et les alarmes existantes, comment utiliser SNMP pour la surveillance et comment obtenir des données StorageGRID supplémentaires, notamment des mesures et des diagnostics.

Avant de commencer

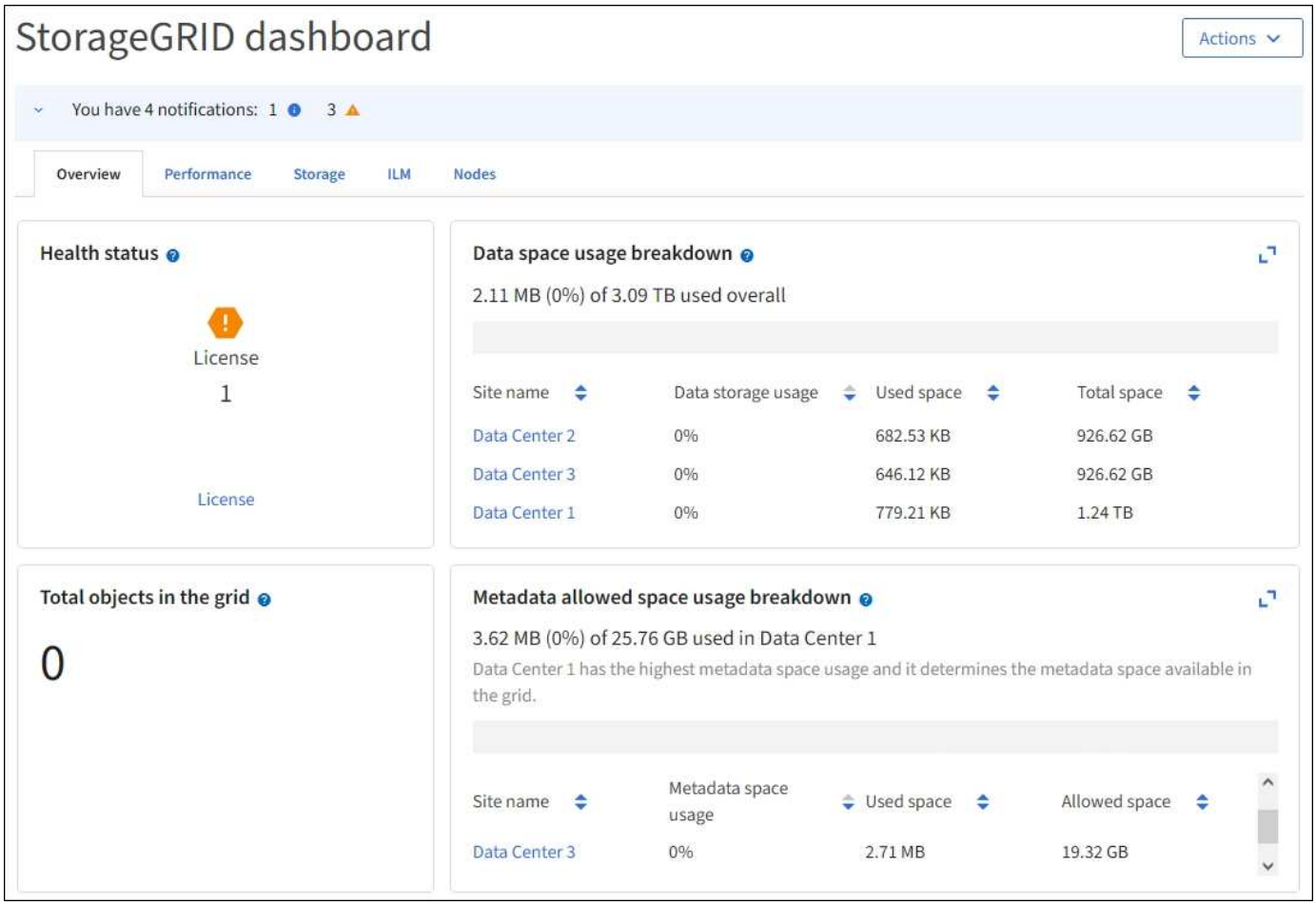
- Vous devez être connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous devez avoir "autorisations d'accès spécifiques".

> Pour modifier les unités des valeurs de stockage affichées dans le Gestionnaire de grille, sélectionnez la liste déroulante utilisateur dans le coin supérieur droit du Gestionnaire de grille, puis sélectionnez **Préférences utilisateur**.

Affichez et gérez le tableau de bord

Vous pouvez utiliser le tableau de bord pour surveiller les activités du système en un coup d'œil. Vous pouvez créer des tableaux de bord personnalisés pour contrôler votre implémentation de StorageGRID.

> Pour modifier les unités des valeurs de stockage affichées dans le Gestionnaire de grille, sélectionnez la liste déroulante utilisateur dans le coin supérieur droit du Gestionnaire de grille, puis sélectionnez **Préférences utilisateur**.



Afficher le tableau de bord

Le tableau de bord se compose d'onglets contenant des informations spécifiques sur le système StorageGRID. Chaque onglet contient des catégories d'informations affichées sur les cartes.

Vous pouvez utiliser le tableau de bord fourni par le système, tel qu'il est. En outre, vous pouvez créer des tableaux de bord personnalisés contenant uniquement les onglets et cartes pertinents pour la surveillance de votre implémentation de StorageGRID.

Les onglets du tableau de bord fournis par le système contiennent des cartes présentant les types d'informations suivants :

Du tableau de bord fourni par le système	Contient
Présentation	Informations générales sur la grille, telles que les alertes actives, l'utilisation de l'espace et le nombre total d'objets de la grille.
Performance	Utilisation de l'espace, stockage utilisé au fil du temps, opérations S3 ou Swift, durée de la demande, taux d'erreur.
Stockage	Utilisation des quotas des locataires et de l'espace logique. Prévisions de l'utilisation de l'espace pour les données utilisateur et les métadonnées.

Du tableau de bord fourni par le système	Contient
ILM	File d'attente de gestion du cycle de vie des informations et taux d'évaluation.
Nœuds	Utilisation du CPU, des données et de la mémoire par nœud. Opérations S3 ou Swift par nœud. Distribution nœud à site.

Certaines cartes peuvent être agrandies pour faciliter la visualisation. Sélectionnez l'icône Agrandir dans le coin supérieur droit de la carte. Pour fermer une carte agrandie, sélectionnez l'icône réduire Ou sélectionnez **Fermer**.

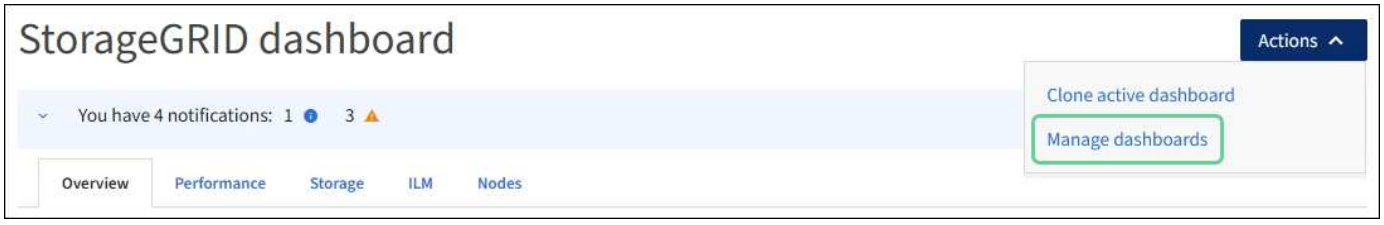
Gestion des tableaux de bord

Si vous disposez d'un accès racine (voir "Autorisations de groupe d'administration"), vous pouvez effectuer les tâches de gestion suivantes pour les tableaux de bord :

- Créez un tableau de bord personnalisé à partir de zéro. Vous pouvez utiliser des tableaux de bord personnalisés pour contrôler quelles informations StorageGRID sont affichées et comment elles sont organisées.
- Cloner un tableau de bord pour créer des tableaux de bord personnalisés.
- Définir un tableau de bord actif pour un utilisateur. Le tableau de bord actif peut être celui fourni par le système ou un tableau de bord personnalisé.
- Définissez un tableau de bord par défaut, qui correspond à ce que tous les utilisateurs voient, à moins qu'ils n'activent leur propre tableau de bord.
- Modifiez le nom d'un tableau de bord.
- Modifiez un tableau de bord pour ajouter ou supprimer des onglets et des cartes. Vous pouvez avoir un minimum de 1 et un maximum de 20 onglets.
- Déposer un tableau de bord.

Si vous disposez d'une autre autorisation que l'accès racine, vous ne pouvez définir qu'un tableau de bord actif.

Pour gérer les tableaux de bord, sélectionnez **actions** > **gérer les tableaux de bord**.



Configurer les tableaux de bord

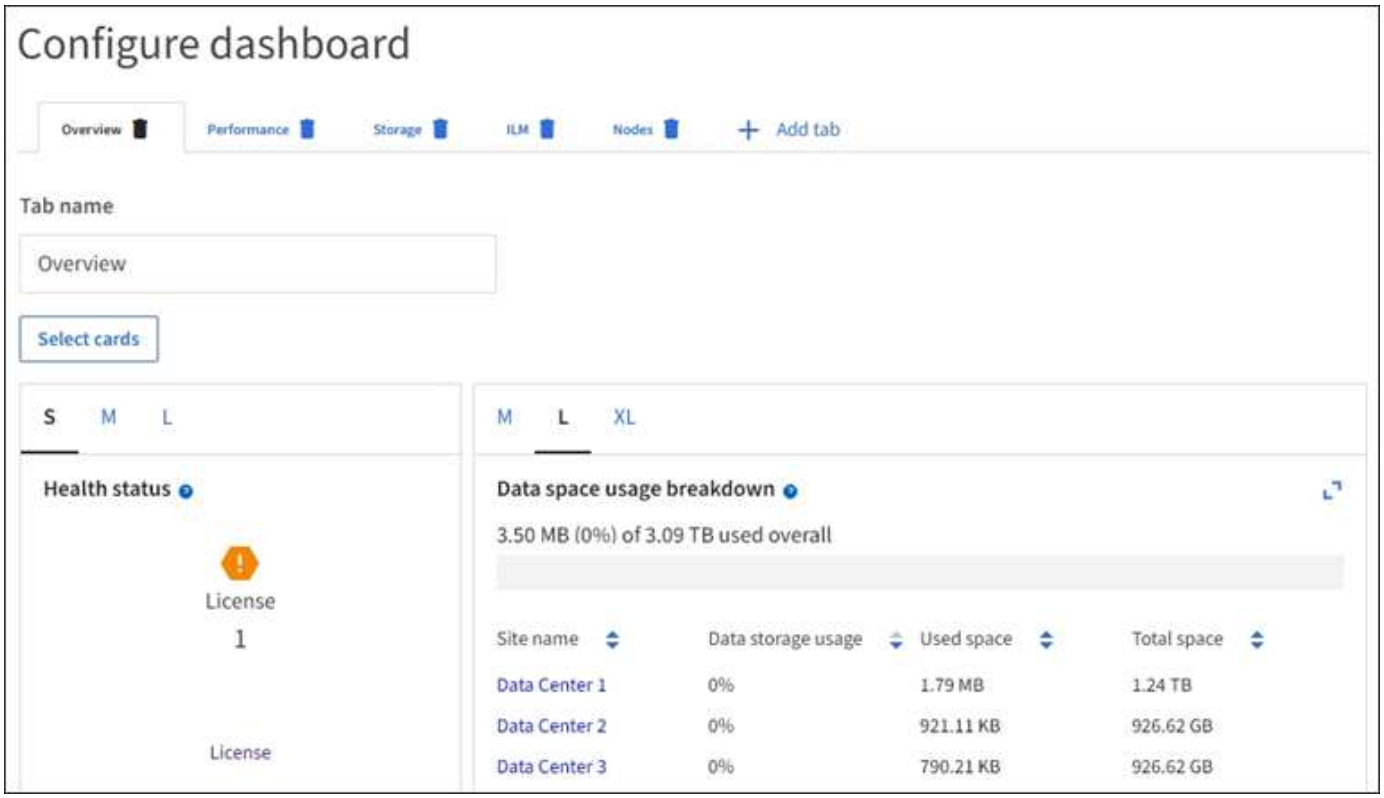
Pour créer un nouveau tableau de bord en clonant le tableau de bord actif, sélectionnez **actions** > **Cloner le tableau de bord actif**.

Pour modifier ou cloner un tableau de bord existant, sélectionnez **actions** > **gérer les tableaux de bord**.

Le tableau de bord fourni par le système ne peut pas être modifié ou supprimé.

Lors de la configuration d'un tableau de bord, vous pouvez :

- Ajouter ou supprimer des onglets
- Renommez les onglets et donnez des noms uniques aux nouveaux onglets
- Ajoutez, supprimez ou réorganisez (faites glisser) des cartes pour chaque onglet
- Sélectionnez la taille des cartes individuelles en sélectionnant **S**, **M**, **L** ou **XL** en haut de la carte



Afficher la page nœuds

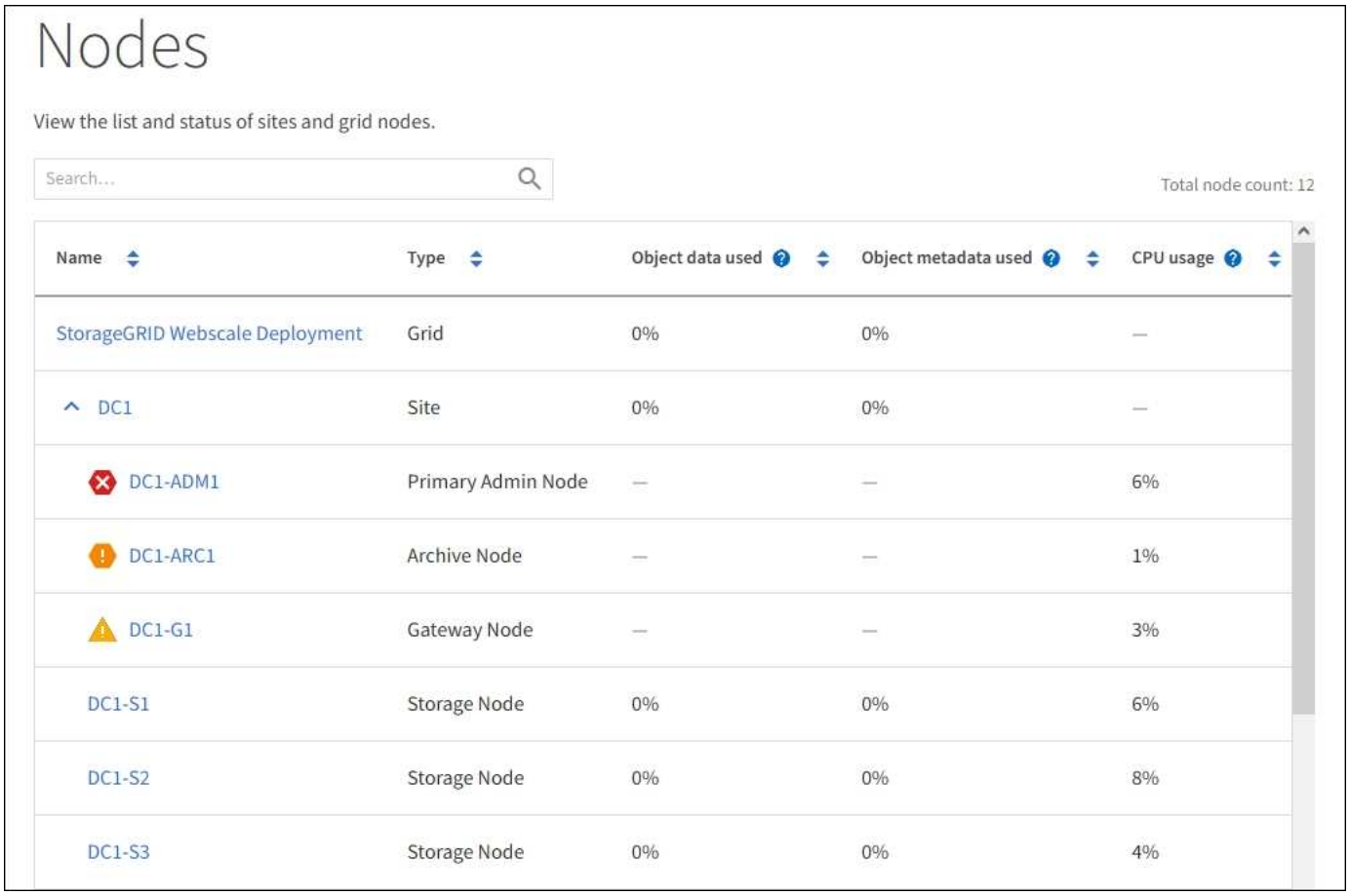
Affichez la page nœuds : présentation

Si vous avez besoin d'informations plus détaillées sur votre système StorageGRID que le tableau de bord ne l'indique, vous pouvez utiliser la page nœuds pour afficher les mesures de la grille dans son intégralité, de chaque site de la grille et de chaque nœud d'un site.

Le tableau nœuds répertorie les informations récapitulatives pour l'ensemble de la grille, chaque site et chaque nœud. Si un nœud est déconnecté ou dispose d'une alerte active, une icône s'affiche en regard du nom du nœud. Si le nœud est connecté et ne dispose d'aucune alerte active, aucune icône n'est affichée.

Lorsqu'un nœud n'est pas connecté à la grille, comme lors de la mise à niveau ou lorsqu'il est déconnecté, certains metrics peuvent être indisponibles ou exclus des totaux site et grid. Après qu'un nœud se reconnecte à la grille, attendez plusieurs minutes que les valeurs se stabilisent.

Pour modifier les unités des valeurs de stockage affichées dans le Gestionnaire de grille, sélectionnez la liste déroulante utilisateur dans le coin supérieur droit du Gestionnaire de grille, puis sélectionnez **Préférences utilisateur**.



Icônes d'état de connexion

Si un nœud est déconnecté de la grille, l'une des icônes suivantes s'affiche en regard du nom du nœud.

Icône	Description	Action requise
	Non connecté - Inconnu Pour une raison inconnue, un nœud est déconnecté ou les services du nœud sont arrêtés de manière inattendue. Par exemple, un service du nœud peut être arrêté, ou le nœud a perdu sa connexion réseau en raison d'une panne de courant ou d'une panne imprévue. L'alerte **Impossible de communiquer avec le noeud** peut également être déclenchée. D'autres alertes peuvent également être actives.	Nécessite une attention immédiate. "Sélectionnez chaque alerte" et suivre les actions recommandées. Par exemple, vous devrez peut-être redémarrer un service qui a arrêté ou redémarré l'hôte du nœud. **Remarque** : un nœud peut apparaître comme inconnu pendant les opérations d'arrêt gérées. Dans ces cas, vous pouvez ignorer l'état Inconnu.

Icône	Description	Action requise
	Non connecté - Arrêt administratif Pour une raison prévue, le nœud n'est pas connecté au grid. Par exemple, le nœud ou les services du nœud ont été normalement arrêtés, le nœud est en cours de redémarrage ou le logiciel est mis à niveau. Une ou plusieurs alertes peuvent également être actives. En fonction du problème sous-jacent, ces nœuds sont souvent remis en ligne sans intervention.	Déterminez si des alertes affectent ce nœud. Si une ou plusieurs alertes sont actives, "Sélectionnez chaque alerte" et suivre les actions recommandées.

Si un noeud est déconnecté de la grille, il peut y avoir une alerte sous-jacente, mais seule l'icône « non connecté » s'affiche. Pour afficher les alertes actives d'un nœud, sélectionnez le nœud.

Icônes d'alerte

Si une alerte est active pour un nœud, l'une des icônes suivantes s'affiche à côté du nom du nœud :

Critique : il existe une condition anormale qui a arrêté les opérations normales d'un noeud ou d'un service StorageGRID. Vous devez immédiatement résoudre le problème sous-jacent. Une interruption du service et une perte de données peuvent se produire si le problème n'est pas résolu.

Majeur : il existe une condition anormale qui affecte les opérations en cours ou qui approche du seuil pour une alerte critique. Vous devez examiner les alertes majeures et résoudre tous les problèmes sous-jacents pour vérifier que leur condition anormale n'arrête pas le fonctionnement normal d'un nœud ou d'un service StorageGRID.

Mineur : le système fonctionne normalement, mais il existe une condition anormale qui pourrait affecter la capacité de fonctionnement du système s'il continue. Vous devez surveiller et résoudre les alertes mineures qui ne sont pas claires par elles-mêmes pour vous assurer qu'elles n'entraînent pas de problème plus grave.

Afficher les détails d'un système, d'un site ou d'un nœud

Pour filtrer les informations affichées dans la table noeuds, entrez une chaîne de recherche dans le champ **Search**. Vous pouvez effectuer une recherche par nom de système, nom d'affichage ou type (par exemple, entrez **gat** pour localiser rapidement tous les nœuds de passerelle).

Pour afficher les informations de la grille, du site ou du nœud :

- Sélectionnez le nom de la grille pour afficher un récapitulatif des agrégats des statistiques de l'ensemble du système StorageGRID.
- Sélectionnez un site de data Center spécifique pour afficher un résumé global des statistiques pour tous les nœuds de ce site.
- Sélectionnez un nœud spécifique pour afficher des informations détaillées sur ce nœud.

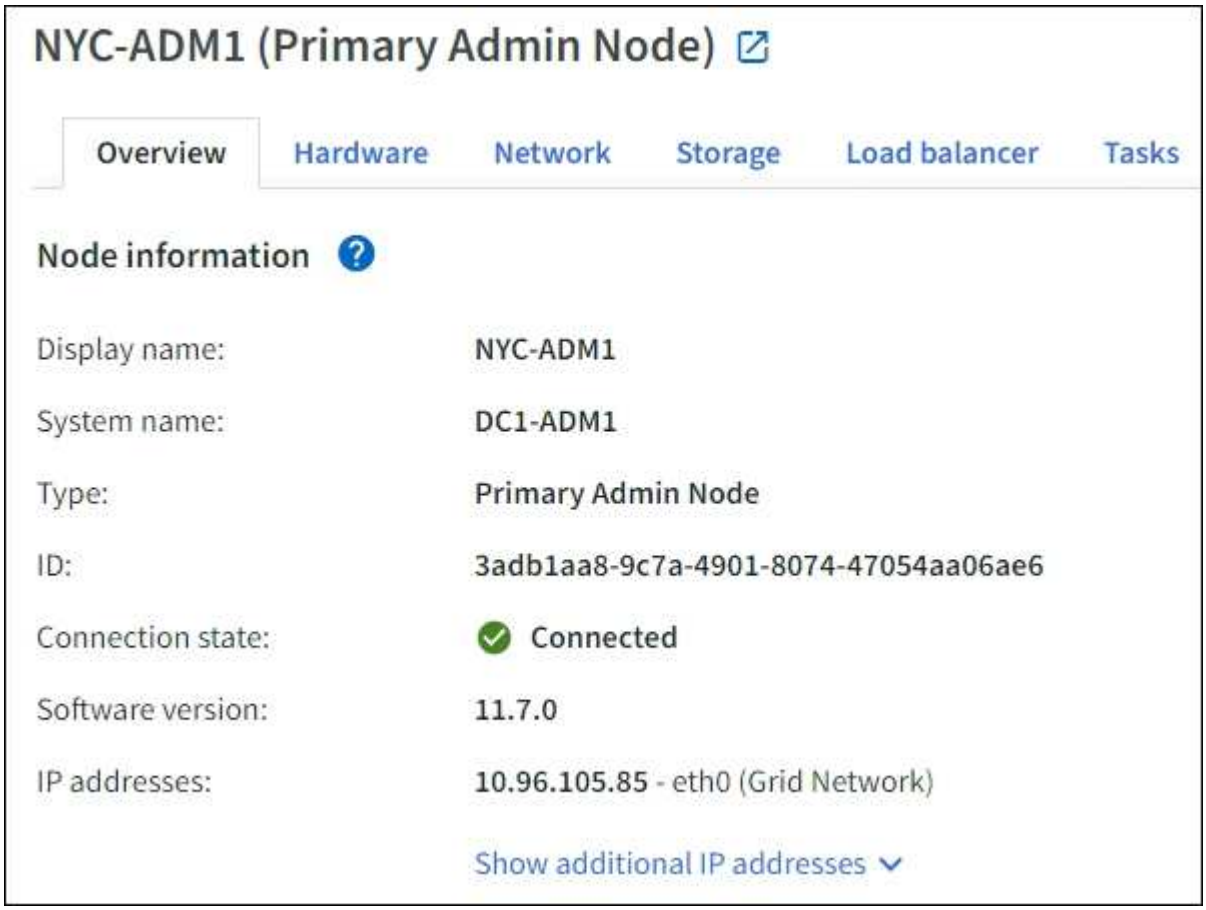
Afficher l'onglet vue d'ensemble

L'onglet Présentation fournit des informations de base sur chaque nœud. Il affiche également toutes les alertes qui affectent actuellement le nœud.

L'onglet vue d'ensemble s'affiche pour tous les nœuds.

Informations sur le nœud

La section informations sur les nœuds de l'onglet vue d'ensemble répertorie les informations de base sur le nœud.



Les informations de présentation d'un nœud incluent les éléments suivants :

- **Nom d'affichage** (affiché uniquement si le noeud a été renommé) : le nom d'affichage actuel du noeud. Utilisez le "Renommage de la grille, du site et des nœuds" procédure de mise à jour de cette valeur.
- **Nom du système** : le nom que vous avez saisi pour le nœud lors de l'installation. Les noms de système sont utilisés pour les opérations StorageGRID internes et ne peuvent pas être modifiés.
- **Type** : type de noeud — noeud d'administration, noeud d'administration principal, noeud de stockage, noeud de passerelle ou noeud d'archivage.

> La prise en charge des nœuds d'archivage (pour l'archivage dans le cloud à l'aide de l'API S3 et l'archivage sur bande à l'aide du middleware TSM) est obsolète et sera supprimée dans une prochaine version. Le déplacement d'objets d'un nœud d'archivage vers un système de stockage d'archives externe a été remplacé par les pools de stockage cloud ILM pour offrir davantage de fonctionnalités.

- **ID** : identificateur unique du noeud, qui est également appelé UUID.
- **Etat de connexion** : l'un des trois États. L'icône de l'état le plus grave est affichée.
  - **Inconnu** : Pour une raison inconnue, le nœud n'est pas connecté à la grille ou un ou plusieurs services sont arrêtés de façon inattendue. Par exemple, la connexion réseau entre les nœuds a été perdue, l'alimentation est en panne ou un service est en panne. L'alerte **Impossible de communiquer avec le noeud** peut également être déclenchée. D'autres alertes peuvent également être actives. Cette situation exige une attention immédiate.

    Un nœud peut apparaître comme inconnu lors des opérations d'arrêt géré. Dans ces cas, vous pouvez ignorer l'état Inconnu.

  - * Arrêt administratif* : Le nœud n'est pas connecté à la grille pour une raison attendue. Par exemple, le nœud ou les services du nœud ont été normalement arrêtés, le nœud est en cours de redémarrage ou le logiciel est mis à niveau. Une ou plusieurs alertes peuvent également être actives.
  - * Connecté* : Le nœud est connecté à la grille.
- **Stockage utilisé** : pour les nœuds de stockage uniquement.
  - **Données d'objet** : pourcentage de l'espace total utilisable pour les données d'objet qui ont été utilisées sur le nœud de stockage.
  - **Métadonnées d'objet** : pourcentage de l'espace total autorisé pour les métadonnées d'objet qui ont été utilisées sur le nœud de stockage.
- **Version du logiciel** : la version de StorageGRID installée sur le nœud.
- **Groupes HA** : pour les nœuds d'administration et de passerelle uniquement. Indique si une interface réseau sur le nœud est incluse dans un groupe haute disponibilité et si cette interface est l'interface principale.
- **Adresses IP** : adresses IP du nœud. Cliquez sur **Afficher des adresses IP supplémentaires** pour afficher les adresses IPv4 et IPv6 du nœud ainsi que les mappages d'interface.

Alertes

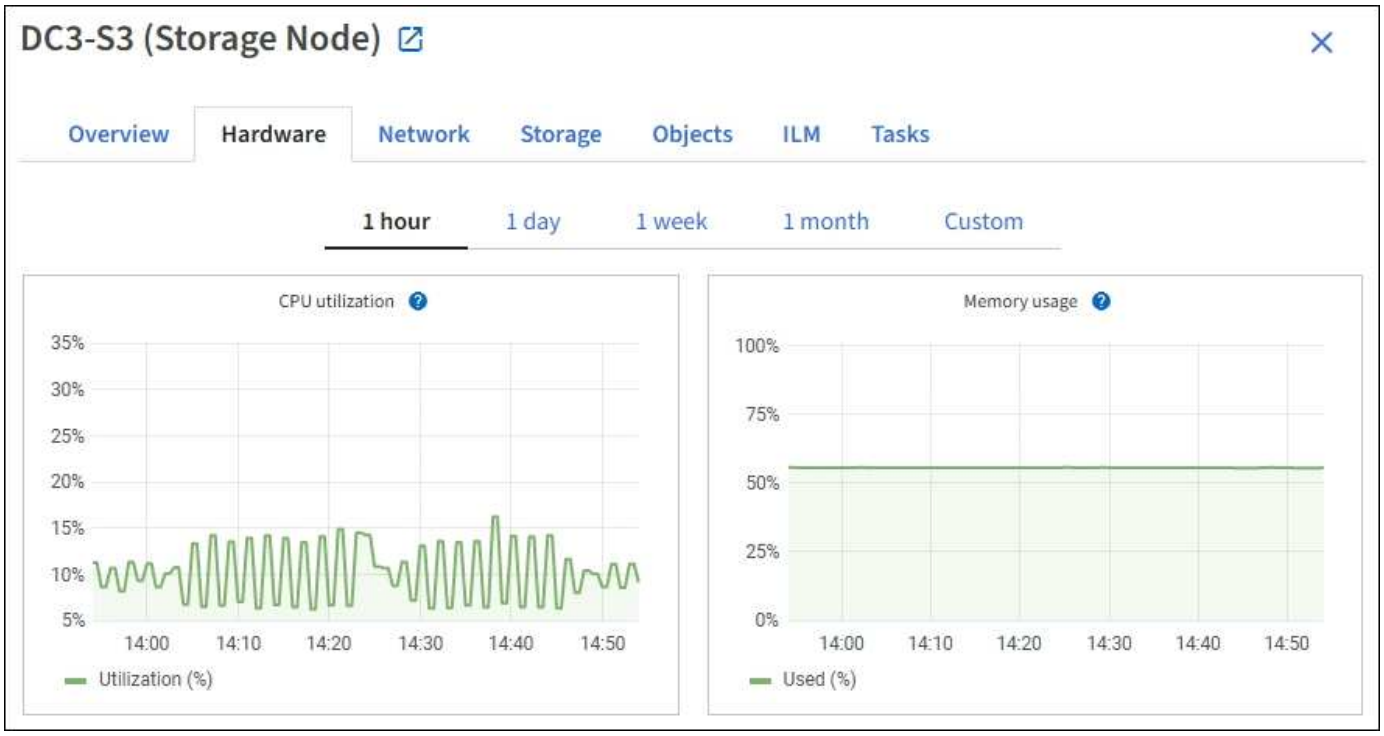
La section alertes de l'onglet vue d'ensemble répertorie tout "alertes affectant actuellement ce nœud qui n'ont pas été neutralisées". Sélectionnez le nom de l'alerte pour afficher des détails supplémentaires et les actions recommandées.

Des alertes sont également incluses pour "états de connexion de nœud".

Afficher l'onglet matériel

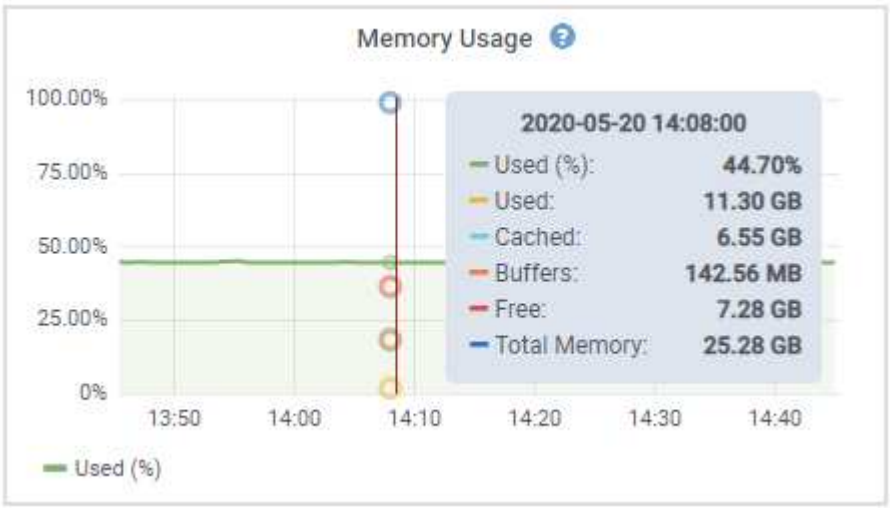
L'onglet matériel affiche l'utilisation du CPU et de la mémoire pour chaque nœud, ainsi que des informations supplémentaires sur le matériel des appliances.

L'onglet matériel s'affiche pour tous les nœuds.



Pour afficher un intervalle de temps différent, sélectionnez l'une des commandes au-dessus du graphique ou du graphique. Vous pouvez afficher les informations disponibles pour les intervalles de 1 heure, 1 jour, 1 semaine ou 1 mois. Vous pouvez également définir un intervalle personnalisé, qui vous permet de spécifier des plages de date et d'heure.

Pour afficher des détails sur l'utilisation du CPU et de la mémoire, placez votre curseur sur chaque graphique.



Si le nœud est un nœud d'appliance, cet onglet inclut également une section contenant des informations supplémentaires sur le matériel de l'appliance.

Afficher des informations sur les nœuds de stockage de l'appliance

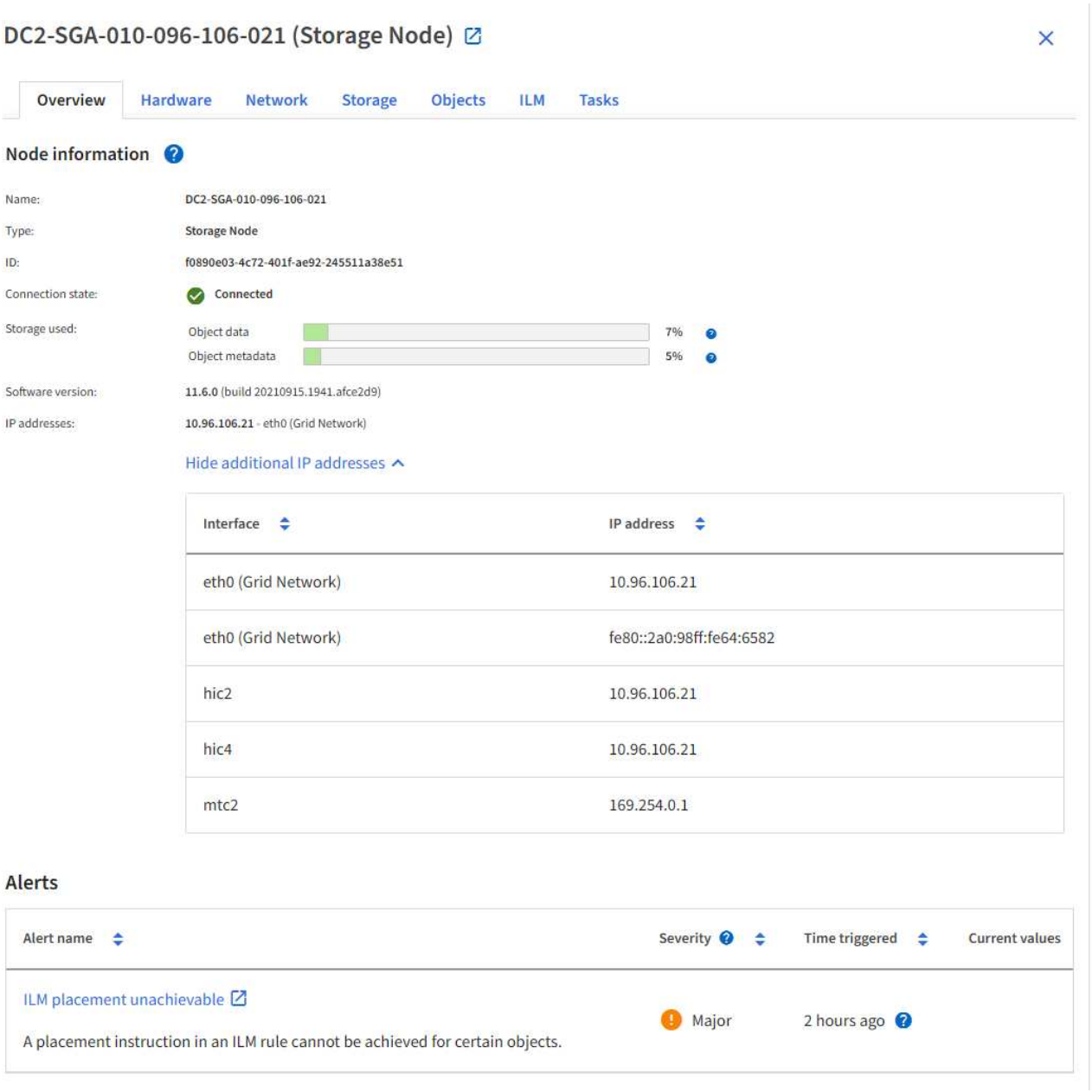
La page nœuds répertorie les informations relatives à l'état des services et à toutes les ressources de calcul, de périphérique de disque et de réseau pour chaque nœud de stockage d'appliance. Vous pouvez également afficher la mémoire, le matériel de stockage, la version du firmware des contrôleurs, les ressources réseau, les interfaces réseau, les adresses réseau et de réception et de transmission des données.

Étapes

1. Sur la page nœuds, sélectionnez un nœud de stockage d'appliance.
2. Sélectionnez **vue d'ensemble**.

   La section informations sur le nœud de l'onglet Présentation affiche un récapitulatif des informations sur le nœud, telles que le nom, le type, l'ID et l'état de connexion du nœud. La liste des adresses IP inclut le nom de l'interface pour chaque adresse, comme suit :

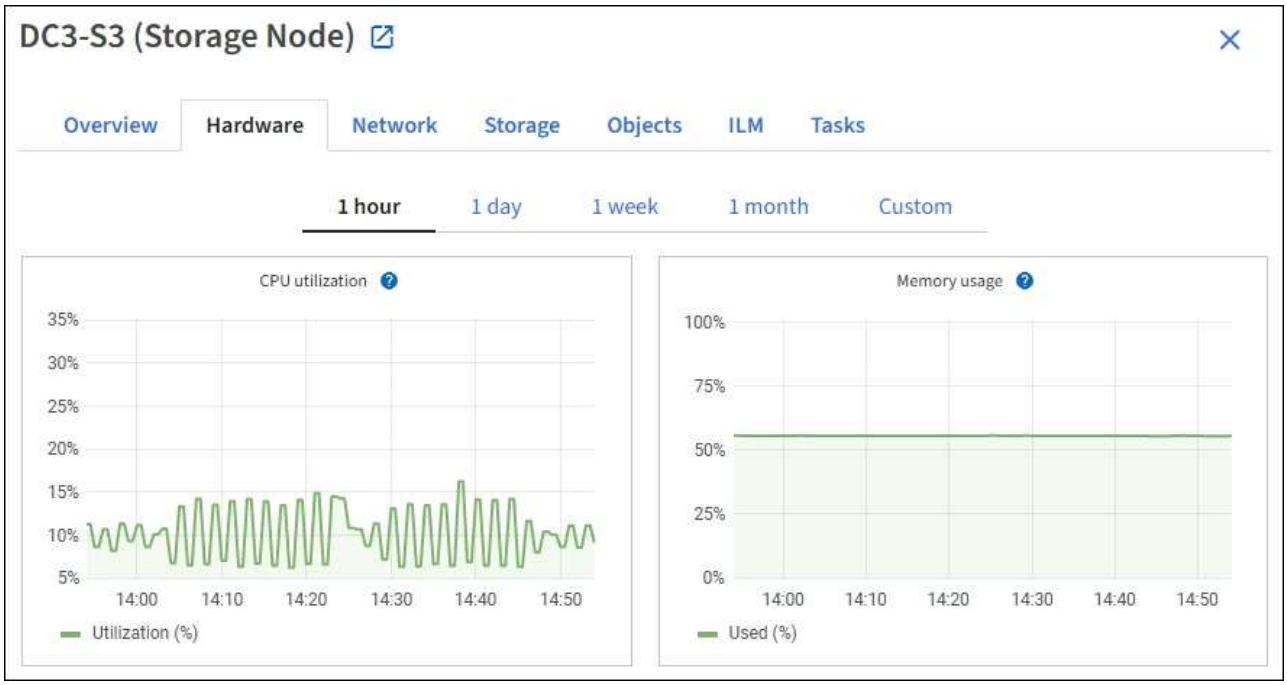
   - **Eth** : réseau Grid, réseau Admin ou réseau client.
   - **Hic** : un des ports physiques 10, 25 ou 100 GbE de l'appareil. Ces ports peuvent être liés ensemble et connectés au réseau StorageGRID Grid Network (eth0) et au réseau client (eth2).
   - **mtc** : l'un des ports physiques 1 GbE de l'appareil. Une ou plusieurs interfaces mtc sont liées pour former l'interface réseau d'administration StorageGRID (eth1). Vous pouvez laisser d'autres interfaces mtc disponibles pour une connectivité locale temporaire pour un technicien du centre de données.



La section alertes de l'onglet Overview affiche toutes les alertes actives du nœud.

3. Sélectionnez **matériel** pour plus d'informations sur l'appareil.

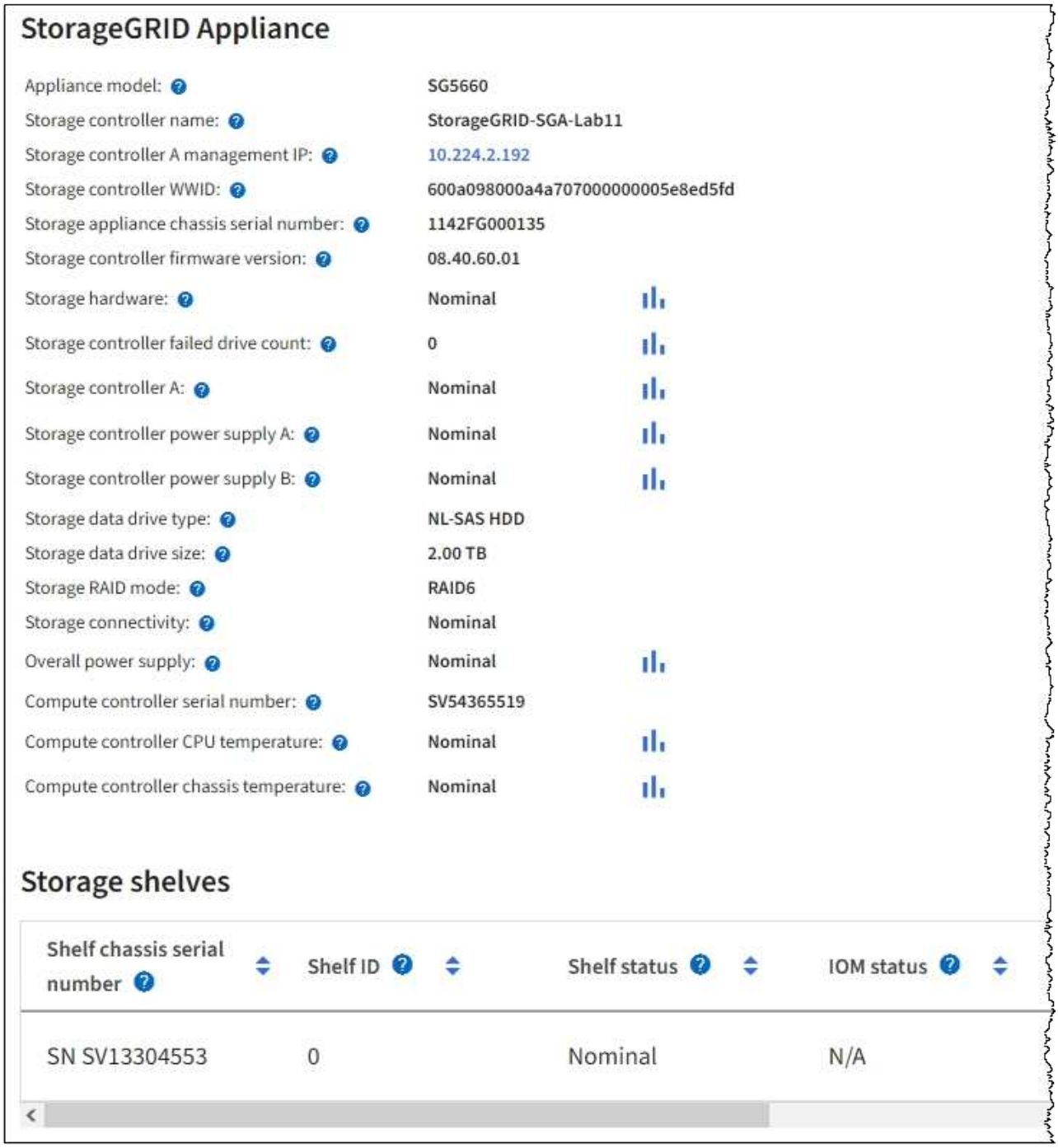
   a. Affichez les graphiques d'utilisation de l'UC et de la mémoire pour déterminer les pourcentages d'utilisation de l'UC et de la mémoire au fil du temps. Pour afficher un intervalle de temps différent, sélectionnez l'une des commandes au-dessus du graphique ou du graphique. Vous pouvez afficher les informations disponibles pour les intervalles de 1 heure, 1 jour, 1 semaine ou 1 mois. Vous pouvez également définir un intervalle personnalisé, qui vous permet de spécifier des plages de date et d'heure.



b. Faites défiler vers le bas pour afficher le tableau des composants de l'appareil. Ce tableau contient des informations telles que le nom du modèle de l'appliance, les noms des contrôleurs, les numéros de série et les adresses IP, ainsi que l'état de chaque composant.

> Certains champs, tels que le contrôleur de calcul BMC IP et le matériel de calcul, apparaissent uniquement pour les appliances dotées de cette fonctionnalité.

Les composants des tiroirs de stockage et des tiroirs d'extension s'ils font partie de l'installation apparaissent dans un tableau séparé sous le tableau de l'appliance.



Dans la table Appliance	Description
Modèle de type appliance	Le numéro de modèle de cette appliance StorageGRID est indiqué dans SANtricity OS.
Nom du contrôleur de stockage	Nom de cette appliance StorageGRID représenté dans SANtricity OS.
IP de gestion A du contrôleur de stockage	Adresse IP du port de gestion 1 sur le contrôleur de stockage A. Cette adresse IP vous permet d'accéder à SANtricity OS et de résoudre les problèmes de stockage.

Dans la table Appliance	Description
IP de gestion du contrôleur de stockage B	Adresse IP du port de gestion 1 du contrôleur de stockage B. Cette adresse IP vous permet d'accéder à SANtricity OS et de résoudre les problèmes de stockage. Certains modèles d'appliance ne disposent pas de contrôleur de stockage B.
WWID du contrôleur de stockage	Identifiant universel du contrôleur de stockage indiqué dans SANtricity OS.
Numéro de série du châssis de l'appliance de stockage	Numéro de série du châssis de l'appareil.
Version du firmware du contrôleur de stockage	Version du firmware du contrôleur de stockage de cette appliance.
Matériel de stockage	État global du matériel du contrôleur de stockage. Si SANtricity System Manager signale un état de nécessite une intervention pour le matériel de stockage, le système StorageGRID signale également cette valeur. Si le statut est « nécessite une intervention », vérifiez d'abord le contrôleur de stockage à l'aide de SANtricity OS. Assurez-vous ensuite qu'aucune autre alarme ne s'applique au contrôleur de calcul.
Nombre de disques défaillants du contrôleur de stockage	Le nombre de disques qui ne sont pas optimaux.
Contrôleur de stockage A	L'état du contrôleur de stockage A.
Contrôleur de stockage B	L'état du contrôleur de stockage B. Certains modèles d'appliance ne disposent pas de contrôleur de stockage B.
Alimentation A du contrôleur de stockage	L'état de l'alimentation A du contrôleur de stockage.
Alimentation B du contrôleur de stockage	L'état de l'alimentation B du contrôleur de stockage.
Type de disque de données de stockage	Type de disque dur (HDD) ou SSD (Solid State Drive) de l'appliance.
Taille du disque de stockage des données	La taille effective d'un lecteur de données. **Remarque** : pour les nœuds avec des tiroirs d'extension, utilisez le Taille de disque des données pour chaque tiroir à la place. La taille effective du disque peut varier en fonction du tiroir.

Dans la table Appliance	Description
Mode de stockage RAID	Mode RAID configuré pour l'appliance.
Connectivité du stockage	État de la connectivité du stockage.
Bloc d'alimentation général	L'état de toutes les alimentations de l'appareil.
IP BMC du contrôleur de calcul	Adresse IP du port du contrôleur de gestion de la carte mère (BMC) dans le contrôleur de calcul. Vous utilisez cette adresse IP pour vous connecter à l'interface BMC afin de surveiller et de diagnostiquer le matériel de l'appliance. Ce champ ne s'affiche pas pour les modèles d'appliance qui ne contiennent pas de contrôleur BMC.
Numéro de série du contrôleur de calcul	Numéro de série du contrôleur de calcul.
Matériel de calcul	L'état du matériel du contrôleur de calcul. Ce champ ne s'affiche pas pour les modèles d'appliance qui ne disposent pas de matériel de calcul et de stockage distinct.
Température du processeur du contrôleur de calcul	L'état de température de l'UC du contrôleur de calcul.
Température du châssis du contrôleur de calcul	État de température du contrôleur de calcul.

+

Dans le tableau tiroirs de stockage	Description
Numéro de série du châssis du tiroir	Numéro de série du châssis du tiroir de stockage.
ID du tiroir	Identificateur numérique du tiroir de stockage. • 99 : tiroir contrôleur de stockage • 0 : premier tiroir d'extension • 1 : second tiroir d'extension **Remarque :** les étagères d'extension s'appliquent uniquement au SG6060.
État du tiroir	État global du shelf de stockage.

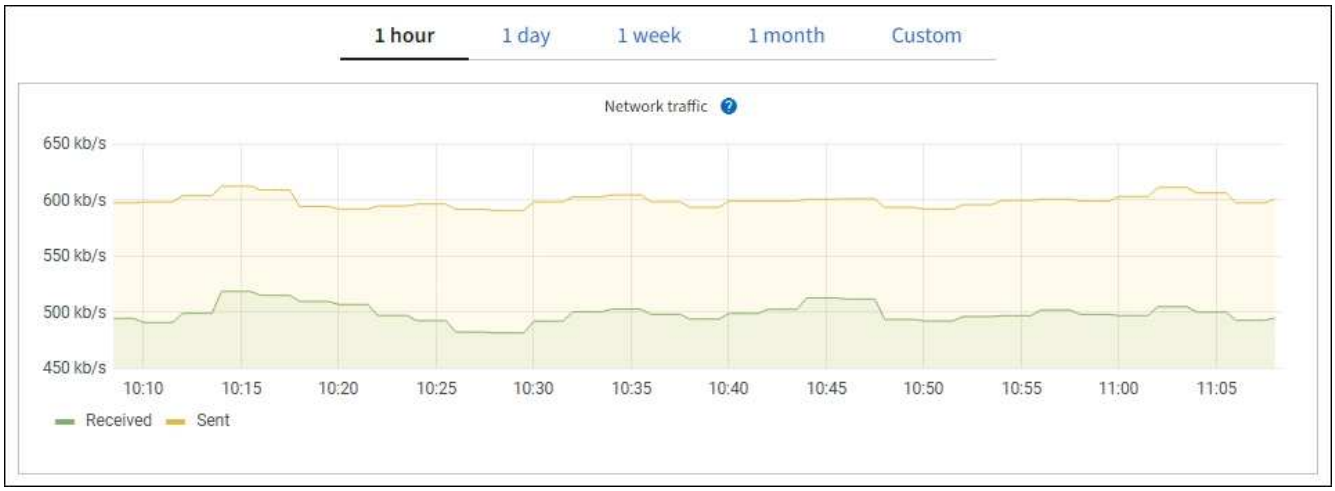
Dans le tableau tiroirs de stockage	Description
État du module d'E/S.	L'état des modules d'entrée/sortie (IOM) de tous les tiroirs d'extension. S/O s'il ne s'agit pas d'un tiroir d'extension.
État de l'alimentation électrique	État global des alimentations du tiroir de stockage.
État du tiroir	L'état des tiroirs dans le tiroir de rangement. N/A si la tablette ne contient pas de tiroirs.
État du ventilateur	État général des ventilateurs dans le shelf de stockage.
Emplacements de lecteur	Nombre total de slots de disque dans le shelf de stockage.
Disques de données	Nombre de disques du tiroir de stockage utilisés pour le stockage de données.
taille du lecteur de données	Taille effective d'un disque de données dans le tiroir de stockage.
Disques en cache	Nombre de disques du tiroir de stockage utilisés comme cache.
Taille du lecteur de cache	La taille du plus petit lecteur de cache dans le tiroir de stockage. En principe, les disques en cache sont de la même taille.
État de la configuration	L'état de configuration du tiroir de stockage.

a. Confirmer que tous les États sont « nominaux ».

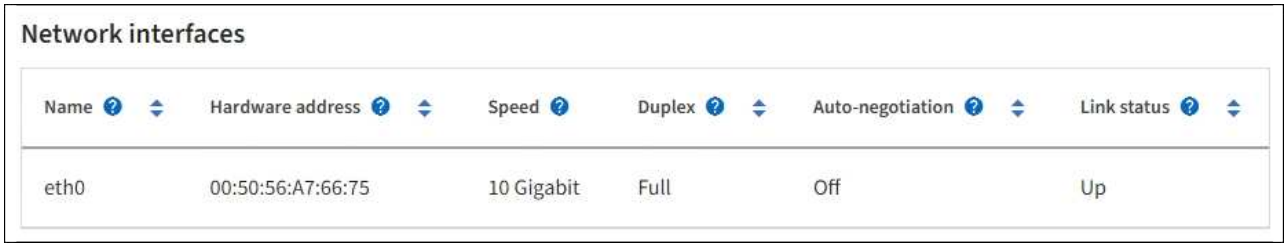
   Si un statut n'est pas « nominal », passez en revue les alertes en cours. Vous pouvez également utiliser SANtricity System Manager pour en savoir plus sur certaines de ces valeurs matérielles. Reportez-vous aux instructions d'installation et d'entretien de votre appareil.

4. Sélectionnez **réseau** pour afficher les informations de chaque réseau.

   Le graphique trafic réseau fournit un récapitulatif du trafic réseau global.



a. Consultez la section interfaces réseau.



Network interfaces

Name	Hardware address	Speed	Duplex	Auto-negotiation	Link status
eth0	00:50:56:A7:66:75	10 Gigabit	Full	Off	Up

Utilisez le tableau suivant avec les valeurs de la colonne **Speed** du tableau interfaces réseau pour déterminer si les ports réseau 10/25-GbE de l'appliance ont été configurés pour utiliser le mode actif/sauvegarde ou le mode LACP.

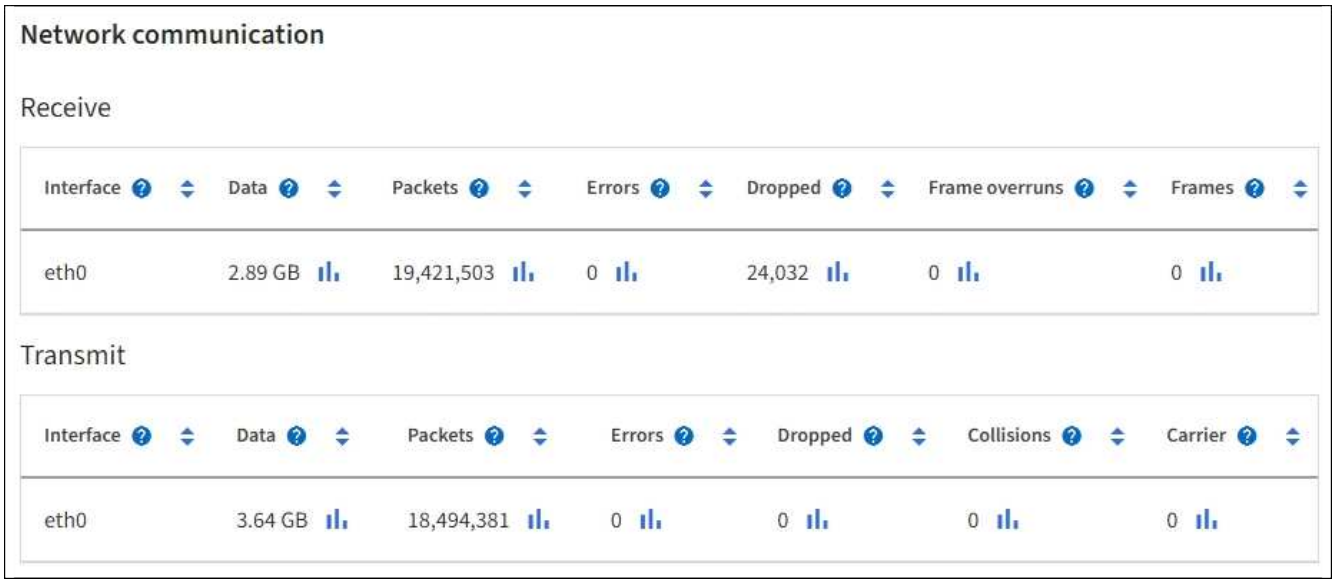
Les valeurs indiquées dans le tableau supposent que les quatre liens sont utilisés.

Mode de liaison	Mode du lien	Vitesse de la liaison HIC individuelle (hic 1, hi2, hic 3, hic 4)	Vitesse réseau prévue pour la grille/le client (eth0, eth2)
Agrégat	LACP	25	100
Fixe	LACP	25	50
Fixe	Actif/sauvegarde	25	25
Agrégat	LACP	10	40
Fixe	LACP	10	20
Fixe	Actif/sauvegarde	10	10

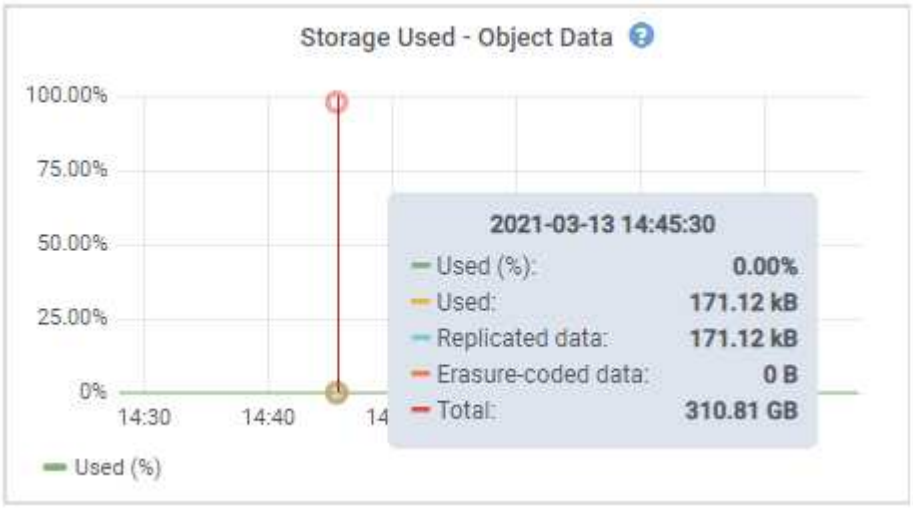
Voir "Configurer les liaisons réseau" Pour plus d'informations sur la configuration des ports 10/25-GbE.

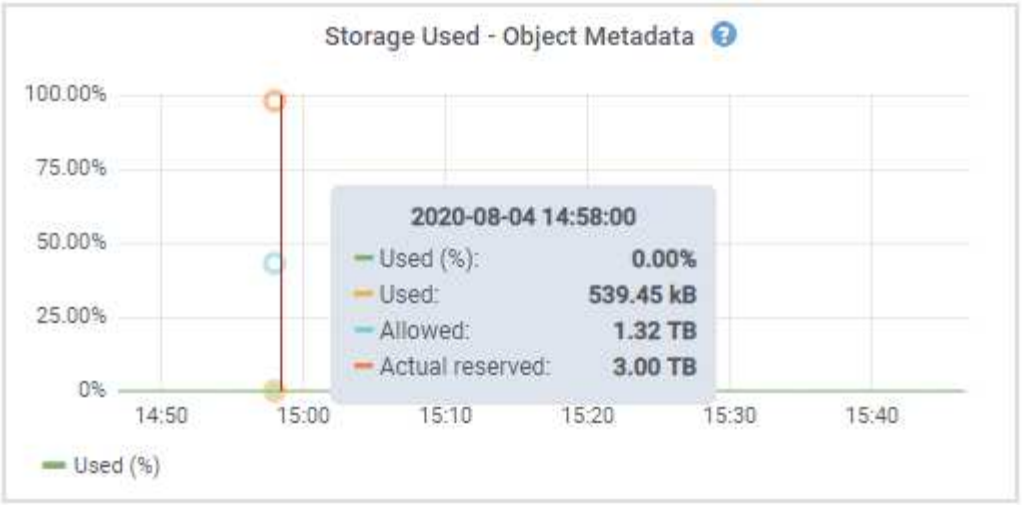
b. Passez en revue la section communication réseau.

Les tableaux de réception et de transmission indiquent le nombre d'octets et de paquets reçus et envoyés sur chaque réseau ainsi que d'autres mesures de réception et de transmission.



5. Sélectionnez **Storage** pour afficher les graphiques qui affichent les pourcentages de stockage utilisés dans le temps pour les données d'objet et les métadonnées d'objet, ainsi que des informations sur les unités de disque, les volumes et les magasins d'objets.

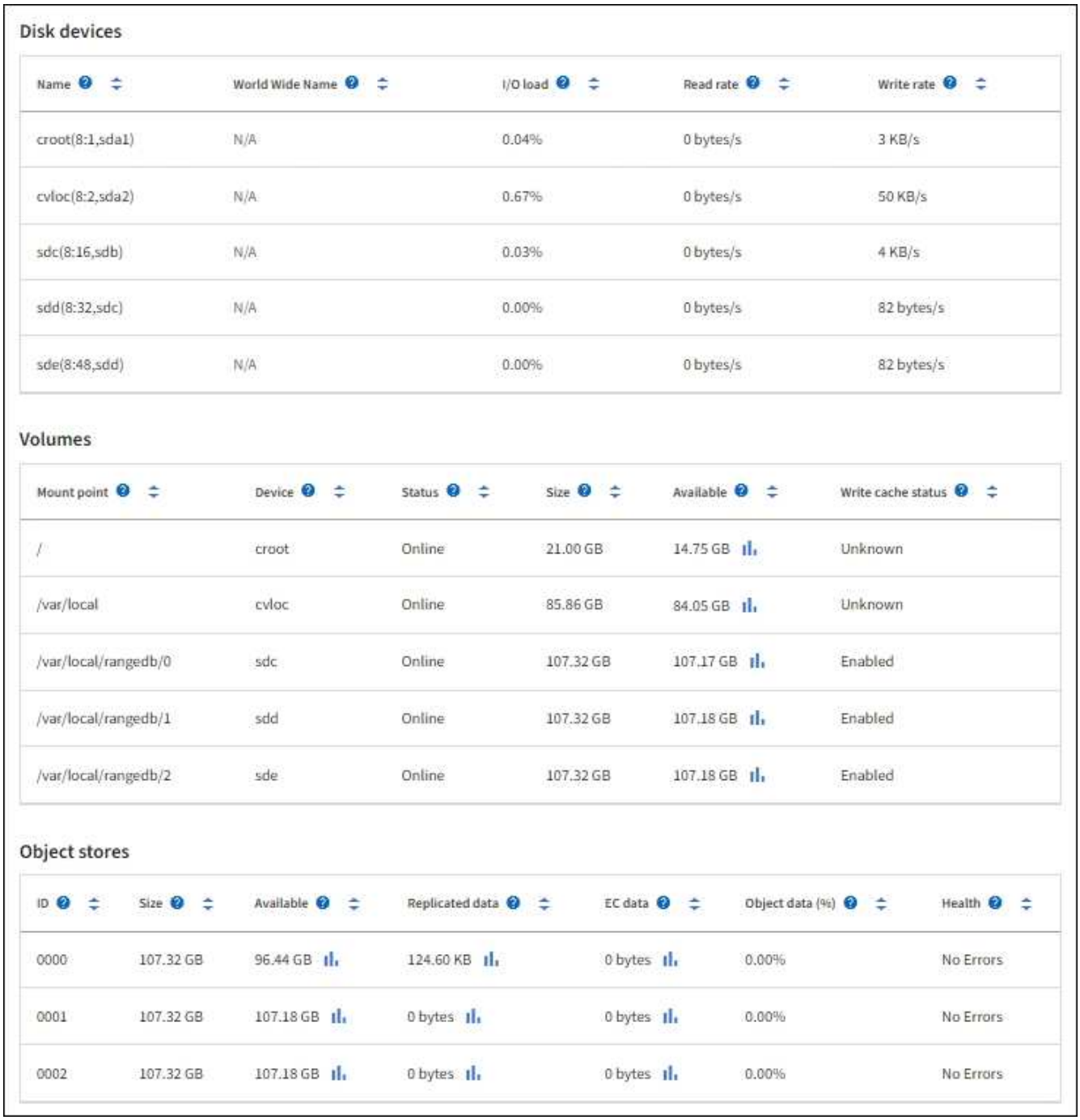




a. Faites défiler vers le bas pour afficher les quantités de stockage disponibles pour chaque volume et magasin d'objets.

   Le nom mondial de chaque disque correspond à l'identifiant universel (WWID) du volume qui s'affiche lorsque vous affichez les propriétés standard du volume dans SANtricity OS (le logiciel de gestion connecté au contrôleur de stockage de l'appliance).

   Pour vous aider à interpréter les statistiques de lecture et d'écriture du disque relatives aux points de montage du volume, la première partie du nom affichée dans la colonne **Name** de la table Disk Devices (c'est-à-dire *sdc*, *sdd*, *sde*, etc.) correspond à la valeur indiquée dans la colonne **Device** de la table volumes.



Disk devices

Name	World Wide Name	I/O load	Read rate	Write rate
croot(8:1,sda1)	N/A	0.04%	0 bytes/s	3 KB/s
cvloc(8:2,sda2)	N/A	0.67%	0 bytes/s	50 KB/s
sdc(8:16,sdb)	N/A	0.03%	0 bytes/s	4 KB/s
sdd(8:32,sdc)	N/A	0.00%	0 bytes/s	82 bytes/s
sde(8:48,sdd)	N/A	0.00%	0 bytes/s	82 bytes/s

Volumes

Mount point	Device	Status	Size	Available	Write cache status
/	croot	Online	21.00 GB	14.75 GB	Unknown
/var/local	cvloc	Online	85.86 GB	84.05 GB	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.17 GB	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/2	sde	Online	107.32 GB	107.18 GB	Enabled

Object stores

ID	Size	Available	Replicated data	EC data	Object data (%)	Health
0000	107.32 GB	96.44 GB	124.60 KB	0 bytes	0.00%	No Errors
0001	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0002	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors

Affiche des informations sur les nœuds d'administration de l'appliance et les nœuds de passerelle

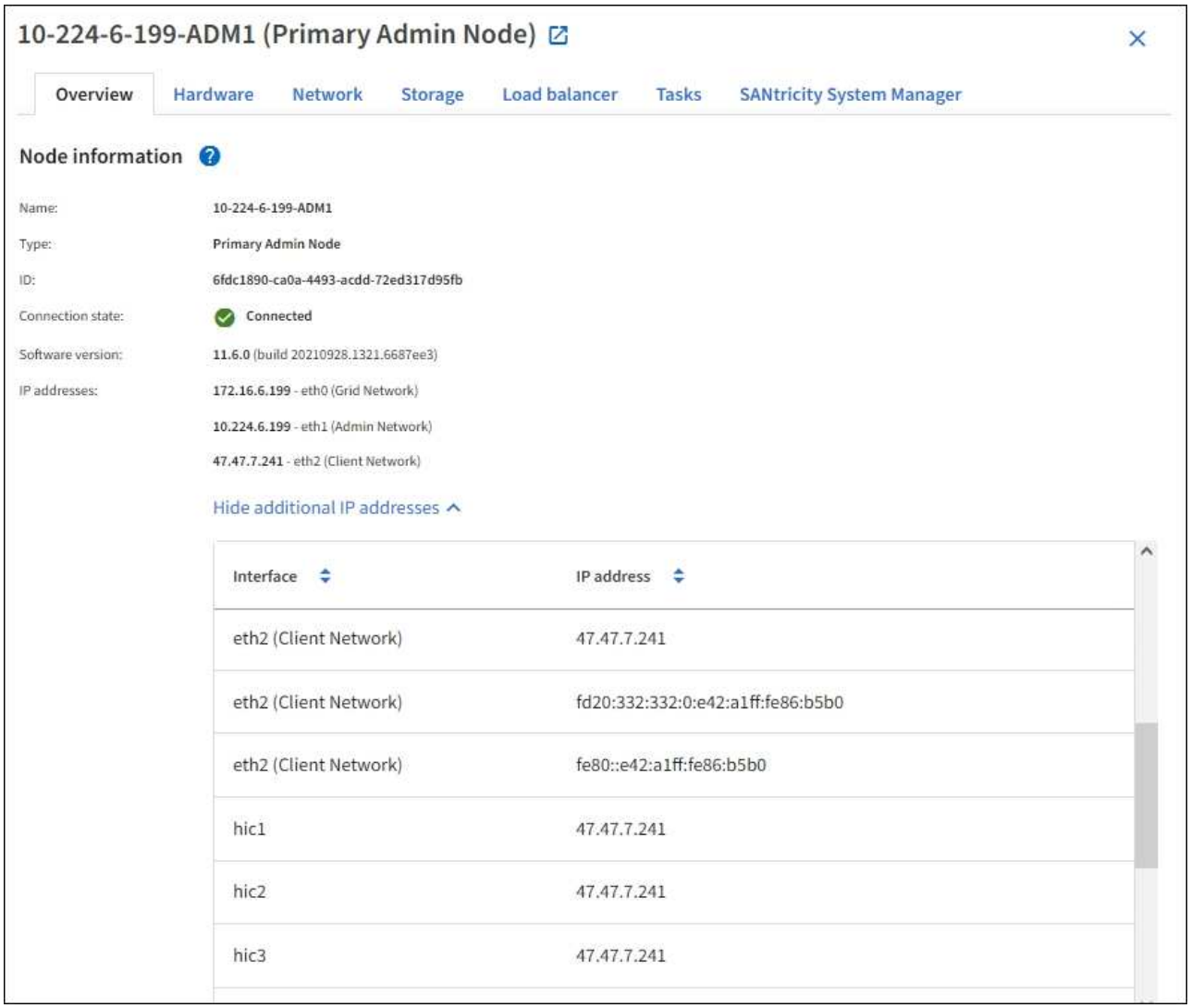
La page nœuds répertorie les informations relatives à l'état des services et à toutes les ressources de calcul, de périphérique de disque et de réseau pour chaque appliance de services utilisée comme nœud d'administration ou comme nœud de passerelle. Vous pouvez également afficher la mémoire, le matériel de stockage, les ressources réseau, les interfaces réseau, les adresses réseau, et recevoir et transmettre des données.

Étapes

1. Sur la page nœuds, sélectionnez un nœud d'administration d'appliance ou un nœud de passerelle d'appliance.
2. Sélectionnez **vue d'ensemble**.

La section informations sur le nœud de l'onglet Présentation affiche un récapitulatif des informations sur le nœud, telles que le nom, le type, l'ID et l'état de connexion du nœud. La liste des adresses IP inclut le nom de l'interface pour chaque adresse, comme suit :

- **Adllb** et **adlli** : affiché si la liaison actif/sauvegarde est utilisée pour l'interface réseau d'administration
- **Eth** : réseau Grid, réseau Admin ou réseau client.
- **Hic** : un des ports physiques 10, 25 ou 100 GbE de l'appareil. Ces ports peuvent être liés ensemble et connectés au réseau StorageGRID Grid Network (eth0) et au réseau client (eth2).
- **mtc** : l'un des ports physiques 1 GbE de l'appareil. Une ou plusieurs interfaces mtc sont liées pour former l'interface réseau Admin (eth1). Vous pouvez laisser d'autres interfaces mtc disponibles pour une connectivité locale temporaire pour un technicien du centre de données.

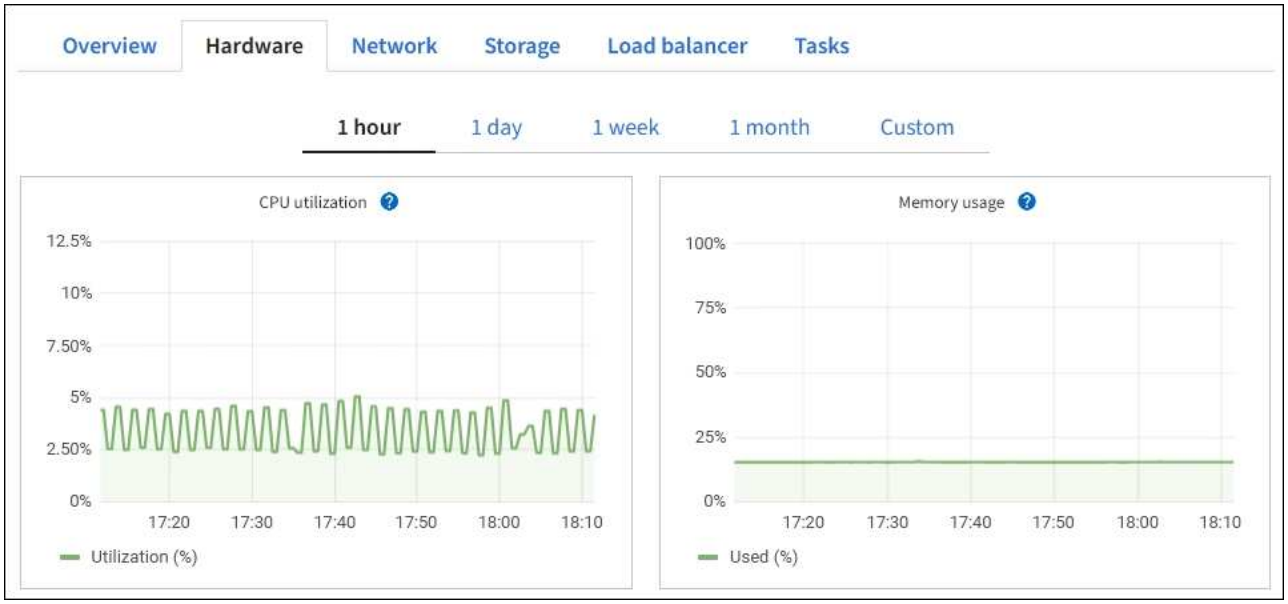


La section alertes de l'onglet Overview affiche toutes les alertes actives du nœud.

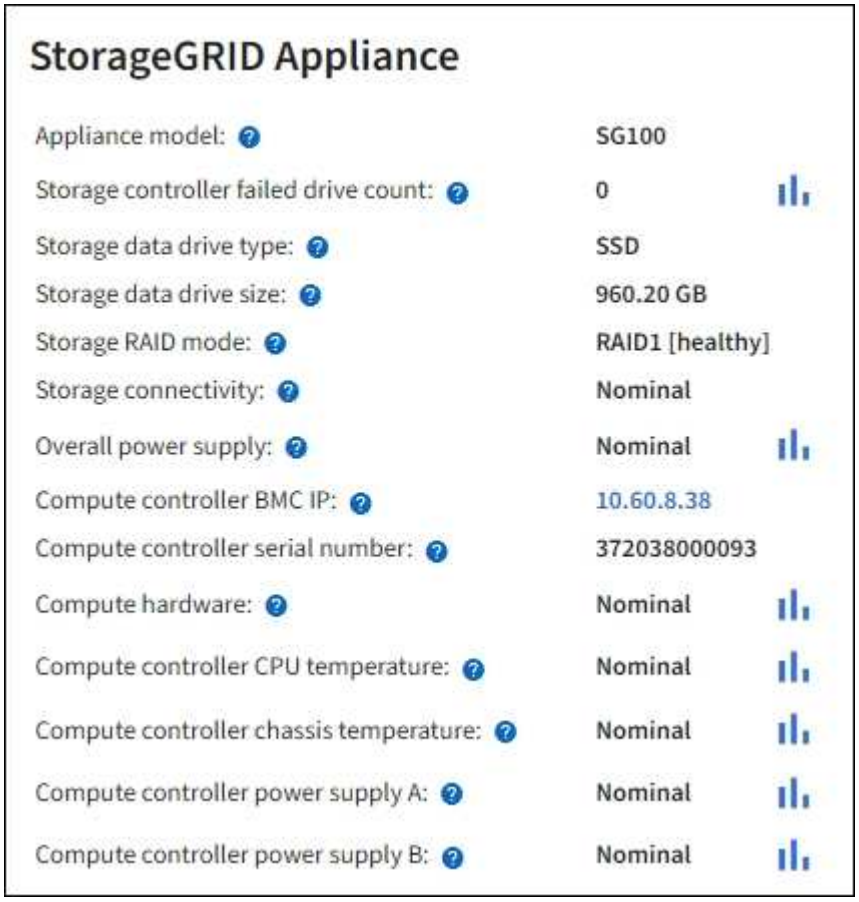
3. Sélectionnez **matériel** pour plus d'informations sur l'appareil.

   a. Affichez les graphiques d'utilisation de l'UC et de la mémoire pour déterminer les pourcentages d'utilisation de l'UC et de la mémoire au fil du temps. Pour afficher un intervalle de temps différent, sélectionnez l'une des commandes au-dessus du graphique ou du graphique. Vous pouvez afficher les informations disponibles pour les intervalles de 1 heure, 1 jour, 1 semaine ou 1 mois. Vous pouvez également définir un intervalle personnalisé, qui vous permet de spécifier des plages de date et

d’heure.



b. Faites défiler vers le bas pour afficher le tableau des composants de l’appareil. Ce tableau contient des informations telles que le nom du modèle, le numéro de série, la version du micrologiciel du contrôleur et l’état de chaque composant.



Dans la table Appliance	Description
Modèle de type appliance	Numéro de modèle de cette appliance StorageGRID.

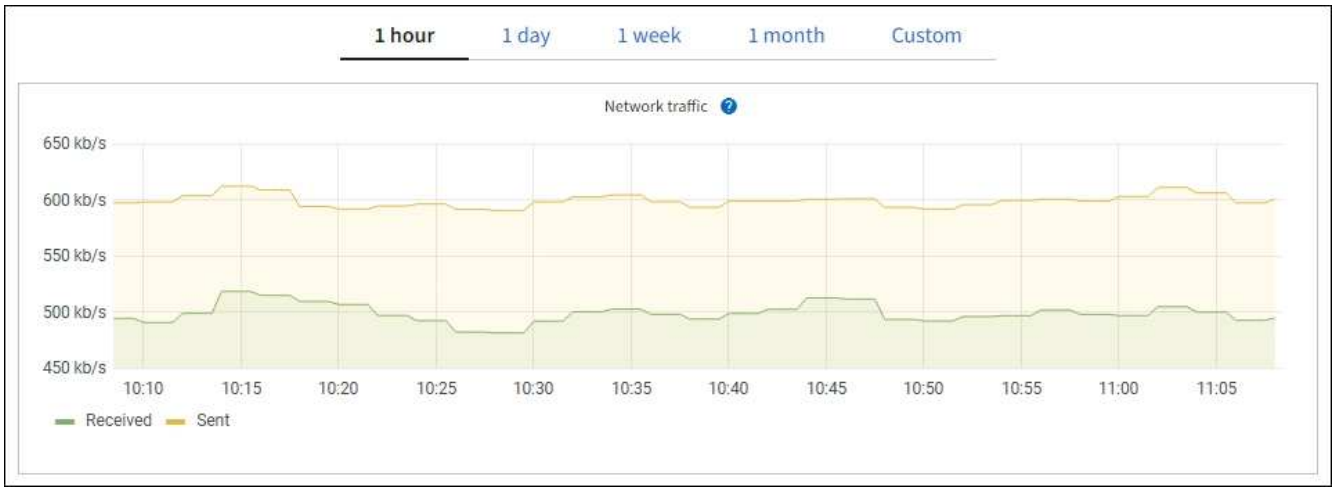
Dans la table Appliance	Description
Nombre de disques défaillants du contrôleur de stockage	Le nombre de disques qui ne sont pas optimaux.
Type de disque de données de stockage	Type de disque dur (HDD) ou SSD (Solid State Drive) de l'appliance.
Taille du disque de stockage des données	La taille effective d'un lecteur de données.
Mode de stockage RAID	Mode RAID de l'appareil.
Bloc d'alimentation général	L'état de toutes les alimentations de l'appareil.
IP BMC du contrôleur de calcul	Adresse IP du port du contrôleur de gestion de la carte mère (BMC) dans le contrôleur de calcul. Vous pouvez utiliser cette adresse IP pour vous connecter à l'interface BMC afin de surveiller et de diagnostiquer le matériel de l'appliance. Ce champ ne s'affiche pas pour les modèles d'appliance qui ne contiennent pas de contrôleur BMC.
Numéro de série du contrôleur de calcul	Numéro de série du contrôleur de calcul.
Matériel de calcul	L'état du matériel du contrôleur de calcul.
Température du processeur du contrôleur de calcul	L'état de température de l'UC du contrôleur de calcul.
Température du châssis du contrôleur de calcul	État de température du contrôleur de calcul.

a. Confirmer que tous les États sont « nominaux ».

   Si un statut n'est pas « nominal », passez en revue les alertes en cours.

4. Sélectionnez **réseau** pour afficher les informations de chaque réseau.

   Le graphique trafic réseau fournit un récapitulatif du trafic réseau global.



a. Consultez la section interfaces réseau.

Network interfaces

Name	Hardware address	Speed	Duplex	Auto-negotiation	Link status
eth0	0C:42:A1:86:B5:B0	100 Gigabit	Full	Off	Up
eth1	B4:A9:FC:71:68:36	Gigabit	Full	Off	Up
eth2	0C:42:A1:86:B5:B0	100 Gigabit	Full	Off	Up
hic1	0C:42:A1:86:B5:B0	25 Gigabit	Full	On	Up
hic2	0C:42:A1:86:B5:B0	25 Gigabit	Full	On	Up
hic3	0C:42:A1:86:B5:B0	25 Gigabit	Full	On	Up
hic4	0C:42:A1:86:B5:B0	25 Gigabit	Full	On	Up
mtc1	B4:A9:FC:71:68:36	Gigabit	Full	On	Up
mtc2	B4:A9:FC:71:68:35	Gigabit	Full	On	Up

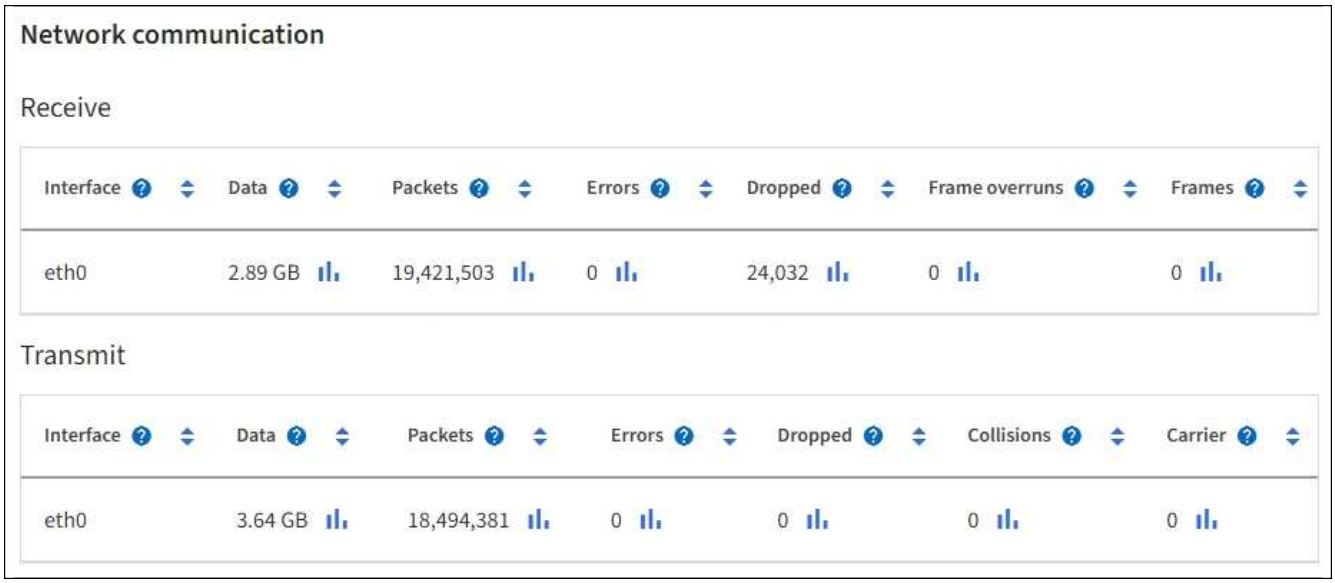
Utilisez le tableau suivant avec les valeurs de la colonne **Speed** du tableau interfaces réseau pour déterminer si les quatre ports réseau 40/100-GbE de l'appliance ont été configurés pour utiliser le mode actif/sauvegarde ou le mode LACP.

Les valeurs indiquées dans le tableau supposent que les quatre liens sont utilisés.

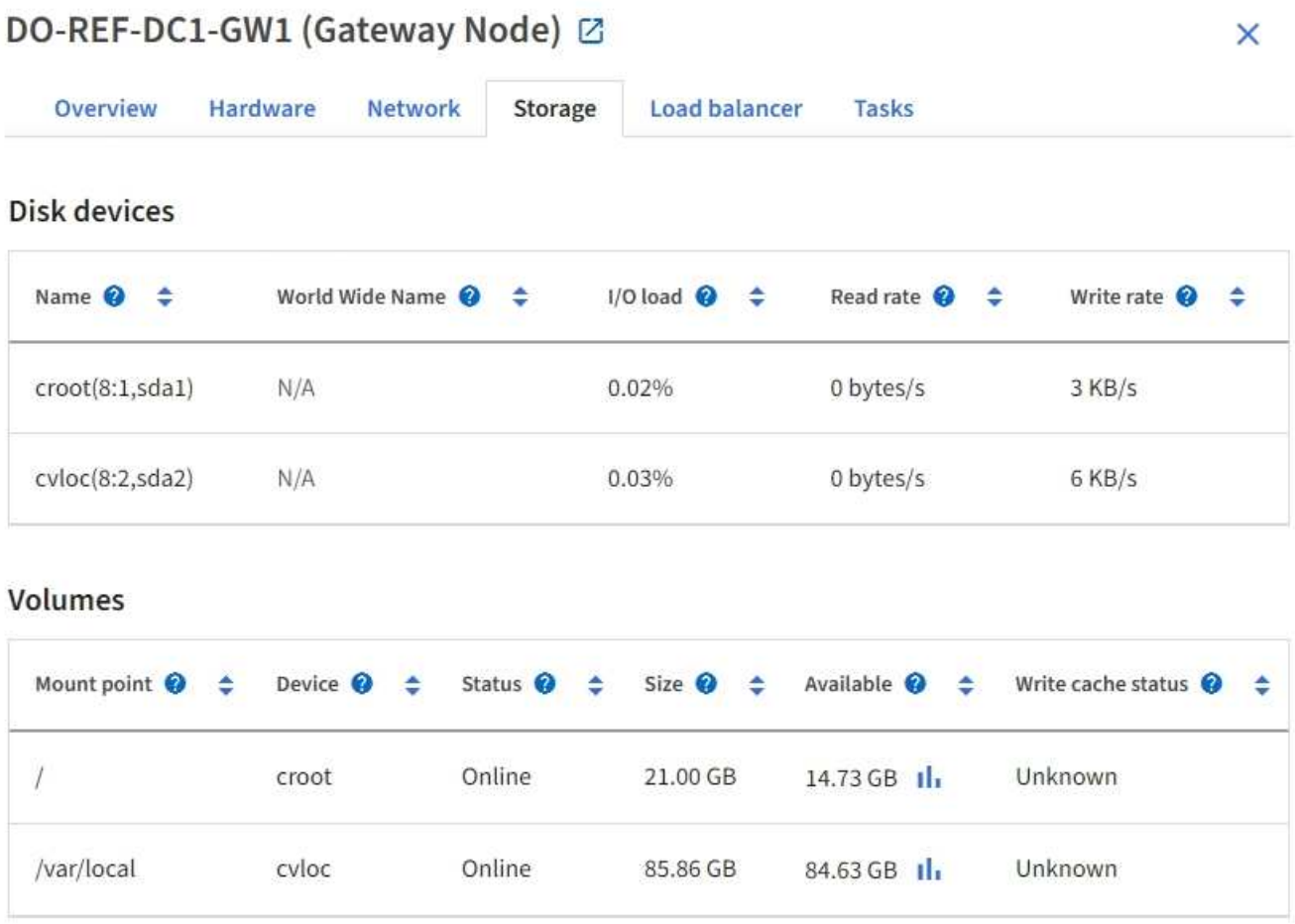
Mode de liaison	Mode du lien	Vitesse de la liaison HIC individuelle (hic 1, hi2, hic 3, hic 4)	Vitesse réseau prévue pour la grille/le client (eth0, eth2)
Agrégat	LACP	100	400
Fixe	LACP	100	200
Fixe	Actif/sauvegarde	100	100
Agrégat	LACP	40	160
Fixe	LACP	40	80
Fixe	Actif/sauvegarde	40	40

b. Passez en revue la section communication réseau.

Les tableaux de réception et de transmission indiquent le nombre d'octets et de paquets reçus et envoyés sur chaque réseau ainsi que d'autres mesures de réception et de transmission.



5. Sélectionnez **Storage** pour afficher des informations sur les unités de disque et les volumes de l'appliance de services.



Informations associées

"Appareils de services SG100 et SG1000"

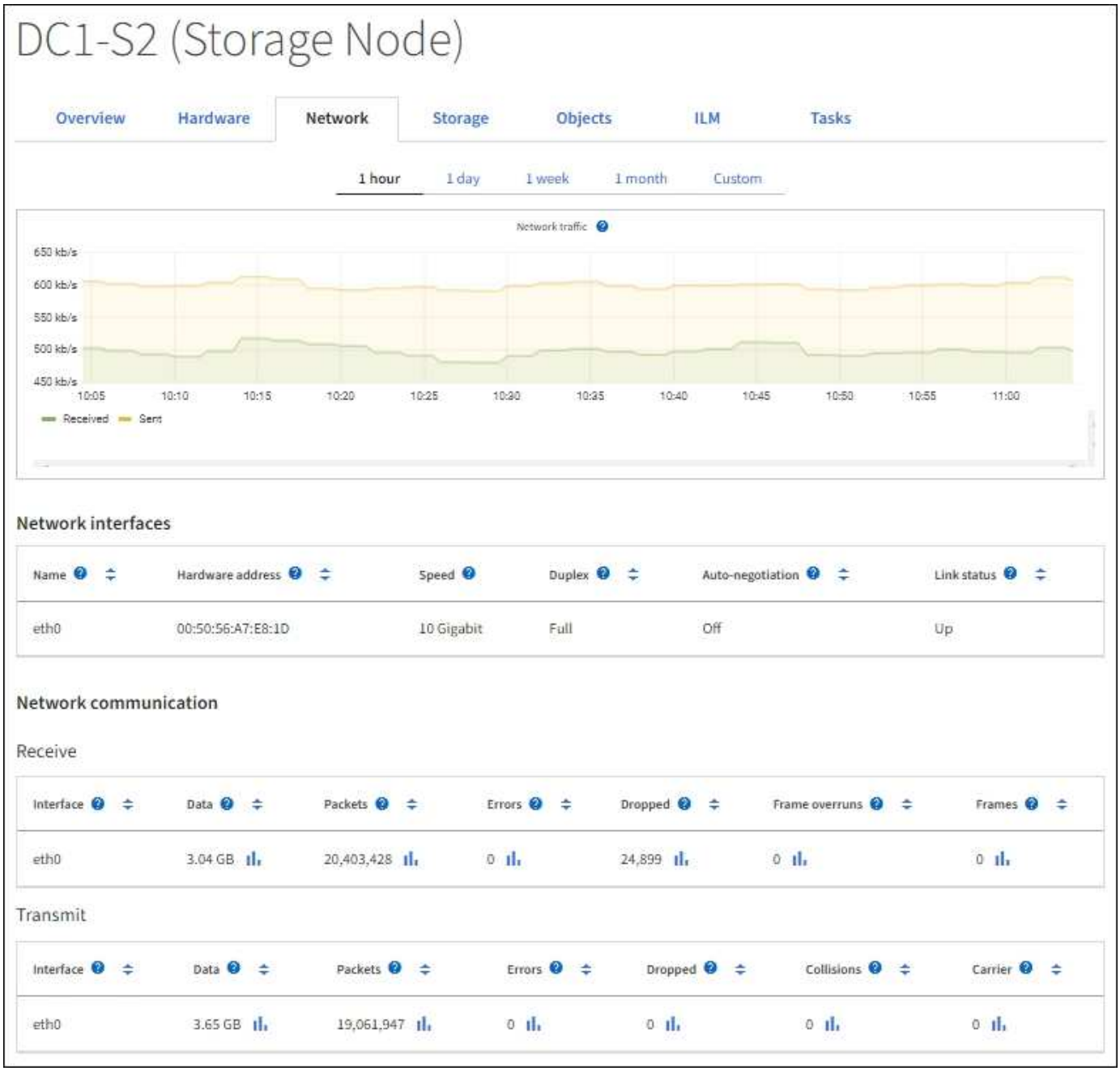
Afficher l'onglet réseau

L'onglet réseau affiche un graphique indiquant le trafic réseau reçu et envoyé sur toutes les interfaces réseau du nœud, du site ou de la grille.

L'onglet réseau s'affiche pour tous les nœuds, chaque site et la grille entière.

Pour afficher un intervalle de temps différent, sélectionnez l'une des commandes au-dessus du graphique ou du graphique. Vous pouvez afficher les informations disponibles pour les intervalles de 1 heure, 1 jour, 1 semaine ou 1 mois. Vous pouvez également définir un intervalle personnalisé, qui vous permet de spécifier des plages de date et d'heure.

Pour les nœuds, le tableau interfaces réseau fournit des informations sur les ports réseau physiques de chaque nœud. Le tableau des communications réseau fournit des détails sur les opérations de réception et de transmission de chaque nœud et sur tout compteur d'erreurs signalé par le pilote.



Informations associées

"Contrôle des connexions réseau et des performances"

Afficher l'onglet stockage

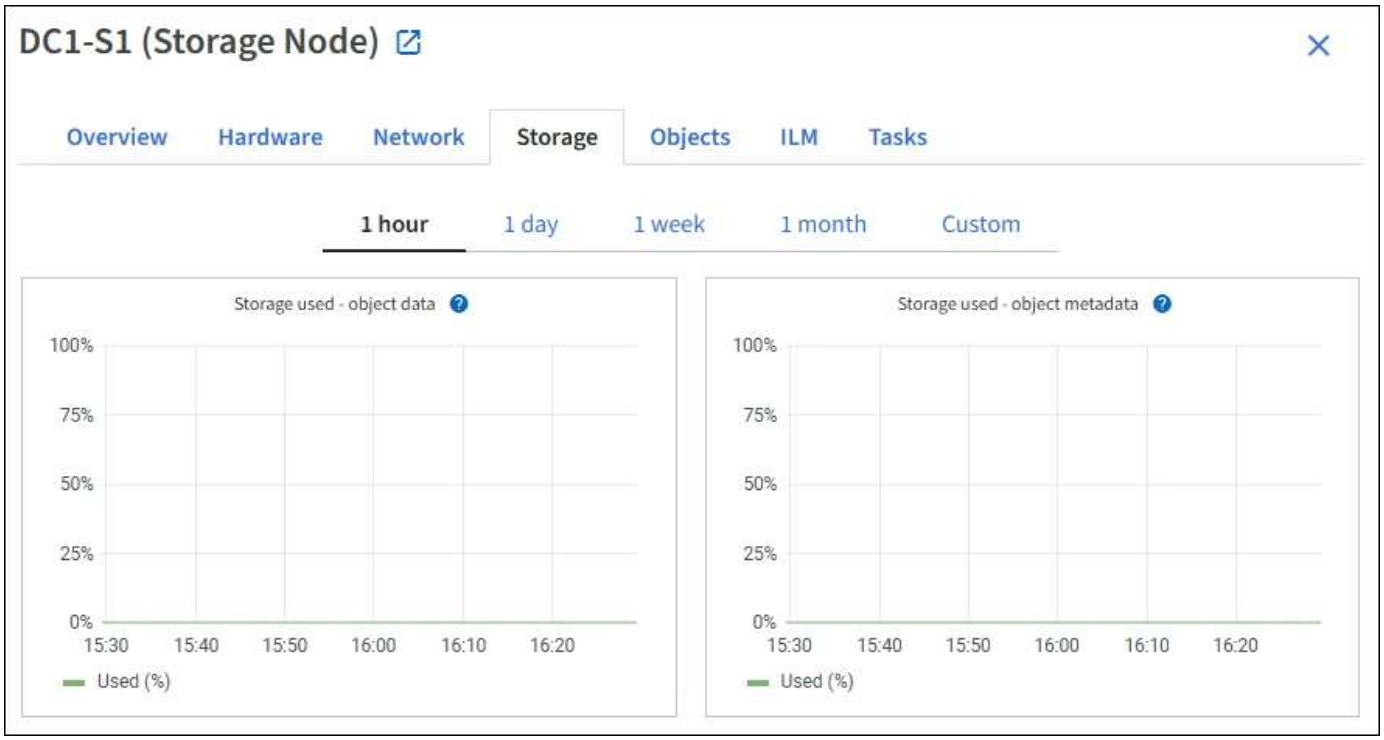
L'onglet stockage récapitule la disponibilité du stockage et d'autres mesures de stockage.

L'onglet stockage s'affiche pour tous les nœuds, chaque site et la grille complète.

Graphiques utilisés pour le stockage

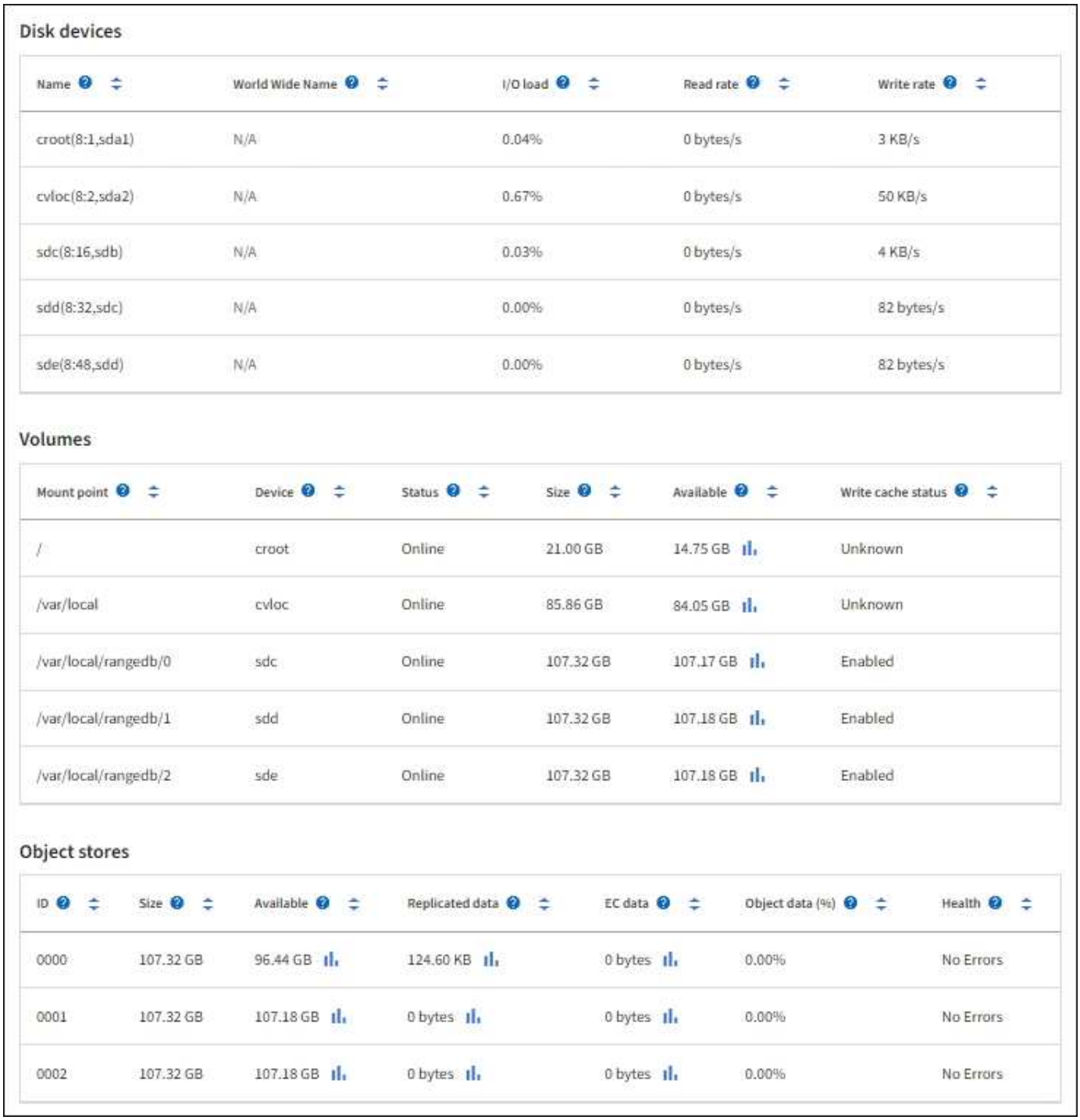
Pour les nœuds de stockage, chaque site et la grille dans son intégralité, l'onglet stockage contient des graphiques indiquant la quantité de stockage utilisée par les données d'objet et les métadonnées d'objet au fil du temps.

Lorsqu'un nœud n'est pas connecté à la grille, comme lors de la mise à niveau ou lorsqu'il est déconnecté, certains metrics peuvent être indisponibles ou exclus des totaux site et grid. Après qu'un nœud se reconnecte à la grille, attendez plusieurs minutes que les valeurs se stabilisent.



Tables de stockage des périphériques de disque, des volumes et des objets

Pour tous les nœuds, l'onglet stockage contient des détails sur les unités de disque et les volumes du nœud. Pour les nœuds de stockage, le tableau magasins d'objets fournit des informations sur chaque volume de stockage.



Disk devices

Name	World Wide Name	I/O load	Read rate	Write rate
croot(8:1,sda1)	N/A	0.04%	0 bytes/s	3 KB/s
cvloc(8:2,sda2)	N/A	0.67%	0 bytes/s	50 KB/s
sdc(8:16,sdb)	N/A	0.03%	0 bytes/s	4 KB/s
sdd(8:32,sdc)	N/A	0.00%	0 bytes/s	82 bytes/s
sde(8:48,sdd)	N/A	0.00%	0 bytes/s	82 bytes/s

Volumes

Mount point	Device	Status	Size	Available	Write cache status
/	croot	Online	21.00 GB	14.75 GB	Unknown
/var/local	cvloc	Online	85.86 GB	84.05 GB	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.17 GB	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/2	sde	Online	107.32 GB	107.18 GB	Enabled

Object stores

ID	Size	Available	Replicated data	EC data	Object data (%)	Health
0000	107.32 GB	96.44 GB	124.60 KB	0 bytes	0.00%	No Errors
0001	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0002	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors

Informations associées

"Surveiller la capacité de stockage"

Utilisez l'onglet tâche pour redémarrer un nœud de la grille

L'onglet tâche permet de redémarrer le nœud sélectionné. L'onglet tâche s'affiche pour tous les nœuds.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".

- Vous disposez de l’autorisation Maintenance ou accès racine.
- Vous avez la phrase secrète pour le provisionnement.

Description de la tâche

Vous pouvez utiliser l’onglet tâche pour redémarrer un nœud. Pour les nœuds d’appliance, vous pouvez également utiliser l’onglet tâche pour placer l’appliance en mode maintenance.

- Le redémarrage d’un nœud de grille à partir de l’onglet tâche émet la commande de redémarrage sur le nœud cible. Lorsque vous redémarrez un nœud, celui-ci s’arrête et redémarre. Tous les services sont redémarrés automatiquement.

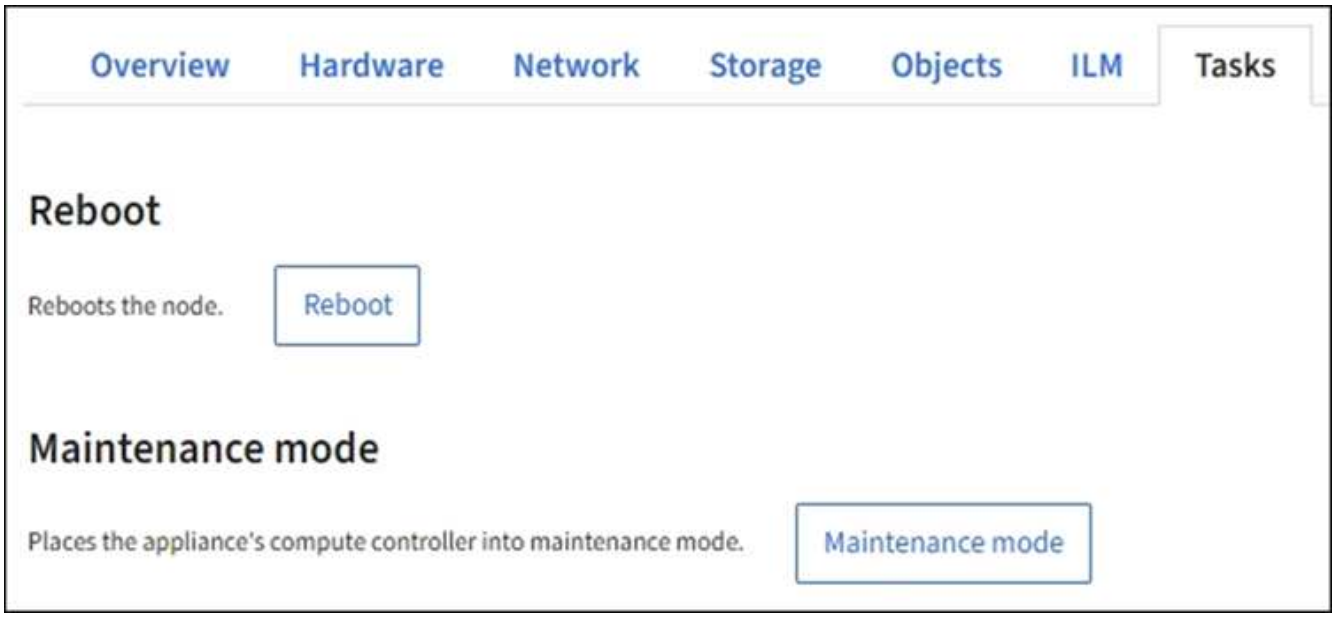
  Si vous prévoyez de redémarrer un nœud de stockage, notez ce qui suit :

  - Si une règle ILM spécifie un comportement d’entrée de la double allocation ou si la règle indique un équilibrage et qu’il n’est pas possible de créer immédiatement toutes les copies nécessaires, StorageGRID valide immédiatement les objets récemment ingérées sur deux nœuds de stockage du même site, et évalue la ILM plus tard. Si vous souhaitez redémarrer deux ou plusieurs nœuds de stockage sur un site donné, il se peut que vous ne puissiez pas accéder à ces objets pendant la durée du redémarrage.
  - Pour vous assurer que vous pouvez accéder à tous les objets lors du redémarrage d’un nœud de stockage, arrêtez de les ingérer sur un site pendant environ une heure avant de redémarrer le nœud.
- Vous devrez peut-être placer une appliance StorageGRID en mode de maintenance pour effectuer certaines procédures comme la modification de la configuration de la liaison ou le remplacement d’un contrôleur de stockage. Pour obtenir des instructions, reportez-vous à la section "Mettez l’appareil en mode maintenance".

  Dans de rares cas, le fait de placer une appliance StorageGRID en mode de maintenance peut rendre l’appliance indisponible pour l’accès à distance.

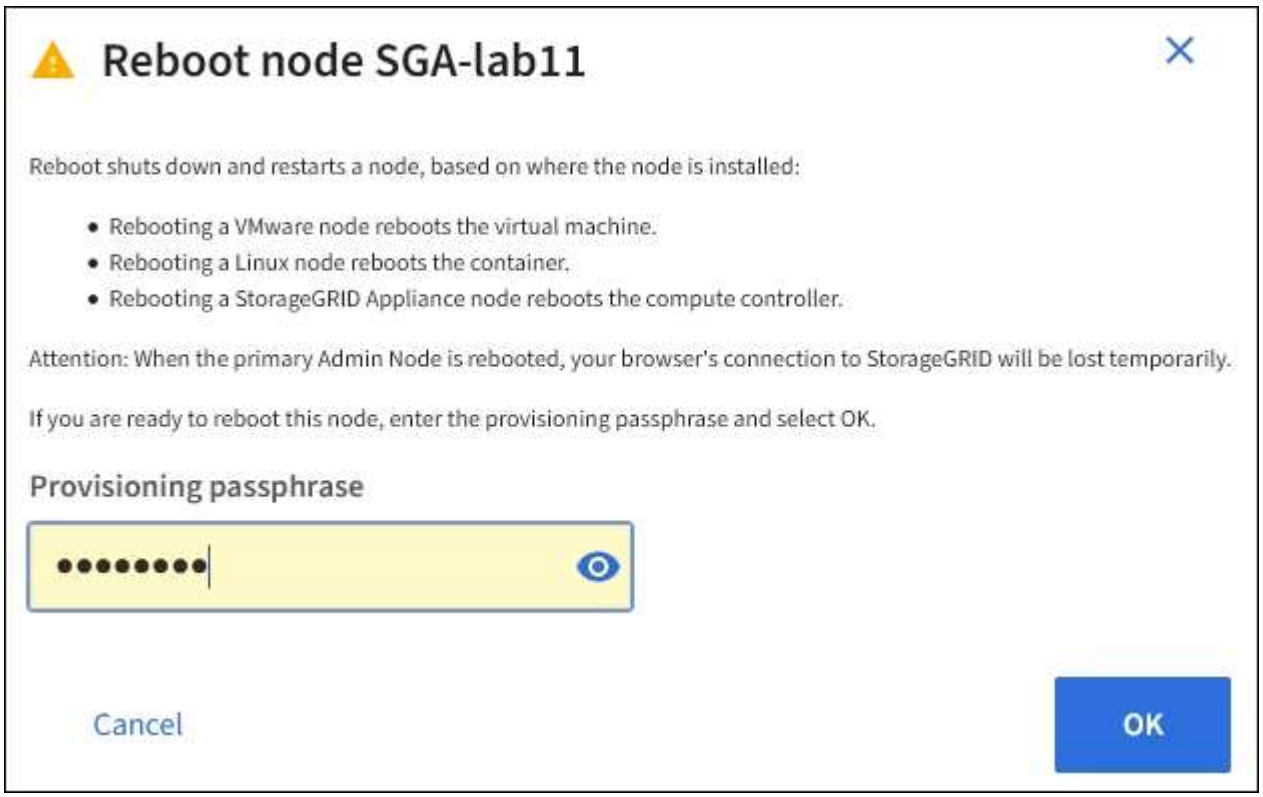
Étapes

1. Sélectionnez **NOEUDS**.
2. Sélectionnez le nœud de grille que vous souhaitez redémarrer.
3. Sélectionnez l’onglet **tâches**.



4. Sélectionnez **Reboot**.

   Une boîte de dialogue de confirmation s'affiche.



> Si vous redémarrez le nœud d'administration principal, la boîte de dialogue de confirmation vous rappelle que la connexion de votre navigateur au Grid Manager sera interrompue temporairement lorsque les services sont arrêtés.

5. Entrez la phrase de passe de provisionnement et sélectionnez **OK**.
6. Attendez que le nœud redémarre.

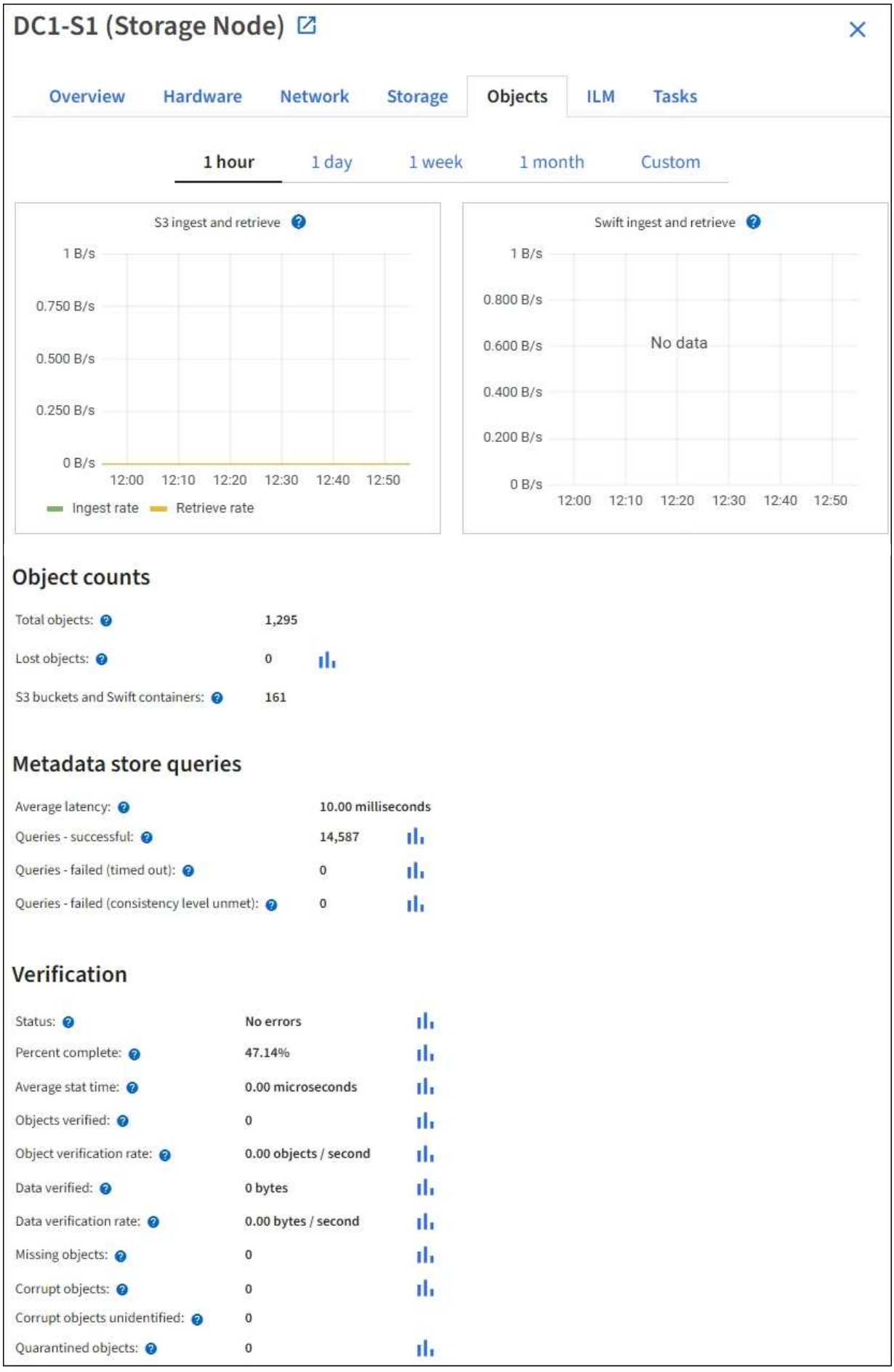
La fermeture des services peut prendre un certain temps.

Lorsque le nœud est en cours de redémarrage, l'icône grise (administrativement en panne) s'affiche sur le côté gauche de la page **Nodes**. Lorsque tous les services ont redémarré et que le nœud est connecté avec succès à la grille, la page **noeuds** doit afficher un état normal (aucune icône à gauche du nom du nœud), indiquant qu'aucune alerte n'est active et que le nœud est connecté à la grille.

Afficher l'onglet objets

L'onglet objets fournit des informations sur "S3" et "SWIFT" taux d'entrée et de récupération.

L'onglet objets s'affiche pour chaque nœud de stockage, chaque site et la grille entière. Pour les nœuds de stockage, l'onglet objets fournit également le nombre d'objets et des informations sur les requêtes de métadonnées et la vérification en arrière-plan.

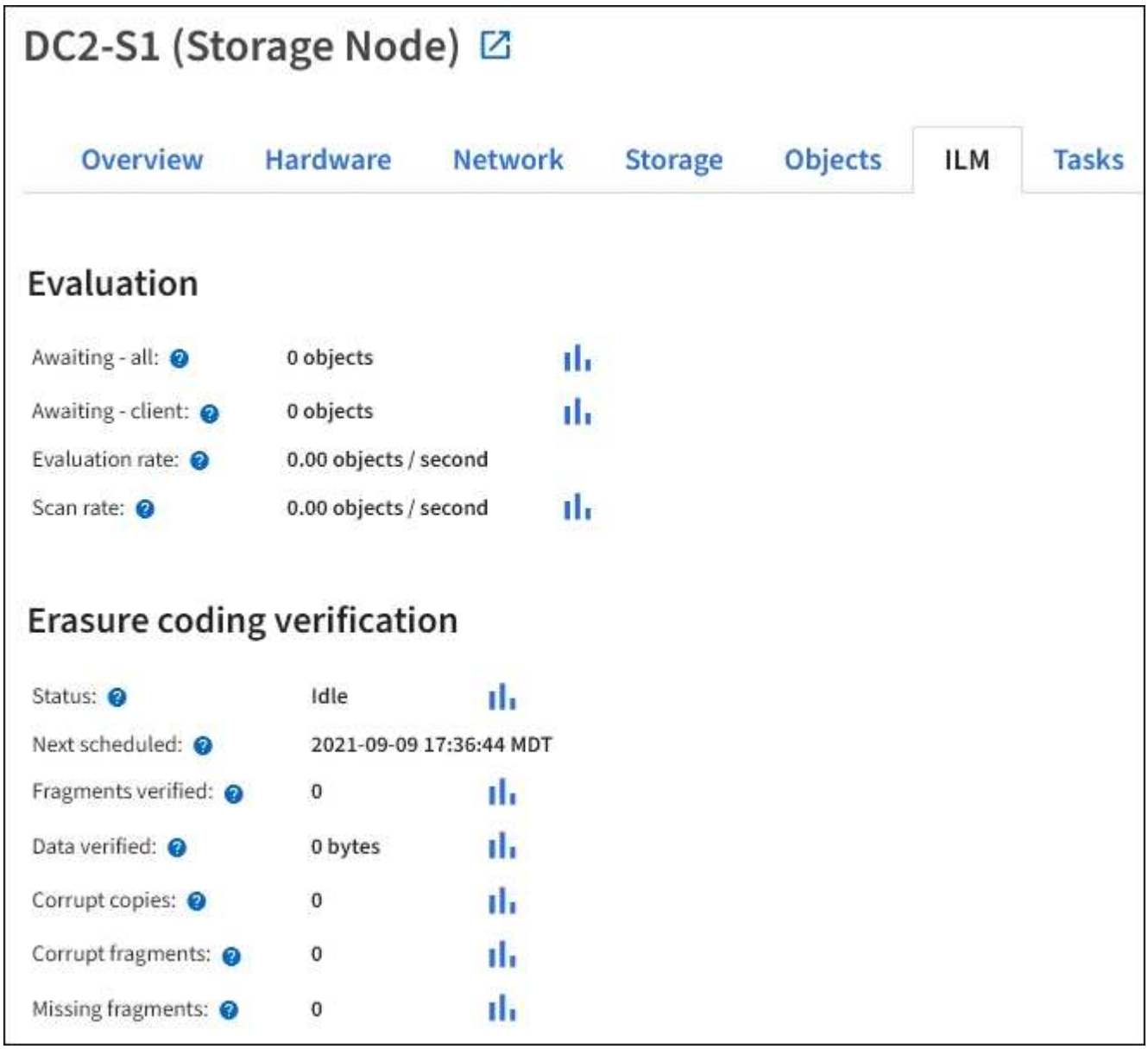

DC1-S1 (Storage Node)
Overview
Hardware
Network
Storage
Objects
ILM
Tasks
1 hour
1 day
1 week
1 month
Custom
S3 ingest and retrieve
1 B/s
0.750 B/s
0.500 B/s
0.250 B/s
0 B/s
12:00
12:10
12:20
12:30
12:40
12:50
Ingest rate
Retrieve rate
Swift ingest and retrieve
1 B/s
0.800 B/s
0.600 B/s
0.400 B/s
0.200 B/s
0 B/s
No data
12:00
12:10
12:20
12:30
12:40
12:50
Object counts
Total objects: 1,295
Lost objects: 0
S3 buckets and Swift containers: 161
Metadata store queries
Average latency: 10.00 milliseconds
Queries - successful: 14,587
Queries - failed (timed out): 0
Queries - failed (consistency level unmet): 0
Verification
Status: No errors
Percent complete: 47.14%
Average stat time: 0.00 microseconds
Objects verified: 0
Object verification rate: 0.00 objects / second
Data verified: 0 bytes
Data verification rate: 0.00 bytes / second
Missing objects: 0
Corrupt objects: 0
Corrupt objects unidentified: 0
Quarantined objects: 0

Afficher l'onglet ILM

L'onglet ILM fournit des informations sur les opérations de gestion du cycle de vie de l'information (ILM).

L'onglet ILM s'affiche pour chaque nœud de stockage, chaque site et la grille dans son ensemble. L'onglet ILM affiche un graphique de la file d'attente ILM sur la durée. Pour la grille, cet onglet indique également le temps estimé de l'analyse ILM complète de tous les objets.

Pour les nœuds de stockage, l'onglet ILM fournit des informations détaillées sur l'évaluation ILM et la vérification en arrière-plan des objets avec code d'effacement.



Informations associées

"Contrôle la gestion du cycle de vie des informations"

"Administrer StorageGRID"

Afficher l'onglet équilibreur de charge

L'onglet Load Balancer contient des graphiques de performance et de diagnostic relatifs au fonctionnement du service Load Balancer.

L'onglet Load Balancer s'affiche pour les nœuds d'administration et les nœuds de passerelle, chaque site et la grille dans son ensemble. Pour chaque site, l'onglet Load Balancer fournit un récapitulatif global des statistiques pour tous les nœuds de ce site. Pour toute la grille, l'onglet Load Balancer fournit un récapitulatif global des statistiques pour tous les sites.

Si aucune E/S n'est exécutée via le service Load Balancer ou si aucun équilibreur de charge n'est configuré, les graphiques affichent « aucune donnée ».

Trafic des demandes

Ce graphique fournit une moyenne mobile de 3 minutes du débit des données transmises entre les terminaux de l'équilibreur de charge et les clients effectuant les demandes, en bits par seconde.

Cette valeur est mise à jour à la fin de chaque demande. Par conséquent, cette valeur peut différer du débit en temps réel à des taux de demande faibles ou pour des demandes très longues. Vous pouvez consulter l'onglet réseau pour obtenir une vue plus réaliste du comportement actuel du réseau.

Taux de demande entrante

Ce graphique fournit une moyenne mobile de 3 minutes du nombre de nouvelles demandes par seconde, ventilées par type de demande (OBTENIR, PLACER, TÊTE et SUPPRIMER). Cette valeur est mise à jour lorsque les en-têtes d'une nouvelle demande ont été validés.

Durée moyenne de la demande (non-erreur)

Ce graphique fournit une moyenne mobile de 3 minutes des durées de requête, ventilées par type de demande (OBTENIR, PLACER, TÊTE et SUPPRIMER). Chaque durée de la demande commence lorsqu'un en-tête de requête est analysé par le service Load Balancer et se termine lorsque le corps de réponse complet est renvoyé au client.

Taux de réponse à l'erreur

Ce graphique fournit une moyenne mobile de 3 minutes du nombre de réponses d'erreur renvoyées aux clients par seconde, ventilées par le code de réponse d'erreur.

Informations associées

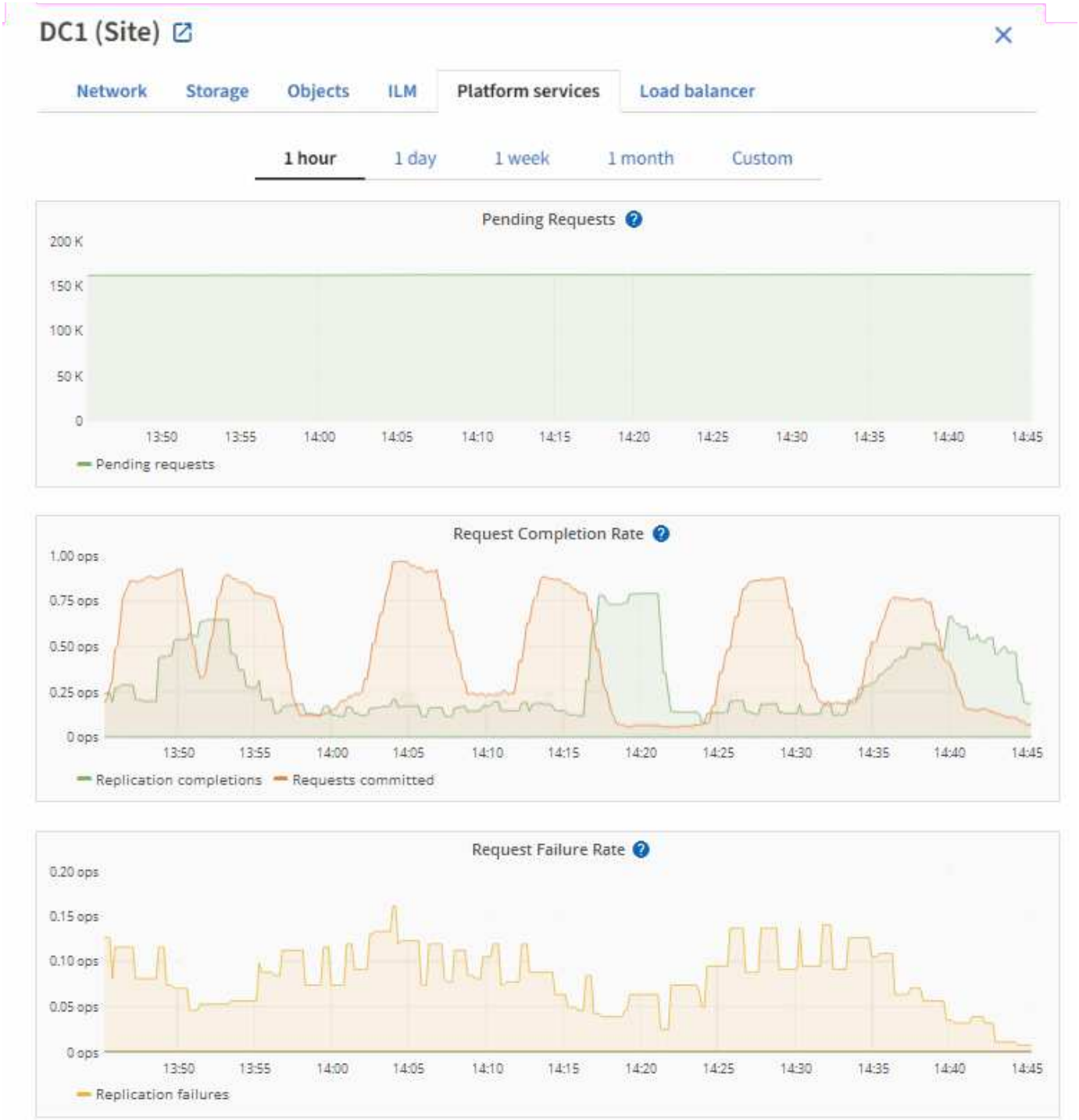
"Surveiller les opérations d'équilibrage de charge"

"Administrer StorageGRID"

Afficher l'onglet Platform Services

L'onglet Services de plateforme fournit des informations sur les opérations de service de la plateforme S3 sur un site.

L'onglet Platform Services s'affiche pour chaque site. Cet onglet fournit des informations sur les services de la plateforme S3, comme la réplication CloudMirror et le service d'intégration de la recherche. Les graphiques de cet onglet affichent des mesures telles que le nombre de requêtes en attente, le taux d'achèvement de la requête et le taux d'échec de la requête.



Pour plus d'informations sur les services de la plateforme S3, notamment des informations de dépannage, consultez le "Instructions d'administration de StorageGRID".

Affichez l'onglet SANtricity System Manager

L'onglet Gestionnaire système SANtricity de la page nœuds du Gestionnaire de grid vous permet d'accéder à SANtricity System Manager sans avoir à configurer ni à connecter le port de gestion de l'appliance de stockage. Cet onglet permet de consulter les informations de diagnostic du matériel et les informations environnementales, ainsi que les problèmes liés aux lecteurs.

L'onglet SANtricity System Manager s'affiche uniquement pour les nœuds d'appliance de stockage qui utilisent le matériel E-Series.

Grâce à SANtricity System Manager, vous pouvez effectuer les opérations suivantes :

- Affichez des données sur les performances, telles que les performances au niveau des baies de stockage, la latence des E/S, l'utilisation du CPU du contrôleur de stockage et le débit.
- Vérifiez l'état des composants matériels.
- Exécutez des fonctions de support, notamment l'affichage des données de diagnostic et la configuration du système E-Series AutoSupport.

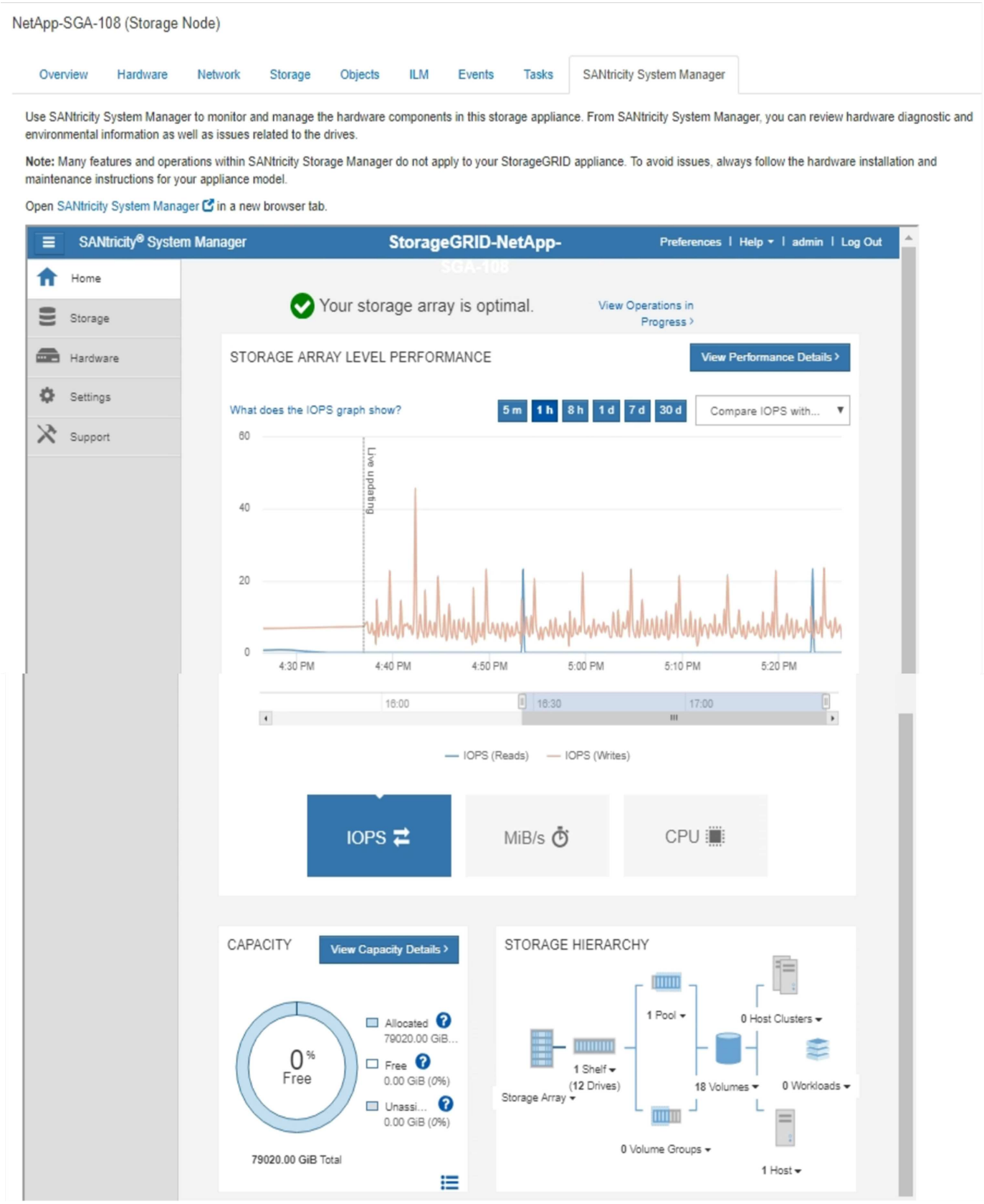
Pour utiliser SANtricity System Manager afin de configurer un proxy pour E-Series AutoSupport, reportez-vous à la section "Envoyez des messages AutoSupport E-Series via StorageGRID".

Pour accéder au Gestionnaire système SANtricity via le Gestionnaire de grille, vous devez disposer de l'autorisation d'administrateur de l'appliance de stockage ou de l'autorisation d'accès racine.

Vous devez disposer d'un firmware SANtricity 8.70 ou supérieur pour accéder à SANtricity System Manager à l'aide de Grid Manager.

L'accès à SANtricity System Manager à partir de Grid Manager se limite généralement à la surveillance du matériel de l'appliance et à la configuration des baies E-Series AutoSupport. De nombreuses fonctionnalités et opérations dans SANtricity System Manager, telles que la mise à niveau du firmware, ne s'appliquent pas à la surveillance de l'appliance StorageGRID. Pour éviter tout problème, suivez toujours les instructions de maintenance du matériel de votre appareil.

L'onglet affiche la page d'accueil de SANtricity System Manager.



Pour plus de facilité, vous pouvez utiliser le lien SANtricity System Manager pour ouvrir SANtricity System Manager dans une nouvelle fenêtre de navigateur.

Pour afficher des informations détaillées sur les performances au niveau de la baie de stockage et l'utilisation

de la capacité, positionnez le curseur sur chaque graphique.

Pour plus de détails sur l'affichage des informations accessibles depuis l'onglet SANtricity System Manager, reportez-vous à la section "Documentation sur les systèmes NetApp E-Series et SANtricity".

Informations associées

- "Entretenir l'appareil SG6000"
- "Conservez l'appliance SG5700"

Informations à surveiller régulièrement

Quoi et quand surveiller

Même si le système StorageGRID peut continuer à fonctionner lorsque des erreurs se produisent ou que des parties de la grille sont indisponibles, vous devez surveiller et résoudre les problèmes potentiels avant qu'ils n'affectent l'efficacité ou la disponibilité de la grille.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous disposez d'autorisations d'accès spécifiques.

A propos des tâches de surveillance

Un système occupé génère de grandes quantités d'informations. La liste suivante fournit des conseils sur les informations les plus importantes à surveiller en permanence.

Quoi surveiller	Fréquence
"État de santé du système"	Tous les jours
Taux auquel "Capacité des objets et des métadonnées du nœud de stockage" est en cours de consommation	Hebdomadaire
"Opérations de gestion du cycle de vie des informations"	Hebdomadaire
"Ressources réseau et système"	Hebdomadaire
"Activité des locataires"	Hebdomadaire
"Opérations d'équilibrage de la charge"	Après la configuration initiale et après toute modification de la configuration
"Connexions de fédération de grille"	Hebdomadaire
"Disponibilité des correctifs logiciels et des mises à niveau logicielles"	Tous les mois

Quoi surveiller	Fréquence
"Capacité du système de stockage d'archives externe"	Hebdomadaire

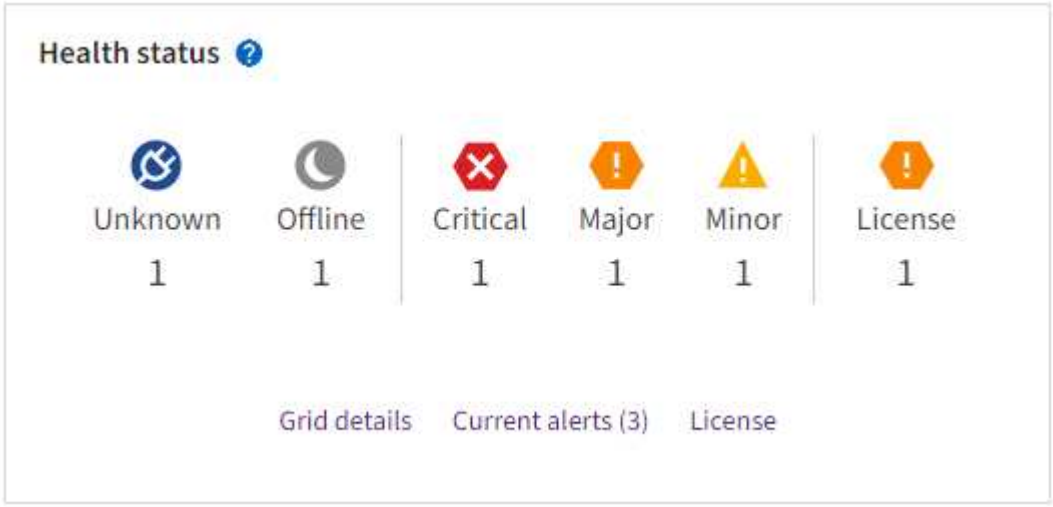
Contrôle de l'état des systèmes

Surveillez quotidiennement l'état global de votre système StorageGRID.

Description de la tâche

Le système StorageGRID peut continuer à fonctionner lorsque certaines parties de la grille ne sont pas disponibles. Les problèmes potentiels signalés par des alertes ou des alarmes (système hérité) ne sont pas nécessairement des problèmes liés aux opérations du système. Examinez les problèmes résumés sur la carte d'état de santé du tableau de bord Grid Manager.

Pour être averti des alertes dès qu'elles sont déclenchées, vous pouvez le faire "configurez les notifications par e-mail pour les alertes" ou "Configurer les interruptions SNMP".



Lorsque des problèmes existent, des liens s'affichent pour vous permettre d'afficher des détails supplémentaires :

Lien	Apparaît lorsque…
Détails de la grille	Tous les nœuds sont déconnectés (état de connexion inconnu ou arrêté administrativement).
Alertes actuelles (critique, majeure, mineure)	Les alertes le sont actuellement actif.
Alertes récemment résolues	Alertes déclenchées au cours de la semaine dernière sont maintenant résolus.
Licence	Il y a un problème avec la licence logicielle de ce système StorageGRID. C'est possible "mettez à jour les informations de licence si nécessaire".

Surveiller les États de connexion du nœud

Si un ou plusieurs nœuds sont déconnectés de la grille, les opérations StorageGRID stratégiques peuvent être affectées. Surveillez les États de connexion des nœuds et traitez tous les problèmes rapidement.

Icône	Description	Action requise
	Non connecté - Inconnu Pour une raison inconnue, un nœud est déconnecté ou les services du nœud sont arrêtés de manière inattendue. Par exemple, un service du nœud peut être arrêté, ou le nœud a perdu sa connexion réseau en raison d'une panne de courant ou d'une panne imprévue. L'alerte **Impossible de communiquer avec le noeud** peut également être déclenchée. D'autres alertes peuvent également être actives.	Nécessite une attention immédiate. Sélectionnez chaque alerte et suivre les actions recommandées. Par exemple, vous devrez peut-être redémarrer un service qui a arrêté ou redémarré l'hôte du nœud. **Remarque** : un nœud peut apparaître comme inconnu pendant les opérations d'arrêt gérées. Dans ces cas, vous pouvez ignorer l'état Inconnu.
	Non connecté - Arrêt administratif Pour une raison prévue, le nœud n'est pas connecté au grid. Par exemple, le nœud ou les services du nœud ont été normalement arrêtés, le nœud est en cours de redémarrage ou le logiciel est mis à niveau. Une ou plusieurs alertes peuvent également être actives. En fonction du problème sous-jacent, ces nœuds sont souvent remis en ligne sans intervention.	Déterminez si des alertes affectent ce nœud. Si une ou plusieurs alertes sont actives, sélectionnez chaque alerte et suivre les actions recommandées.
	• Connecté* Le nœud est connecté à la grille.	Aucune action requise.

Afficher les alertes actuelles et résolues

Alertes actuelles : lorsqu'une alerte est déclenchée, une icône d'alerte s'affiche sur le tableau de bord. Une icône d'alerte s'affiche également pour le nœud sur la page nœuds. Si "les notifications par e-mail d'alerte sont configurées", une notification par e-mail sera également envoyée, sauf si l'alerte a été neutralisée.

Alertes résolues : vous pouvez rechercher et afficher un historique des alertes qui ont été résolues.

Vous pouvez également regarder la vidéo : "Vidéo : présentation des alertes pour StorageGRID 11.7"

Le tableau suivant décrit les informations affichées dans Grid Manager pour les alertes en cours et résolues.

En-tête de colonne	Description
Nom ou titre	Le nom de l'alerte et sa description.
Gravité	Gravité de l'alerte. Pour les alertes actuelles, si plusieurs alertes sont regroupées, la ligne de titre indique le nombre d'instances de cette alerte qui se produisent à chaque gravité. **Critique** : il existe une condition anormale qui a arrêté les opérations normales d'un noeud ou d'un service StorageGRID. Vous devez immédiatement résoudre le problème sous-jacent. Une interruption du service et une perte de données peuvent se produire si le problème n'est pas résolu. **Majeur** : il existe une condition anormale qui affecte les opérations en cours ou qui approche du seuil pour une alerte critique. Vous devez examiner les alertes majeures et résoudre tous les problèmes sous-jacents pour vérifier que leur condition anormale n'arrête pas le fonctionnement normal d'un nœud ou d'un service StorageGRID. **Mineur** : le système fonctionne normalement, mais il existe une condition anormale qui pourrait affecter la capacité de fonctionnement du système s'il continue. Vous devez surveiller et résoudre les alertes mineures qui ne sont pas claires par elles-mêmes pour vous assurer qu'elles n'entraînent pas de problème plus grave.
Temps déclenché	**Alertes actuelles** : date et heure auxquelles l'alerte a été déclenchée à l'heure locale et en UTC. Si plusieurs alertes sont regroupées, la ligne de titre affiche les heures de l'instance la plus récente de l'alerte (*le plus récent*) et de l'instance la plus ancienne de l'alerte (*le plus ancien*). **Alertes résolues** : il y a combien de temps l'alerte a été déclenchée.
Site/nœud	Nom du site et du nœud où l'alerte a eu lieu ou s'est produite.
État	Indique si l'alerte est active, neutralisée ou résolue. Si plusieurs alertes sont regroupées et que **toutes les alertes** sont sélectionnées dans la liste déroulante, la ligne de titre indique le nombre d'instances de cette alerte actives et le nombre d'instances désactivées.

En-tête de colonne	Description
Temps résolu (alertes résolues uniquement)	Il y a combien de temps l'alerte a été résolue.
Valeurs actuelles ou *valeurs de données*	Valeur de la mesure à l'origine du déclenchement de l'alerte. Pour certaines alertes, des valeurs supplémentaires sont affichées pour vous aider à comprendre et à examiner l'alerte. Par exemple, les valeurs affichées pour une alerte **stockage de données d'objet bas** comprennent le pourcentage d'espace disque utilisé, la quantité totale d'espace disque et la quantité d'espace disque utilisée. **Remarque :** si plusieurs alertes actuelles sont regroupées, les valeurs actuelles ne sont pas affichées dans la ligne de titre.
Valeurs déclenchées (alertes résolues uniquement)	Valeur de la mesure à l'origine du déclenchement de l'alerte. Pour certaines alertes, des valeurs supplémentaires sont affichées pour vous aider à comprendre et à examiner l'alerte. Par exemple, les valeurs affichées pour une alerte **stockage de données d'objet bas** comprennent le pourcentage d'espace disque utilisé, la quantité totale d'espace disque et la quantité d'espace disque utilisée.

Étapes

1. Sélectionnez le lien **alertes actuelles** ou **alertes résolues** pour afficher la liste des alertes de ces catégories. Vous pouvez également afficher les détails d'une alerte en sélectionnant **nœuds** > ***nœud*** > **vue d'ensemble**, puis en sélectionnant l'alerte dans le tableau alertes.

   Par défaut, les alertes actuelles s'affichent comme suit :

   - Les alertes déclenchées les plus récemment sont affichées en premier.
   - Plusieurs alertes du même type sont affichées sous la forme d'un groupe.
   - Les alertes qui ont été neutralisées ne sont pas affichées.
   - Pour une alerte spécifique sur un nœud spécifique, si les seuils sont atteints pour plus d'un niveau de gravité, seule l'alerte la plus grave est affichée. C'est-à-dire, si les seuils d'alerte sont atteints pour les niveaux de gravité mineur, majeur et critique, seule l'alerte critique s'affiche.

     La page d'alertes en cours est actualisée toutes les deux minutes.

2. Pour développer des groupes d'alertes, sélectionnez la touche d'avertissement vers le bas ⌄. Pour réduire les alertes individuelles d'un groupe, sélectionnez la touche UP caret ⌃, ou sélectionnez le nom du groupe.
3. Pour afficher des alertes individuelles au lieu de groupes d'alertes, décochez la case **alertes de groupe**.
4. Pour trier les alertes ou les groupes d'alertes actuels, sélectionnez les flèches haut/bas ⇅ dans chaque en-tête de colonne.
   - Lorsque **alertes de groupe** est sélectionné, les groupes d'alertes et les alertes individuelles de chaque groupe sont triés. Par exemple, vous pouvez trier les alertes d'un groupe par **heure déclenchée** pour trouver l'instance la plus récente d'une alerte spécifique.
   - Lorsque **alertes de groupe** est effacé, la liste complète des alertes est triée. Par exemple, vous pouvez trier toutes les alertes par **nœud/site** pour voir toutes les alertes affectant un nœud spécifique.

5. Pour filtrer les alertes actuelles par état (**toutes les alertes**, **Active** ou **Silence**, utilisez le menu déroulant situé en haut du tableau.

   Voir "Notifications d'alerte de silence".

6. Pour trier les alertes résolues :
   - Sélectionnez une période dans le menu déroulant **lorsqu'elle est déclenchée**.
   - Sélectionnez une ou plusieurs gravité dans le menu déroulant **gravité**.
   - Sélectionnez une ou plusieurs règles d'alerte par défaut ou personnalisées dans le menu déroulant **règle d'alerte** pour filtrer les alertes résolues associées à une règle d'alerte spécifique.
   - Sélectionnez un ou plusieurs nœuds dans le menu déroulant **Node** pour filtrer les alertes résolues liées à un nœud spécifique.
7. Pour afficher les détails d'une alerte spécifique, sélectionnez l'alerte. Une boîte de dialogue fournit des détails et des actions recommandées pour l'alerte que vous avez sélectionnée.
8. (Facultatif) pour une alerte spécifique, sélectionnez silence cette alerte pour désactiver la règle d'alerte qui a déclenché cette alerte.

   Vous devez disposer de l'autorisation gérer les alertes ou accès racine pour désactiver une règle d'alerte.

   > Soyez prudent lorsque vous décidez de désactiver une règle d'alerte. Si une règle d'alerte est mise en mode silencieux, il est possible que vous ne détectiez pas un problème sous-jacent tant qu'elle n'empêche pas l'exécution d'une opération critique.

9. Pour afficher les conditions actuelles de la règle d'alerte :
   a. Dans les détails de l'alerte, sélectionnez **Afficher les conditions**.

      Une fenêtre contextuelle s'affiche, répertoriant l'expression Prometheus pour chaque gravité définie.

   b. Pour fermer la fenêtre contextuelle, cliquez n'importe où en dehors de la fenêtre contextuelle.
10. Vous pouvez également sélectionner **Modifier la règle** pour modifier la règle d'alerte qui a déclenché cette alerte.

    Vous devez disposer de l'autorisation gérer les alertes ou accès racine pour modifier une règle d'alerte.

    > Soyez prudent lorsque vous décidez de modifier une règle d'alerte. Si vous modifiez les valeurs de déclenchement, il est possible que vous ne déteciez pas de problème sous-jacent tant qu'elle n'empêche pas l'exécution d'une opération critique.

11. Pour fermer les détails de l'alerte, sélectionnez **Fermer**.

Surveiller la capacité de stockage

Contrôlez l'espace total disponible pour vérifier que le système StorageGRID ne manque pas d'espace de stockage pour les objets ou les métadonnées d'objet.

StorageGRID stocke séparément les données d'objet et les métadonnées d'objet. Il réserve un espace spécifique pour une base de données Cassandra distribuée qui contient les métadonnées d'objet. Surveiller la quantité totale d'espace consommée pour les objets et les métadonnées d'objet, ainsi que les tendances en matière de quantité d'espace consommée pour chaque. Vous pourrez ainsi planifier l'ajout de nœuds et éviter toute panne de service.

C’est possible "affichez des informations sur la capacité de stockage" Pour la grille complète, pour chaque site et pour chaque nœud de stockage de votre système StorageGRID.

Surveiller la capacité de stockage pour l’ensemble de la grille

Surveillez la capacité de stockage globale de votre grid afin de vous assurer qu’il reste un espace libre adéquat pour les données d’objet et les métadonnées d’objet. Pour mieux comprendre les variations de capacité de stockage dans le temps, vous pouvez planifier l’ajout de nœuds de stockage ou de volumes avant de consommer la capacité de stockage utilisable de la grille.

Le tableau de bord de Grid Manager vous permet d’évaluer rapidement la quantité de stockage disponible pour l’ensemble du grid et pour chaque data Center. La page nœuds fournit des valeurs plus détaillées pour les données d’objet et les métadonnées d’objet.

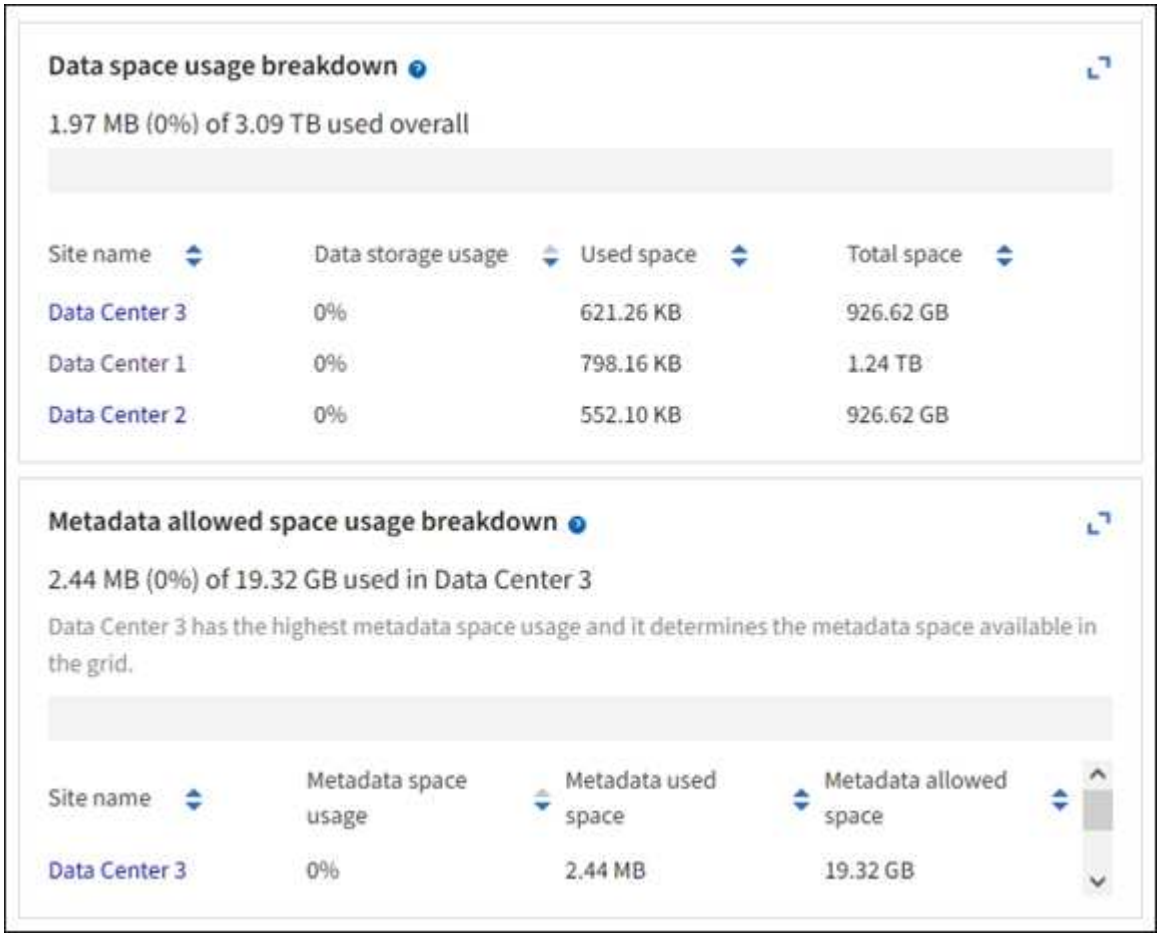
Étapes

1. Évaluez la quantité de stockage disponible pour l’ensemble du grid et pour chaque data Center.

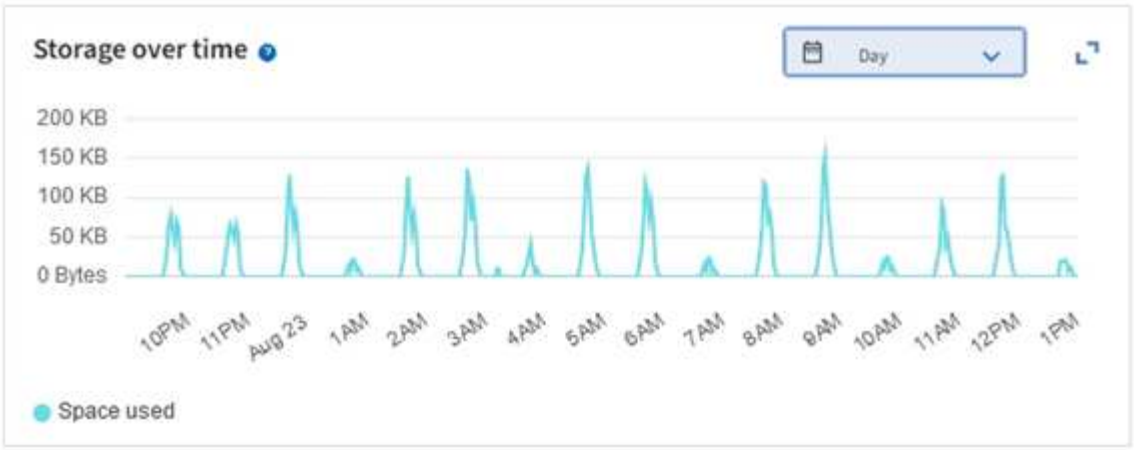
   a. Sélectionnez **Tableau de bord > vue d’ensemble**.

   b. Notez les valeurs de la répartition de l’utilisation de l’espace de données et les cartes de répartition de l’utilisation de l’espace autorisé dans les métadonnées. Chaque carte indique un pourcentage d’utilisation du stockage, la capacité de l’espace utilisé et l’espace total disponible ou autorisé par site.

   > Le résumé n’inclut pas les supports d’archivage.



   a. Notez le tableau sur la carte de stockage dans le temps. Utilisez la liste déroulante période pour vous aider à déterminer la rapidité de consommation du stockage.



2. Pour plus d'informations sur la quantité de stockage utilisée et la quantité de stockage restant disponible dans la grille pour les données d'objet et les métadonnées d'objet, consultez la page nœuds.
   a. Sélectionnez **NOEUDS**.
   b. Sélectionnez ***GRID*** > **stockage**.

   c. Placez votre curseur sur les graphiques **stockage utilisé - données d'objet** et **stockage utilisé - métadonnées d'objet** pour connaître la quantité de stockage d'objet et de métadonnées d'objet disponible pour l'ensemble de la grille, ainsi que la quantité utilisée au fil du temps.

> Les valeurs totales d'un site ou de la grille n'incluent pas les nœuds qui n'ont pas signalé de mesures depuis au moins cinq minutes, comme les nœuds hors ligne.

3. Planifiez une extension permettant d'ajouter des nœuds de stockage ou des volumes de stockage avant l'utilisation de la capacité de stockage utilisable de la grille.

   Lors de la planification d'une extension, réfléchissez au temps nécessaire pour approvisionner et installer du stockage supplémentaire.

Si votre règle ILM utilise le code d'effacement, vous pouvez préférer une extension lorsque les nœuds de stockage existants sont remplis à environ 70 % pour réduire le nombre de nœuds à ajouter.

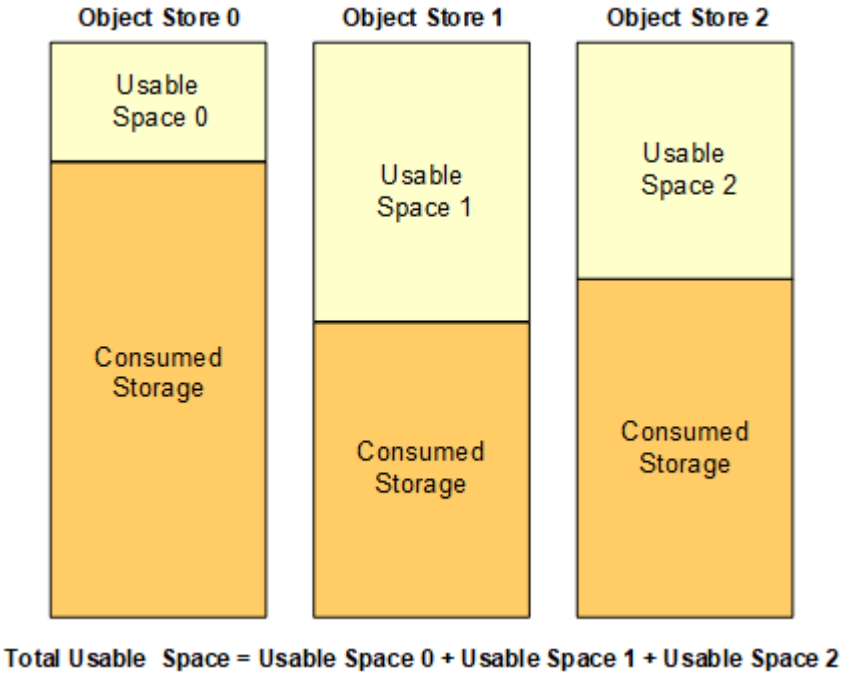
Pour plus d'informations sur la planification d'une extension de stockage, reportez-vous au "Instructions d'extension de StorageGRID".

Surveillez la capacité de stockage de chaque nœud de stockage

Surveillez l'espace total utilisable pour chaque nœud de stockage pour vous assurer que le nœud dispose de suffisamment d'espace pour les nouvelles données d'objet.

Description de la tâche

L'espace utilisable correspond à la quantité d'espace de stockage disponible pour stocker des objets. L'espace total utilisable d'un nœud de stockage est calculé en ajoutant ensemble l'espace disponible sur tous les magasins d'objets du nœud.



Étapes

1. Sélectionnez **NODES** > ***Storage Node*** > **Storage**.

   Les graphiques et les tableaux du nœud apparaissent.

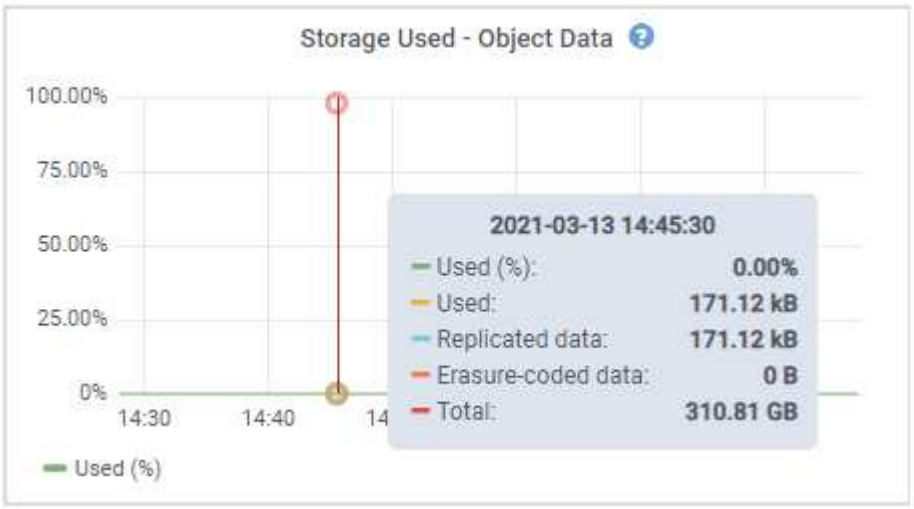
2. Positionnez le curseur sur le graphique de données d'objet stockage utilisé -.

   Les valeurs suivantes sont affichées :

   - **Utilisé (%)** : pourcentage de l'espace utilisable total qui a été utilisé pour les données d'objet.
   - **Used** : quantité de l'espace utilisable total qui a été utilisé pour les données d'objet.
   - **Données répliquées** : estimation de la quantité de données d'objet répliqué sur ce nœud, site ou grille.
   - **Données avec code d'effacement** : estimation de la quantité de données d'objet avec code

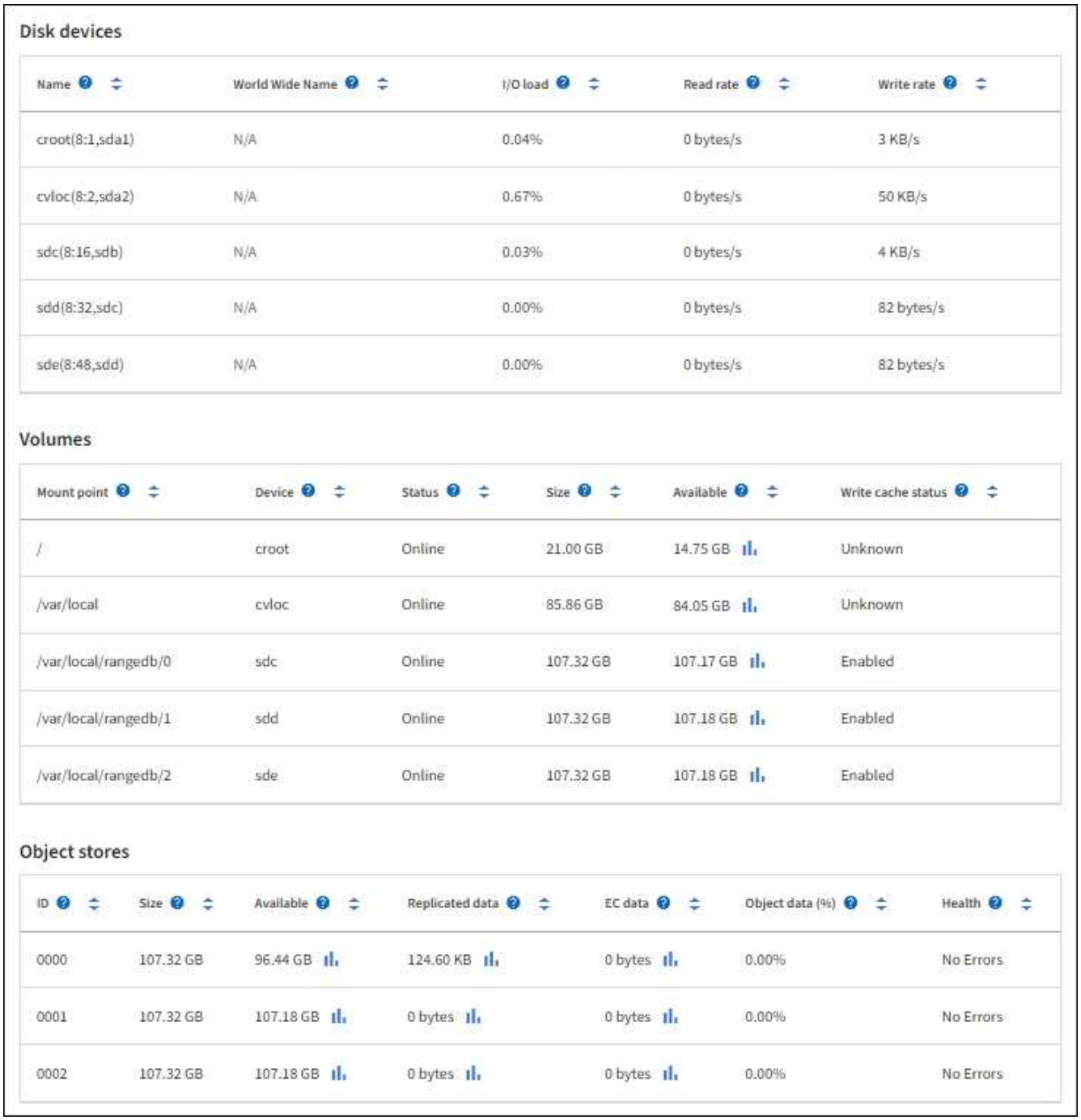
d’effacement sur ce nœud, ce site ou ce grid.

- **Total** : la quantité totale d’espace utilisable sur ce nœud, site ou grille. La valeur utilisée est la `storagegrid_storage_utilization_data_bytes` métrique.



3. Passez en revue les valeurs disponibles dans les tableaux volumes et magasins d’objets, sous les graphiques.

Pour afficher les graphiques de ces valeurs, cliquez sur les icônes du graphique Dans les colonnes disponibles.



Disk devices

Name	World Wide Name	I/O load	Read rate	Write rate
croot(8:1,sda1)	N/A	0.04%	0 bytes/s	3 KB/s
cvloc(8:2,sda2)	N/A	0.67%	0 bytes/s	50 KB/s
sdc(8:16,sdb)	N/A	0.03%	0 bytes/s	4 KB/s
sdd(8:32,sdc)	N/A	0.00%	0 bytes/s	82 bytes/s
sde(8:48,sdd)	N/A	0.00%	0 bytes/s	82 bytes/s

Volumes

Mount point	Device	Status	Size	Available	Write cache status
/	croot	Online	21.00 GB	14.75 GB	Unknown
/var/local	cvloc	Online	85.86 GB	84.05 GB	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.17 GB	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/2	sde	Online	107.32 GB	107.18 GB	Enabled

Object stores

ID	Size	Available	Replicated data	EC data	Object data (%)	Health
0000	107.32 GB	96.44 GB	124.60 KB	0 bytes	0.00%	No Errors
0001	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0002	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors

4. Surveillez les valeurs dans le temps pour estimer le taux de consommation de l'espace de stockage utilisable.
5. Pour préserver le fonctionnement normal du système, ajoutez des nœuds de stockage, ajoutez des volumes de stockage ou archivez les données d'objet avant de consommer l'espace utilisable.

   Lors de la planification d'une extension, réfléchissez au temps nécessaire pour approvisionner et installer du stockage supplémentaire.

> Si votre règle ILM utilise le code d'effacement, vous pouvez préférer une extension lorsque les nœuds de stockage existants sont remplis à environ 70 % pour réduire le nombre de nœuds à ajouter.

Pour plus d'informations sur la planification d'une extension de stockage, reportez-vous au "Instructions

d'extension de StorageGRID".

Le "Faible stockage des données objet" L'alerte est déclenchée lorsque l'espace restant insuffisant pour stocker les données d'objet sur un nœud de stockage.

Surveillez la capacité des métadonnées d'objet pour chaque nœud de stockage

Surveillez l'utilisation des métadonnées pour chaque nœud de stockage afin de garantir qu'un espace adéquat reste disponible pour les opérations essentielles de la base de données. Vous devez ajouter de nouveaux nœuds de stockage sur chaque site avant que les métadonnées d'objet dépassent 100 % de l'espace autorisé pour les métadonnées.

Description de la tâche

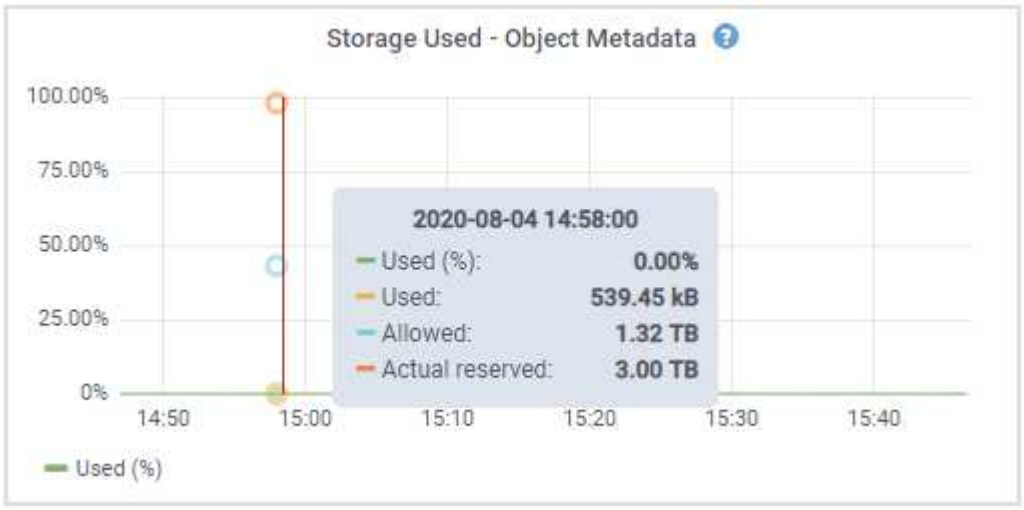
StorageGRID conserve trois copies des métadonnées d'objet sur chaque site pour assurer la redondance et protéger les métadonnées d'objet contre la perte. Les trois copies sont réparties de manière homogène sur tous les nœuds de stockage de chaque site, en utilisant l'espace réservé aux métadonnées sur le volume de stockage 0 de chaque nœud de stockage.

Dans certains cas, la capacité des métadonnées d'objet de la grille peut être utilisée plus rapidement que la capacité de stockage objet. Par exemple, si vous ingérer généralement un grand nombre d'objets de petite taille, vous devrez ajouter des nœuds de stockage pour augmenter la capacité des métadonnées, même si la capacité de stockage objet est suffisante.

L'utilisation des métadonnées peut notamment être augmentée, comme la taille et la quantité des métadonnées et du balisage, le nombre total d'éléments d'un téléchargement partitionné et la fréquence des modifications apportées aux emplacements de stockage ILM.

Étapes

1. Sélectionnez **NODES** > ***Storage Node*** > **Storage**.
2. Positionnez le curseur sur le graphique de métadonnées de l'objet stockage utilisé - pour afficher les valeurs d'une heure spécifique.



Utilisé (%)

Pourcentage de l'espace de métadonnées autorisé utilisé sur ce nœud de stockage.

Metrics Prometheus : `storagegrid_storage_utilization_metadata_bytes` et `storagegrid_storage_utilization_metadata_allowed_bytes`

Utilisé

Les octets de l'espace de métadonnées autorisé qui ont été utilisés sur ce nœud de stockage.

Prometheus métrique : `storagegrid_storage_utilization_metadata_bytes`

Autorisé

Espace autorisé pour les métadonnées d'objet sur ce nœud de stockage. Pour découvrir comment cette valeur est définie pour chaque nœud de stockage, reportez-vous à la section "Description complète de l'espace de métadonnées autorisé".

Prometheus métrique : `storagegrid_storage_utilization_metadata_allowed_bytes`

Réservé réelle

Espace réel réservé aux métadonnées sur ce nœud de stockage. Inclut l'espace autorisé et l'espace requis pour les opérations essentielles sur les métadonnées. Pour découvrir comment cette valeur est calculée pour chaque nœud de stockage, reportez-vous au "Description complète de l'espace réservé réel pour les métadonnées".

Prometheus métrique sera ajouté dans une prochaine version.

> ⓘ Les valeurs totales d'un site ou de la grille n'incluent pas les nœuds qui n'ont pas signalé de mesures depuis au moins cinq minutes, comme les nœuds hors ligne.

3. Si la valeur **utilisée (%)** est de 70 % ou plus, développez votre système StorageGRID en ajoutant des nœuds de stockage à chaque site.

> ⓘ L'alerte **stockage de métadonnées faible** est déclenchée lorsque la valeur **utilisée (%)** atteint certains seuils. Les résultats indésirables peuvent se produire si les métadonnées de l'objet utilisent plus de 100 % de l'espace autorisé.

Lorsque vous ajoutez des nœuds, le système rééquilibre automatiquement les métadonnées d'objet sur tous les nœuds de stockage du site. Voir la "Instructions d'extension d'un système StorageGRID".

Surveillez les prévisions d'utilisation de l'espace

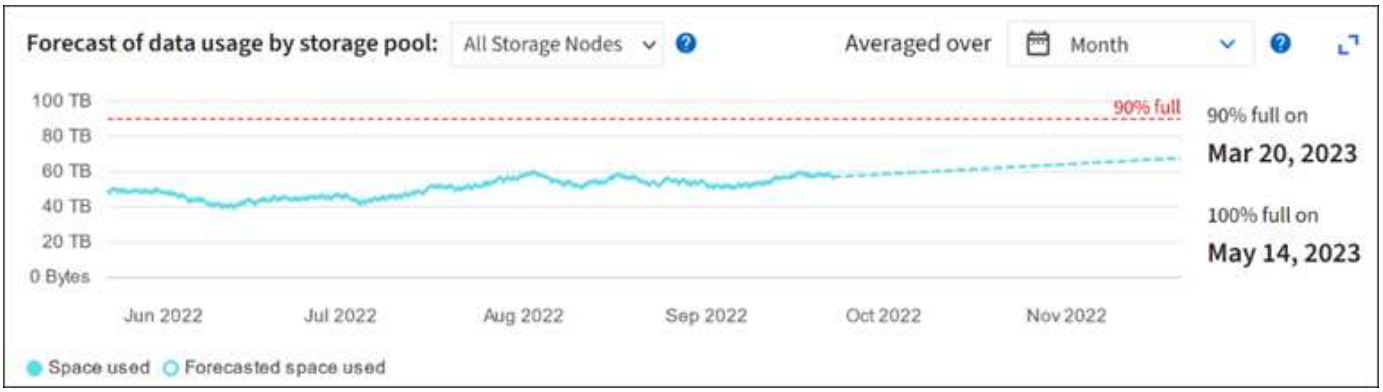
Surveillez les prévisions d'utilisation de l'espace pour les données utilisateur et les métadonnées afin d'estimer le moment opportun "développez votre grille".

Si vous remarquez que le taux de consommation change au fil du temps, sélectionnez une plage plus courte dans le menu déroulant **moyenne sur** pour refléter uniquement les modèles d'ingestion les plus récents. Si vous remarquez des motifs saisonniers, sélectionnez une plage plus longue.

Si vous disposez d'une nouvelle installation StorageGRID, autorisez l'accumulation de données et de métadonnées avant d'évaluer les prévisions d'utilisation de l'espace.

Étapes

1. Sur le tableau de bord, sélectionnez **stockage**.
2. Affichez les cartes du tableau de bord, la prévision de l'utilisation des données par pool de stockage et la prévision de l'utilisation des métadonnées par site.
3. Utilisez ces valeurs pour déterminer quand ajouter de nouveaux nœuds de stockage pour le stockage des données et des métadonnées.



Contrôle la gestion du cycle de vie des informations

Le système de gestion du cycle de vie des informations (ILM) assure la gestion des données de tous les objets stockés sur la grille. Vous devez surveiller les opérations ILM pour déterminer si la grille peut traiter la charge actuelle ou si d'autres ressources sont requises.

Description de la tâche

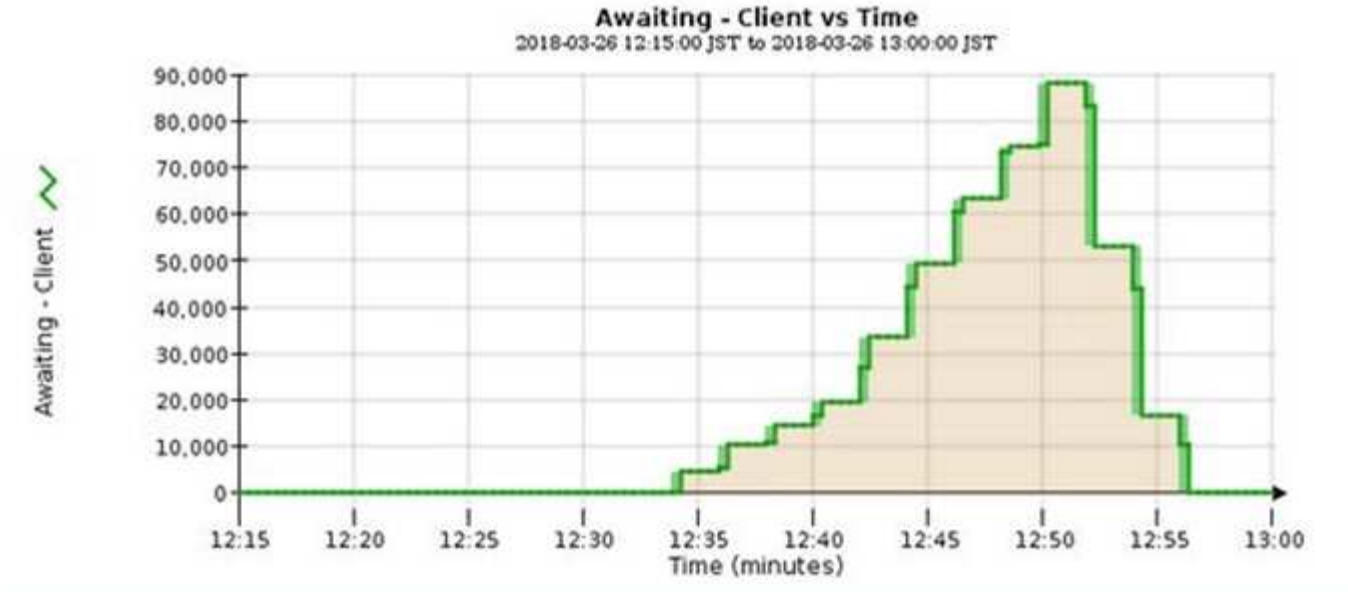
Le système StorageGRID gère les objets en appliquant la règle ILM active. La politique ILM et les règles ILM associées déterminent le nombre de copies, le type de copies créées, le lieu où les copies sont placées, ainsi que la durée de conservation de chaque copie.

L'ingestion d'objets et d'autres activités liées aux objets peuvent dépasser la vitesse à laquelle StorageGRID peut évaluer la gestion des règles ILM. Le système peut ainsi mettre en file d'attente des objets dont les instructions de placement des règles ILM ne peuvent pas être exécutées en temps quasi réel. Vous pouvez contrôler si StorageGRID maintient les actions du client en transcritant l'attribut attente - client.

Pour tracer cet attribut :

1. Connectez-vous au Grid Manager.
2. Dans le tableau de bord, localisez l'entrée **Awaiting - client** dans l'onglet information Lifecycle Management (ILM).
3. Cliquez sur l'icône du graphique .

Le graphique illustre une situation dans laquelle le nombre d'objets en attente d'évaluation ILM a temporairement augmenté de façon non viable, puis a finalement diminué. Une telle tendance indique que la gestion du cycle de vie des informations (ILM) n'a été temporairement pas respectée en temps réel.



Des pics temporaires dans le graphique d'attente - client doivent être attendus. Si la valeur affichée sur le graphique continue d'augmenter et ne diminue jamais, la grille nécessite davantage de ressources pour fonctionner efficacement : plus de nœuds de stockage ou, si la règle ILM place les objets à distance, plus de bande passante réseau.

Vous pouvez approfondir l'analyse des files d'attente ILM à l'aide de la page **NOEUDS**.

Étapes

1. Sélectionnez **NOEUDS**.
2. Sélectionnez ***grid name*** > **ILM**.
3. Positionnez le curseur sur le graphique de la file d'attente ILM pour voir la valeur des attributs suivants à un moment donné :
   - **Objets mis en file d'attente (à partir des opérations client)** : nombre total d'objets en attente d'évaluation ILM en raison des opérations client (par exemple, ingestion).
   - **Objets mis en file d'attente (de toutes les opérations)** : nombre total d'objets en attente d'évaluation ILM.
   - **Taux d'acquisition (objets/s)** : vitesse à laquelle les objets de la grille sont analysés et mis en file d'attente pour ILM.
   - **Taux d'évaluation (objets/s)** : taux actuel auquel les objets sont évalués par rapport à la politique ILM de la grille.
4. Dans la section ILM Queue, observez les attributs suivants.

   La section ILM Queue est incluse uniquement pour la grille. Ces informations ne s'affichent pas dans l'onglet ILM d'un site ou d'un nœud de stockage.

   - **Période d'acquisition - estimé** : temps estimé pour effectuer une analyse ILM complète de tous les objets.

     Une analyse complète ne garantit pas l'application du ILM à tous les objets.

   - **Réparations tentées** : nombre total d'opérations de réparation d'objet pour les données répliquées qui

ont été tentées. Ce nombre est incrémenté chaque fois qu'un nœud de stockage tente de réparer un objet à haut risque. Les réparations ILM à haut risque sont hiérarchisées si le grid est occupé.

> La réparation d'un même objet peut être de nouveau incrémentée si la réplication a échoué après la réparation.

Ces attributs peuvent être utiles lorsque vous surveillez la progression de la récupération de volume du nœud de stockage. Si le nombre de réparations effectuées a cessé d'augmenter et qu'une analyse complète a été effectuée, la réparation est probablement terminée.

Surveiller les ressources réseau et système

L'intégrité et la bande passante du réseau entre les nœuds et les sites, ainsi que l'utilisation des ressources par les nœuds de grid individuels, sont essentielles à l'efficacité des opérations.

Contrôle des connexions réseau et des performances

La connectivité réseau et la bande passante sont d'autant plus importantes si votre stratégie de gestion du cycle de vie des informations (ILM) copie les objets répliqués entre des sites ou stocke des objets avec code d'effacement au moyen d'un système qui assure la protection contre la perte de site. Si le réseau entre les sites n'est pas disponible, que la latence du réseau est trop élevée ou que la bande passante du réseau est insuffisante, certaines règles ILM risquent de ne pas pouvoir placer les objets là où prévu. Cela peut entraîner des échecs d'ingestion (lorsque l'option d'ingestion stricte est sélectionnée pour les règles ILM) ou de mauvaises performances d'ingestion et de journalisation des règles ILM.

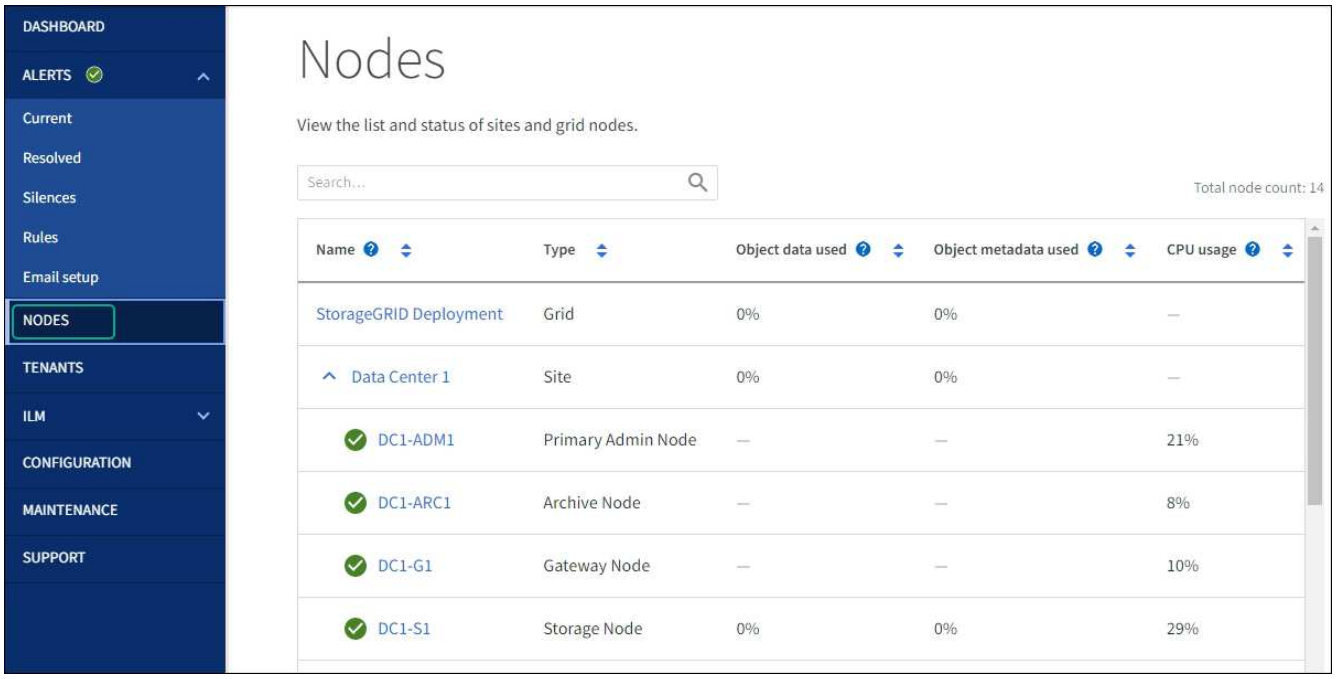
Utilisez le gestionnaire de grille pour surveiller la connectivité et les performances du réseau, afin de résoudre rapidement tout problème.

De plus, n'oubliez pas "création de stratégies de classification du trafic réseau" afin de surveiller le trafic lié à des locataires, des compartiments, des sous-réseaux ou des terminaux d'équilibrage de la charge spécifiques. Vous pouvez définir des règles de limitation du trafic selon vos besoins.

Étapes

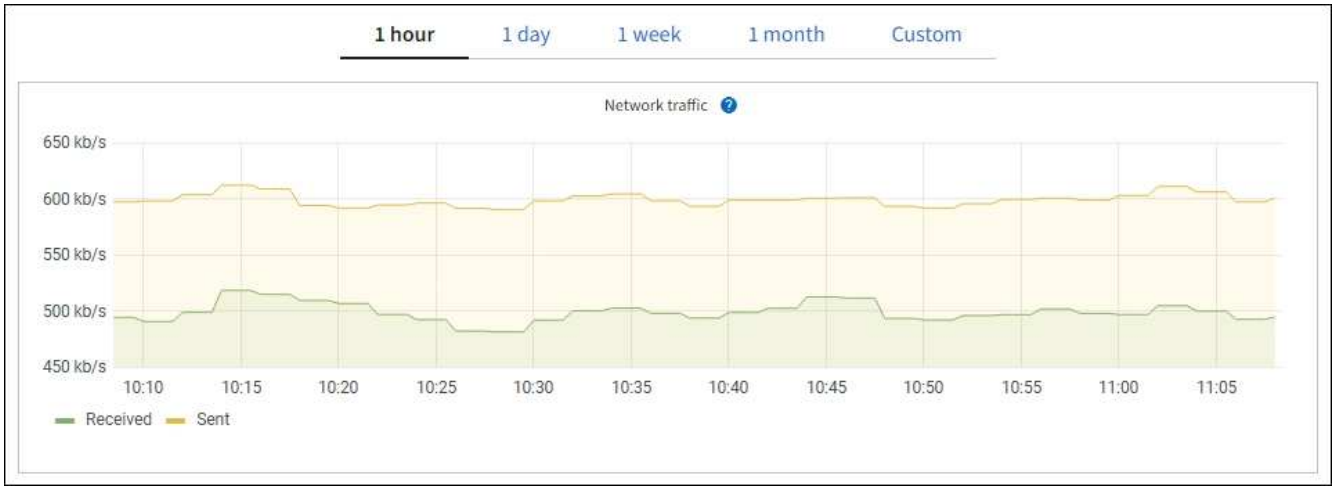
1. Sélectionnez **NOEUDS**.

   La page nœuds s'affiche. Chaque nœud de la grille est répertorié au format de tableau.

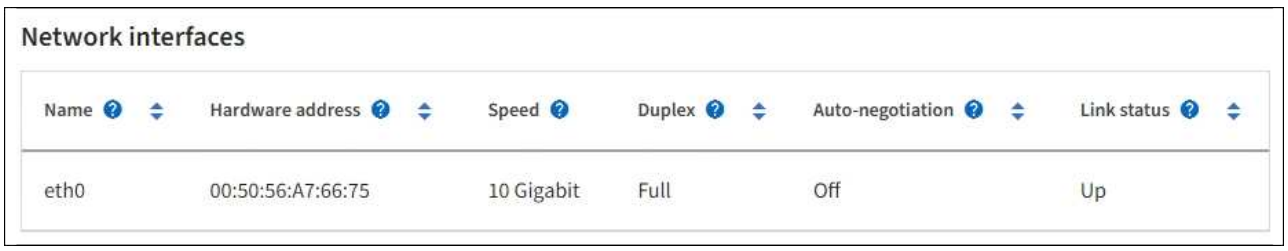


2. Sélectionnez le nom de la grille, un site de centre de données spécifique ou un nœud de grille, puis sélectionnez l'onglet **réseau**.

   Le graphique trafic réseau fournit un récapitulatif du trafic réseau global pour la grille dans son ensemble, le site du centre de données ou le nœud.

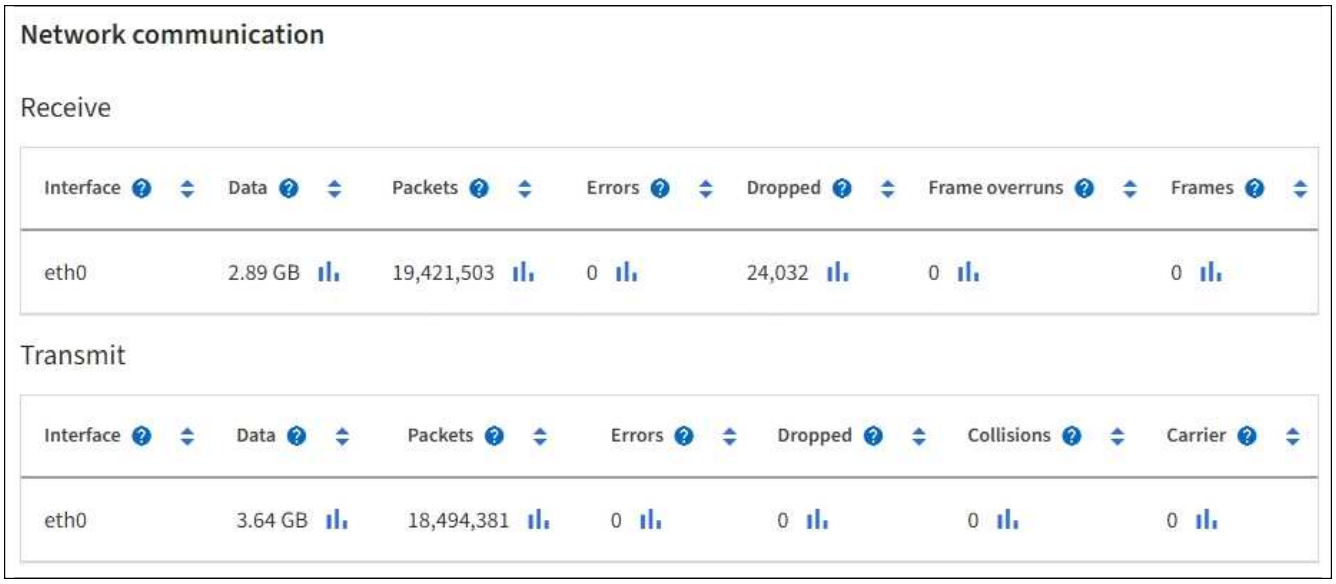


   a. Si vous avez sélectionné un nœud de grille, faites défiler vers le bas pour consulter la section **interfaces réseau** de la page.



   b. Pour les nœuds de grille, faites défiler vers le bas pour consulter la section **communication réseau** de la page.

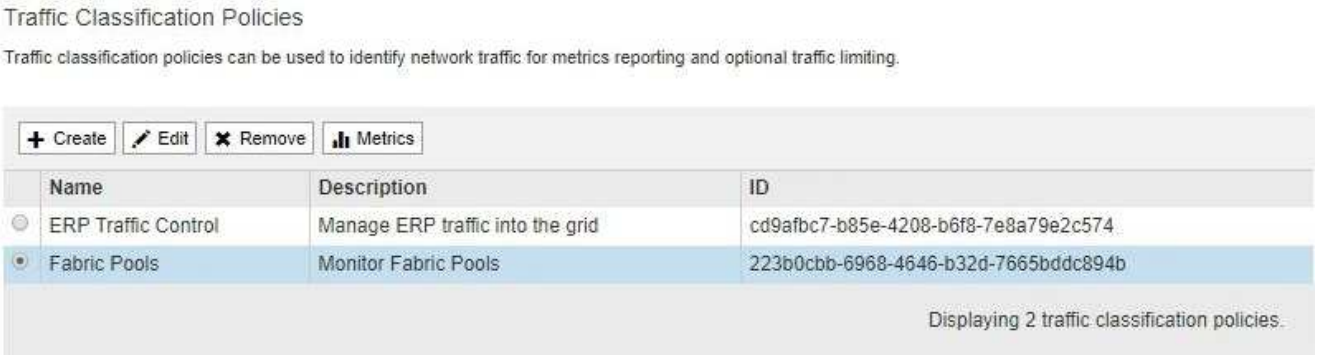
Les tableaux de réception et de transmission indiquent le nombre d'octets et de paquets reçus et envoyés sur chaque réseau ainsi que d'autres mesures de réception et de transmission.



3. Utilisez les indicateurs associés à vos stratégies de classification de trafic pour surveiller le trafic réseau.

   a. Sélectionnez **CONFIGURATION** > **réseau** > **classification du trafic**.

      La page règles de classification du trafic s'affiche et les stratégies existantes sont répertoriées dans le tableau.



   a. Pour afficher les graphiques présentant les mesures de réseau associées à une stratégie, sélectionnez le bouton radio à gauche de la stratégie, puis cliquez sur **métriques**.

   b. Consultez les graphiques pour comprendre le trafic réseau associé à la stratégie.

      Si une politique de classification du trafic est conçue pour limiter le trafic réseau, analysez la fréquence à laquelle le trafic est limité et déterminez si la politique continue de répondre à vos besoins. De temps à autre, "ajustez chaque stratégie de classification du trafic au besoin".

Informations associées

"Afficher l'onglet réseau"

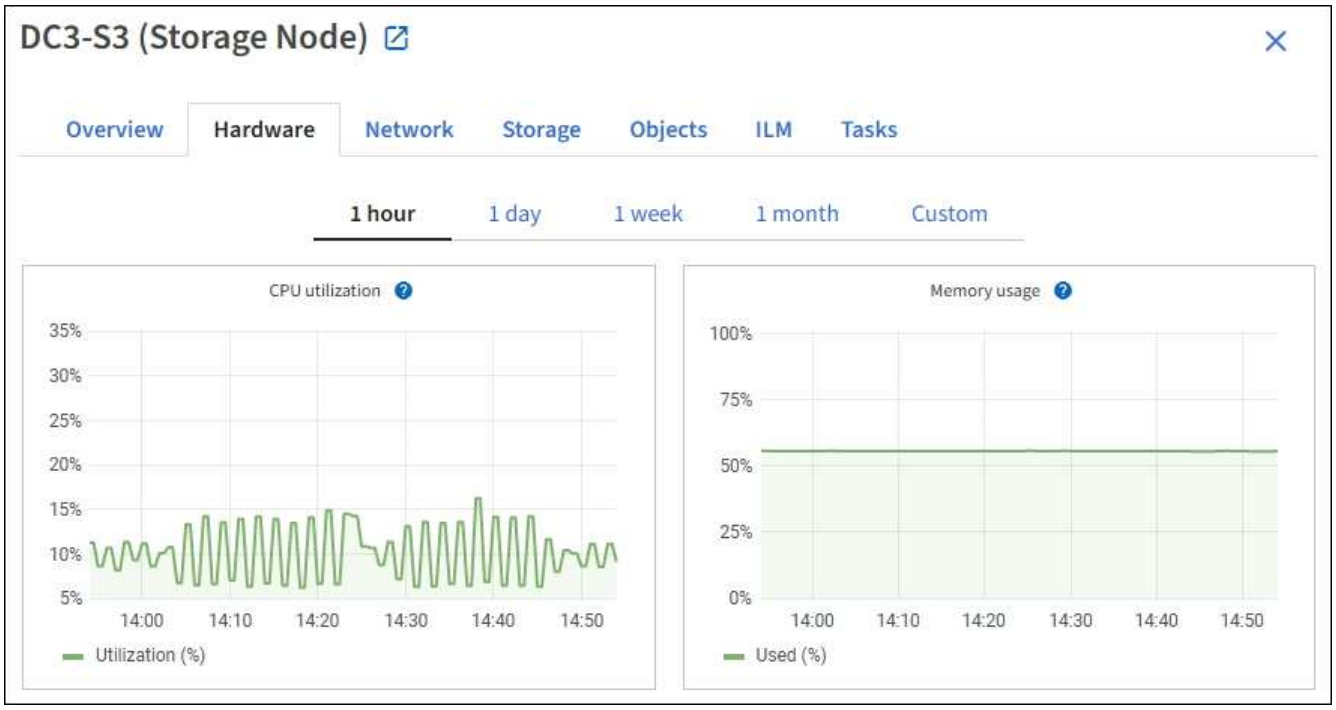
"Surveiller les États de connexion du nœud"

Contrôle des ressources au niveau des nœuds

Surveiller les nœuds de grid individuels pour vérifier leurs niveaux d'utilisation des ressources. Si les nœuds sont constamment surchargés, un nombre plus élevé de nœuds peut être requis pour une efficacité optimale des opérations.

Étapes

1. Dans la page **NODES**, sélectionnez le noeud.
2. Sélectionnez l'onglet **matériel** pour afficher les graphiques de l'utilisation de l'UC et de la mémoire.



3. Pour afficher un intervalle de temps différent, sélectionnez l'une des commandes au-dessus du graphique ou du graphique. Vous pouvez afficher les informations disponibles pour les intervalles de 1 heure, 1 jour, 1 semaine ou 1 mois. Vous pouvez également définir un intervalle personnalisé, qui vous permet de spécifier des plages de date et d'heure.
4. Si le nœud est hébergé sur une appliance de stockage ou sur une appliance de services, faites défiler la page vers le bas pour afficher les tableaux des composants. L'état de tous les composants doit être « nominal ». Rechercher les composants ayant un autre état.

Informations associées

"Afficher des informations sur les nœuds de stockage de l'appliance"

"Affiche des informations sur les nœuds d'administration de l'appliance et les nœuds de passerelle"

Surveillez l'activité des locataires

Toutes les activités des clients S3 et Swift sont associées aux comptes de locataires StorageGRID. Vous pouvez utiliser Grid Manager pour surveiller l'utilisation du stockage ou le trafic réseau de tous les locataires ou d'un locataire spécifique. Vous pouvez utiliser le journal des audits ou les tableaux de bord Grafana pour collecter des informations plus détaillées sur l'utilisation de StorageGRID par les locataires.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous disposez de l'autorisation accès racine ou comptes de tenant.

Afficher tous les locataires

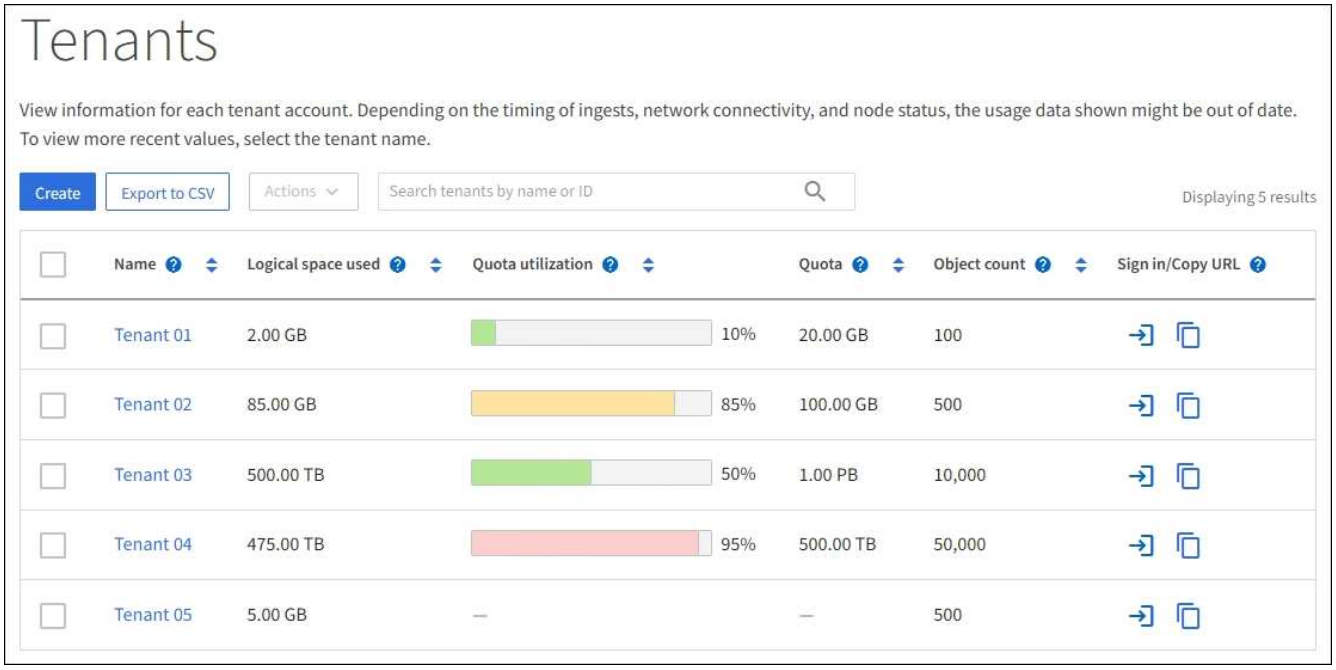
La page tenants affiche les informations de base pour tous les comptes de locataires actuels.

Étapes

1. Sélectionnez **LOCATAIRES**.
2. Vérifiez les informations affichées sur les pages tenant.

   L'espace logique utilisé, l'utilisation du quota, l'quota et le nombre d'objets sont répertoriés pour chaque locataire. Si un quota n'est pas défini pour un locataire, les champs utilisation du quota et quota contiennent un tiret (—).

   > Les valeurs de l'espace utilisé sont des estimations. Ces estimations sont affectées par le moment de l'ingestion, la connectivité réseau et l'état des nœuds.



3. Vous pouvez également vous connecter à un compte de locataire en sélectionnant le lien de connexion Dans la colonne **se connecter/Copier l'URL**.
4. Vous pouvez également copier l'URL de la page de connexion d'un locataire en sélectionnant le lien Copier l'URL Dans la colonne **se connecter/Copier l'URL**.
5. Si vous le souhaitez, sélectionnez **Exporter au format CSV** pour afficher et exporter un `.csv` fichier contenant les valeurs d'utilisation pour tous les locataires.

   Vous êtes invité à ouvrir ou enregistrer le `.csv` fichier.

   Le contenu du `.csv` le fichier ressemble à l'exemple suivant :

Tenant ID	Display Name	Space Used (Bytes)	Quota utilization (%)	Quota (Bytes)	Object Count	Protocol
12659822378459233654	Tenant 01	2000000000	10	20000000000	100	S3
99658234112547853685	Tenant 02	85000000000	85	110000000	500	S3
03521145586975586321	Tenant 03	60500000000	50	150000	10000	S3
44251365987569885632	Tenant 04	4750000000	95	140000000	50000	S3
36521587546689565123	Tenant 05	5000000000	Infinity		500	S3

Vous pouvez ouvrir le `.csv` classez-les dans une feuille de calcul ou utilisez-les dans l'automatisation.

6. Si aucun objet n'est répertorié, sélectionnez **actions** > **Supprimer** pour supprimer un ou plusieurs locataires. Voir "Supprimer le compte de locataire".

   Vous ne pouvez pas supprimer un compte de locataire si le compte inclut des compartiments ou des conteneurs.

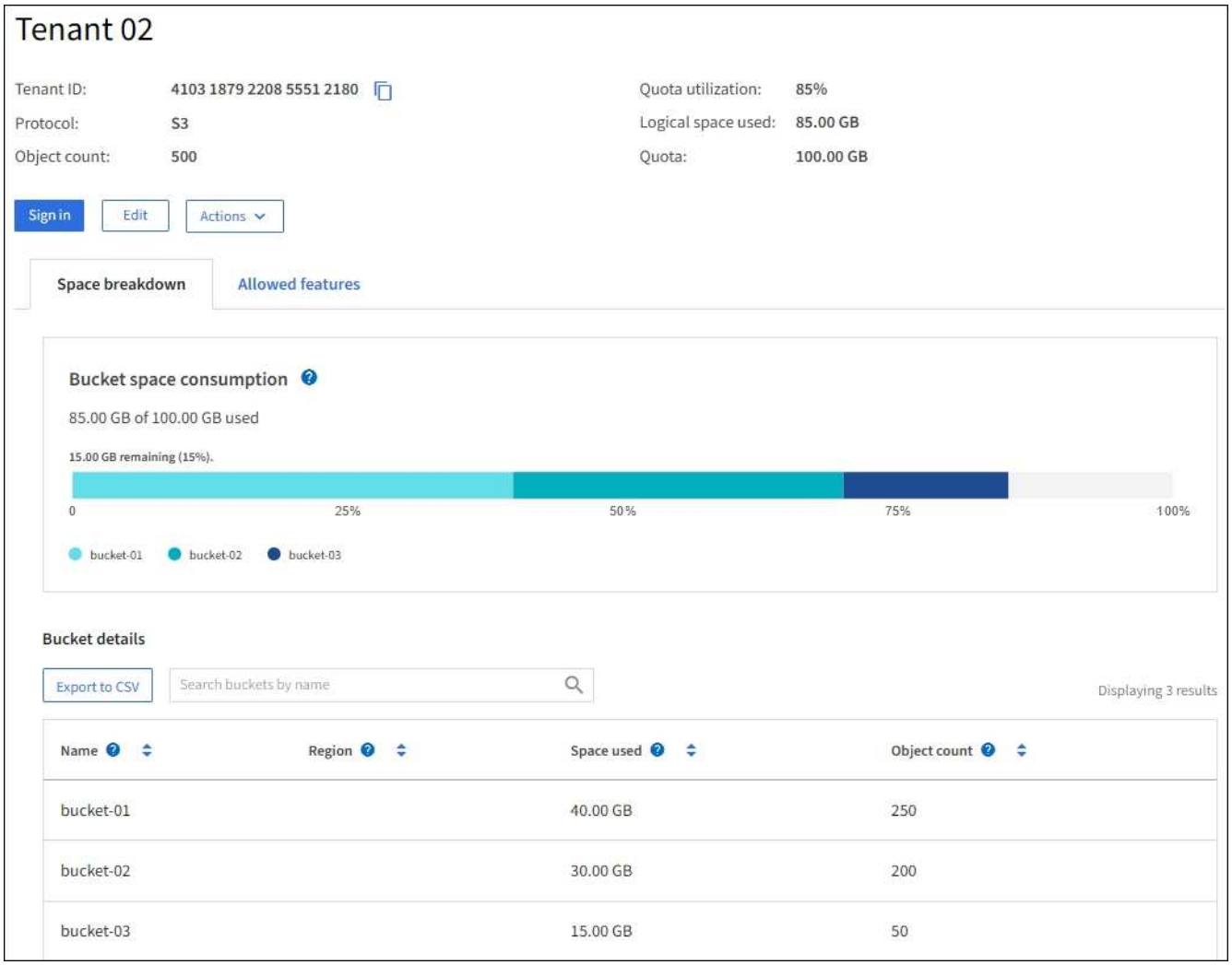
Afficher un locataire spécifique

Vous pouvez afficher les détails d'un locataire spécifique.

Étapes

1. Sélectionnez le nom du locataire dans la page locataires.

   La page des détails du locataire s'affiche.



2. Consultez la présentation du locataire en haut de la page.

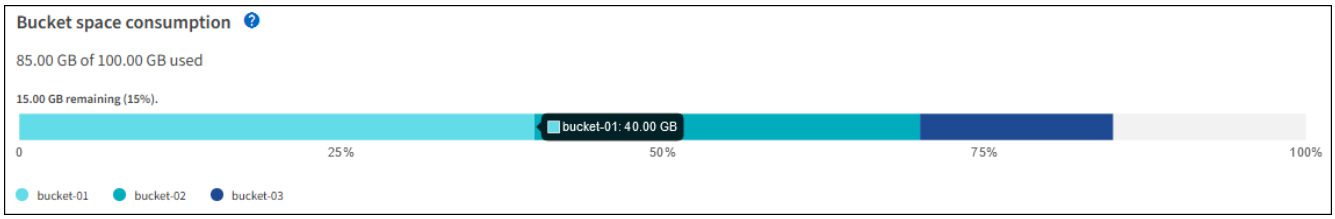
   Cette section de la page de détails fournit un récapitulatif des informations relatives au locataire, notamment le nombre d'objets du locataire, l'utilisation du quota, l'espace logique utilisé et la définition du quota.

3. Dans l'onglet **Space Dclaquage**, consultez le graphique **Space Consumption**.

   Ce tableau présente la consommation totale d'espace pour tous les compartiments S3 (ou conteneurs Swift) du locataire.

   Si un quota a été défini pour ce locataire, le montant du quota utilisé et restant est affiché dans le texte (par exemple, `85.00 GB of 100 GB used`). Si aucun quota n'a été défini, le locataire a un quota illimité et le texte ne comprend qu'une quantité d'espace utilisé (par exemple, `85.00 GB used`). Le graphique à barres indique le pourcentage de quota dans chaque compartiment ou conteneur. Si le locataire a dépassé le quota de stockage de plus de 1 % et d'au moins 1 Go, le graphique indique le quota total et le montant de l'excès.

   Vous pouvez placer le curseur sur le graphique à barres pour voir le stockage utilisé par chaque compartiment ou conteneur. Vous pouvez placer votre curseur sur le segment de l'espace libre pour voir la quantité de quota de stockage restant.



> L'utilisation des quotas est basée sur des estimations internes et peut être dépassée dans certains cas. Par exemple, StorageGRID vérifie le quota lorsqu'un locataire commence à charger des objets et rejette les nouvelles ingère si le locataire a dépassé le quota. Cependant, StorageGRID ne prend pas en compte la taille du téléchargement actuel lors de la détermination du dépassement du quota. Si des objets sont supprimés, un locataire peut être temporairement empêché de charger de nouveaux objets jusqu'à ce que l'utilisation des quotas soit recalculée. Le calcul de l'utilisation des quotas peut prendre au moins 10 minutes.

> L'utilisation des quotas d'un locataire indique la quantité totale des données d'objet que le locataire a téléchargées sur StorageGRID (taille logique). L'utilisation du quota ne représente pas l'espace utilisé pour stocker les copies de ces objets et de leurs métadonnées (taille physique).

> Vous pouvez activer la règle d'alerte **tenant quota usage high** pour déterminer si les locataires utilisent leurs quotas. Si elle est activée, cette alerte est déclenchée lorsqu'un locataire a utilisé 90 % de son quota. Pour obtenir des instructions, reportez-vous à la section "Modifiez les règles d'alerte".

4. Dans l'onglet **Space Dclaquage**, passez en revue les détails **Bucket Details**.

   Ce tableau répertorie les compartiments S3 (ou conteneurs Swift) pour le locataire. L'espace utilisé correspond à la quantité totale de données d'objet dans le compartiment ou le conteneur. Cette valeur ne représente pas l'espace de stockage requis pour les copies ILM et les métadonnées d'objet.

5. Vous pouvez également sélectionner **Exporter au format CSV** pour afficher et exporter un fichier .csv contenant les valeurs d'utilisation de chaque compartiment ou conteneur.

   Contenu des locataires S3 `.csv` le fichier ressemble à l'exemple suivant :

Tenant ID	Bucket Name	Space Used (Bytes)	Number of Objects
64796966429038923647	bucket-01	88717711	14
64796966429038923647	bucket-02	21747507	11
64796966429038923647	bucket-03	15294070	3

   Vous pouvez ouvrir le `.csv` classez-les dans une feuille de calcul ou utilisez-les dans l'automatisation.

6. Vous pouvez également sélectionner l'onglet **fonctions autorisées** pour afficher la liste des autorisations et fonctionnalités activées pour le tenant. Voir "Modifiez le compte de tenant" si vous devez modifier l'un de ces paramètres.
7. Si le locataire dispose de l'autorisation **utiliser la connexion de fédération de grille**, sélectionnez éventuellement l'onglet **fédération de grille** pour en savoir plus sur la connexion.

   Voir "Qu'est-ce que la fédération de grille ?" et "Gérer les locataires autorisés pour la fédération dans le grid".

Affichez le trafic réseau

Si des stratégies de classification du trafic sont en place pour un locataire, examinez le trafic réseau de ce locataire.

Étapes

1. Sélectionnez **CONFIGURATION** > **réseau** > **classification du trafic**.

   La page règles de classification du trafic s'affiche et les stratégies existantes sont répertoriées dans le tableau.

2. Consultez la liste des politiques pour identifier celles qui s'appliquent à un locataire spécifique.
3. Pour afficher les mesures associées à une stratégie, sélectionnez le bouton radio à gauche de la stratégie et sélectionnez **métriques**.
4. Analysez les graphiques pour déterminer à quelle fréquence la stratégie limite le trafic et si vous devez ajuster la stratégie.

Voir "Gérer les stratégies de classification du trafic" pour en savoir plus.

Utilisez le journal d'audit

Vous pouvez également utiliser le journal des audits pour une surveillance plus granulaire des activités d'un locataire.

Par exemple, vous pouvez surveiller les types d'informations suivants :

- Des opérations client spécifiques, telles QUE METTRE, OBTENIR ou SUPPRIMER
- Tailles d'objet
- Règle ILM appliquée aux objets

- Adresse IP source des requêtes client

Les journaux d'audit sont écrits dans des fichiers texte que vous pouvez analyser à l'aide de l'outil d'analyse des journaux de votre choix. Vous pouvez ainsi mieux comprendre les activités des clients ou implémenter des modèles de facturation et de refacturation sophistiqués.

Voir "Examiner les journaux d'audit" pour en savoir plus.

Utilisez des metrics Prometheus

Éventuellement, utilisez des metrics Prometheus pour générer des rapports sur l'activité des locataires.

- Dans le Gestionnaire de grille, sélectionnez **SUPPORT** > **Outils** > **métriques**. Vous pouvez utiliser les tableaux de bord existants, tels que S3 Overview, pour examiner les activités des clients.

> Les outils disponibles sur la page métriques sont principalement destinés au support technique. Certaines fonctions et options de menu de ces outils ne sont intentionnellement pas fonctionnelles.

- En haut du Gestionnaire de grille, sélectionnez l'icône d'aide et sélectionnez **documentation API**. Vous pouvez utiliser les mesures de la section Metrics de l'API de gestion du grid pour créer des règles d'alerte et des tableaux de bord personnalisés pour l'activité des locataires.

Voir "Examinez les metrics de support" pour en savoir plus.

Surveiller les opérations d'équilibrage de charge

Si vous utilisez un équilibreur de charge pour gérer les connexions client à StorageGRID, vous devez surveiller les opérations d'équilibrage de charge après avoir configuré le système initialement et après avoir effectué des modifications de configuration ou effectué une extension.

Description de la tâche

Vous pouvez utiliser le service Load Balancer sur les nœuds d'administration ou les nœuds de passerelle, ou un équilibreur de charge tiers externe pour distribuer les requêtes client sur plusieurs nœuds de stockage.

Une fois l'équilibrage de la charge configuré, vérifiez que les opérations d'ingestion et de récupération des objets sont réparties de manière homogène entre les nœuds de stockage. La répartition homogène des demandes permet à StorageGRID de rester réactif aux demandes des clients sous charge et de maintenir les performances des clients.

Si vous avez configuré un groupe haute disponibilité de nœuds de passerelle ou de nœuds d'administration en mode de sauvegarde active/active, seul un nœud du groupe distribue activement les requêtes client.

Pour plus d'informations, voir "Configurez les connexions des clients S3 et Swift".

Étapes

1. Si les clients S3 ou Swift se connectent à l'aide du service Load Balancer, vérifiez que les nœuds d'administration ou les nœuds de passerelle distribuent le trafic activement, comme indiqué :
   a. Sélectionnez **NOEUDS**.
   b. Sélectionnez un nœud de passerelle ou un nœud d'administration.

c. Dans l'onglet **Overview**, vérifiez si une interface de nœud fait partie d'un groupe HA et si l'interface de nœud a le rôle Primary.

   Les nœuds ayant le rôle de nœud principal et les nœuds qui ne font pas partie d'un groupe haute disponibilité doivent distribuer activement les demandes aux clients.

d. Pour chaque nœud devant distribuer activement des demandes client, sélectionnez le "Onglet Load Balancer".

e. Consultez le graphique du trafic des demandes d'équilibrage de charge pour la dernière semaine afin de vous assurer que le nœud distribue activement les demandes.

   Les nœuds d'un groupe haute disponibilité à sauvegarde active peuvent parfois prendre le rôle de sauvegarde. Pendant ce temps, les nœuds ne distribuent pas les requêtes client.

f. Consultez le graphique du taux de demande entrant de Load Balancer pour la dernière semaine afin de vérifier le débit d'objet du nœud.

g. Répétez cette procédure pour chaque nœud d'administration ou de passerelle du système StorageGRID.

h. Vous pouvez également utiliser les stratégies de classification du trafic pour afficher une analyse plus détaillée du trafic desservi par le service Load Balancer.

2. Vérifiez que ces demandes sont réparties de manière homogène vers les nœuds de stockage.
   a. Sélectionnez ***Storage Node*** > **LDR** > **HTTP**.
   b. Examiner le nombre de **sessions entrantes actuellement établies**.
   c. Répétez l'opération pour chaque nœud de stockage de la grille.

      Le nombre de sessions doit être approximativement égal sur tous les nœuds de stockage.

Surveiller les connexions de fédération de grille

Vous pouvez contrôler les informations de base sur tous "connexions de fédération de grille", Informations détaillées sur une connexion spécifique ou metrics Prometheus sur les opérations de réplication entre les grilles. Vous pouvez surveiller une connexion à partir de l'une ou l'autre des grilles.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille sur l'une des grilles à l'aide d'un "navigateur web pris en charge".
- Vous disposez de l'autorisation d'accès racine pour la grille à laquelle vous êtes connecté.

Afficher toutes les connexions

La page Grid federation affiche des informations de base sur toutes les connexions de fédération de grille et sur tous les comptes de locataire autorisés à utiliser les connexions de fédération de grille.

Étapes

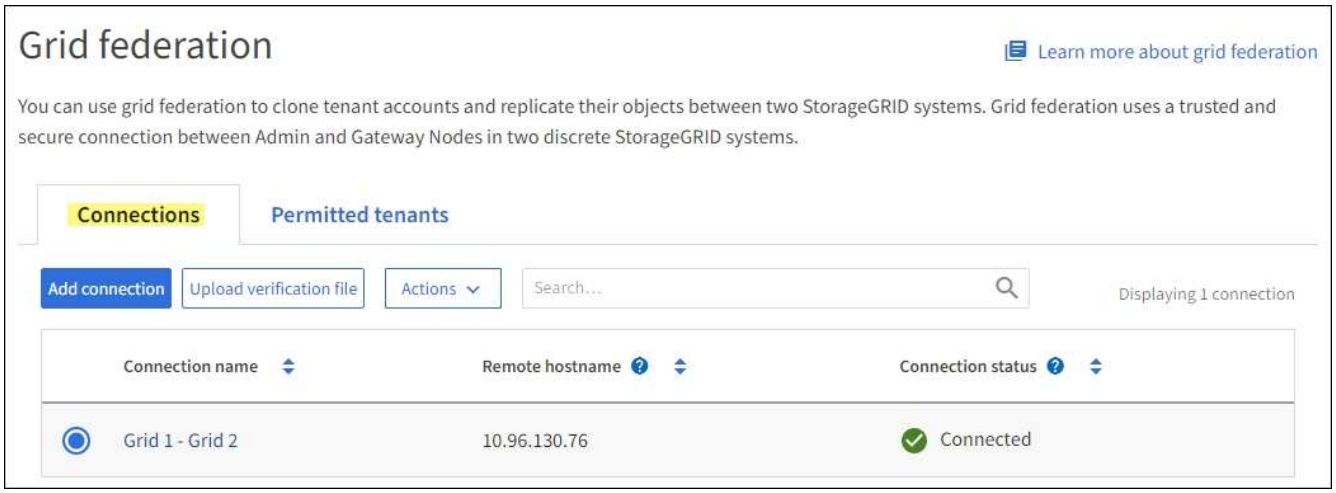
1. Sélectionnez **CONFIGURATION** > **système** > **fédération de grille**.

   La page grid federation s'affiche.

2. Pour afficher des informations de base sur toutes les connexions de cette grille, sélectionnez l'onglet **connexions**.

   À partir de cet onglet, vous pouvez :

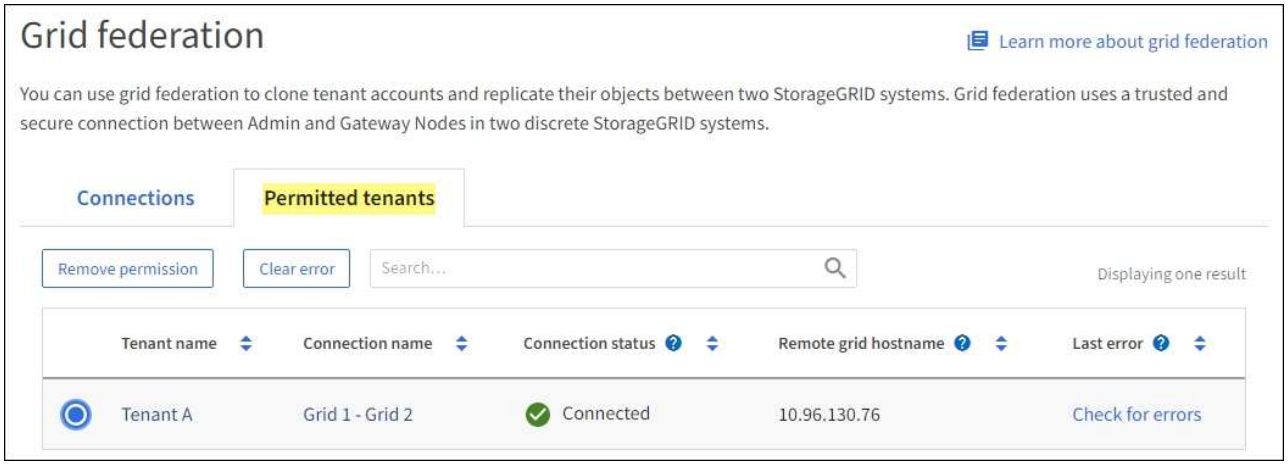
   - "Créer une nouvelle connexion".
   - Sélectionnez une connexion existante à "modifier ou tester".



3. Pour afficher les informations de base de tous les comptes de locataires de cette grille disposant de l'autorisation **utiliser la connexion de fédération de grille**, sélectionnez l'onglet **locataires autorisés**.

   À partir de cet onglet, vous pouvez :

   - "Afficher la page de détails pour chaque locataire autorisé".
   - Afficher la page de détails de chaque connexion. Voir Afficher une connexion spécifique.
   - Sélectionnez un locataire autorisé et "supprimez l'autorisation".
   - Vérifiez la présence d'erreurs de réplication inter-grille et effacez la dernière erreur, le cas échéant. Voir "Dépanner les erreurs de fédération de grille".



permet d'afficher une connexion spécifique

Vous pouvez afficher les détails d'une connexion de fédération de grille spécifique.

Étapes

1. Sélectionnez l'un des onglets de la page fédération de grille, puis sélectionnez le nom de la connexion dans le tableau.

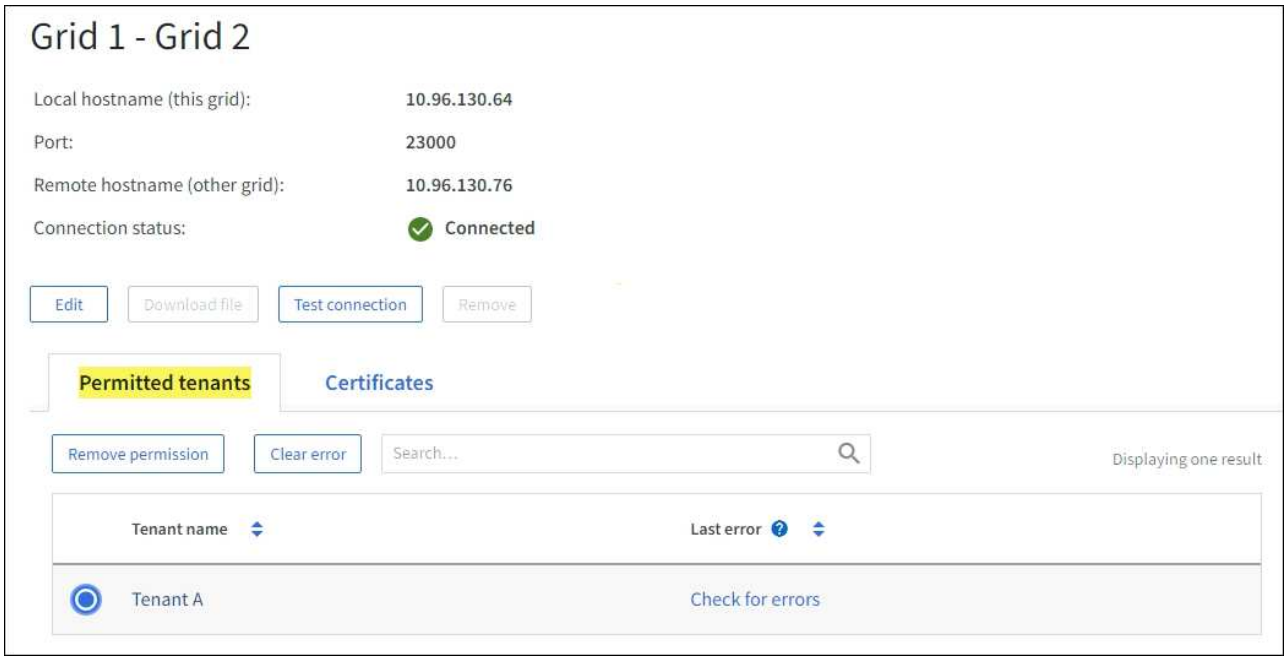
   Dans la page de détails de la connexion, vous pouvez :

   - Consultez les informations d'état de base sur la connexion, y compris les noms d'hôtes locaux et distants, le port et l'état de la connexion.
   - Sélectionnez une connexion à "modifier, tester ou supprimer".

2. Lors de l'affichage d'une connexion spécifique, sélectionnez l'onglet **locataires autorisés** pour afficher des détails sur les locataires autorisés pour la connexion.

   À partir de cet onglet, vous pouvez :

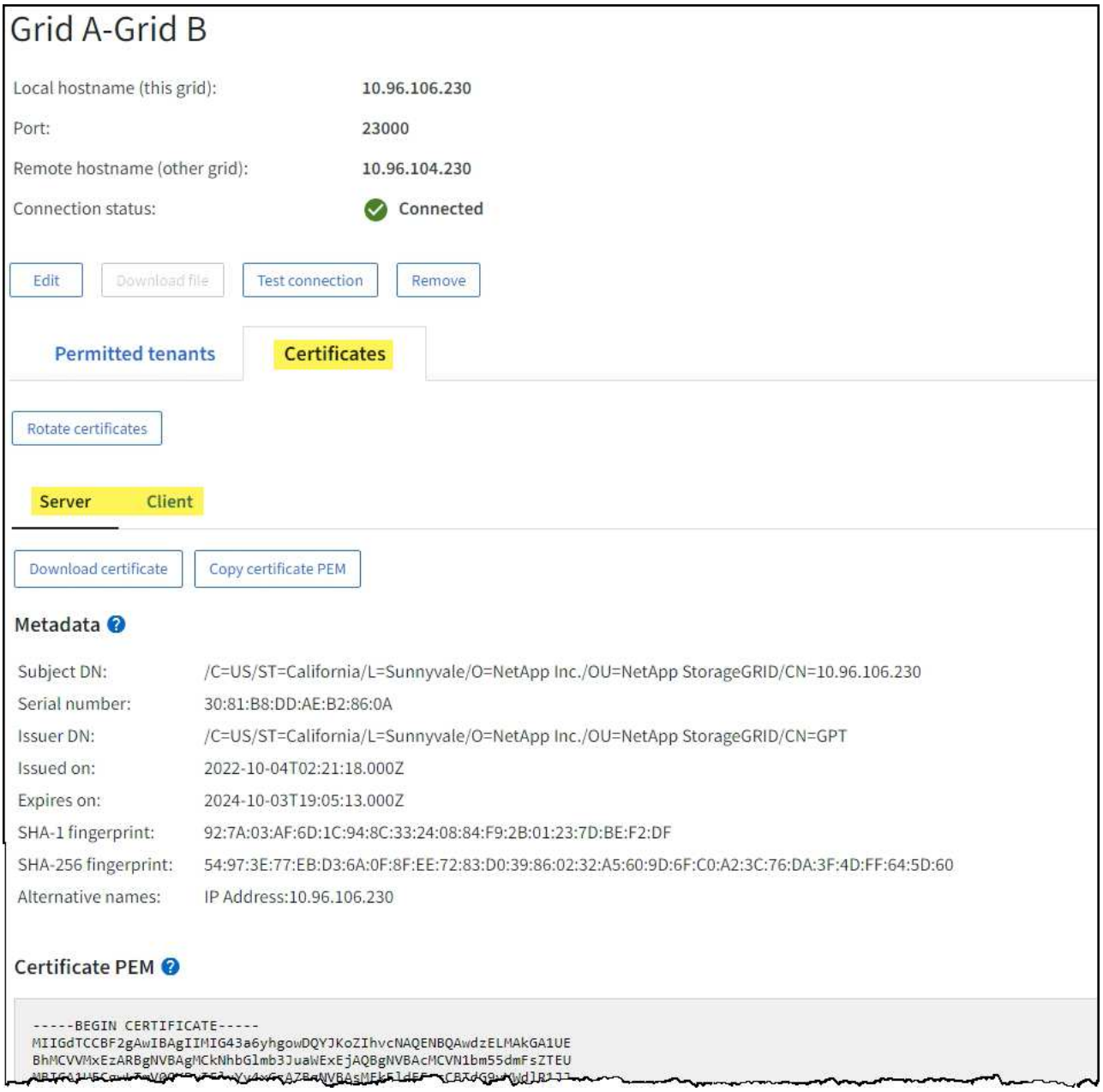
   - "Afficher la page de détails pour chaque locataire autorisé".
   - "Supprimer l'autorisation d'un locataire" pour utiliser la connexion.
   - Recherchez les erreurs de réplication inter-grille et effacez la dernière erreur. Voir "Dépanner les erreurs de fédération de grille".



3. Lors de l'affichage d'une connexion spécifique, sélectionnez l'onglet **certificats** pour afficher les certificats de serveur et de client générés par le système pour cette connexion.

   À partir de cet onglet, vous pouvez :

   - "Faire pivoter les certificats de connexion".
   - Sélectionnez **Server** ou **client** pour afficher ou télécharger le certificat associé ou copier le certificat PEM.



Examinez les metrics de réplication entre les grilles

Vous pouvez utiliser le tableau de bord de réplication Cross-Grid de Grafana pour afficher les metrics Prometheus sur les opérations de réplication cross-grid sur votre grille.

Étapes

1. Dans le Gestionnaire de grille, sélectionnez **SUPPORT** > **Outils** > **métriques**.

   Les outils disponibles sur la page métriques sont destinés au support technique. Certaines fonctions et options de menu de ces outils sont intentionnellement non fonctionnelles et peuvent faire l'objet de modifications. Voir la liste des "Metrics Prometheus couramment utilisés".

2. Dans la section Grafana de la page, sélectionnez **Cross Grid Replication**.

   Pour obtenir des instructions détaillées, reportez-vous à la section "Examinez les metrics de support".

3. Pour réessayer la réplication d'objets qui n'ont pas pu être répliqués, reportez-vous à la section "Identifier et réessayer les opérations de réplication ayant échoué".

Application des correctifs ou des mises à niveau logicielles si nécessaire

Si un correctif ou une nouvelle version du logiciel StorageGRID est disponible, vous devez déterminer si la mise à jour est adaptée à votre système et l'installer si nécessaire.

Description de la tâche

Les correctifs StorageGRID contiennent des modifications logicielles qui sont disponibles en dehors d'une version de fonctionnalité ou de correctif. Les mêmes modifications seront incluses dans une prochaine version.

Étapes

1. Accédez àhttps://mysupport.netapp.com/site/products/all/details/storagegrid/downloads-tab["Téléchargement NetApp : StorageGRID"^].
2. Sélectionnez la flèche vers le bas du champ **Type/Sélectionner version** pour afficher la liste des mises à jour disponibles au téléchargement :
   - **Versions du logiciel StorageGRID** : 11.*x.y*
   - **Correctifs StorageGRID**: 11.*x. .yz*
3. Vérifiez les modifications qui sont incluses dans la mise à jour :
   a. Sélectionnez la version dans le menu, puis sélectionnez **Go**.
   b. Connectez-vous en utilisant le nom d'utilisateur et le mot de passe de votre compte NetApp.
   c. Lisez et acceptez le contrat de licence de l'utilisateur final.

      La page des téléchargements de la version sélectionnée s'affiche.
4. Découvrez les changements inclus dans la version du logiciel ou le correctif.
   - Pour obtenir une nouvelle version du logiciel, reportez-vous à la section "Quoi de neuf" pour la version que vous avez sélectionnée.
   - Pour un correctif, téléchargez le fichier README pour un résumé des modifications incluses dans le correctif.
5. Si vous décidez qu'une mise à jour logicielle est nécessaire, suivez les instructions avant de continuer.
   - Pour une nouvelle version du logiciel, suivez attentivement les instructions de "mise à niveau du logiciel".
   - Pour obtenir un correctif, reportez-vous au "Procédure de correctif StorageGRID".

Surveiller la capacité d'archivage

Il est impossible de surveiller directement la capacité d'un système de stockage d'archives externe via le système StorageGRID. Vous pouvez toutefois contrôler si le nœud d'archivage peut toujours envoyer des données d'objet à la destination d'archivage, ce qui peut indiquer qu'une extension de support d'archivage est nécessaire.

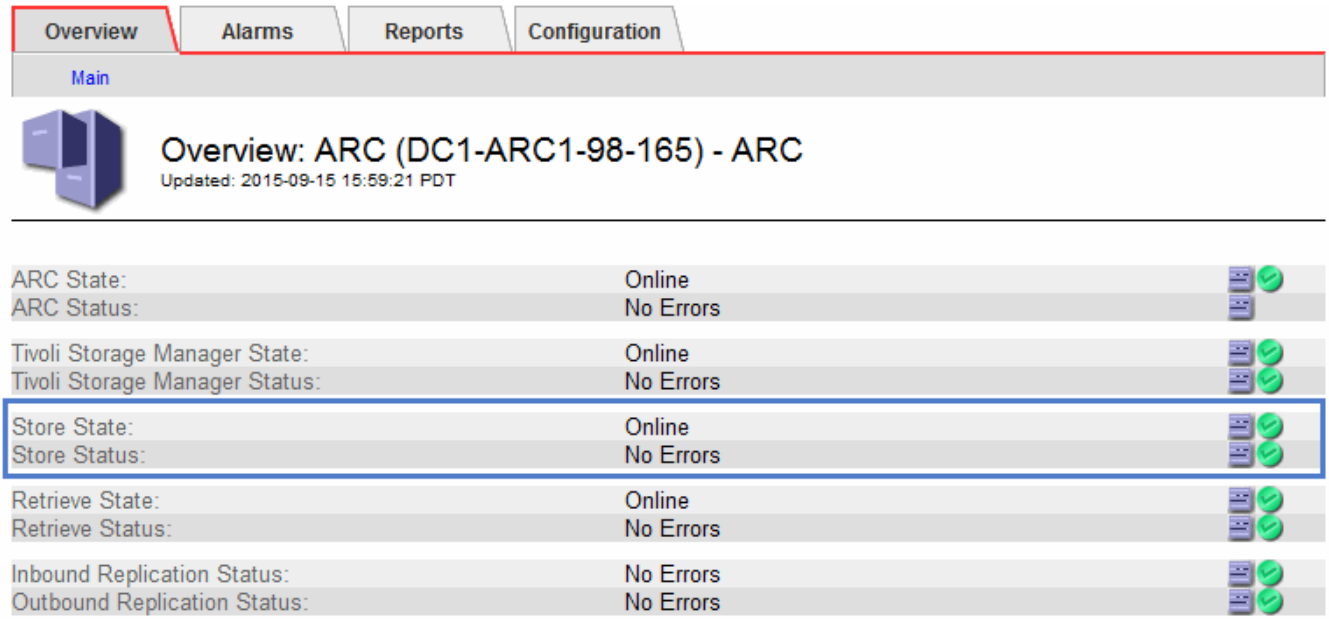
Description de la tâche

Vous pouvez surveiller le composant de stockage pour vérifier si le nœud d'archivage peut toujours envoyer des données d'objet au système de stockage d'archives ciblé. L'alarme Store Failures (ARVF) peut également indiquer que le système de stockage d'archives ciblé a atteint sa capacité et qu'il ne peut plus accepter les

données d'objet.

Étapes

1. Sélectionnez **SUPPORT** > **Outils** > **topologie de grille**.
2. Sélectionnez ***Archive Node*** > **ARC> vue d'ensemble> main**.
3. Vérifiez les attributs Etat du magasin et Etat du magasin pour confirmer que le composant Store est en ligne sans erreur.



Un composant de stockage hors ligne ou un composant contenant des erreurs peut indiquer que le système de stockage d'archivage ciblé ne peut plus accepter les données d'objet en raison de sa capacité atteinte.

Alertes et alarmes

Gestion des alertes et des alarmes : présentation

Le système d'alerte StorageGRID est conçu pour vous informer des problèmes opérationnels qui requièrent votre attention. L'ancien système d'alarme est obsolète.

Système d'alerte

Le système d'alerte est conçu pour être votre outil principal de surveillance des problèmes susceptibles de survenir dans votre système StorageGRID. Le système d'alerte offre une interface facile à utiliser pour détecter, évaluer et résoudre les problèmes.

Les alertes sont déclenchées à des niveaux de gravité spécifiques lorsque les conditions des règles d'alerte sont définies comme vrai. Lorsqu'une alerte est déclenchée, les actions suivantes se produisent :

- Une icône de gravité d'alerte s'affiche sur le tableau de bord dans le Gestionnaire de grille et le nombre d'alertes actuelles est incrémenté.
- L'alerte s'affiche sur la page de résumé **NODES** et sur l'onglet **NODES** > ***node*** > **Overview**.
- Une notification par e-mail est envoyée, en supposant que vous avez configuré un serveur SMTP et fourni des adresses e-mail aux destinataires.

- Une notification SNMP (simple Network Management Protocol) est envoyée, en supposant que vous avez configuré l'agent SNMP StorageGRID.

Système d'alarme existant

Comme les alertes, les alarmes sont déclenchées à des niveaux de gravité spécifiques lorsque les attributs atteignent des valeurs de seuil définies. Toutefois, contrairement aux alertes, de nombreuses alarmes sont déclenchées pour les événements que vous pouvez ignorer en toute sécurité, ce qui peut entraîner un nombre excessif de notifications par e-mail ou SNMP.

> Le système d'alarme est obsolète et sera supprimé dans une version ultérieure. Si vous utilisez toujours des alarmes héritées, vous devez effectuer la transition complète vers le système d'alerte dès que possible.

Lorsqu'une alarme est déclenchée, les actions suivantes se produisent :

- L'alarme s'affiche sur la page **SUPPORT** > **alarmes (hérité)** > **alarmes actuelles**.
- Une notification par e-mail est envoyée, en supposant que vous avez configuré un serveur SMTP et configuré une ou plusieurs listes de diffusion.
- Une notification SNMP peut être envoyée, en supposant que vous avez configuré l'agent SNMP StorageGRID. (Les notifications SNMP ne sont pas envoyées pour toutes les alarmes ou tous les niveaux d'alarme.)

Comparez les alertes et les alarmes

Il existe plusieurs similitudes entre le système d'alerte et le système d'alarme hérité, mais le système d'alerte offre des avantages significatifs et est plus facile à utiliser.

Reportez-vous au tableau suivant pour savoir comment effectuer des opérations similaires.

	Alertes	Alarmes (système hérité)
Comment puis-je voir quelles alertes ou alarmes sont actives ?	• Sélectionnez le lien **alertes actuelles** sur le tableau de bord. • Sélectionnez l'alerte sur la page **NOEUDS** > **Présentation**. • Sélectionnez **ALERTES** > **actuel**. "Afficher les alertes en cours"	Sélectionnez **SUPPORT** > **alarmes (hérité)** > **alarmes actuelles**. "Gestion des alarmes (système hérité)"
Quelle est la cause du déclenchement d'une alerte ou d'une alarme ?	Les alertes sont déclenchées lorsqu'une expression Prometheus dans une règle d'alerte est évaluée comme TRUE pour une condition de déclenchement et une durée spécifiques. "Afficher les règles d'alerte"	Les alarmes sont déclenchées lorsqu'un attribut StorageGRID atteint une valeur de seuil. "Gestion des alarmes (système hérité)"

	Alertes	Alarmes (système hérité)
Si une alerte ou une alarme est déclenchée, comment résoudre le problème sous-jacent ?	Les actions recommandées pour une alerte sont incluses dans les notifications par e-mail et sont disponibles dans les pages alertes du Gestionnaire de grille. Si nécessaire, des informations supplémentaires sont fournies dans la documentation StorageGRID. "Référence des alertes"	Pour en savoir plus sur une alarme, sélectionnez le nom de l'attribut ou recherchez un code d'alarme dans la documentation StorageGRID. "Référence des alarmes (système hérité)"
Où puis-je voir une liste d'alertes ou d'alarmes qui ont été résolues ?	Sélectionnez **ALERTES** > **résolu**. "Afficher les alertes actuelles et résolues"	Sélectionnez **SUPPORT** > **alarmes (hérité)** > **alarmes historiques**. "Gestion des alarmes (système hérité)"
Où puis-je gérer les paramètres ?	Sélectionnez **ALERTES** > **règles**. "Gérer les alertes"	Sélectionnez **SUPPORT**. Utilisez ensuite les options de la section **alarmes (hérité)** du menu. "Gestion des alarmes (système hérité)"
Quelles autorisations de groupe d'utilisateurs ai-je besoin ?	• Toute personne qui peut se connecter au Grid Manager peut afficher les alertes actuelles et résolues. • Vous devez disposer de l'autorisation gérer les alertes pour gérer les silences, les notifications d'alerte et les règles d'alerte. "Administrer StorageGRID"	• Toute personne qui peut se connecter à Grid Manager peut afficher les alarmes héritées. • Vous devez disposer de l'autorisation d'acquittement des alarmes pour accuser réception des alarmes. • Pour gérer les alarmes globales et les notifications par e-mail, vous devez disposer à la fois de la configuration de la page topologie de la grille et d'autres autorisations de configuration de la grille. "Administrer StorageGRID"

	Alertes	Alarmes (système hérité)
Comment puis-je gérer les notifications par e-mail ?	Sélectionnez **ALERTES** > **Configuration de la messagerie**. **Remarque :** puisque les alarmes et les alertes sont des systèmes indépendants, la configuration des e-mails utilisée pour les notifications d'alarme et de AutoSupport n'est pas utilisée pour les notifications d'alerte. Cependant, vous pouvez utiliser le même serveur de messagerie pour toutes les notifications. "Configurez les notifications par e-mail pour les alertes"	Sélectionnez **SUPPORT** > **alarmes (hérité)** > **Configuration messagerie héritée**. "Gestion des alarmes (système hérité)"
Comment gérer les notifications SNMP ?	Sélectionnez **CONFIGURATION** > **surveillance** > **agent SNMP**. "Utiliser la surveillance SNMP"	*Non pris en charge*
Comment puis-je contrôler qui reçoit les notifications ?	1. Sélectionnez **ALERTES** > **Configuration de la messagerie**. 2. Dans la section **destinataires**, entrez une adresse e-mail pour chaque liste d'e-mails ou personne qui doit recevoir un e-mail lorsqu'une alerte se produit. "Configurez les notifications par e-mail pour les alertes"	1. Sélectionnez **SUPPORT** > **alarmes (hérité)** > **Configuration messagerie héritée**. 2. Création d'une liste de diffusion. 3. Sélectionnez **Notifications**. 4. Sélectionnez la liste de diffusion. "Gestion des alarmes (système hérité)"
Quels nœuds d'administration envoient des notifications ?	Un seul nœud d'administration (l'expéditeur préféré). "Qu'est-ce qu'un nœud d'administration ?"	Un seul nœud d'administration (l'expéditeur préféré). "Qu'est-ce qu'un nœud d'administration ?"

	Alertes	Alarmes (système hérité)
Comment supprimer certaines notifications ?	1. Sélectionnez **ALERTES** > **silences**. 2. Sélectionnez la règle d'alerte que vous souhaitez désactiver. 3. Spécifiez une durée pour le silence. 4. Sélectionnez la gravité de l'alerte que vous souhaitez désactiver. 5. Sélectionnez cette option pour appliquer le silence à la grille entière, à un seul site ou à un seul nœud. **Remarque** : si vous avez activé l'agent SNMP, les silences suppriment également les interruptions SNMP et informe. "Notifications d'alerte de silence"	1. Sélectionnez **SUPPORT** > **alarmes (hérité)** > **Configuration messagerie héritée**. 2. Sélectionnez **Notifications**. 3. Sélectionnez une liste de diffusion et sélectionnez **Supprimer**. "Gestion des alarmes (système hérité)"
Comment supprimer toutes les notifications ?	Sélectionnez **ALERTES** > **silences**.sélectionnez alors **toutes les règles**. **Remarque** : si vous avez activé l'agent SNMP, les silences suppriment également les interruptions SNMP et informe. "Notifications d'alerte de silence"	*Non pris en charge*
Comment personnaliser les conditions et les déclencheurs ?	1. Sélectionnez **ALERTES** > **règles**. 2. Sélectionnez une règle par défaut à modifier ou sélectionnez **Créer une règle personnalisée**. "Modifiez les règles d'alerte" "Création de règles d'alerte personnalisées"	1. Sélectionnez **SUPPORT** > **alarmes (hérité)** > **alarmes globales**. 2. Créez une alarme personnalisée globale pour remplacer une alarme par défaut ou pour surveiller un attribut qui n'a pas d'alarme par défaut. "Gestion des alarmes (système hérité)"

	Alertes	Alarmes (système hérité)
Comment désactiver une alerte ou une alarme individuelle ?	1. Sélectionnez **ALERTES** > **règles**. 2. Sélectionnez la règle et sélectionnez **Modifier la règle**. 3. Décochez la case **activé**. "Désactiver les règles d'alerte"	1. Sélectionnez **SUPPORT** > **alarmes (hérité)** > **alarmes globales**. 2. Sélectionnez la règle et sélectionnez l'icône Modifier. 3. Décochez la case **activé**. "Gestion des alarmes (système hérité)"

Gérer les alertes

Gérer les alertes : présentation

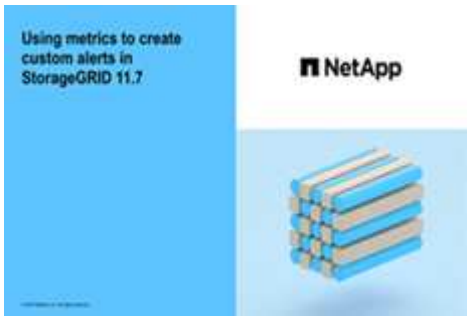
Le système d'alerte offre une interface facile à utiliser pour détecter, évaluer et résoudre les problèmes susceptibles de se produire lors du fonctionnement de StorageGRID.

Vous pouvez créer des alertes personnalisées, modifier ou désactiver des alertes et gérer les notifications d'alerte.

Pour en savoir plus :

- Regardez la vidéo : "Vidéo : présentation des alertes pour StorageGRID 11.7"

- Regardez la vidéo : "Vidéo : utilisation de metrics pour créer des alertes personnalisées dans StorageGRID 11.7"



- Voir la "Référence des alertes".

Afficher les règles d'alerte

Les règles d'alerte définissent les conditions qui se déclenchent "alertes spécifiques". StorageGRID inclut un ensemble de règles d'alerte par défaut que vous pouvez utiliser en l'état ou en modifier, ou vous pouvez créer des règles d'alerte personnalisées.

Vous pouvez afficher la liste de toutes les règles d'alerte par défaut et personnalisées pour savoir quelles conditions déclenchent chaque alerte et pour déterminer si les alertes sont désactivées.

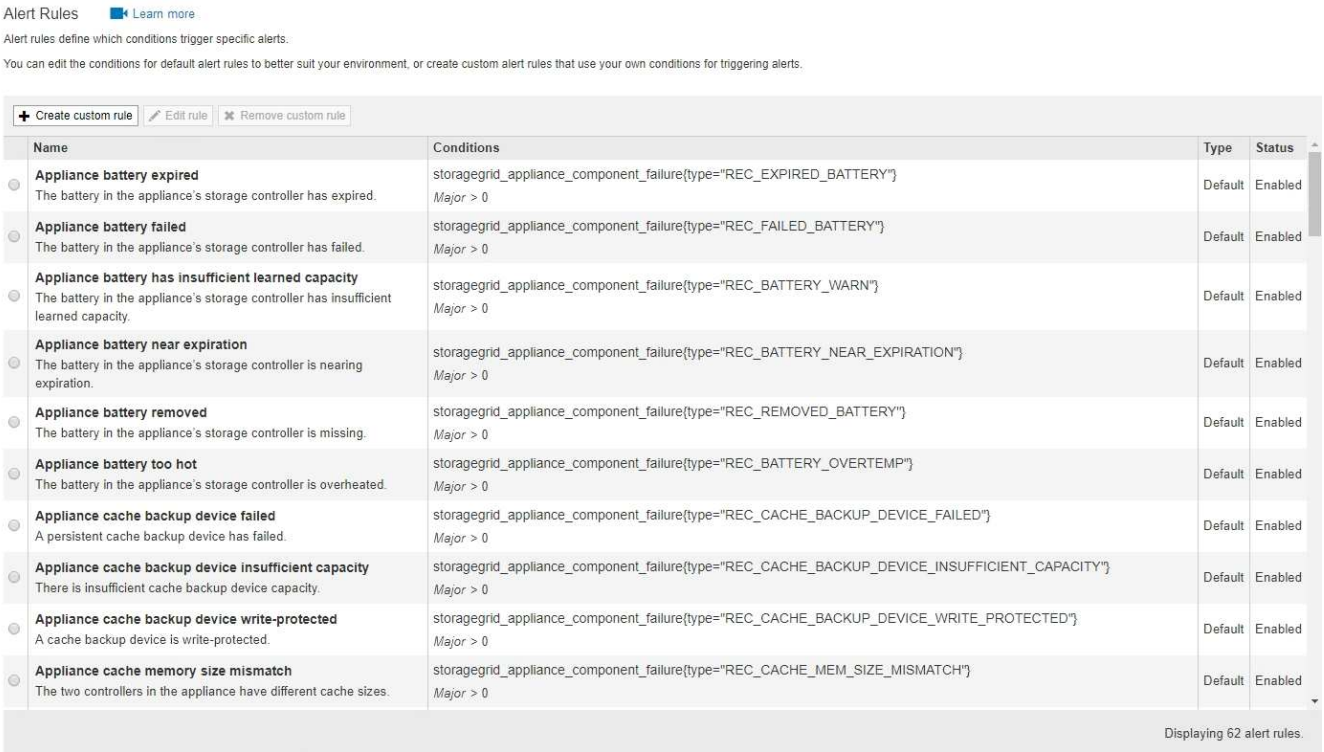
Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous disposez de l'autorisation gérer les alertes ou l'accès racine.
- Vous pouvez également regarder la vidéo : "Vidéo : présentation des alertes pour StorageGRID 11.7"

Étapes

1. Sélectionnez **ALERTES** > **règles**.

   La page règles d'alerte s'affiche.



2. Vérifiez les informations du tableau des règles d'alerte :

En-tête de colonne	Description
Nom	Nom et description uniques de la règle d'alerte. Les règles d'alerte personnalisées sont répertoriées en premier, suivies des règles d'alerte par défaut. Le nom de la règle d'alerte est l'objet des notifications par e-mail.
Conditions	Expressions Prometheus qui déterminent le moment où cette alerte est déclenchée. Une alerte peut être déclenchée à un ou plusieurs des niveaux de sévérité suivants, mais une condition pour chaque gravité n'est pas requise. • **Critique** : Il existe une condition anormale qui a arrêté les opérations normales d'un nœud ou service StorageGRID. Vous devez immédiatement résoudre le problème sous-jacent. Une interruption du service et une perte de données peuvent se produire si le problème n'est pas résolu. • **Majeur** : Il existe une condition anormale affectant les opérations en cours ou approchant le seuil d'une alerte critique. Vous devez examiner les alertes majeures et résoudre tous les problèmes sous-jacents pour vérifier que leur condition anormale n'arrête pas le fonctionnement normal d'un nœud ou d'un service StorageGRID. • **Mineur** : Le système fonctionne normalement, mais il existe une condition anormale qui pourrait affecter la capacité du système à fonctionner s'il continue. Vous devez surveiller et résoudre les alertes mineures qui ne sont pas claires par elles-mêmes pour vous assurer qu'elles n'entraînent pas de problème plus grave.
Type	Type de règle d'alerte : • **Default** : règle d'alerte fournie avec le système. Vous pouvez désactiver une règle d'alerte par défaut ou modifier les conditions et la durée d'une règle d'alerte par défaut. Vous ne pouvez pas supprimer une règle d'alerte par défaut. • **Par défaut*** : règle d'alerte par défaut qui inclut une condition ou une durée modifiée. Si nécessaire, vous pouvez facilement rétablir une condition modifiée par défaut. • **Custom** : une règle d'alerte que vous avez créée. Vous pouvez désactiver, modifier et supprimer des règles d'alerte personnalisées.
État	Si cette règle d'alerte est actuellement activée ou désactivée. Les conditions des règles d'alerte désactivées ne sont pas évaluées et aucune alerte n'est déclenchée.

Création de règles d'alerte personnalisées

Vous pouvez créer des règles d'alerte personnalisées afin de définir vos propres conditions pour déclencher des alertes.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge"
- Vous disposez de l'autorisation gérer les alertes ou l'accès racine
- Vous connaissez le "Metrics Prometheus couramment utilisés"
- Vous comprenez le "Syntaxe des requêtes Prometheus"
- Vous pouvez également regarder la vidéo : "Vidéo : utilisation de metrics pour créer des alertes personnalisées dans StorageGRID 11.7"

Description de la tâche

StorageGRID ne valide pas les alertes personnalisées. Si vous décidez de créer des règles d'alerte personnalisées, suivez les consignes générales suivantes :

- Consultez les conditions des règles d'alerte par défaut et utilisez-les comme exemples pour vos règles d'alerte personnalisées.
- Si vous définissez plusieurs conditions pour une règle d'alerte, utilisez la même expression pour toutes les conditions. Modifiez ensuite la valeur seuil pour chaque condition.
- Vérifier soigneusement chaque condition pour détecter les fautes de frappe et les erreurs logiques.
- Utilisez uniquement les metrics répertoriées dans l'API Grid Management.
- Lors du test d'une expression à l'aide de l'API de gestion de grille, sachez qu'une réponse « sucs » peut être un corps de réponse vide (aucune alerte déclenchée). Pour vérifier si l'alerte est déclenchée, vous pouvez définir temporairement une valeur de seuil sur laquelle vous vous attendez à ce que la valeur soit vraie actuellement.

  Par exemple, pour tester l'expression `node_memory_MemTotal_bytes < 24000000000`, première exécution `node_memory_MemTotal_bytes >= 0` et assurez-vous d'obtenir les résultats attendus (tous les nœuds renvoient une valeur). Ensuite, remplacez l'opérateur et le seuil par les valeurs prévues et recommencez. Aucun résultat n'indique qu'il n'y a pas d'alerte en cours pour cette expression.

- Ne supposez pas qu'une alerte personnalisée fonctionne, sauf si vous avez validé que l'alerte est déclenchée quand vous le souhaitez.

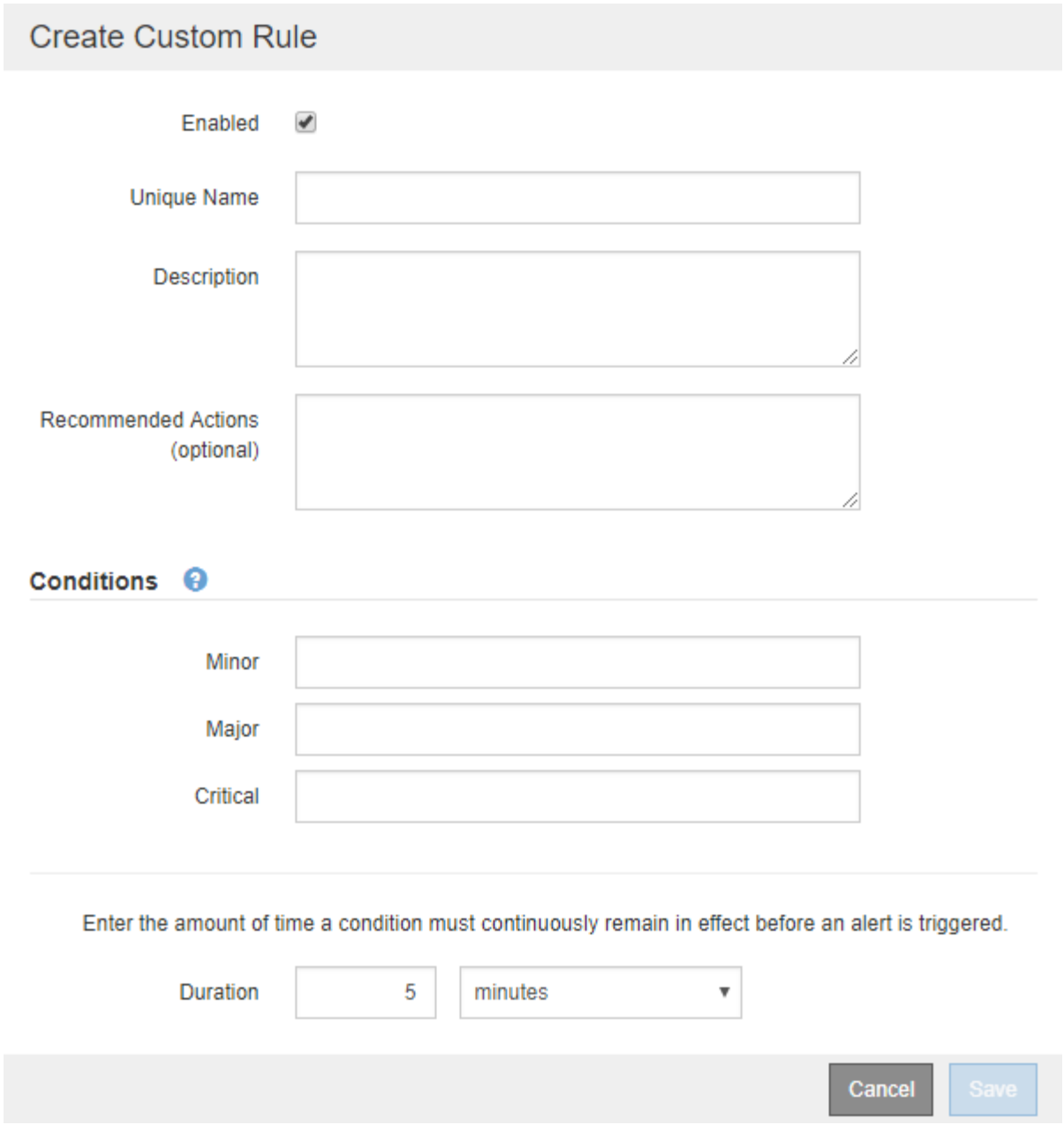
Étapes

1. Sélectionnez **ALERTES** > **règles**.

   La page règles d'alerte s'affiche.

2. Sélectionnez **Créer règle personnalisée**.

   La boîte de dialogue Créer une règle personnalisée s'affiche.



3. Cochez ou décochez la case **activé** pour déterminer si cette règle d'alerte est actuellement activée.

   Si une règle d'alerte est désactivée, ses expressions ne sont pas évaluées et aucune alerte n'est déclenchée.

4. Saisissez les informations suivantes :

Champ	Description
Nom unique	Un nom unique pour cette règle. Le nom de la règle d'alerte s'affiche sur la page alertes et est également l'objet des notifications par e-mail. Les noms des règles d'alerte peuvent comporter entre 1 et 64 caractères.

Champ	Description
Description	Description du problème. La description est le message d'alerte affiché sur la page alertes et dans les notifications par e-mail. Les descriptions des règles d'alerte peuvent comporter entre 1 et 128 caractères.
Actions recommandées	En option, les actions recommandées à effectuer lorsque cette alerte est déclenchée. Saisissez les actions recommandées en texte brut (aucun code de mise en forme). Les actions recommandées pour les règles d'alerte peuvent comporter entre 0 et 1,024 caractères.

5. Dans la section Conditions, entrez une expression Prometheus pour un ou plusieurs niveaux de gravité d'alerte.

   Une expression de base est généralement de la forme :

   ```
   [metric] [operator] [value]
   ```

   Les expressions peuvent être de toute longueur, mais apparaissent sur une seule ligne dans l'interface utilisateur. Au moins une expression est requise.

   Cette expression déclenche une alerte si la quantité de RAM installée pour un nœud est inférieure à 24,000,000,000 octets (24 Go).

   ```
   node_memory_MemTotal_bytes < 24000000000
   ```

   Pour afficher les metrics disponibles et tester les expressions Prometheus, sélectionnez l'icône d'aide Et suivez le lien vers la section Metrics de l'API de gestion du grid.

6. Dans le champ **durée**, entrez la durée pendant laquelle une condition doit rester en vigueur en continu avant le déclenchement de l'alerte et sélectionnez une unité de temps.

   Pour déclencher une alerte immédiatement lorsqu'une condition devient vraie, entrez **0**. Augmentez cette valeur pour éviter que des conditions temporaires ne déclenchent des alertes.

   La valeur par défaut est 5 minutes.

7. Sélectionnez **Enregistrer**.

   La boîte de dialogue se ferme et la nouvelle règle d'alerte personnalisée apparaît dans le tableau règles d'alerte.

Modifiez les règles d'alerte

Vous pouvez modifier une règle d'alerte pour modifier les conditions de déclenchement, pour une règle d'alerte personnalisée, vous pouvez également mettre à jour le nom de la règle, sa description et les actions recommandées.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous disposez de l'autorisation gérer les alertes ou l'accès racine.

Description de la tâche

Lorsque vous modifiez une règle d'alerte par défaut, vous pouvez modifier les conditions pour les alertes mineures, majeures et critiques, ainsi que la durée. Lorsque vous modifiez une règle d'alerte personnalisée, vous pouvez également modifier le nom, la description et les actions recommandées de la règle.

> Soyez prudent lorsque vous décidez de modifier une règle d'alerte. Si vous modifiez les valeurs de déclenchement, il est possible que vous ne déteciez pas de problème sous-jacent tant qu'elle n'empêche pas l'exécution d'une opération critique.

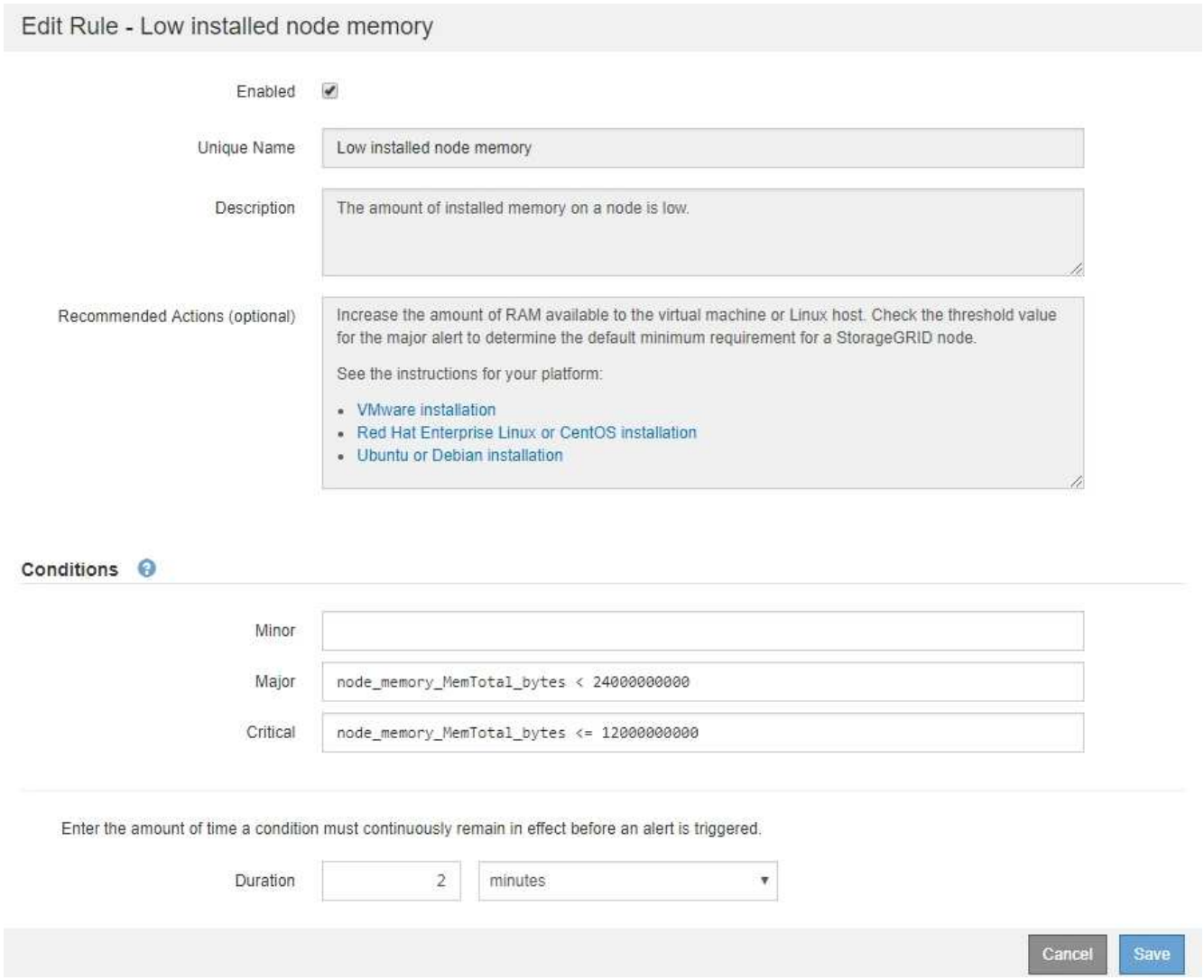
Étapes

1. Sélectionnez **ALERTES** > **règles**.

   La page règles d'alerte s'affiche.

2. Sélectionnez le bouton radio correspondant à la règle d'alerte que vous souhaitez modifier.
3. Sélectionnez **Modifier la règle**.

   La boîte de dialogue Modifier la règle s'affiche. Cet exemple montre une règle d'alerte par défaut, les champs Nom unique, Description et actions recommandées sont désactivés et ne peuvent pas être modifiés.



4. Cochez ou décochez la case **activé** pour déterminer si cette règle d'alerte est actuellement activée.

   Si une règle d'alerte est désactivée, ses expressions ne sont pas évaluées et aucune alerte n'est déclenchée.

   Si vous désactivez la règle d'alerte pour une alerte en cours, vous devez attendre quelques minutes que l'alerte n'apparaisse plus comme une alerte active.

   En général, la désactivation d'une règle d'alerte par défaut n'est pas recommandée. Si une règle d'alerte est désactivée, vous risquez de ne pas détecter un problème sous-jacent tant qu'elle n'empêche pas l'exécution d'une opération critique.

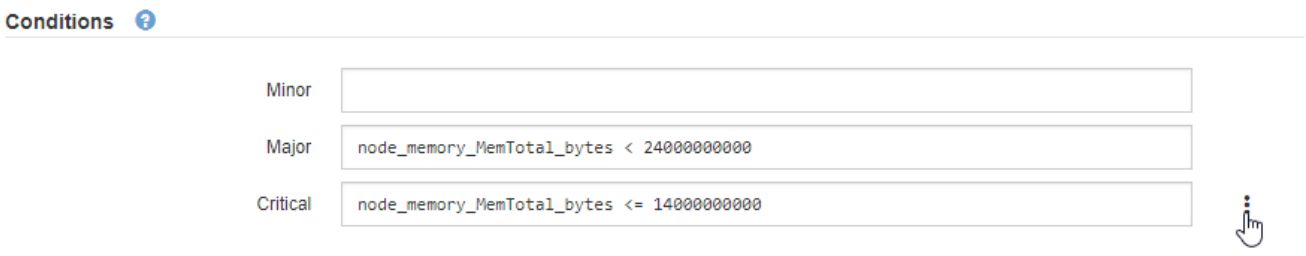
5. Pour les règles d'alerte personnalisées, mettez à jour les informations suivantes si nécessaire.

   Vous ne pouvez pas modifier ces informations pour les règles d'alerte par défaut.

Champ	Description
Nom unique	Un nom unique pour cette règle. Le nom de la règle d'alerte s'affiche sur la page alertes et est également l'objet des notifications par e-mail. Les noms des règles d'alerte peuvent comporter entre 1 et 64 caractères.
Description	Description du problème. La description est le message d'alerte affiché sur la page alertes et dans les notifications par e-mail. Les descriptions des règles d'alerte peuvent comporter entre 1 et 128 caractères.
Actions recommandées	En option, les actions recommandées à effectuer lorsque cette alerte est déclenchée. Saisissez les actions recommandées en texte brut (aucun code de mise en forme). Les actions recommandées pour les règles d'alerte peuvent comporter entre 0 et 1,024 caractères.

6. Dans la section Conditions, entrez ou mettez à jour l'expression Prometheus pour un ou plusieurs niveaux de gravité d'alerte.

   Si vous souhaitez restaurer une condition pour une règle d'alerte par défaut modifiée à sa valeur d'origine, sélectionnez les trois points à droite de la condition modifiée.



Si vous mettez à jour les conditions d'une alerte en cours, vos modifications risquent de ne pas être appliquées tant que la condition précédente n'est pas résolue. La prochaine fois que l'une des conditions de la règle est remplie, l'alerte reflète les valeurs mises à jour.

Une expression de base est généralement de la forme :

```
[metric] [operator] [value]
```

Les expressions peuvent être de toute longueur, mais apparaissent sur une seule ligne dans l'interface utilisateur. Au moins une expression est requise.

Cette expression déclenche une alerte si la quantité de RAM installée pour un nœud est inférieure à 24,000,000,000 octets (24 Go).

```
node_memory_MemTotal_bytes < 24000000000
```

7. Dans le champ **durée**, entrez la durée pendant laquelle une condition doit rester en vigueur en continu avant le déclenchement de l'alerte et sélectionnez l'unité de temps.

   Pour déclencher une alerte immédiatement lorsqu'une condition devient vraie, entrez **0**. Augmentez cette valeur pour éviter que des conditions temporaires ne déclenchent des alertes.

   La valeur par défaut est 5 minutes.

8. Sélectionnez **Enregistrer**.

   Si vous avez modifié une règle d'alerte par défaut, **default*** apparaît dans la colonne Type. Si vous avez désactivé une règle d'alerte par défaut ou personnalisée, **Disabled** apparaît dans la colonne **Status**.

Désactiver les règles d'alerte

Vous pouvez modifier l'état activé/désactivé pour une règle d'alerte par défaut ou personnalisée.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous disposez de l'autorisation gérer les alertes ou l'accès racine.

Description de la tâche

Lorsqu'une règle d'alerte est désactivée, ses expressions ne sont pas évaluées et aucune alerte n'est déclenchée.

En général, la désactivation d'une règle d'alerte par défaut n'est pas recommandée. Si une règle d'alerte est désactivée, vous risquez de ne pas détecter un problème sous-jacent tant qu'elle n'empêche pas l'exécution d'une opération critique.

Étapes

1. Sélectionnez **ALERTES** > **règles**.

   La page règles d'alerte s'affiche.

2. Sélectionnez le bouton radio de la règle d'alerte que vous souhaitez désactiver ou activer.

3. Sélectionnez **Modifier la règle**.

   La boîte de dialogue Modifier la règle s'affiche.

4. Cochez ou décochez la case **activé** pour déterminer si cette règle d'alerte est actuellement activée.

   Si une règle d'alerte est désactivée, ses expressions ne sont pas évaluées et aucune alerte n'est déclenchée.

   > Si vous désactivez la règle d'alerte pour une alerte en cours, vous devez attendre quelques minutes que l'alerte ne s'affiche plus comme alerte active.

5. Sélectionnez **Enregistrer**.

   Disabled apparaît dans la colonne **Status**.

Supprimez les règles d'alerte personnalisées

Vous pouvez supprimer une règle d'alerte personnalisée si vous ne souhaitez plus l'utiliser.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous disposez de l'autorisation gérer les alertes ou l'accès racine.

Étapes

1. Sélectionnez **ALERTES** > **règles**.

   La page règles d'alerte s'affiche.

2. Sélectionnez le bouton radio de la règle d'alerte personnalisée que vous souhaitez supprimer.

   Vous ne pouvez pas supprimer une règle d'alerte par défaut.

3. Sélectionnez **Supprimer la règle personnalisée**.

   Une boîte de dialogue de confirmation s'affiche.

4. Sélectionnez **OK** pour supprimer la règle d'alerte.

   Toutes les instances actives de l'alerte seront résolues dans un délai de 10 minutes.

Gérer les notifications d'alerte

Configurez les notifications SNMP pour les alertes

Si vous souhaitez que StorageGRID envoie des notifications SNMP lorsque des alertes se produisent, vous devez activer l'agent SNMP StorageGRID et configurer une ou plusieurs destinations d'interruption.

Vous pouvez utiliser l'option **CONFIGURATION** > **surveillance** > **agent SNMP** dans le Gestionnaire de grille ou les noeuds finaux SNMP pour l'API de gestion de grille pour activer et configurer l'agent SNMP

StorageGRID. L'agent SNMP prend en charge les trois versions du protocole SNMP.

Pour savoir comment configurer l'agent SNMP, reportez-vous à la section "Utiliser la surveillance SNMP".

Après avoir configuré l'agent SNMP StorageGRID, deux types de notifications basées sur les événements peuvent être envoyées :

- Les interruptions sont des notifications envoyées par l'agent SNMP qui ne nécessitent pas d'accusé de réception par le système de gestion. Les interruptions servent à signaler au système de gestion qu'une alerte s'est produite au sein de StorageGRID, par exemple. Les traps sont pris en charge dans les trois versions de SNMP.
- Les informations sont similaires aux pièges, mais elles nécessitent une reconnaissance par le système de gestion. Si l'agent SNMP ne reçoit pas d'accusé de réception dans un certain temps, il renvoie l'information jusqu'à ce qu'un accusé de réception soit reçu ou que la valeur de nouvelle tentative maximale ait été atteinte. Les informations sont prises en charge dans SNMPv2c et SNMPv3.

Des notifications d'interruption et d'information sont envoyées lorsqu'une alerte par défaut ou personnalisée est déclenchée à n'importe quel niveau de gravité. Pour supprimer les notifications SNMP pour une alerte, vous devez configurer un silence pour l'alerte. Voir "Notifications d'alerte de silence".

Si votre déploiement StorageGRID inclut plusieurs nœuds d'administration, le nœud d'administration principal est l'expéditeur préféré pour les notifications d'alerte, les messages AutoSupport, les traps et les notifications SNMP et les notifications d'alarme héritées. Si le nœud d'administration principal n'est plus disponible, les notifications sont envoyées temporairement par d'autres nœuds d'administration. Voir "Qu'est-ce qu'un nœud d'administration ?".

Configurez les notifications par e-mail pour les alertes

Si vous souhaitez que des notifications par e-mail soient envoyées lorsque des alertes se produisent, vous devez fournir des informations sur votre serveur SMTP. Vous devez également saisir des adresses e-mail pour les destinataires des notifications d'alerte.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous disposez de l'autorisation gérer les alertes ou l'accès racine.

Description de la tâche

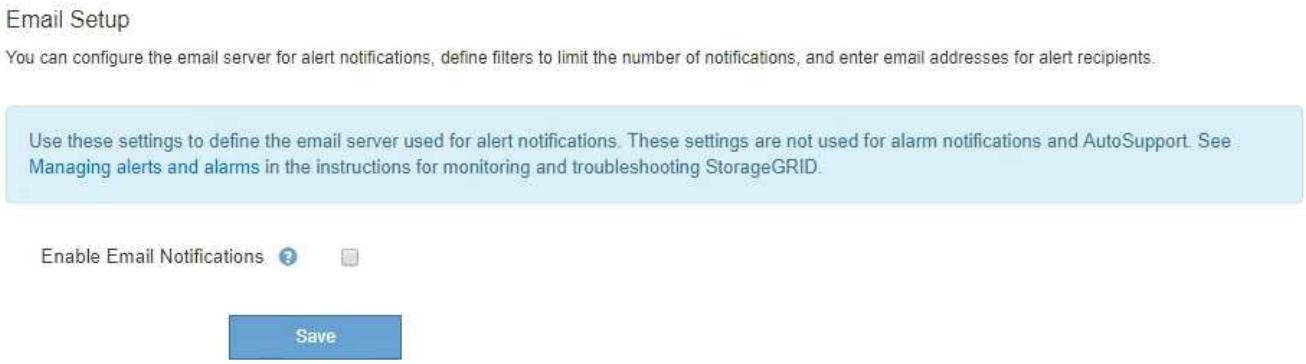
Comme les alarmes et les alertes sont des systèmes indépendants, la configuration des e-mails utilisée pour les notifications d'alerte n'est pas utilisée pour les notifications d'alarme et les messages AutoSupport. Cependant, vous pouvez utiliser le même serveur de messagerie pour toutes les notifications.

Si votre déploiement StorageGRID inclut plusieurs nœuds d'administration, le nœud d'administration principal est l'expéditeur préféré pour les notifications d'alerte, les messages AutoSupport, les traps et les notifications SNMP et les notifications d'alarme héritées. Si le nœud d'administration principal n'est plus disponible, les notifications sont envoyées temporairement par d'autres nœuds d'administration. Voir "Qu'est-ce qu'un nœud d'administration ?".

Étapes

1. Sélectionnez **ALERTES** > **Configuration de la messagerie**.

   La page Configuration de l'e-mail s'affiche.



2. Cochez la case **Activer les notifications par e-mail** pour indiquer que vous souhaitez que les e-mails de notification soient envoyés lorsque les alertes atteignent des seuils configurés.

   Les sections serveur d'e-mail (SMTP), sécurité de la couche de transport (TLS), adresses e-mail et filtres s'affichent.

3. Dans la section serveur de messagerie (SMTP), entrez les informations dont StorageGRID a besoin pour accéder à votre serveur SMTP.

   Si votre serveur SMTP nécessite une authentification, vous devez fournir à la fois un nom d'utilisateur et un mot de passe.

Champ	Entrez
Serveur de messagerie	Nom de domaine complet (FQDN) ou adresse IP du serveur SMTP.
Port	Port utilisé pour accéder au serveur SMTP. Doit être compris entre 1 et 65535.
Nom d'utilisateur (facultatif)	Si votre serveur SMTP nécessite une authentification, entrez le nom d'utilisateur à authentifier.
Mot de passe (facultatif)	Si votre serveur SMTP nécessite une authentification, entrez le mot de passe à authentifier auprès de.

4. Dans la section adresses e-mail, entrez les adresses e-mail de l'expéditeur et de chaque destinataire.

   a. Pour l'adresse électronique **expéditeur**, spécifiez une adresse e-mail valide à utiliser comme adresse de pour les notifications d'alerte.

Par exemple : `storagegrid-alerts@example.com`

b. Dans la section destinataires, entrez une adresse e-mail pour chaque liste d'e-mails ou personne devant recevoir un e-mail lorsqu'une alerte se produit.

Sélectionnez l'icône plus ➕ pour ajouter des destinataires.

5. Si transport Layer Security (TLS) est requis pour les communications avec le serveur SMTP, sélectionnez **exiger TLS** dans la section transport Layer Security (TLS).

a. Dans le champ **certificat CA**, indiquez le certificat CA qui sera utilisé pour vérifier l'identification du serveur SMTP.

Vous pouvez copier et coller le contenu dans ce champ ou sélectionner **Parcourir** et sélectionner le fichier.

Vous devez fournir un seul fichier contenant les certificats de chaque autorité de certification intermédiaire (AC). Le fichier doit contenir chacun des fichiers de certificat d'autorité de certification codés au PEM, concaténés dans l'ordre de la chaîne de certificats.

b. Cochez la case **Envoyer le certificat client** si votre serveur de messagerie SMTP requiert que les expéditeurs de courrier électronique fournissent des certificats client pour l'authentification.

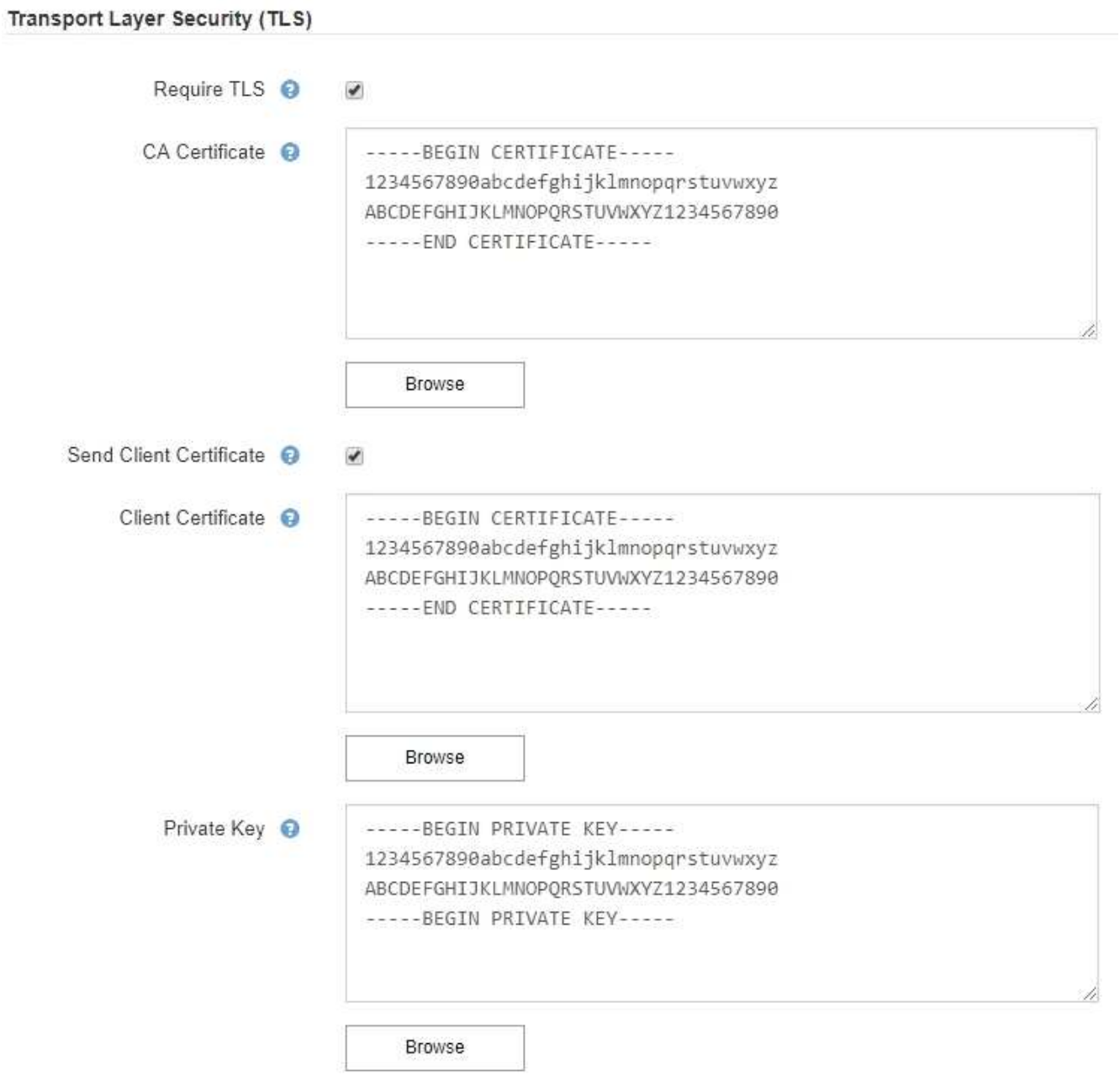
c. Dans le champ **certificat client**, fournissez le certificat client codé PEM à envoyer au serveur SMTP.

Vous pouvez copier et coller le contenu dans ce champ ou sélectionner **Parcourir** et sélectionner le fichier.

d. Dans le champ **Private Key**, saisissez la clé privée du certificat client dans le codage PEM non chiffré.

Vous pouvez copier et coller le contenu dans ce champ ou sélectionner **Parcourir** et sélectionner le fichier.

> ⓘ Si vous devez modifier la configuration de la messagerie, sélectionnez l'icône crayon pour mettre à jour ce champ.



6. Dans la section filtres, sélectionnez les niveaux de gravité des alertes qui doivent donner lieu à des notifications par e-mail, sauf si la règle d'une alerte spécifique a été mise en silence.

Gravité	Description
Mineur, majeur, critique	Une notification par e-mail est envoyée lorsque la condition mineure, majeure ou critique d'une règle d'alerte est remplie.
Important, critique	Une notification par e-mail est envoyée lorsque la condition principale ou critique d'une règle d'alerte est remplie. Les notifications ne sont pas envoyées pour les alertes mineures.

Gravité	Description
Critique uniquement	Une notification par e-mail est envoyée uniquement lorsque la condition critique d'une règle d'alerte est remplie. Les notifications ne sont pas envoyées pour les alertes mineures ou majeures.

7. Lorsque vous êtes prêt à tester vos paramètres de messagerie, procédez comme suit :
   a. Sélectionnez **Envoyer e-mail test**.

      Un message de confirmation s'affiche, indiquant qu'un e-mail de test a été envoyé.

   b. Cochez les cases de tous les destinataires d'e-mail et confirmez qu'un e-mail de test a été reçu.

      Si l'e-mail n'est pas reçu dans quelques minutes ou si l'alerte **échec de notification par e-mail** est déclenchée, vérifiez vos paramètres et réessayez.

   c. Connectez-vous à tout autre nœud d'administration et envoyez un e-mail de test pour vérifier la connectivité de tous les sites.

      Lorsque vous testez les notifications d'alertes, vous devez vous connecter à chaque nœud d'administration pour vérifier la connectivité. Cela contraste avec le test des messages AutoSupport et des notifications d'alarme héritées, où tous les nœuds d'administration envoient l'e-mail test.

8. Sélectionnez **Enregistrer**.

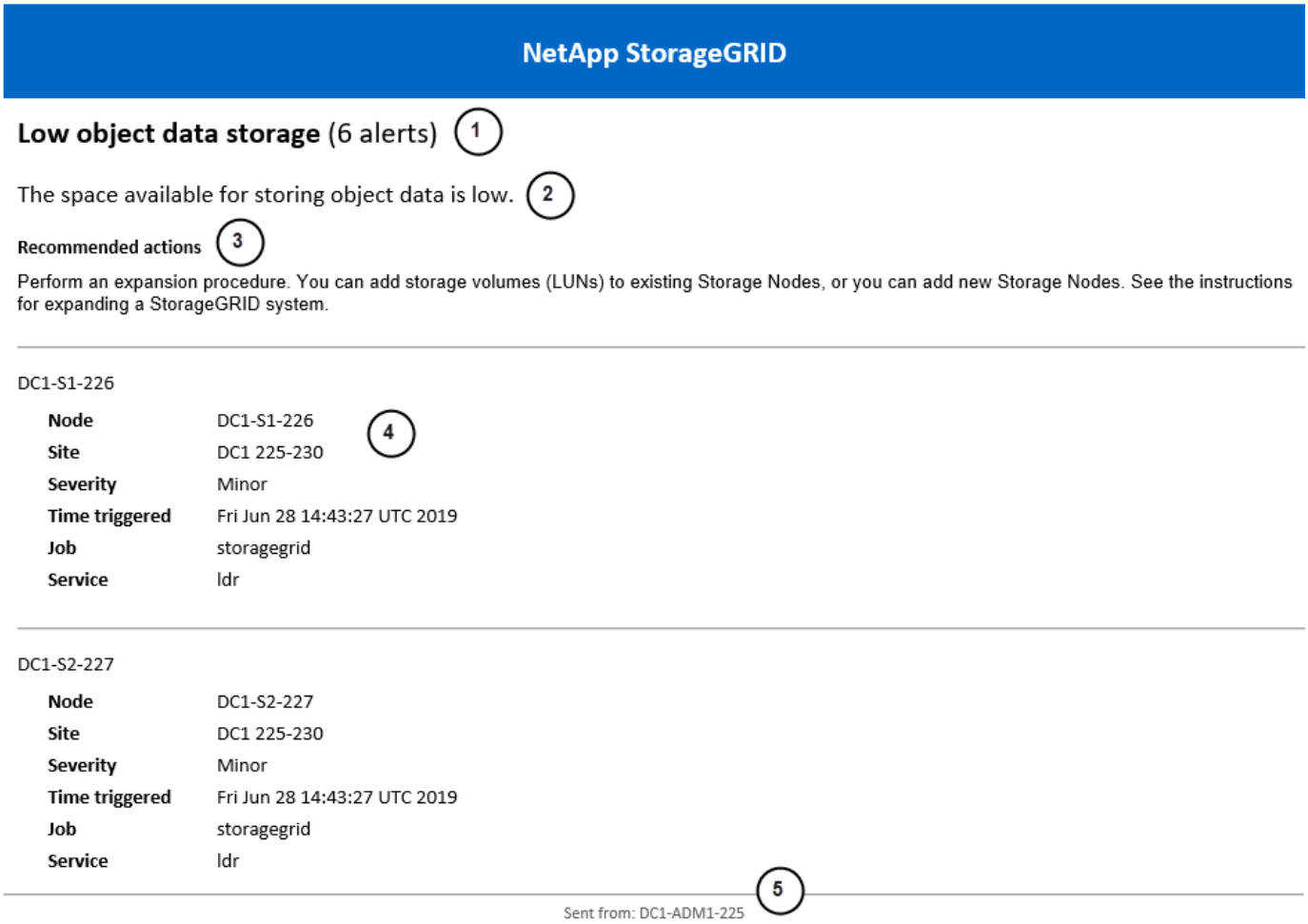
   L'envoi d'un e-mail de test n'enregistre pas vos paramètres. Vous devez sélectionner **Enregistrer**.

   Les paramètres de messagerie sont enregistrés.

Informations incluses dans les notifications par e-mail d'alerte

Après avoir configuré le serveur de messagerie SMTP, des notifications par e-mail sont envoyées aux destinataires désignés lorsqu'une alerte est déclenchée, à moins que la règle d'alerte ne soit supprimée par un silence. Voir "Notifications d'alerte de silence".

Les notifications par e-mail incluent les informations suivantes :



Légende	Description
1	Nom de l'alerte, suivi du nombre d'instances actives de cette alerte.
2	Description de l'alerte.
3	Toutes les actions recommandées pour l'alerte.
4	Détails sur chaque instance active de l'alerte, y compris le nœud et le site affectés, la gravité de l'alerte, l'heure UTC au moment où la règle d'alerte a été déclenchée, ainsi que le nom du travail et du service affectés.
5	Nom d'hôte du nœud d'administration qui a envoyé la notification.

Mode de regroupement des alertes

Pour empêcher l'envoi d'un nombre excessif de notifications par e-mail lorsque des alertes sont déclenchées, StorageGRID tente de regrouper plusieurs alertes dans la même notification.

Reportez-vous au tableau suivant pour obtenir des exemples de la manière dont StorageGRID regroupe plusieurs alertes dans les notifications par e-mail.

Comportement	Exemple
Chaque notification d'alerte s'applique uniquement aux alertes portant le même nom. Si deux alertes avec des noms différents sont déclenchées en même temps, deux notifications par e-mail sont envoyées.	• L'alerte A est déclenchée en même temps sur deux nœuds. Une seule notification est envoyée. • L'alerte A est déclenchée sur le nœud 1 et l'alerte B est déclenchée simultanément sur le nœud 2. Deux notifications sont envoyées : une pour chaque alerte.
Pour une alerte spécifique sur un nœud spécifique, si les seuils sont atteints pour plus d'un degré de sévérité, une notification est envoyée uniquement pour l'alerte la plus grave.	• L'alerte A est déclenchée et le seuil d'alerte secondaire, majeur et critique est atteint. Une notification est envoyée pour l'alerte critique.
La première fois qu'une alerte est déclenchée, StorageGRID attend 2 minutes avant d'envoyer une notification. Si d'autres alertes du même nom sont déclenchées pendant ce temps, StorageGRID regroupe toutes les alertes de la notification initiale.	1. L'alerte A est déclenchée sur le nœud 1 à 08:00. Aucune notification n'a été envoyée. 2. L'alerte A est déclenchée sur le nœud 2 à 08:01. Aucune notification n'a été envoyée. 3. À 08 h 02, une notification est envoyée pour signaler les deux instances de l'alerte.
Si une autre alerte du même nom est déclenchée, StorageGRID attend 10 minutes avant d'envoyer une nouvelle notification. La nouvelle notification signale toutes les alertes actives (alertes en cours qui n'ont pas été désactivées), même si elles ont été signalées précédemment.	1. L'alerte A est déclenchée sur le nœud 1 à 08:00. Une notification est envoyée à 08:02. 2. L'alerte A est déclenchée sur le nœud 2 à 08:05. Une seconde notification est envoyée à 08:15 (10 minutes plus tard). Les deux nœuds sont signalés.
Si plusieurs alertes en cours portent le même nom et que l'une de ces alertes est résolue, une nouvelle notification n'est pas envoyée si l'alerte se reproduit sur le nœud pour lequel l'alerte a été résolue.	1. L'alerte A est déclenchée pour le nœud 1. Une notification est envoyée. 2. L'alerte A est déclenchée pour le nœud 2. Une seconde notification est envoyée. 3. L'alerte A est résolue pour le nœud 2, mais elle reste active pour le nœud 1. 4. L'alerte A est à nouveau déclenchée pour le nœud 2. Aucune nouvelle notification n'est envoyée, car l'alerte est toujours active pour le nœud 1.
StorageGRID continue à envoyer des notifications par e-mail tous les 7 jours jusqu'à ce que toutes les instances de l'alerte soient résolues ou que la règle d'alerte soit désactivée.	1. L'alerte A est déclenchée pour le nœud 1 le 8 mars. Une notification est envoyée. 2. L'alerte A n'est pas résolue ou arrêtée. Des notifications supplémentaires sont envoyées le 15 mars, le 22 mars, le 29 mars, etc.

Dépanner les notifications d'alerte par e-mail

Si l'alerte **échec de notification par e-mail** est déclenchée ou si vous ne parvenez pas à recevoir la notification par e-mail d'alerte de test, procédez comme suit pour résoudre le problème.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous disposez de l'autorisation gérer les alertes ou l'accès racine.

Étapes

1. Vérifiez vos paramètres.
   a. Sélectionnez **ALERTES** > **Configuration de la messagerie**.
   b. Vérifiez que les paramètres du serveur de messagerie (SMTP) sont corrects.
   c. Vérifiez que vous avez spécifié des adresses e-mail valides pour les destinataires.
2. Vérifiez votre filtre de spam et assurez-vous que l'e-mail n'a pas été envoyé à un dossier indésirable.
3. Demandez à votre administrateur de messagerie de confirmer que les e-mails de l'adresse de l'expéditeur ne sont pas bloqués.
4. Collectez un fichier journal pour le nœud d'administration, puis contactez le support technique.

   Le support technique peut utiliser les informations contenues dans les journaux pour vous aider à déterminer ce qui s'est mal passé. Par exemple, le fichier prometheus.log peut afficher une erreur lors de la connexion au serveur spécifié.

   Voir "Collecte de fichiers journaux et de données système".

Notifications d'alerte de silence

Si vous le souhaitez, vous pouvez configurer des silences pour supprimer temporairement les notifications d'alerte.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous disposez de l'autorisation gérer les alertes ou l'accès racine.

Description de la tâche

Vous pouvez désactiver les règles d'alerte sur toute la grille, sur un seul site ou sur un seul nœud et pour une ou plusieurs niveaux de gravité. Chaque silence supprime toutes les notifications d'une règle d'alerte unique ou de toutes les règles d'alerte.

Si vous avez activé l'agent SNMP, les silences suppriment également les interruptions SNMP et informent.

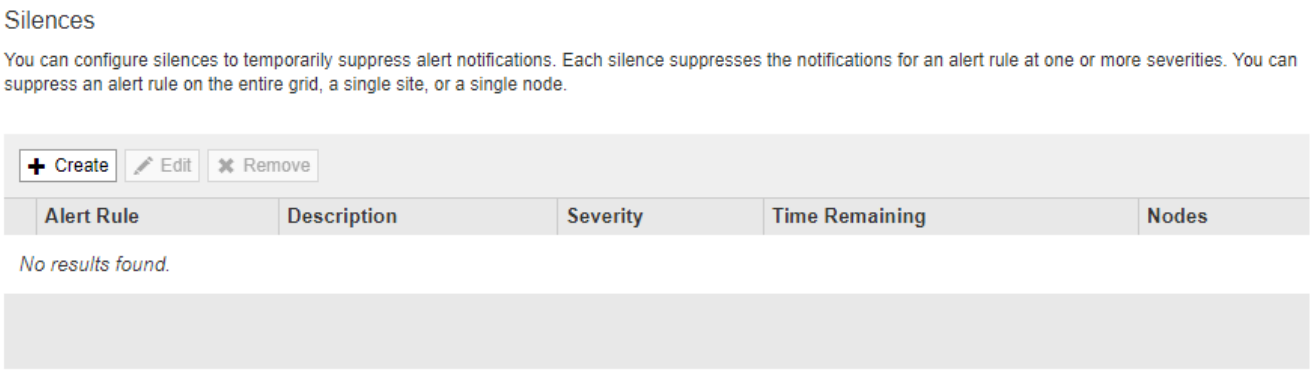
> Soyez prudent lorsque vous décidez de désactiver une règle d'alerte. Si vous neutralisez une alerte, il est possible que vous ne détectez pas un problème sous-jacent tant qu'elle n'empêche pas l'exécution d'une opération critique.

> Comme les alarmes et les alertes sont des systèmes indépendants, vous ne pouvez pas utiliser cette fonctionnalité pour supprimer les notifications d'alarme.

Étapes

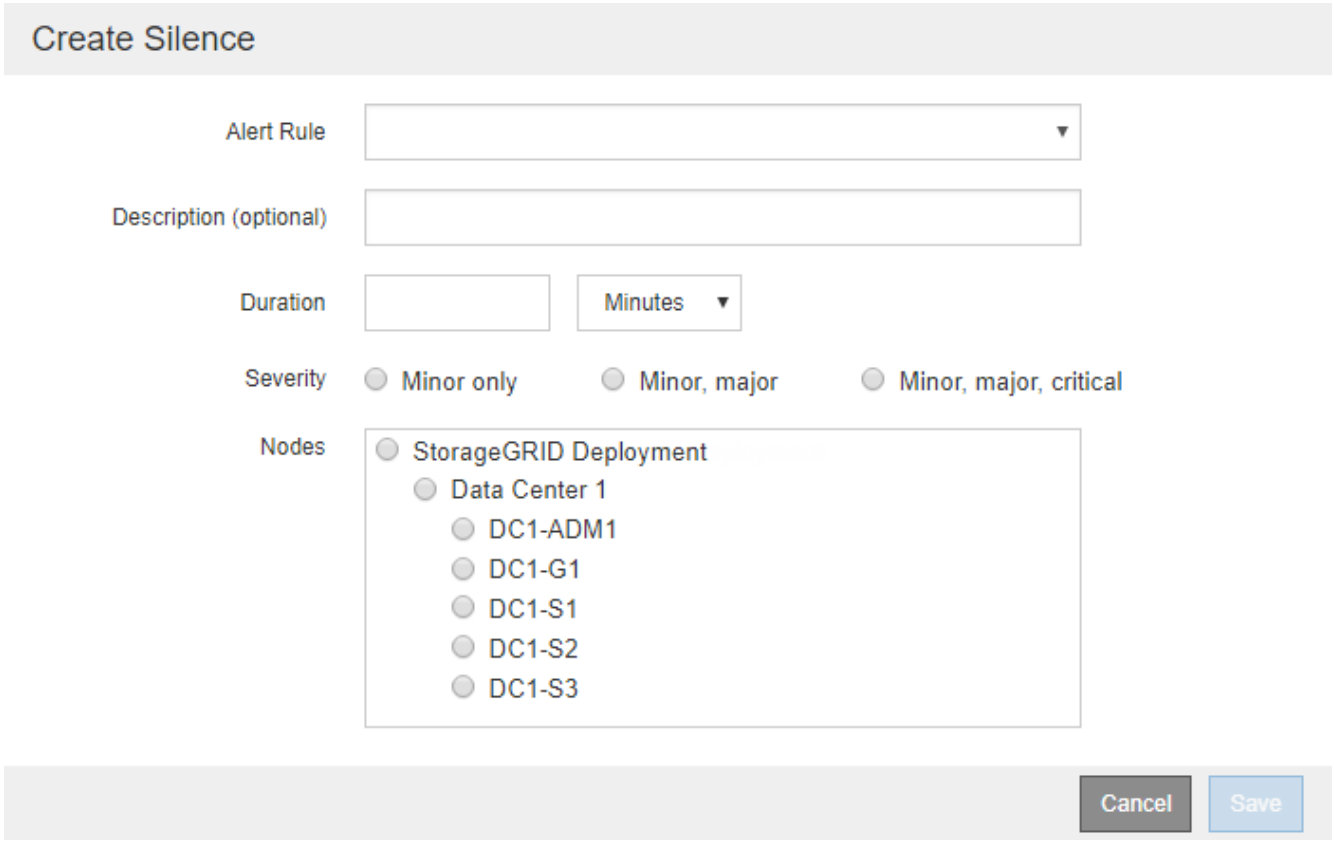
1. Sélectionnez **ALERTES** > **silences**.

   La page silences s'affiche.



2. Sélectionnez **Créer**.

   La boîte de dialogue Créer une Silence s'affiche.



3. Sélectionnez ou entrez les informations suivantes :

Champ	Description
Règle d’alerte	Le nom de la règle d’alerte que vous souhaitez désactiver. Vous pouvez sélectionner n’importe quelle règle d’alerte par défaut ou personnalisée, même si la règle d’alerte est désactivée. **Remarque :** sélectionnez **toutes les règles** si vous voulez désactiver toutes les règles d’alerte en utilisant les critères spécifiés dans cette boîte de dialogue.
Description	Éventuellement, une description du silence. Par exemple, décrivez le but de ce silence.
Durée	Combien de temps vous voulez que ce silence reste en vigueur, en minutes, heures ou jours. Un silence peut être en vigueur de 5 minutes à 1,825 jours (5 ans). **Remarque:** vous ne devez pas désactiver une règle d’alerte pour une durée prolongée. Si une règle d’alerte est mise en mode silencieux, il est possible que vous ne détectiez pas un problème sous-jacent tant qu’elle n’empêche pas l’exécution d’une opération critique. Cependant, vous devrez peut-être utiliser un silence étendu si une alerte est déclenchée par une configuration intentionnelle spécifique, par exemple pour les alertes **liaison appliance Services Down** et les alertes **liaison appliance Storage Down**.
Gravité	Quelle alerte de gravité ou de gravité doit être neutralisée. Si l’alerte est déclenchée à l’un des niveaux de gravité sélectionnés, aucune notification n’est envoyée.
Nœuds	À quel nœud ou nœud vous souhaitez que ce silence s’applique. Vous pouvez supprimer une règle d’alerte ou toutes les règles de la grille dans son ensemble, un seul site ou un seul nœud. Si vous sélectionnez l’ensemble de la grille, le silence s’applique à tous les sites et à tous les nœuds. Si vous sélectionnez un site, le silence s’applique uniquement aux nœuds de ce site. **Note:** vous ne pouvez pas sélectionner plus d’un nœud ou plus d’un site pour chaque silence. Vous devez créer des silences supplémentaires si vous souhaitez supprimer la même règle d’alerte sur plusieurs nœuds ou plusieurs sites à la fois.

4. Sélectionnez **Enregistrer**.
5. Si vous souhaitez modifier ou mettre fin à un silence avant son expiration, vous pouvez le modifier ou le supprimer.

Option	Description
Modifier un silence	a. Sélectionnez **ALERTES** > **silences**. b. Dans le tableau, sélectionnez le bouton radio correspondant au silence que vous souhaitez modifier. c. Sélectionnez **Modifier**. d. Modifiez la description, le temps restant, les niveaux de gravité sélectionnés ou le nœud affecté. e. Sélectionnez **Enregistrer**.
Supprimer un silence	a. Sélectionnez **ALERTES** > **silences**. b. Dans le tableau, sélectionnez le bouton radio correspondant au silence que vous souhaitez supprimer. c. Sélectionnez **Supprimer**. d. Sélectionnez **OK** pour confirmer que vous souhaitez supprimer ce silence. **Remarque** : les notifications sont maintenant envoyées lorsque cette alerte est déclenchée (sauf si elle est supprimée par un autre silence). Si cette alerte est déclenchée, l'envoi de notifications par e-mail ou SNMP peut prendre quelques minutes et la mise à jour de la page alertes.

Informations associées

- "Configurez l'agent SNMP"

Référence des alertes

Cette référence répertorie les alertes par défaut qui apparaissent dans le Gestionnaire de grille. Les actions recommandées sont dans le message d'alerte que vous recevez.

Si nécessaire, vous pouvez créer des règles d'alerte personnalisées en fonction de votre approche de gestion du système.

Certaines des alertes par défaut utilisent "Metrics Prometheus".

Alertes de l'appliance

Nom de l'alerte	Description
Batterie de l'appareil expirée	La batterie du contrôleur de stockage de l'appareil a expiré.
La batterie de l'appareil est défectueuse	La batterie du contrôleur de stockage de l'appareil est défectueuse.
La capacité de la batterie de l'appareil est insuffisante	La capacité de la batterie du contrôleur de stockage de l'appareil est insuffisante.

Nom de l’alerte	Description
La batterie de l’appareil est presque déchargée	La batterie du contrôleur de stockage de l’appliance arrive à expiration.
Batterie de l’appareil retirée	La batterie du contrôleur de stockage de l’appareil est manquante.
Batterie de l’appareil trop chaude	La batterie du contrôleur de stockage de l’appareil est en surchauffe.
Erreur de communication du BMC de l’appliance	La communication avec le contrôleur de gestion de la carte mère (BMC) a été perdue.
Échec du périphérique de sauvegarde du cache de l’appliance	Échec d’un périphérique de sauvegarde de cache persistant.
Capacité insuffisante du périphérique de sauvegarde en cache de l’appliance	La capacité du périphérique de sauvegarde du cache est insuffisante.
Dispositif de sauvegarde cache de l’appliance protégé en écriture	Un périphérique de sauvegarde de cache est protégé en écriture.
La taille de la mémoire cache de l’appliance ne correspond pas	Le cache des deux contrôleurs de l’appliance est de différentes tailles.
La température du châssis du contrôleur de calcul de l’appliance est trop élevée	La température du contrôleur de calcul d’une appliance StorageGRID a dépassé le seuil nominal.
Température trop élevée du processeur du contrôleur de calcul de l’appliance	La température du processeur dans le contrôleur de calcul d’une appliance StorageGRID a dépassé le seuil nominal.
Le contrôleur de calcul de l’appliance doit faire attention	Une défaillance matérielle a été détectée dans le contrôleur de calcul d’une appliance StorageGRID.
L’alimentation A du contrôleur de calcul de l’appliance présente un problème	L’alimentation A du contrôleur de calcul présente un problème.
L’alimentation B du contrôleur de calcul de l’appliance présente un problème	L’alimentation B du contrôleur de calcul présente un problème.
Service de surveillance du matériel de calcul de l’appliance bloqué	Le service qui surveille l’état du matériel de stockage est bloqué.

Nom de l’alerte	Description
Panne du lecteur DAS de l’appliance détectée	Un problème a été détecté au niveau d’un disque DAS (Direct-Attached Storage) dans l’appliance.
Reconstruction des disques DAS du dispositif	Un disque DAS (Direct-Attached Storage) est en cours de reconstruction. Ceci est attendu s’il a été récemment remplacé ou supprimé/réinséré.
Panne du ventilateur de l’appareil détectée	Un problème de ventilateur dans l’appareil a été détecté.
Panne Fibre Channel de l’appliance détectée	Un problème de liaison Fibre Channel a été détecté entre le contrôleur de stockage de l’appliance et le contrôleur de calcul
Défaillance du port HBA Fibre Channel de l’appliance	Un port HBA Fibre Channel est défectueux ou est défectueux.
Flash cache de l’appliance ne sont pas optimaux	Les disques utilisés pour la mise en cache SSD ne sont pas optimaux.
Interconnexion de l’appareil/boîtier de la batterie retiré	Le boîtier d’interconnexion/de batterie est manquant.
Port d’appliance LACP manquant	Aucun port d’une appliance StorageGRID ne participe au lien LACP.
Défaillance de la carte réseau de l’appareil détectée	Un problème de carte d’interface réseau (NIC) a été détecté sur le serveur.
L’alimentation générale de l’appareil est dégradée	La puissance d’un dispositif StorageGRID s’est déviée de la tension de fonctionnement recommandée.
Avertissement critique sur les disques SSD de l’appliance	Un SSD d’appliance signale un avertissement critique.
Défaillance Du contrôleur de stockage De l’appliance	Le contrôleur de stockage A d’une appliance StorageGRID est en panne.
Défaillance du contrôleur B de stockage de l’appliance	Le contrôleur de stockage B d’une appliance StorageGRID est en panne.
Panne de disque du contrôleur de stockage de l’appliance	Un ou plusieurs disques d’une appliance StorageGRID sont défectueux ou non optimaux.
Problème matériel du contrôleur de stockage de l’appliance	Le logiciel SANtricity signale les besoins d’attention d’un composant d’une appliance StorageGRID.

Nom de l’alerte	Description
Panne de l’alimentation Du contrôleur de stockage de l’appliance	L’alimentation A d’un dispositif StorageGRID s’est déviée de la tension de fonctionnement recommandée.
Panne de l’alimentation B du contrôleur de stockage de l’appliance	L’alimentation B d’un dispositif StorageGRID s’est déviée de la tension de fonctionnement recommandée.
Entretien du moniteur matériel de stockage de l’appliance bloqué	Le service qui surveille l’état du matériel de stockage est bloqué.
Dégradation des tiroirs de stockage de l’appliance	L’état de l’un des composants du tiroir de stockage d’une appliance de stockage est dégradé.
Température de l’appareil dépassée	La température nominale ou maximale du contrôleur de stockage de l’appareil a été dépassée.
Capteur de température de l’appareil retiré	Un capteur de température a été déposé.
Les E/S du disque sont très lentes	Les E/S de disque très lentes peuvent affecter les performances du grid.
Panne du ventilateur du dispositif de stockage détectée	Un problème de ventilateur dans le contrôleur de stockage d’un dispositif a été détecté.
Dégradation de la connectivité du stockage de l’appliance de stockage	Un problème se produit au niveau d’une ou plusieurs connexions entre le contrôleur de calcul et le contrôleur de stockage.
Périphérique de stockage inaccessible	Impossible d’accéder à un périphérique de stockage.

Alertes d’audit et syslog

Nom de l’alerte	Description
Des journaux d’audit sont ajoutés à la file d’attente en mémoire	Le nœud ne peut pas envoyer de journaux au serveur syslog local et la file d’attente en mémoire est saturée.
Erreur de transfert du serveur syslog externe	Le nœud ne peut pas transférer les journaux au serveur syslog externe.
Grande file d’attente d’audit	La file d’attente des messages d’audit est pleine. Si cette condition n’est pas résolue, les opérations S3 ou Swift risquent d’échouer.

Nom de l’alerte	Description
Des journaux sont ajoutés à la file d’attente sur disque	Le nœud ne peut pas transférer les journaux vers le serveur syslog externe et la file d’attente sur disque est saturée.

Alertes de compartiment

Nom de l’alerte	Description
Le paramètre de cohérence du compartiment FabricPool n’est pas pris en charge	Un compartiment FabricPool utilise le niveau de cohérence disponible, qui n’est pas pris en charge.

Alertes Cassandra

Nom de l’alerte	Description
Erreur du compacteur automatique Cassandra	Le compacteur automatique Cassandra a rencontré une erreur.
Indicateurs du compacteur automatique Cassandra obsolètes	Les mesures qui décrivent le compacteur automatique Cassandra sont obsolètes.
Erreur de communication Cassandra	Les nœuds qui exécutent le service Cassandra rencontrent des problèmes.
Compression Cassandra surchargée	Le processus de compactage Cassandra est surchargé.
Erreur d’écriture surdimensionnée Cassandra	Un processus StorageGRID interne a envoyé à Cassandra une demande d’écriture trop volumineuse.
Les metrics de réparation de Cassandra sont obsolètes	Les mesures qui décrivent les tâches de réparation de Cassandra sont obsolètes.
La progression de la réparation de Cassandra est lente	La progression des réparations des bases de données Cassandra est lente.
Le service de réparation Cassandra n’est pas disponible	Le service de réparation Cassandra n’est pas disponible.
La corruption des tables Cassandra	Cassandra a détecté une corruption de table. Cassandra redémarre automatiquement si elle détecte une corruption de la table.
Disponibilité de lecture améliorée désactivée	Lorsque l’amélioration de la disponibilité en lecture est désactivée, les requêtes GET et HEAD peuvent échouer lorsque les nœuds de stockage ne sont pas disponibles.

Alertes de pool de stockage cloud

Nom de l'alerte	Description
Erreur de connectivité de Cloud Storage Pool	Le contrôle de l'état des pools de stockage cloud a détecté une ou plusieurs nouvelles erreurs.

Alertes de réplication intergrid

Nom de l'alerte	Description
Défaillance permanente de la réplication entre les grilles	Une erreur de réplication inter-grille s'est produite et nécessite une intervention de l'utilisateur pour la résoudre.
Ressources de réplication intergrid indisponibles	Les demandes de réplication multigrille sont en attente car une ressource n'est pas disponible.

Alertes DHCP

Nom de l'alerte	Description
Bail DHCP expiré	Le bail DHCP sur une interface réseau a expiré.
La location DHCP expire bientôt	Le bail DHCP sur une interface réseau expire bientôt.
Serveur DHCP indisponible	Le serveur DHCP n'est pas disponible.

Alertes de débogage et de suivi

Nom de l'alerte	Description
Impact sur les performances de débogage	Lorsque le mode débogage est activé, les performances du système peuvent être affectées négativement.
Configuration de trace activée	Lorsque la configuration de trace est activée, les performances du système peuvent être affectées de façon négative.

Alertes par e-mail et AutoSupport

Nom de l'alerte	Description
Échec de l'envoi du message AutoSupport	L'envoi du message AutoSupport le plus récent a échoué.
Échec de la notification par e-mail	Impossible d'envoyer la notification par e-mail pour une alerte.

Alertes de code d'effacement (EC)

Nom de l'alerte	Description
Défaillance du rééquilibrage EC	La procédure de rééquilibrage EC a échoué ou a été arrêtée.
Échec de réparation EC	Une tâche de réparation pour les données EC a échoué ou a été arrêtée.
Réparation EC bloquée	Un travail de réparation pour les données EC est bloqué.

Expiration des alertes de certificats

Nom de l'alerte	Description
Expiration du certificat client	Un ou plusieurs certificats client sont sur le point d'expirer.
Expiration du certificat de serveur global pour S3 et Swift	Le certificat de serveur global pour S3 et Swift est sur le point d'expirer.
Expiration du certificat de point final de l'équilibreur de charge	Un ou plusieurs certificats de noeud final de l'équilibreur de charge vont expirer.
Expiration du certificat de serveur pour l'interface de gestion	Le certificat de serveur utilisé pour l'interface de gestion est sur le point d'expirer.
Expiration du certificat d'autorité de certification syslog externe	Le certificat d'autorité de certification (CA) utilisé pour signer le certificat de serveur syslog externe est sur le point d'expirer.
Expiration du certificat du client syslog externe	Le certificat client d'un serveur syslog externe est sur le point d'expirer.
Expiration du certificat du serveur syslog externe	Le certificat de serveur présenté par le serveur syslog externe arrive à expiration.

Alertes réseau Grid

Nom de l'alerte	Description
Non-concordance de MTU du réseau de grid	Le paramètre MTU de l'interface réseau Grid (eth0) diffère de manière significative sur tous les nœuds de la grille.

Alertes de fédération du grid

Nom de l'alerte	Description
Expiration du certificat de fédération GRID	Un ou plusieurs certificats de fédération de grille sont sur le point d'expirer.

Nom de l’alerte	Description
Échec de la connexion de fédération de grille	La connexion de fédération de grille entre la grille locale et la grille distante ne fonctionne pas.

Alertes d’utilisation élevée ou de latence élevée

Nom de l’alerte	Description
Utilisation du segment de mémoire Java élevée	Un pourcentage élevé d’espace de tas Java est utilisé.
Latence élevée pour les requêtes de métadonnées	La durée moyenne des requêtes de métadonnées Cassandra est trop longue.

Alertes de fédération des identités

Nom de l’alerte	Description
Échec de synchronisation de la fédération d’identités	Impossible de synchroniser des groupes fédérés et des utilisateurs à partir du référentiel d’identité.
Échec de la synchronisation de la fédération des identités pour un locataire	Impossible de synchroniser les groupes fédérés et les utilisateurs à partir du référentiel d’identité configuré par un locataire.

Alertes de gestion du cycle de vie des informations (ILM)

Nom de l’alerte	Description
Placement ILM impossible à atteindre	Aucune instruction de placement dans une règle ILM ne peut être obtenue pour certains objets.
Analyse ILM trop longue	Le temps nécessaire à l’analyse, à l’évaluation et à l’application des règles ILM aux objets est trop long.
Taux d’analyse ILM faible	La vitesse d’analyse ILM est définie sur moins de 100 objets/seconde.

Alertes du serveur de gestion des clés (KMS

Nom de l’alerte	Description
Expiration du certificat CA KMS	Le certificat de l’autorité de certification (CA) utilisé pour signer le certificat du serveur de gestion des clés (KMS) est sur le point d’expirer.
Expiration du certificat client KMS	Le certificat client d’un serveur de gestion des clés est sur le point d’expirer

Nom de l’alerte	Description
Echec du chargement de la configuration DES KMS	La configuration du serveur de gestion des clés existe mais n’a pas pu être chargée.
Erreur de connectivité KMS	Un nœud d’appliance n’a pas pu se connecter au serveur de gestion des clés de son site.
Nom de la clé de cryptage KMS introuvable	Le serveur de gestion des clés configuré ne dispose pas d’une clé de chiffrement correspondant au nom fourni.
Echec de la rotation de la clé de chiffrement KMS	Tous les volumes de l’appliance ont été décryptés avec succès, mais un ou plusieurs volumes n’ont pas pu tourner vers la clé la plus récente.
LES KMS ne sont pas configurés	Aucun serveur de gestion des clés n’existe pour ce site.
La clé KMS n’a pas réussi à décrypter un volume d’appliance	Impossible de décrypter un ou plusieurs volumes sur une appliance dont le chiffrement de nœud est activé avec la clé KMS actuelle.
Expiration du certificat du serveur KMS	Le certificat de serveur utilisé par le serveur de gestion des clés (KMS) est sur le point d’expirer.

Alertes de décalage d’horloge locale

Nom de l’alerte	Description
Décalage horaire grand horloge locale	Le décalage entre l’horloge locale et l’heure NTP (Network Time Protocol) est trop important.

Alertes de mémoire insuffisante ou d’espace insuffisant

Nom de l’alerte	Description
Capacité du disque du journal d’audit faible	L’espace disponible pour les journaux d’audit est faible. Si cette condition n’est pas résolue, les opérations S3 ou Swift risquent d’échouer.
Mémoire de nœud faible disponibilité	La quantité de RAM disponible sur un nœud est faible.
Faible espace libre pour le pool de stockage	L’espace disponible pour le stockage des données d’objet dans le nœud de stockage est faible.
Mémoire insuffisante sur les nœuds installés	La quantité de mémoire installée sur un nœud est faible.
Faibles capacités de stockage de métadonnées	L’espace disponible pour le stockage des métadonnées d’objet est faible.

Nom de l'alerte	Description
Capacité disque de metrics faible	L'espace disponible pour la base de données de metrics est faible.
Faible stockage des données objet	L'espace disponible pour le stockage des données d'objet est faible.
Remplacement du filigrane en lecture seule faible	Le remplacement du filigrane en lecture seule progressif du volume de stockage est inférieur au seuil minimal optimisé pour un nœud de stockage.
Capacité du disque racine faible	L'espace disponible sur le disque racine est faible.
Faible capacité des données système	L'espace disponible pour les données système StorageGRID sur le point de montage /var/local est faible.
Petit répertoire tmp espace libre	L'espace disponible dans le répertoire /tmp est faible.

Alertes de réseau de nœuds ou de nœuds

Nom de l'alerte	Description
Échec de la configuration du pare-feu	Impossible d'appliquer la configuration du pare-feu.
Erreur de connectivité réseau du nœud	Des erreurs se sont produites lors du transfert des données entre les nœuds.
Erreur de trame de réception du réseau du nœud	Un pourcentage élevé des trames réseau reçues par un nœud a rencontré des erreurs.
Nœud non synchronisé avec le serveur NTP	Le nœud n'est pas synchronisé avec le serveur NTP (Network Time Protocol).
Nœud non verrouillé avec le serveur NTP	Le nœud n'est pas verrouillé sur un serveur NTP (Network Time Protocol).
Réseau de nœuds non appliances arrêté	Un ou plusieurs périphériques réseau sont en panne ou déconnectés.
Liaison de l'appliance de services vers le réseau d'administration	L'interface de l'appliance vers le réseau d'administration (eth1) est en panne ou déconnectée.
Interruption de la liaison de l'appliance de services sur le port réseau d'administration 1	Le port réseau Admin 1 de l'appliance est arrêté ou déconnecté.

Nom de l’alerte	Description
Liaison de l’appliance de services vers le réseau client	L’interface de l’appliance vers le réseau client (eth2) est en panne ou déconnectée.
Liaison de l’appliance de services vers le bas sur le port réseau 1	Le port réseau 1 de l’appliance est en panne ou déconnecté.
La liaison de l’appliance de services est inactive sur le port réseau 2	Le port réseau 2 de l’appliance est en panne ou déconnecté.
La liaison de l’appliance de services est inactive sur le port réseau 3	Le port réseau 3 de l’appliance est en panne ou déconnecté.
La liaison de l’appliance de services est inactive sur le port réseau 4	Le port réseau 4 de l’appliance est en panne ou déconnecté.
Liaison de l’appliance de stockage indisponible sur le réseau d’administration	L’interface de l’appliance vers le réseau d’administration (eth1) est en panne ou déconnectée.
Liaison du dispositif de stockage inactive sur le port réseau d’administration 1	Le port réseau Admin 1 de l’appliance est arrêté ou déconnecté.
La liaison de l’appliance de stockage sur le réseau client est inactive	L’interface de l’appliance vers le réseau client (eth2) est en panne ou déconnectée.
La liaison de l’appliance de stockage est inactive sur le port réseau 1	Le port réseau 1 de l’appliance est en panne ou déconnecté.
La liaison de l’appliance de stockage est inactive sur le port réseau 2	Le port réseau 2 de l’appliance est en panne ou déconnecté.
La liaison du dispositif de stockage est inactive sur le port réseau 3	Le port réseau 3 de l’appliance est en panne ou déconnecté.
La liaison du dispositif de stockage est inactive sur le port réseau 4	Le port réseau 4 de l’appliance est en panne ou déconnecté.
Le nœud de stockage n’est pas dans l’état de stockage souhaité	Le service LDR d’un nœud de stockage ne peut pas passer à l’état souhaité en raison d’une erreur interne ou d’un problème lié au volume

Nom de l’alerte	Description
Impossible de communiquer avec le nœud	Un ou plusieurs services ne répondent pas ou le nœud ne peut pas être atteint.
Redémarrage de nœud inattendu	Un nœud a été redémarré de manière inattendue au cours des 24 dernières heures.

Alertes sur les objets

Nom de l’alerte	Description
Échec de la vérification de l’existence de l’objet	Le travail de vérification de l’existence de l’objet a échoué.
La vérification de l’existence d’objet est bloquée	Le travail de vérification de l’existence de l’objet est bloqué.
Objets perdus	Un ou plusieurs objets ont été perdus de la grille.
S3 PLACEZ la taille de l’objet trop grande	Un client tente une opération PUT Object qui dépasse les limites de taille S3.
Objet corrompu non identifié détecté	Un fichier a été trouvé dans le stockage objet répliqué qui n’a pas pu être identifié en tant qu’objet répliqué.

Alertes de services de plateforme

Nom de l’alerte	Description
Services de plateforme non disponibles	Trop peu de nœuds de stockage avec le service RSM sont en cours d’exécution ou disponibles sur un site.

Alertes de volume de stockage

Nom de l’alerte	Description
Le volume de stockage nécessite votre attention	Un volume de stockage est hors ligne et nécessite votre attention.
Le volume de stockage doit être restauré	Un volume de stockage a été restauré et doit être restauré.
Volume de stockage hors ligne	Un volume de stockage est hors ligne depuis plus de 5 minutes, probablement parce que le nœud a redémarré pendant l’étape de formatage du volume.

Nom de l'alerte	Description
La restauration de volume n'a pas pu démarrer la réparation des données répliquées	La réparation des données répliquées pour un volume réparé n'a pas pu être démarrée automatiquement.

Alertes des services StorageGRID

Nom de l'alerte	Description
service nginx utilisant la configuration de sauvegarde	La configuration du service nginx n'est pas valide. La configuration précédente est maintenant utilisée.
le service nginx-gw utilise la configuration de sauvegarde	La configuration du service nginx-gw n'est pas valide. La configuration précédente est maintenant utilisée.
Service SSH utilisant la configuration de sauvegarde	La configuration du service SSH n'est pas valide. La configuration précédente est maintenant utilisée.

Alertes aux locataires

Nom de l'alerte	Description
Utilisation élevée du quota par les locataires	Un pourcentage élevé de l'espace de quota est utilisé. Cette règle est désactivée par défaut car elle peut entraîner un trop grand nombre de notifications.

Metrics Prometheus couramment utilisés

Consultez cette liste de metrics Prometheus les plus utilisés pour mieux comprendre les conditions des règles d'alerte par défaut ou pour construire les conditions des règles d'alerte personnalisées.

Vous pouvez également obtenez une liste complète de toutes les mesures.

Pour plus de détails sur la syntaxe des requêtes Prometheus, voir "Interrogation de Prometheus".

Quels sont les metrics Prometheus ?

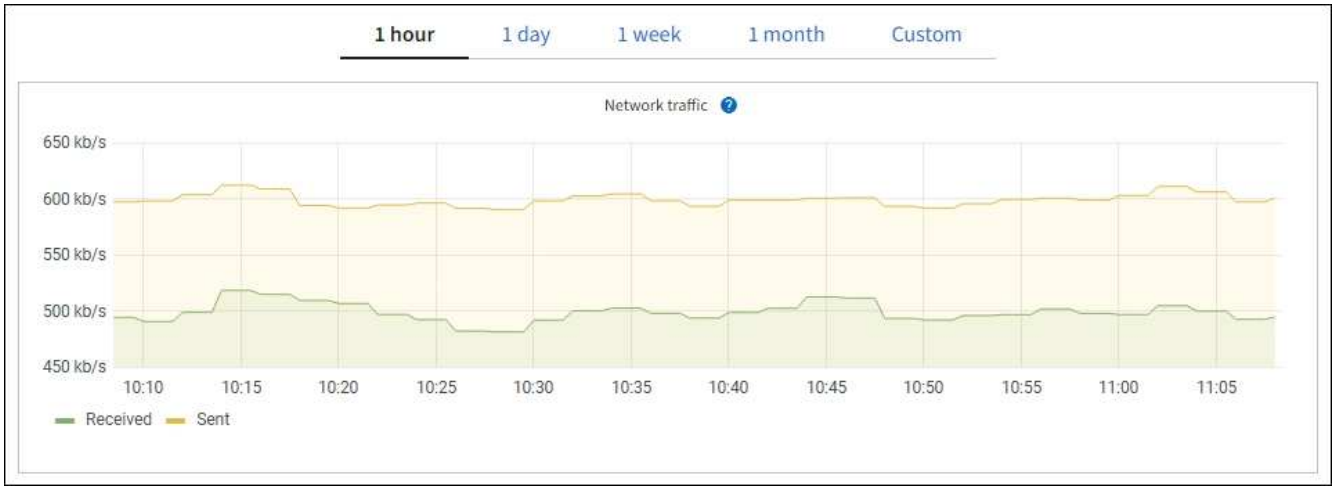
Les metrics Prometheus sont des mesures de séries chronologiques. Le service Prometheus sur les nœuds d'administration collecte ces metrics à partir des services sur tous les nœuds. Des metrics sont stockés sur chaque nœud d'administration jusqu'à ce que l'espace réservé aux données Prometheus soit plein. Lorsque le `/var/local/mysql_ibdata/` le volume atteint la capacité maximale, les mesures les plus anciennes sont supprimées en premier.

Où sont utilisés les metrics Prometheus ?

Les metrics collectées par Prometheus sont utilisés à plusieurs endroits dans Grid Manager :

- **Page noeuds** : les graphiques et graphiques des onglets disponibles sur la page noeuds utilisent l'outil de

visualisation Grafana pour afficher les metrics de séries chronologiques recueillies par Prometheus. Grafana affiche les données de séries chronologiques aux formats graphique et graphique, tandis que Prometheus sert de source de données back-end.



- **Alertes** : les alertes sont déclenchées à des niveaux de gravité spécifiques lorsque les conditions de règle d'alerte qui utilisent des metrics Prometheus sont définies comme vraies.
- **Grid Management API** : vous pouvez utiliser des metrics Prometheus dans des règles d'alerte personnalisées ou avec des outils d'automatisation externes pour surveiller votre système StorageGRID. La liste complète des metrics de Prometheus est disponible via l'API Grid Management. (En haut de Grid Manager, sélectionnez l'icône d'aide et sélectionnez **documentation API** > **metrics**.) Bien que plus d'un millier de mesures soient disponibles, seul un nombre relativement faible est requis pour surveiller les opérations StorageGRID les plus critiques.

> Les indicateurs qui incluent *private* dans leurs noms sont destinés à un usage interne uniquement et peuvent être modifiés sans préavis entre les versions de StorageGRID.

- La page **SUPPORT** > **Tools** > **Diagnostics** et la page **SUPPORT** > **Tools** > **Metrics** : ces pages, qui sont principalement destinées au support technique, fournissent plusieurs outils et graphiques qui utilisent les valeurs des mesures Prometheus.

> Certaines fonctions et options de menu de la page métriques sont intentionnellement non fonctionnelles et peuvent faire l'objet de modifications.

Liste des mesures les plus courantes

La liste suivante répertorie les metrics Prometheus les plus utilisés.

> Les indicateurs incluant *private* dans leur nom sont destinés à un usage interne uniquement et sont susceptibles d'être modifiés sans préavis entre les versions de StorageGRID.

alertmanager_notifications_failed_total

Nombre total de notifications d'alerte ayant échoué.

node_filesystem_dispo_octets

Espace système de fichiers disponible pour les utilisateurs non root en octets.

Node_Memory_MemAvailable_Bytes

Champ informations mémoire MemAvailable_Bytes.

node_network_carrier

Valeur porteuse de `/sys/class/net/iface`.

node_network_recy_errs_total

Statistiques du périphérique réseau `receive_errs`.

node_network_transmit_errs_total

Statistiques du périphérique réseau `transmit_errs`.

storagegrid_panne_administrative

Le nœud n'est pas connecté à la grille pour une raison attendue. Par exemple, le nœud ou les services du nœud ont été normalement arrêtés, le nœud est en cours de redémarrage ou le logiciel est mis à niveau.

storagegrid_appliance_compute_controller_status

L'état du matériel du contrôleur de calcul d'une appliance.

disques_défaillants_appliance_storagegrid

Pour le contrôleur de stockage d'une appliance, le nombre de disques qui ne sont pas optimaux.

état_matériel_contrôleur_stockage_appliance_storagegrid

État global du matériel du contrôleur de stockage d'une appliance.

conteneurs_contenu_seaux_et_conteneurs_storagegrid

Le nombre total de compartiments S3 et de conteneurs Swift connus par ce nœud de stockage.

objets_contenu_storagegrid

Le nombre total d'objets de données S3 et Swift connus de ce nœud de stockage. Nombre n'est valide que pour les objets de données créés par les applications client qui communiquent avec le système via S3 ou Swift.

objet_contenu_storagegrid_perdu

Le nombre total d'objets détectés par ce service est manquant dans le système StorageGRID. Des mesures doivent être prises pour déterminer la cause de la perte et si la récupération est possible.

"Dépanner les données d'objet perdues ou manquantes"

storagegrid_http_sessions_entrant_tenté

Nombre total de sessions HTTP ayant été tentées vers un noeud de stockage.

storagegrid_http_sessions_entrant_actuellement_établi

Nombre de sessions HTTP actuellement actives (ouvertes) sur le nœud de stockage.

storagegrid_http_sessions_incoming_failed

Nombre total de sessions HTTP qui n'ont pas réussi à se terminer correctement, soit en raison d'une requête HTTP mal formée, soit en cas d'échec du traitement d'une opération.

storagegrid_http_sessions_entrant_réussi

Nombre total de sessions HTTP terminées avec succès.

objets_ilm_en_attente_arrière-plan

Le nombre total d'objets sur ce nœud en attente d'évaluation ILM à partir de l'analyse.

storagegrid_ilm_en_attente_client_évaluation_objets_par_seconde

Vitesse actuelle d'évaluation des objets par rapport à la règle ILM de ce nœud.

objet_client_attente_ilm_en_attente

Le nombre total d'objets de ce nœud attend l'évaluation ILM des opérations client (par exemple, ingestion).

objets_ilm_en_attente_total_storagegrid

Le nombre total d'objets en attente d'évaluation ILM.

ilm_scan_objets_par_seconde

Vitesse à laquelle les objets appartenant à ce nœud sont analysés et mis en file d'attente d'ILM.

storagegrid_ilm_scan_perce_estimé_minutes

Durée estimée d'une analyse ILM complète sur ce nœud.

Remarque : Une analyse complète ne garantit pas que ILM a été appliquée à tous les objets appartenant à ce nœud.

storagegrid_load_balancer_cert_exexpiration_time

Le temps d'expiration du certificat de noeud final de l'équilibreur de charge en secondes depuis l'époque.

storagegrid_metadata_requêtes_moyenne_latence_millisecondes

Temps moyen requis pour exécuter une requête sur le magasin de métadonnées via ce service.

storagegrid_réseau_reçu_octets

Quantité totale de données reçues depuis l'installation.

octets_réseau_transmis_storagegrid

Quantité totale de données envoyées depuis l'installation.

pourcentage_utilisation_cpu_storagegrid_nœud_nœud

Pourcentage de temps CPU disponible actuellement utilisé par ce service. Indique le niveau d'occupation du service. Le temps CPU disponible dépend du nombre de CPU du serveur.

storagegrid_ntp_choisi_source_temps_offset_millisecondes

Décalage systématique du temps fourni par une source de temps choisie. Le décalage est introduit lorsque le délai d'accès à une source de temps n'est pas égal au temps requis pour que la source de temps atteigne le client NTP.

storagegrid_ntp_verrouillé

Le nœud n'est pas verrouillé sur un serveur NTP (Network Time Protocol).

storagegrid_s3_data_transferts_octets_ingérés

Quantité totale de données ingérées à partir des clients S3 pour ce nœud de stockage, depuis la dernière réinitialisation de l'attribut.

storagegrid_s3_data_transferts_octets_récupéré

Quantité totale de données récupérées par les clients S3 à partir de ce noeud de stockage depuis la dernière réinitialisation de l'attribut.

storagegrid_s3_operations_failed

Le nombre total d'opérations S3 ayant échoué (codes d'état HTTP 4xx et 5xx), à l'exclusion des opérations causées par l'échec d'autorisation S3.

opérations_storagegrid_s3_couronnées_succès

Nombre total d'opérations S3 réussies (code d'état HTTP 2xx).

opérations_storagegrid_s3_non autorisées

Nombre total d'opérations S3 ayant échoué à la suite d'une échec d'autorisation.

storagegrid_servercertificate_management_interface_cert_expiration_days

Nombre de jours avant l'expiration du certificat de l'interface de gestion.

storagegrid_servercertificate_storage_api_endpoints_cert_expiration_days

Nombre de jours avant l'expiration du certificat de l'API de stockage objet.

storagegrid_service_cpu_secondes

Durée cumulée pendant laquelle le CPU a été utilisé par ce service depuis l'installation.

octets_usage_mémoire_service_storagegrid

La quantité de mémoire (RAM) actuellement utilisée par ce service. Cette valeur est identique à celle affichée par l'utilitaire Linux TOP sous RES.

octets_réseau_service_storagegrid_reçus_netapp

Quantité totale de données reçues par ce service depuis l'installation.

octets_réseau_service_storagegrid_transmis_netapp

Quantité totale de données envoyées par ce service.

redémarrages_service_storagegrid

Nombre total de fois où le service a été redémarré.

storagegrid_service_runtime_seconds

Durée totale d'exécution du service depuis l'installation.

temps_disponibilité_service_storagegrid_secondes

Durée totale d'exécution du service depuis son dernier redémarrage.

storage_state_current_storagegrid

État actuel des services de stockage. Les valeurs d'attribut sont :

- 10 = hors ligne
- 15 = entretien
- 20 = lecture seule
- 30 = en ligne

état_stockage_storage_storagegrid

État actuel des services de stockage. Les valeurs d'attribut sont :

- 0 = aucune erreur

- 10 = en transition
- 20 = espace libre insuffisant
- 30 = Volume(s) indisponible
- 40 = erreur

storagegrid_utilisation_données_octets

Estimation de la taille totale des données d'objet répliquées et codées d'effacement sur le nœud de stockage.

storage_utilisation_métadonnées_autorisés_storagegrid_octets

Espace total sur le volume 0 de chaque nœud de stockage autorisé pour les métadonnées d'objet. Cette valeur est toujours inférieure à l'espace réel réservé aux métadonnées sur un nœud, car une partie de l'espace réservé est requise pour les opérations essentielles de base de données (telles que la compaction et la réparation) et les futures mises à niveau matérielles et logicielles.l'espace autorisé pour les métadonnées de l'objet contrôle la capacité globale des objets.

octets_métadonnées_utilisation_stockage_storagegrid

Volume des métadonnées d'objet sur le volume de stockage 0, en octets.

storage_usage_total_octets_espace_stockage_storagegrid

Quantité totale d'espace de stockage alloué à tous les magasins d'objets.

octets_stockage_utilisation_de_stockage_utilisables_storagegrid

Quantité totale d'espace de stockage objet restant. Calculé en ajoutant ensemble la quantité d'espace disponible pour tous les magasins d'objets du nœud de stockage.

storagegrid_swift_data_transfère_octets_ingérés

Quantité totale de données ingérées à partir des clients Swift vers ce nœud de stockage depuis la dernière réinitialisation de l'attribut.

storagegrid_swift_data_transferts_octets_récupéré

Quantité totale de données récupérées par les clients Swift à partir de ce noeud de stockage depuis la dernière réinitialisation de l'attribut.

storagegrid_swift_operations_failed

Nombre total d'opérations Swift ayant échoué (codes d'état HTTP 4xx et 5xx), à l'exclusion des opérations causées par l'échec de l'autorisation Swift.

storagegrid_swift_operations_successful

Nombre total d'opérations Swift réussies (code d'état HTTP 2xx).

storagegrid_swift_operations_non autorisé

Nombre total d'opérations Swift ayant échoué à la suite d'une erreur d'autorisation (codes d'état HTTP 401, 403, 405).

octets_données_utilisation_storagegrid_tenant

Taille logique de tous les objets pour le locataire.

nombre_d'objets_usage_storagegrid_tenant_storagegrid

Le nombre d'objets pour le locataire.

octets_quota_utilisation_storagegrid_tenant_octets

Quantité maximale d'espace logique disponible pour les objets du locataire. Si aucune mesure de quota n'est fournie, une quantité illimitée d'espace est disponible.

Obtenez une liste de toutes les mesures

pour obtenir la liste complète des mesures, utilisez l'API de gestion de grille.

1. En haut du Gestionnaire de grille, sélectionnez l'icône d'aide et sélectionnez **documentation API**.
2. Localisez les opérations **métriques**.
3. Exécutez le `GET /grid/metric-names` fonctionnement.
4. Téléchargez les résultats.

Gestion des alarmes (système hérité)

Gestion des alarmes (système hérité)

Le système d'alarme StorageGRID est l'ancien système utilisé pour identifier les points de défaillance qui se produisent parfois pendant le fonctionnement normal.

> Bien que le système d'alarme existant continue d'être pris en charge, le système d'alerte offre des avantages significatifs et est plus facile à utiliser.

Classes d'alarme (système hérité)

Une alarme héritée peut appartenir à l'une des deux classes d'alarme mutuellement exclusives.

- Les alarmes par défaut sont fournies avec chaque système StorageGRID et ne peuvent pas être modifiées. Vous pouvez cependant désactiver les alarmes par défaut ou les remplacer en définissant les alarmes personnalisées globales.
- Les alarmes personnalisées globales contrôlent l'état de tous les services d'un type donné dans le système StorageGRID. Vous pouvez créer une alarme personnalisée globale pour remplacer une alarme par défaut. Vous pouvez également créer une nouvelle alarme personnalisée globale. Cela peut être utile pour la surveillance de toutes les conditions personnalisées de votre système StorageGRID.

Logique de déclenchement d'alarme (système hérité)

Une alarme héritée est déclenchée lorsqu'un attribut StorageGRID atteint une valeur de seuil qui évalue à TRUE par rapport à une combinaison de classe d'alarme (personnalisée par défaut ou personnalisé global) et de niveau de gravité d'alarme.

Icône	Couleur	Gravité de l'alarme	Signification
	Jaune	Avertissement	Le nœud est connecté à la grille, mais il existe une condition inhabituelle qui n'affecte pas les opérations normales.

Icône	Couleur	Gravité de l'alarme	Signification
	Orange clair	Mineur	Le nœud est connecté à la grille, mais il existe une condition anormale qui pourrait affecter son fonctionnement à l'avenir. Vous devez étudier pour éviter la remontée des problèmes.
	Orange foncé	Majeur	Le nœud est connecté à la grille, mais il existe une condition anormale qui affecte actuellement le fonctionnement. Cela nécessite une attention particulière afin d'éviter la remontée des problèmes.
	Rouge	Primordial	Le nœud est connecté à la grille, mais il existe une condition anormale qui a arrêté des opérations normales. Vous devez résoudre le problème immédiatement.

La gravité de l'alarme et la valeur de seuil correspondante peuvent être définies pour chaque attribut numérique. Le service NMS sur chaque noeud d'administration surveille en permanence les valeurs d'attribut actuelles par rapport aux seuils configurés. Lorsqu'une alarme est déclenchée, une notification est envoyée à tout le personnel désigné.

Notez qu'un niveau de gravité Normal ne déclenche pas d'alarme.

Les valeurs d'attribut sont évaluées par rapport à la liste des alarmes activées définies pour cet attribut. La liste des alarmes est vérifiée dans l'ordre suivant pour trouver la première classe d'alarme avec une alarme définie et activée pour l'attribut :

1. Alarmes personnalisées globales avec niveaux de gravité d'alarme allant de critique à avertissement.
2. Alarmes par défaut avec niveaux de gravité d'alarme de critique à avertissement.

Une fois qu'une alarme activée pour un attribut est détectée dans la classe d'alarme supérieure, le service NMS ne s'évalue qu'au sein de cette classe. Le service NMS ne s'évalue pas par rapport aux autres catégories de priorité inférieure. En d'autres termes, si une alarme personnalisée globale est activée pour un attribut, le service NMS évalue uniquement la valeur de l'attribut par rapport aux alarmes personnalisées globales. Les alarmes par défaut ne sont pas évaluées. Ainsi, une alarme par défaut activée pour un attribut peut répondre aux critères requis pour déclencher une alarme, mais elle ne sera pas déclenchée car une alarme personnalisée globale (qui ne répond pas aux critères spécifiés) pour le même attribut est activée. Aucune alarme n'est déclenchée et aucune notification n'est envoyée.

Exemple de déclenchement d'alarme

Cet exemple permet de comprendre comment les alarmes personnalisées globales et les alarmes par défaut sont déclenchées.

Pour l'exemple suivant, un attribut possède une alarme personnalisée globale et une alarme par défaut définie et activée, comme indiqué dans le tableau suivant.

	Seuil d'alarme personnalisé global (activé)	Seuil d'alarme par défaut (activé)
Avertissement	>= 1500	>= 1000
Mineur	>= 15,000	>= 1000
Majeur	>=150,000	>= 250,000

Si l'attribut est évalué lorsque sa valeur est 1000, aucune alarme n'est déclenchée et aucune notification n'est envoyée.

L'alarme personnalisée globale est prioritaire sur l'alarme par défaut. Une valeur de 1000 n'atteint pas la valeur seuil d'un niveau de gravité quelconque pour l'alarme personnalisée globale. Par conséquent, le niveau d'alarme est évalué à Normal.

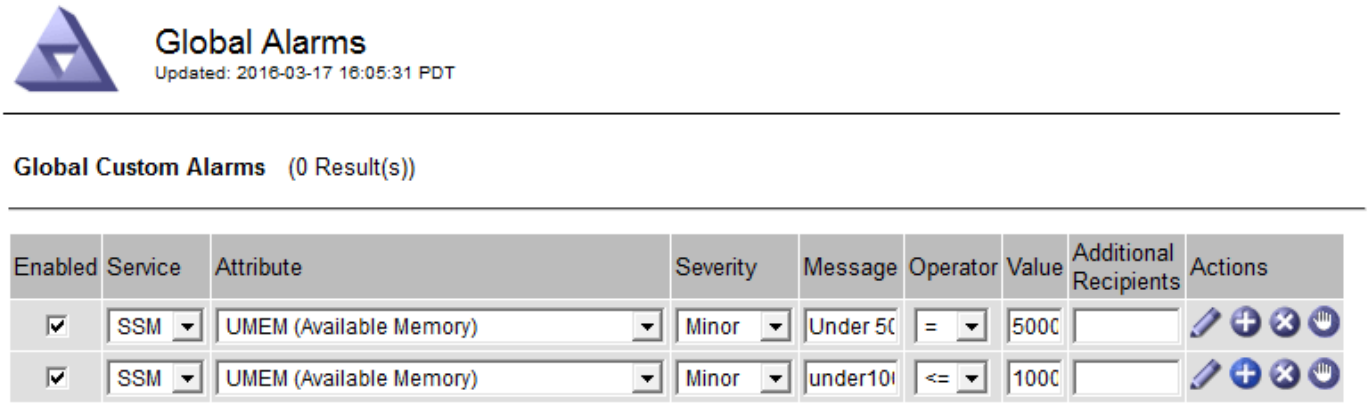
Après le scénario ci-dessus, si l'alarme personnalisée globale est désactivée, rien ne change. La valeur de l'attribut doit être réévaluée avant qu'un nouveau niveau d'alarme ne soit déclenché.

Lorsque l'alarme personnalisée globale est désactivée, lorsque la valeur de l'attribut est réévaluée, la valeur de l'attribut est évaluée par rapport aux valeurs de seuil de l'alarme par défaut. Le niveau d'alarme déclenche une alarme de niveau d'avertissement et une notification par e-mail est envoyée au personnel désigné.

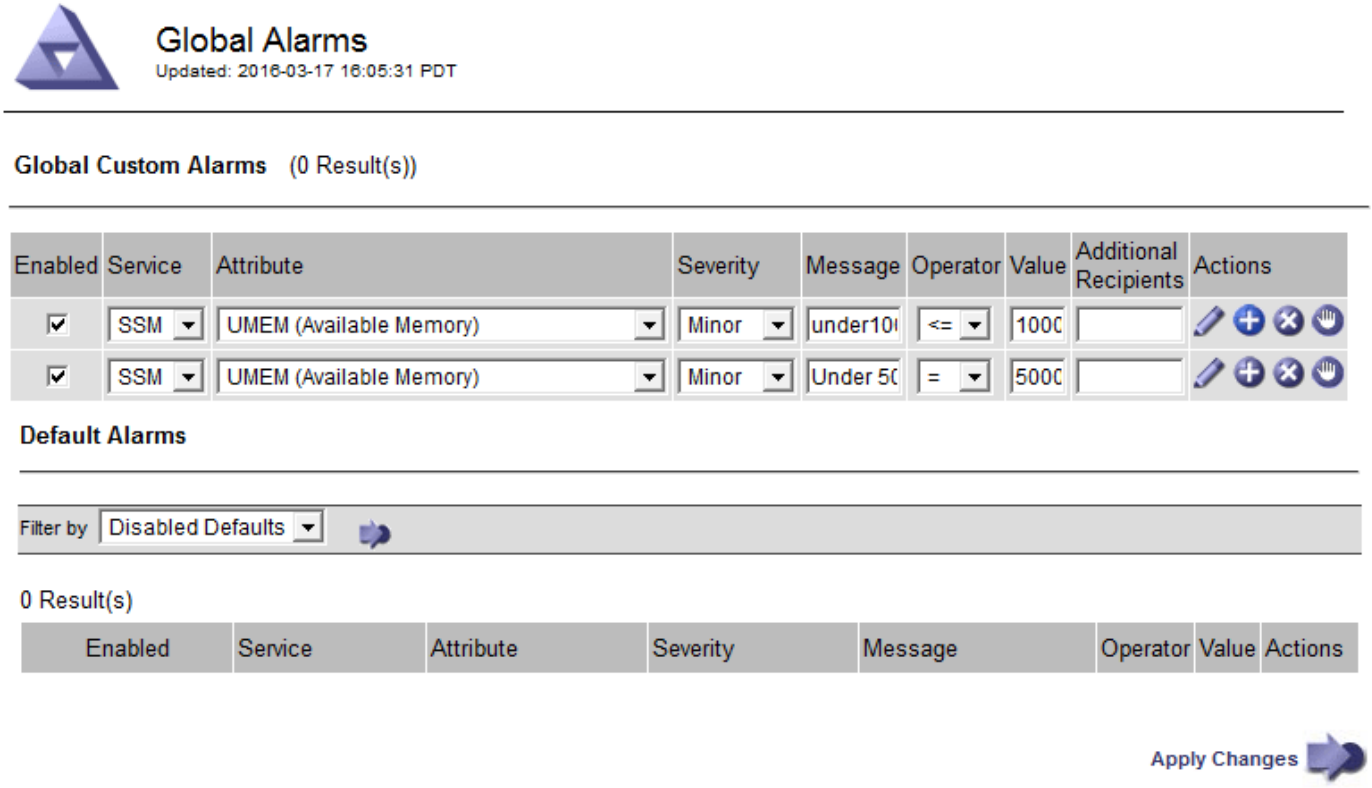
Alarmes de même gravité

Si deux alarmes personnalisées globales pour le même attribut ont la même gravité, les alarmes sont évaluées par une priorité « top down ».

Par exemple, si UMEM tombe à 50 Mo, la première alarme est déclenchée (= 50000000), mais pas celle en dessous (<=100000000).



Si l'ordre est inversé, lorsque UMEM tombe à 100 Mo, la première alarme (<=100000000) est déclenchée, mais pas celle en dessous (= 50000000).



Notifications

Une notification signale l'occurrence d'une alarme ou le changement d'état d'un service. Les notifications d'alarme peuvent être envoyées par e-mail ou via SNMP.

Pour éviter l'envoi de plusieurs alarmes et notifications lorsqu'une valeur de seuil d'alarme est atteinte, la gravité de l'alarme est vérifiée par rapport à la gravité actuelle de l'alarme pour l'attribut. S'il n'y a pas de changement, aucune autre action n'est entreprise. Cela signifie que, lorsque le service NMS continue à surveiller le système, il déclenche une alarme et envoie des notifications la première fois qu'il remarque une condition d'alarme pour un attribut. Si un nouveau seuil de valeur pour l'attribut est atteint et détecté, la gravité de l'alarme change et une nouvelle notification est envoyée. Les alarmes sont effacées lorsque les conditions reviennent au niveau Normal.

La valeur de déclenchement indiquée dans la notification d'un état d'alarme est arrondie à trois décimales. Par conséquent, une valeur d'attribut de 1.9999 déclenche une alarme dont le seuil est inférieur à (<) 2.0, bien que la notification d'alarme indique la valeur de déclenchement comme 2.0.

Nouveaux services

Lorsque de nouveaux services sont ajoutés par l'ajout de nouveaux nœuds ou sites de grille, ils héritent des alarmes par défaut et des alarmes personnalisées globales.

Alarmes et tableaux

Les attributs d'alarme affichés dans les tableaux peuvent être désactivés au niveau du système. Les alarmes ne peuvent pas être désactivées pour des lignes individuelles d'une table.

Par exemple, le tableau suivant montre deux entrées critiques disponibles (VMFI) alarmes. (Sélectionnez **SUPPORT** > **Outils** > **topologie de grille**. Sélectionnez ensuite ***Storage Node*** > **SSM** > **Resources**.)

Vous pouvez désactiver l'alarme VMFI de sorte que l'alarme VMFI de niveau critique ne soit pas déclenchée

(les deux alarmes critiques actuelles apparaissent en vert dans le tableau) ; Cependant, vous ne pouvez pas désactiver une seule alarme dans une ligne de table de sorte qu'une alarme VMFI s'affiche comme une alarme de niveau critique alors que l'autre reste verte.

Volumes

Mount Point	Device	Status	Size	Space Available	Total Entries	Entries Available	Write Cache
/	sda1	Online	10.6 GB	7.46 GB	655,360	559,263	Enabled
/var/local	sda3	Online	63.4 GB	59.4 GB	3,932,160	3,931,842	Unknown
/var/local/rangedb/0	sdb	Online	53.4 GB	53.4 GB	52,428,800	52,427,856	Enabled
/var/local/rangedb/1	sdc	Online	53.4 GB	53.4 GB	52,428,800	52,427,848	Enabled
/var/local/rangedb/2	sdd	Online	53.4 GB	53.4 GB	52,428,800	52,427,856	Enabled

Acquitter les alarmes actuelles (système hérité)

Les alarmes héritées sont déclenchées lorsque les attributs système atteignent les valeurs de seuil d'alarme. Si vous souhaitez réduire ou effacer la liste des alarmes existantes, vous pouvez également accuser réception des alarmes.

Avant de commencer

- Vous devez être connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous devez disposer de l'autorisation d'acquittement des alarmes.

Description de la tâche

Comme le système d'alarme existant continue d'être pris en charge, la liste des alarmes existantes sur la page alarmes en cours est augmentée chaque fois qu'une nouvelle alarme se déclenche. Vous pouvez généralement ignorer les alarmes (car les alertes offrent une meilleure vue du système) ou vous pouvez acquitter les alarmes.

> En option, lorsque vous avez effectué une transition complète vers le système d'alerte, vous pouvez désactiver chaque alarme existante pour l'empêcher d'être déclenchée et ajoutée au nombre d'alarmes existantes.

Lorsque vous reconnaissez une alarme, elle ne figure plus dans la page alarmes en cours du Gestionnaire de grille, sauf si l'alarme est déclenchée au niveau de gravité suivant ou si elle est résolue et se déclenche à nouveau.

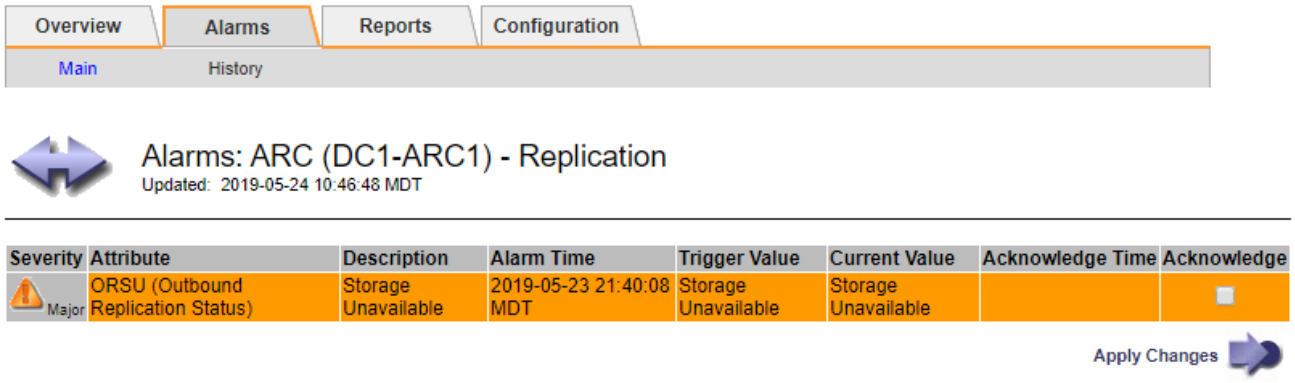
> Bien que le système d'alarme existant continue d'être pris en charge, le système d'alerte offre des avantages significatifs et est plus facile à utiliser.

Étapes

1. Sélectionnez **SUPPORT** > **alarmes (hérité)** > **alarmes actuelles**.

2. Sélectionnez le nom du service dans le tableau.

   L'onglet alarmes du service sélectionné apparaît (**SUPPORT** > **Outils** > **topologie de grille** > ***Grid Node*** > ***Service*** > **alarmes**).



3. Cochez la case **Acknowledge** pour l'alarme, puis cliquez sur **Apply Changes**.

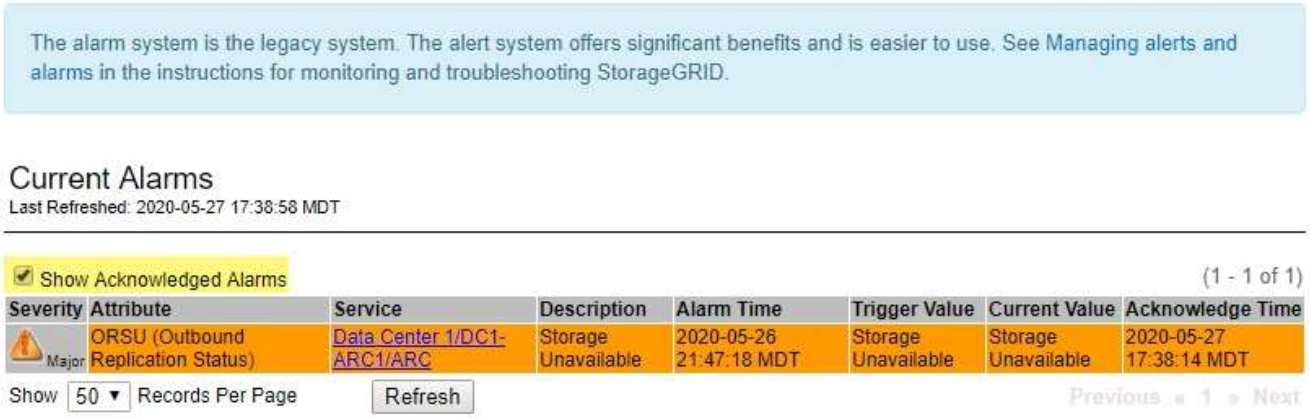
   L'alarme n'apparaît plus sur le tableau de bord ou sur la page alarmes actuelles.

   > Lorsque vous reconnaissez une alarme, l'accusé de réception n'est pas copié sur d'autres nœuds d'administration. Par conséquent, si vous affichez le tableau de bord à partir d'un autre nœud d'administration, vous pouvez continuer à voir l'alarme active.

4. Si nécessaire, affichez les alarmes acquittées.

   a. Sélectionnez **SUPPORT** > **alarmes (hérité)** > **alarmes actuelles**.
   b. Sélectionnez **Afficher les alarmes acquittées**.

      Toutes les alarmes acquittées sont affichées.



Afficher les alarmes par défaut (système hérité)

Vous pouvez afficher la liste de toutes les alarmes héritées par défaut.

Avant de commencer

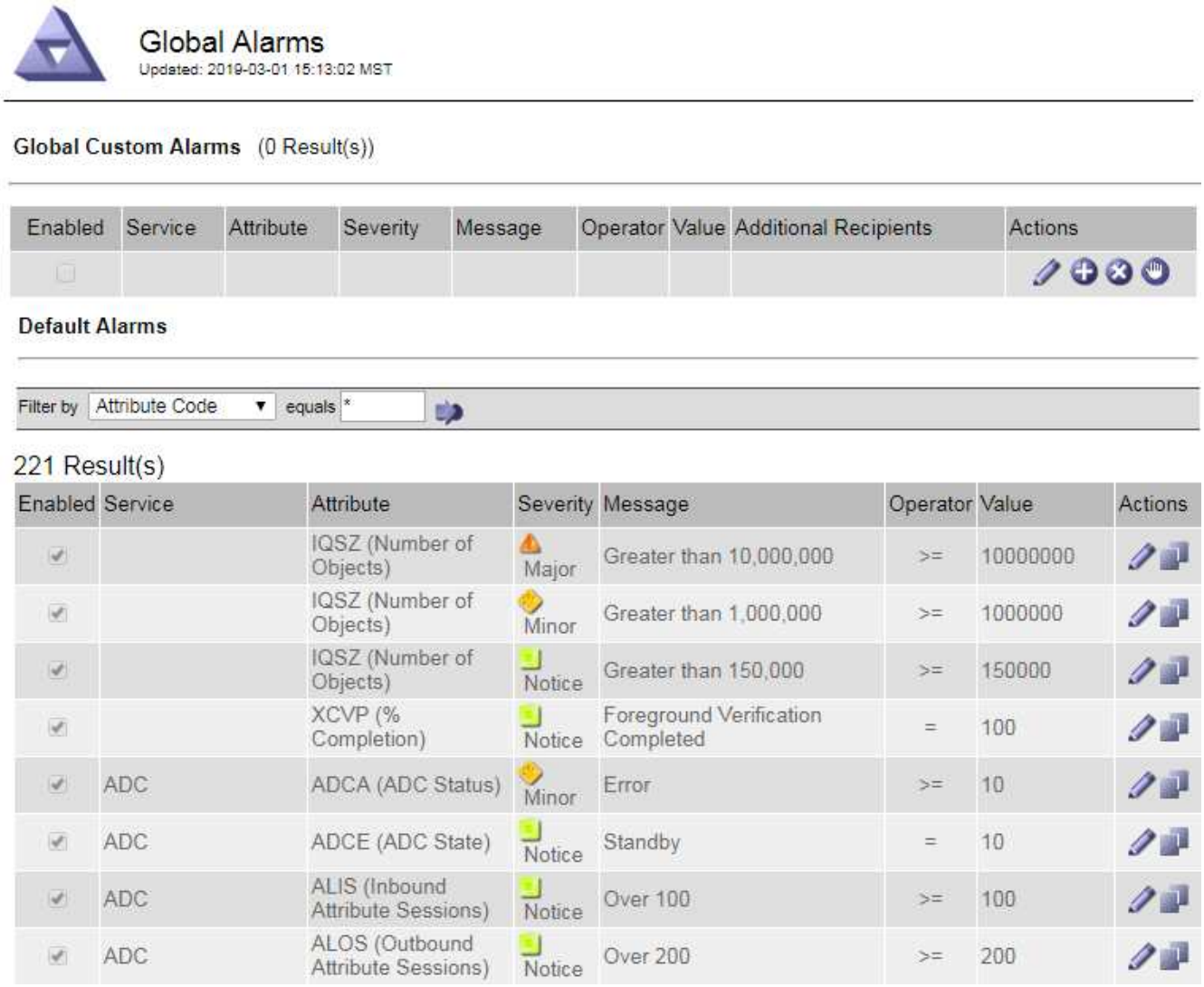
- Vous devez être connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous devez disposer d'autorisations d'accès spécifiques.

> Bien que le système d'alarme existant continue d'être pris en charge, le système d'alerte offre des avantages significatifs et est plus facile à utiliser.

Étapes

1. Sélectionnez **SUPPORT** > **alarmes (hérité)** > **alarmes globales**.
2. Pour Filtrer par, sélectionnez **Code d'attribut** ou **Nom d'attribut**.
3. Pour Egal, entrez un astérisque : *
4. Cliquez sur la flèche Ou appuyez sur **entrée**.

   Toutes les alarmes par défaut sont répertoriées.



Examiner les alarmes historiques et la fréquence des alarmes (système hérité)

Lors du dépannage d'un problème, vous pouvez vérifier la fréquence à laquelle une alarme héritée a été déclenchée par le passé.

Avant de commencer

- Vous devez être connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous devez disposer d'autorisations d'accès spécifiques.

> Bien que le système d'alarme existant continue d'être pris en charge, le système d'alerte offre des avantages significatifs et est plus facile à utiliser.

Étapes

1. Procédez comme suit pour obtenir une liste de toutes les alarmes déclenchées sur une période donnée.
   a. Sélectionnez **SUPPORT** > **alarmes (hérité)** > **alarmes historiques**.
   b. Effectuez l'une des opérations suivantes :
      - Cliquez sur l'une des périodes.
      - Entrez une plage personnalisée, puis cliquez sur **requête personnalisée**.

2. Procédez comme suit pour découvrir la fréquence à laquelle les alarmes ont été déclenchées pour un attribut particulier.
   a. Sélectionnez **SUPPORT** > **Outils** > **topologie de grille**.
   b. Sélectionnez ***grid node*** > ***service ou composant*** > **alarmes** > **Historique**.
   c. Sélectionnez l'attribut dans la liste.
   d. Effectuez l'une des opérations suivantes :
      - Cliquez sur l'une des périodes.
      - Entrez une plage personnalisée, puis cliquez sur **requête personnalisée**.

      Les alarmes sont répertoriées dans l'ordre chronologique inverse.
   e. Pour revenir au formulaire de demande d'historique des alarmes, cliquez sur **Historique**.

Créer des alarmes personnalisées globales (système hérité)

Vous avez peut-être utilisé des alarmes personnalisées globales pour l'ancien système pour répondre à des exigences de surveillance spécifiques. Les alarmes personnalisées globales peuvent avoir des niveaux d'alarme qui remplacent les alarmes par défaut ou surveiller des attributs qui ne possèdent pas d'alarme par défaut.

Avant de commencer

- Vous devez être connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous devez disposer d'autorisations d'accès spécifiques.

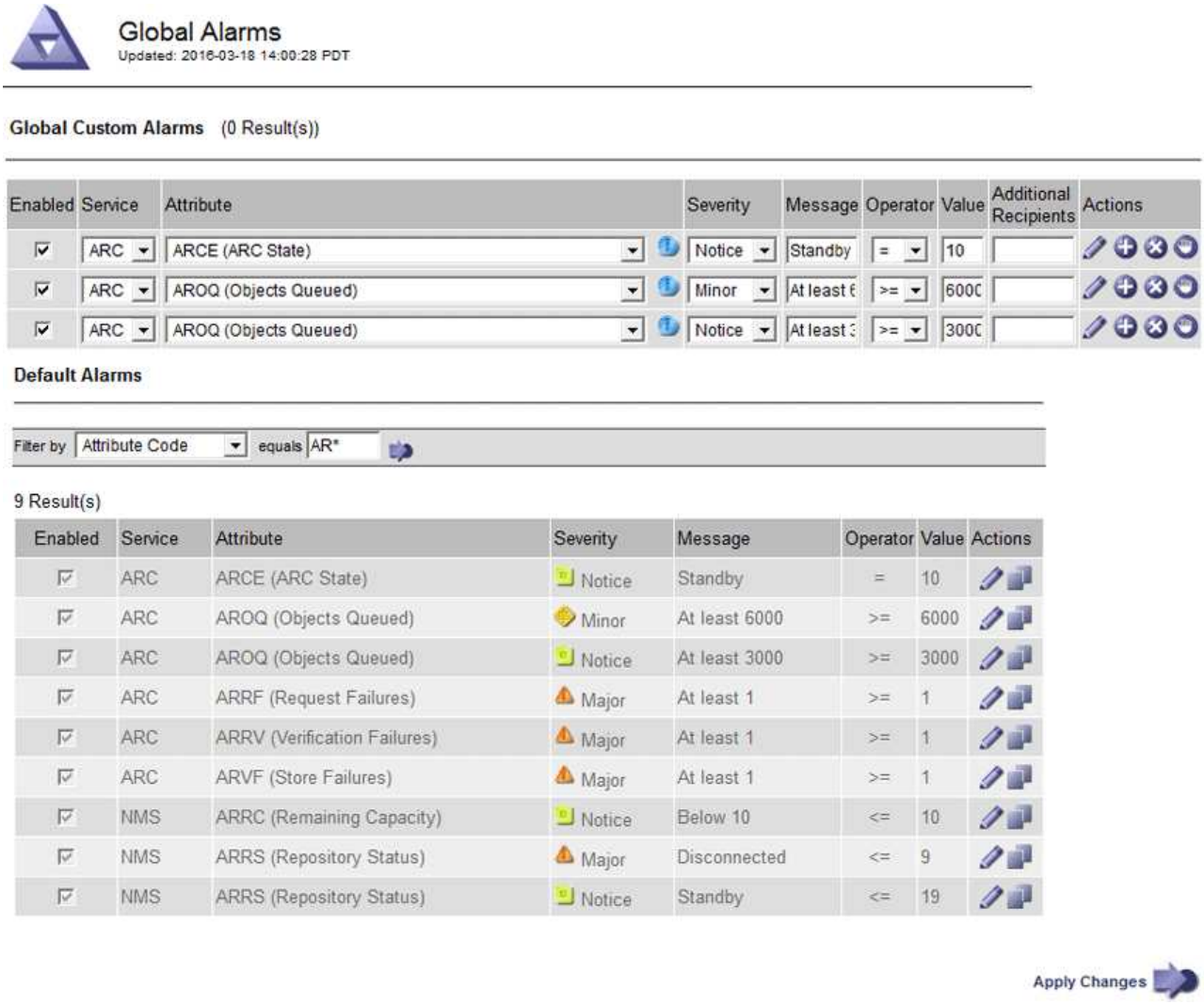
> Bien que le système d'alarme existant continue d'être pris en charge, le système d'alerte offre des avantages significatifs et est plus facile à utiliser.

Les alarmes personnalisées globales remplacent les alarmes par défaut. Vous ne devez pas modifier les valeurs d'alarme par défaut, sauf si cela est absolument nécessaire. En modifiant les alarmes par défaut, vous courez le risque de dissimulation de problèmes qui pourraient déclencher une alarme.

> Soyez prudent si vous modifiez les paramètres d'alarme. Par exemple, si vous augmentez la valeur seuil d'une alarme, il se peut que vous ne déteciez pas un problème sous-jacent. Discutez de vos modifications proposées avec le support technique avant de modifier un réglage d'alarme.

Étapes

1. Sélectionnez **SUPPORT** > **alarmes (hérité)** > **alarmes globales**.
2. Ajouter une nouvelle ligne au tableau des alarmes personnalisées globales :
   - Pour ajouter une nouvelle alarme, cliquez sur **Modifier** (S'il s'agit de la première entrée) ou **Insérer**.



- Pour modifier une alarme par défaut, recherchez l'alarme par défaut.
  i. Sous Filtrer par, sélectionnez **Code d'attribut** ou **Nom d'attribut**.
  ii. Saisissez une chaîne de recherche.

  Spécifiez quatre caractères ou utilisez des caractères génériques (Par exemple, Un ???? Ou AB*). Les astérisques (*) représentent plusieurs caractères et les points d'interrogation (?) représenter un seul caractère.

  iii. Cliquez sur la flèche , Ou appuyez sur **entrée**.
  iv. Dans la liste des résultats, cliquez sur **copie** en regard de l'alarme que vous souhaitez modifier.

  L'alarme par défaut est copiée dans le tableau des alarmes personnalisées globales.

3. Apportez toutes les modifications nécessaires aux paramètres d'alarmes personnalisées globales :

En-tête	Description
Activé	Cochez ou décochez la case pour activer ou désactiver l'alarme.

En-tête	Description
Attribut	Sélectionnez le nom et le code de l'attribut surveillé dans la liste de tous les attributs applicables au service ou au composant sélectionné. Pour afficher des informations sur l'attribut, cliquez sur **Info** à côté du nom de l'attribut.
Gravité	L'icône et le texte indiquant le niveau de l'alarme.
Messagerie	La raison de l'alarme (perte de connexion, espace de stockage inférieur à 10 %, etc.).
Opérateur	Opérateurs pour tester la valeur d'attribut actuelle par rapport au seuil de valeur : • = est égal à • > supérieur à • < moins de • >= supérieur ou égal à • <= inférieur ou égal à • ≠ non égal à
Valeur	Valeur de seuil de l'alarme utilisée pour tester la valeur réelle de l'attribut à l'aide de l'opérateur. L'entrée peut être un nombre unique, une plage de nombres spécifiée avec un signe deux-points (1:3) ou une liste de nombres et de plages délimitée par des virgules.
Destinataires supplémentaires	Une liste supplémentaire d'adresses e-mail à notifier lorsque l'alarme est déclenchée. Ceci s'ajoute à la liste de diffusion configurée sur la page **alarmes** > **Configuration de la messagerie**. Les listes sont délimitées par des virgules. **Remarque :** les listes de diffusion nécessitent la configuration du serveur SMTP pour fonctionner. Avant d'ajouter des listes de diffusion, vérifiez que SMTP est configuré. Les notifications pour les alarmes personnalisées peuvent remplacer les notifications des alarmes Global Custom ou par défaut.
Actions	Boutons de commande pour : Modifier une ligne + Insérer une ligne + Supprimer une ligne + Faites glisser une ligne vers le haut ou vers le bas + Copier une ligne

4. Cliquez sur **appliquer les modifications**.

Désactiver les alarmes (système hérité)

Les alarmes du système d'alarme hérité sont activées par défaut, mais vous pouvez désactiver les alarmes qui ne sont pas requises. Vous pouvez également désactiver les anciennes alarmes après avoir été complètement transférées vers le nouveau système d'alerte.

> Bien que le système d'alarme existant continue d'être pris en charge, le système d'alerte offre des avantages significatifs et est plus facile à utiliser.

Désactiver une alarme par défaut (système hérité)

Vous pouvez désactiver l'une des alarmes par défaut héritées pour l'ensemble du système.

Avant de commencer

- Vous devez être connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous devez disposer d'autorisations d'accès spécifiques.

Description de la tâche

La désactivation d'une alarme pour un attribut qui a actuellement une alarme déclenchée n'efface pas l'alarme en cours. L'alarme sera désactivée lors du prochain dépassement du seuil d'alarme par l'attribut, ou vous pouvez effacer l'alarme déclenchée.

> Ne désactivez aucune des alarmes héritées tant que vous n'avez pas complètement migré vers le nouveau système d'alerte. Dans le cas contraire, vous risquez de ne pas détecter un problème sous-jacent avant d'empêcher la réalisation d'une opération critique.

Étapes

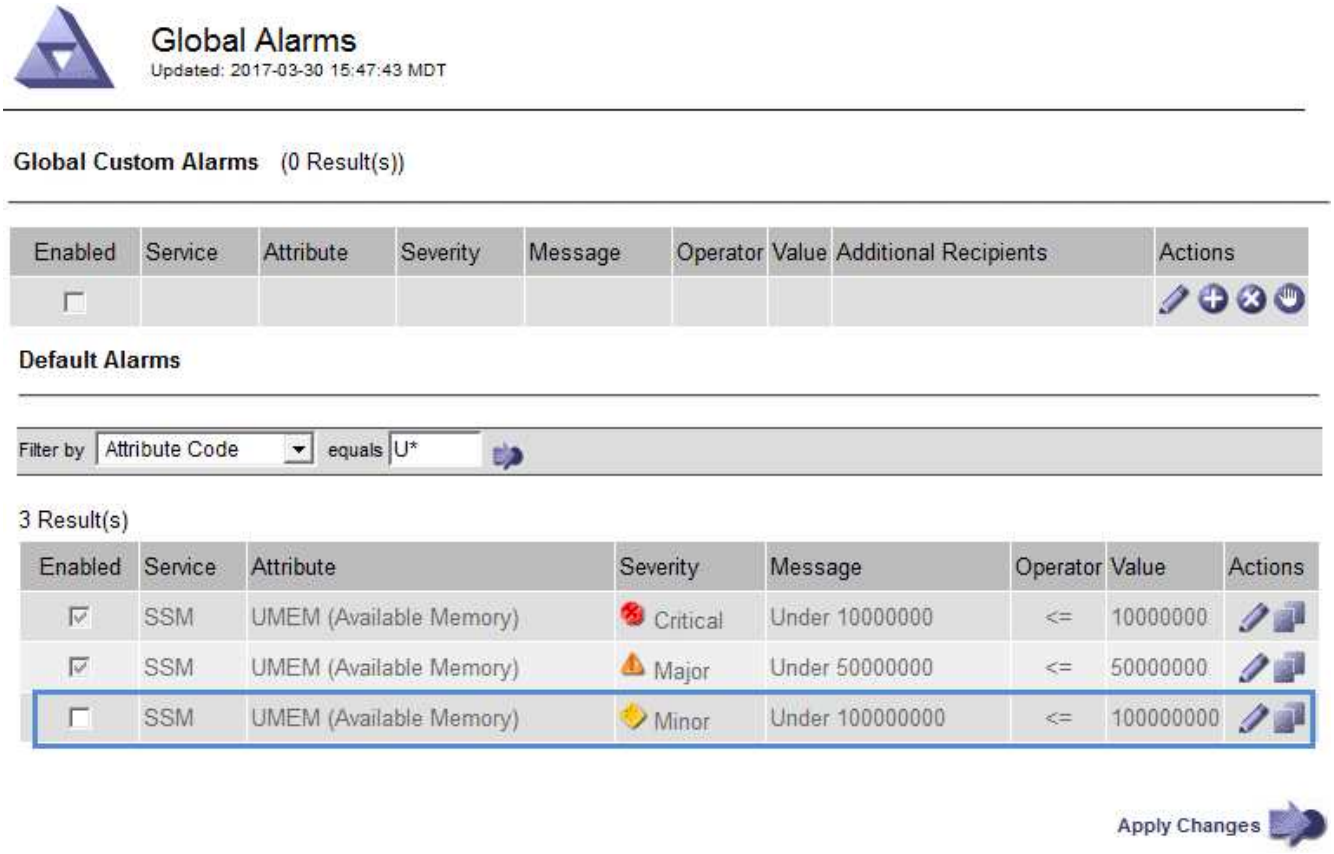
1. Sélectionnez **SUPPORT** > **alarmes (hérité)** > **alarmes globales**.
2. Recherchez l'alarme par défaut à désactiver.
   a. Dans la section alarmes par défaut, sélectionnez **Filtrer par** > **Code d'attribut** ou **Nom d'attribut**.
   b. Saisissez une chaîne de recherche.

      Spécifiez quatre caractères ou utilisez des caractères génériques (Par exemple, Un ???? Ou AB*). Les astérisques (*) représentent plusieurs caractères et les points d'interrogation (?) représenter un seul caractère.

   c. Cliquez sur la flèche , Ou appuyez sur **entrée**.

      > La sélection de **Désactivé par défaut** affiche la liste de toutes les alarmes par défaut actuellement désactivées.

3. Dans le tableau des résultats de la recherche, cliquez sur l'icône Modifier pour l'alarme que vous souhaitez désactiver.



La case **activé** pour l'alarme sélectionnée devient active.

4. Décochez la case **activé**.
5. Cliquez sur **appliquer les modifications**.

   L'alarme par défaut est désactivée.

Désactiver les alarmes personnalisées globales (système hérité)

Vous pouvez désactiver une alarme personnalisée globale héritée pour l'ensemble du système.

Avant de commencer

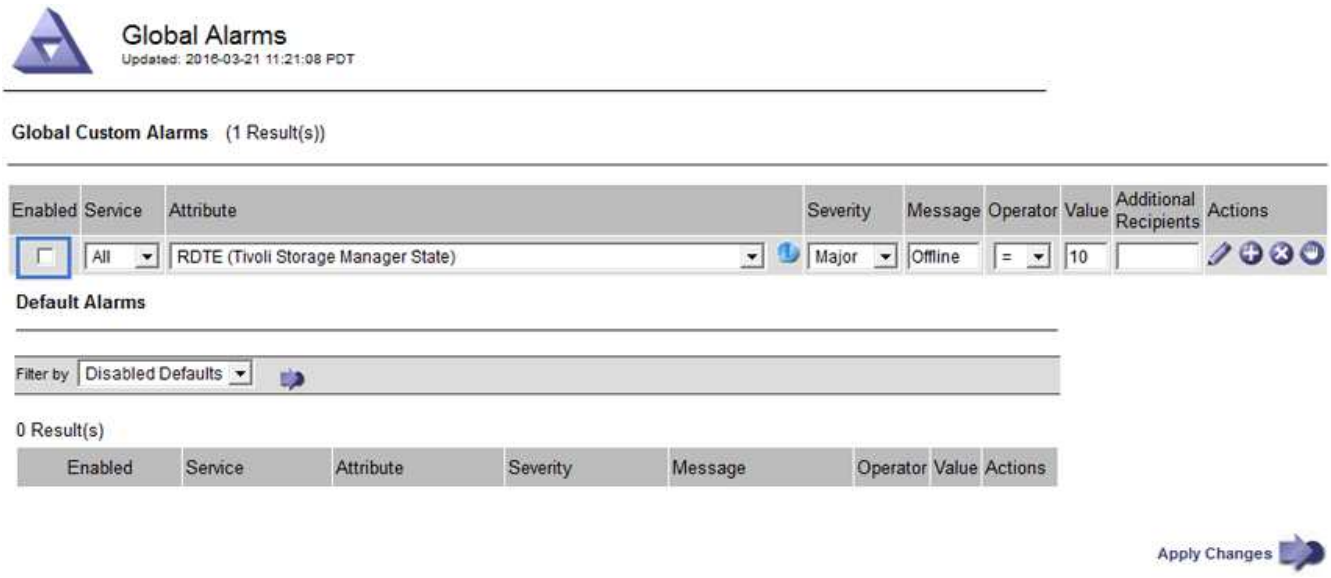
- Vous devez être connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous devez disposer d'autorisations d'accès spécifiques.

Description de la tâche

La désactivation d'une alarme pour un attribut qui a actuellement une alarme déclenchée n'efface pas l'alarme en cours. L'alarme sera désactivée lors du prochain dépassement du seuil d'alarme par l'attribut, ou vous pouvez effacer l'alarme déclenchée.

Étapes

1. Sélectionnez **SUPPORT** > **alarmes (hérité)** > **alarmes globales**.
2. Dans le tableau alarmes personnalisées globales, cliquez sur **Modifier** à côté de l'alarme que vous souhaitez désactiver.
3. Décochez la case **activé**.



4. Cliquez sur **appliquer les modifications**.

   L'alarme personnalisée globale est désactivée.

Effacer les alarmes déclenchées (système hérité)

Si une alarme héritée est déclenchée, vous pouvez l'effacer au lieu de la reconnaître.

Avant de commencer

- Vous devez avoir le `Passwords.txt` fichier.

La désactivation d'une alarme pour un attribut qui a actuellement une alarme déclenchée contre elle n'efface pas l'alarme. L'alarme sera désactivée lors de la prochaine modification de l'attribut. Vous pouvez accuser réception de l'alarme ou, si vous voulez effacer immédiatement l'alarme plutôt que d'attendre que la valeur de l'attribut change (ce qui entraîne un changement de l'état d'alarme), vous pouvez effacer l'alarme déclenchée. Vous pouvez trouver ceci utile si vous voulez effacer une alarme immédiatement contre un attribut dont la valeur ne change pas souvent (par exemple, les attributs d'état).

1. Désactivez l'alarme.
2. Connectez-vous au nœud d'administration principal :
   a. Saisissez la commande suivante : *`ssh admin@primary_Admin_Node_IP`*
   b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
   c. Entrez la commande suivante pour passer à la racine : `su -`
   d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

      Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.
3. Redémarrez le service NMS : `service nms restart`
4. Déconnectez-vous du nœud d'administration : `exit`

   L'alarme est effacée.

Configurer les notifications des alarmes (système hérité)

Le système StorageGRID peut envoyer automatiquement des e-mails et "Notifications SNMP" lorsqu'une alarme est déclenchée ou qu'un état de service change.

Par défaut, les notifications par e-mail d'alarme ne sont pas envoyées. Pour les notifications par e-mail, vous devez configurer le serveur de messagerie et spécifier les destinataires. Pour les notifications SNMP, vous devez configurer l'agent SNMP.

Types de notifications d'alarme (système hérité)

Lorsqu'une alarme héritée est déclenchée, le système StorageGRID envoie deux types de notifications d'alarme : le niveau de gravité et l'état de service.

Notifications de niveau de gravité

Une notification par e-mail d'alarme est envoyée lorsqu'une alarme héritée est déclenchée à un niveau de gravité sélectionné :

- Avertissement
- Mineur
- Majeur
- Primordial

Une liste de diffusion reçoit toutes les notifications relatives à l'alarme pour la gravité sélectionnée. Une notification est également envoyée lorsque l'alarme quitte le niveau d'alarme — soit en étant résolue soit en entrant un niveau de gravité d'alarme différent.

Notifications d'état de service

Une notification d'état de service est envoyée lorsqu'un service (par exemple, le service LDR ou le service NMS) entre dans l'état de service sélectionné et lorsqu'il quitte l'état de service sélectionné. Des notifications d'état de service sont envoyées lorsqu'un service entre ou quitte l'un des États de service suivants :

- Inconnu
- Arrêt administratif

Une liste de diffusion reçoit toutes les notifications associées aux modifications de l'état sélectionné.

Configuration des paramètres du serveur de messagerie pour les alarmes (système hérité)

Si vous souhaitez que StorageGRID envoie des notifications par e-mail lorsqu'une alarme héritée est déclenchée, vous devez spécifier les paramètres du serveur de messagerie SMTP. Le système StorageGRID envoie uniquement des e-mails ; il ne peut pas en recevoir.

Avant de commencer

- Vous devez être connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous devez disposer d'autorisations d'accès spécifiques.

Description de la tâche

Utilisez ces paramètres pour définir le serveur SMTP utilisé pour les notifications par e-mail d'alarme et les e-mails AutoSupport hérités. Ces paramètres ne sont pas utilisés pour les notifications d'alerte.

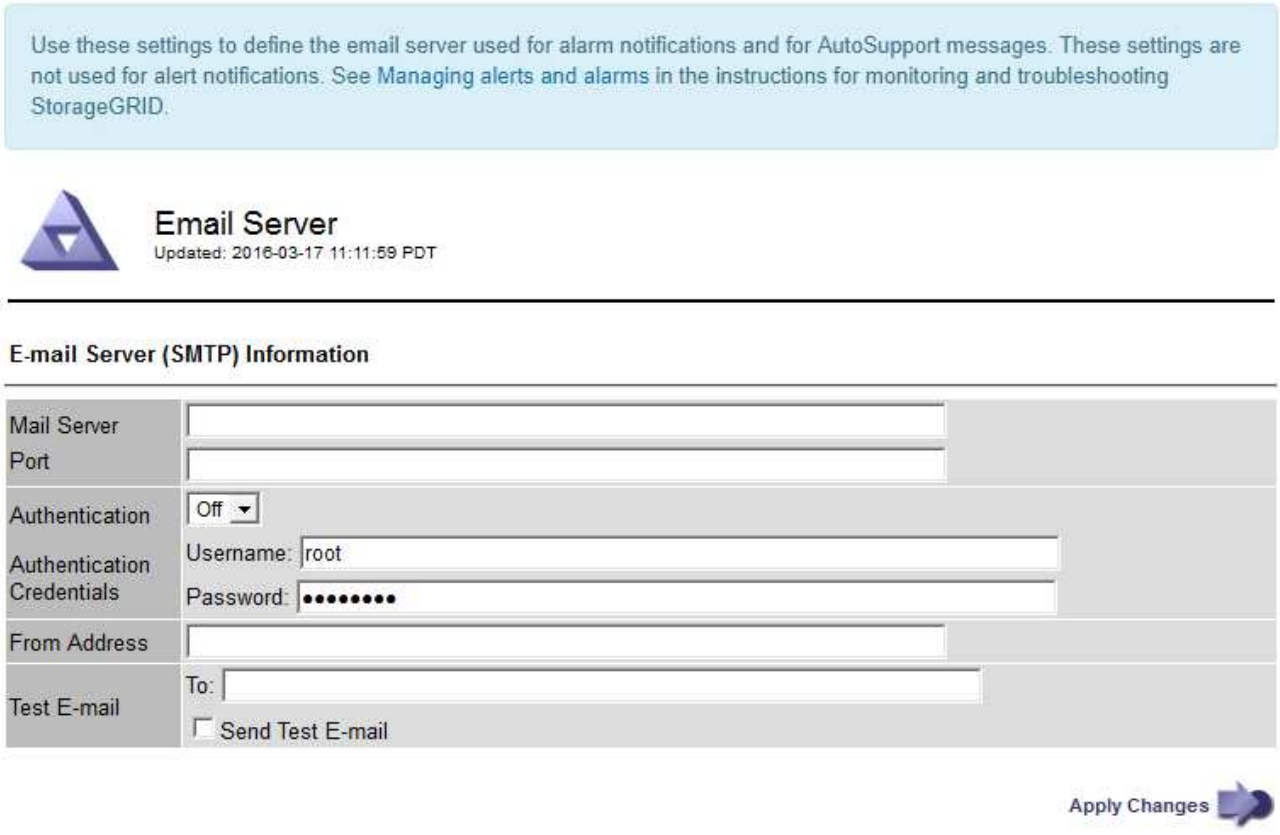
Si vous utilisez SMTP comme protocole pour les messages AutoSupport, vous avez peut-être déjà configuré un serveur de messagerie SMTP. Le même serveur SMTP est utilisé pour les notifications par e-mail d'alarme. Vous pouvez donc ignorer cette procédure. Voir la "Instructions d'administration de StorageGRID".

SMTP est le seul protocole pris en charge pour l'envoi d'e-mails.

Étapes

1. Sélectionnez **SUPPORT** > **alarmes (hérité)** > **Configuration messagerie héritée**.
2. Dans le menu E-mail, sélectionnez **serveur**.

   La page serveur de messagerie s'affiche. Cette page est également utilisée pour configurer le serveur de messagerie pour les messages AutoSupport.



3. Ajoutez les paramètres suivants du serveur de messagerie SMTP :

Élément	Description
Serveur de messagerie	Adresse IP du serveur de messagerie SMTP. Vous pouvez entrer un nom d'hôte plutôt qu'une adresse IP si vous avez déjà configuré les paramètres DNS sur le noeud d'administration.
Port	Numéro de port pour accéder au serveur de messagerie SMTP.
Authentification	Permet l'authentification du serveur de messagerie SMTP. Par défaut, l'authentification est désactivée.

Élément	Description
Informations d'authentification	Nom d'utilisateur et mot de passe du serveur de messagerie SMTP. Si l'authentification est activée, un nom d'utilisateur et un mot de passe doivent être fournis pour accéder au serveur de messagerie SMTP.

4. Sous **de adresse**, entrez une adresse e-mail valide que le serveur SMTP reconnaîtra comme adresse e-mail d'envoi. Il s'agit de l'adresse électronique officielle à partir de laquelle l'e-mail est envoyé.
5. Vous pouvez également envoyer un e-mail de test pour confirmer que les paramètres de votre serveur de messagerie SMTP sont corrects.
   a. Dans la zone **Test E-mail** > **à**, ajoutez une ou plusieurs adresses auxquelles vous pouvez accéder.

      Vous pouvez entrer une seule adresse e-mail ou une liste d'adresses e-mail délimitée par des virgules. Comme le service NMS ne confirme pas le succès ou l'échec lors de l'envoi d'un e-mail de test, vous devez être en mesure de vérifier la boîte de réception du destinataire du test.

   b. Sélectionnez **Envoyer E-mail test**.
6. Cliquez sur **appliquer les modifications**.

   Les paramètres du serveur de messagerie SMTP sont enregistrés. Si vous avez saisi des informations pour un e-mail de test, cet e-mail est envoyé. Les e-mails de test sont immédiatement envoyés au serveur de messagerie et ne sont pas envoyés par la file d'attente des notifications. Dans un système avec plusieurs nœuds d'administration, chaque nœud d'administration envoie un e-mail. La réception de l'e-mail de test confirme que les paramètres de votre serveur de messagerie SMTP sont corrects et que le service NMS se connecte avec succès au serveur de messagerie. Un problème de connexion entre le service NMS et le serveur de messagerie déclenche l'alarme DES MINUTES héritées (état de notification NMS) au niveau de gravité mineure.

Créer des modèles d'e-mails d'alarme (système hérité)

Les modèles de courrier électronique vous permettent de personnaliser l'en-tête, le pied de page et l'objet d'une notification d'alarme existante. Vous pouvez utiliser des modèles d'e-mails pour envoyer des notifications uniques contenant le même corps de texte à différentes listes de diffusion.

Avant de commencer

- Vous devez être connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous devez disposer d'autorisations d'accès spécifiques.

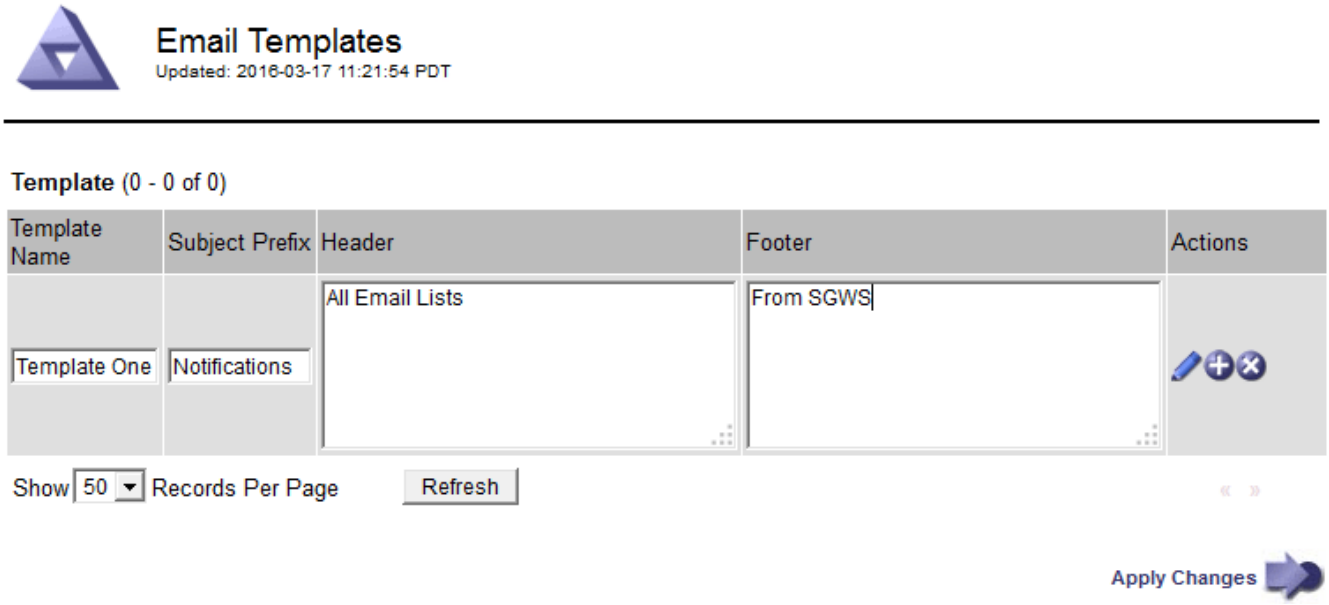
Description de la tâche

Utilisez ces paramètres pour définir les modèles d'e-mails utilisés pour les notifications d'alarme héritées. Ces paramètres ne sont pas utilisés pour les notifications d'alerte.

Différentes listes de diffusion peuvent nécessiter des informations de contact différentes. Les modèles n'incluent pas le corps du message électronique.

Étapes

1. Sélectionnez **SUPPORT** > **alarmes (hérité)** > **Configuration messagerie héritée**.
2. Dans le menu E-mail, sélectionnez **modèles**.
3. Cliquez sur **Modifier** (Ou **Insérer** s'il ne s'agit pas du premier modèle).



4. Dans la nouvelle ligne, ajoutez ce qui suit :

Élément	Description
Nom du modèle	Nom unique utilisé pour identifier le modèle. Les noms de modèles ne peuvent pas être dupliqués.
Préfixe de l'objet	Facultatif. Préfixe qui apparaîtra au début de la ligne d'objet d'un e-mail. Les préfixes peuvent être utilisés pour configurer facilement les filtres d'e-mail et organiser les notifications.
En-tête	Facultatif. Texte d'en-tête qui apparaît au début du corps du message électronique. Le texte d'en-tête peut être utilisé pour prégérer le contenu de l'e-mail avec des informations telles que le nom et l'adresse de l'entreprise.
Pied de page	Facultatif. Texte de pied de page qui apparaît à la fin du corps de l'e-mail. Le texte du pied de page peut être utilisé pour fermer l'e-mail avec des informations de rappel telles qu'un numéro de téléphone de contact ou un lien vers un site Web.

5. Cliquez sur **appliquer les modifications**.

   Un nouveau modèle pour les notifications est ajouté.

Créer des listes de diffusion pour les notifications d'alarme (système hérité)

Les listes de diffusion vous permettent d'avertir les destinataires lorsqu'une alarme héritée est déclenchée ou lorsqu'un état de service change. Vous devez créer au moins une liste de diffusion pour pouvoir envoyer des notifications par e-mail d'alarme. Pour envoyer une notification à un seul destinataire, créez une liste de diffusion avec une adresse e-mail.

Avant de commencer

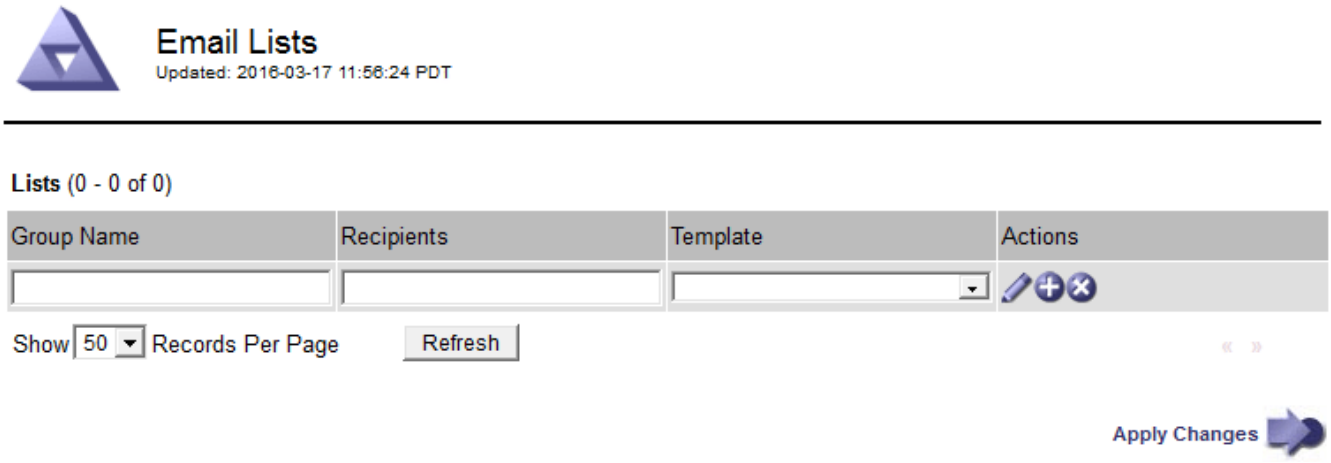
- Vous devez être connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous devez disposer d'autorisations d'accès spécifiques.
- Si vous souhaitez spécifier un modèle de courrier électronique pour la liste de diffusion (en-tête personnalisé, pied de page et ligne d'objet), vous devez avoir déjà créé le modèle.

Description de la tâche

Utilisez ces paramètres pour définir les listes de diffusion utilisées pour les notifications par e-mail d'alarme héritées. Ces paramètres ne sont pas utilisés pour les notifications d'alerte.

Étapes

1. Sélectionnez **SUPPORT** > **alarmes (hérité)** > **Configuration messagerie héritée**.
2. Dans le menu E-mail, sélectionnez **listes**.
3. Cliquez sur **Modifier** (Ou *Insérer* s'il ne s'agit pas de la première liste de diffusion).



4. Dans la nouvelle ligne, ajoutez les éléments suivants :

Élément	Description
Nom du groupe	Nom unique utilisé pour identifier la liste de diffusion. Les noms de listes de diffusion ne peuvent pas être dupliqués. **Remarque :** si vous modifiez le nom d'une liste de diffusion, le changement n'est pas propagé aux autres emplacements qui utilisent le nom de la liste de diffusion. Vous devez mettre à jour manuellement toutes les notifications configurées pour utiliser le nouveau nom de liste de diffusion.
Destinataires	Une seule adresse e-mail, une liste de diffusion précédemment configurée ou une liste délimitée par des virgules d'adresses e-mail et de listes de diffusion auxquelles les notifications seront envoyées. **Remarque :** si une adresse e-mail appartient à plusieurs listes de diffusion, une seule notification par e-mail est envoyée lorsqu'un événement de déclenchement de notification se produit.

Élément	Description
Modèle	Vous pouvez également sélectionner un modèle de courrier électronique pour ajouter un en-tête, un pied de page et une ligne d'objet uniques aux notifications envoyées à tous les destinataires de cette liste de diffusion.

5. Cliquez sur **appliquer les modifications**.

   Une nouvelle liste de diffusion est créée.

Configurer les notifications par e-mail pour les alarmes (système hérité)

Pour recevoir des notifications par e-mail pour le système d'alarme hérité, les destinataires doivent être membres d'une liste de diffusion et cette liste doit être ajoutée à la page Notifications. Les notifications sont configurées pour envoyer des e-mails aux destinataires uniquement lorsqu'une alarme avec un niveau de gravité spécifié est déclenchée ou lorsqu'un état de service change. Ainsi, les destinataires ne reçoivent que les notifications dont ils ont besoin.

Avant de commencer

- Vous devez être connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous devez disposer d'autorisations d'accès spécifiques.
- Vous devez avoir configuré une liste d'e-mails.

Description de la tâche

Utilisez ces paramètres pour configurer les notifications pour les alarmes héritées. Ces paramètres ne sont pas utilisés pour les notifications d'alerte.

Si une adresse e-mail (ou une liste) appartient à plusieurs listes de diffusion, une seule notification par e-mail est envoyée lorsqu'un événement de déclenchement de notification se produit. Par exemple, un groupe d'administrateurs au sein de votre organisation peut être configuré pour recevoir des notifications pour toutes les alarmes, quelle que soit leur gravité. Un autre groupe peut uniquement exiger des notifications pour les alarmes dont la gravité est critique. Vous pouvez appartenir aux deux listes. Si une alarme critique est déclenchée, vous ne recevez qu'une seule notification.

Étapes

1. Sélectionnez **SUPPORT** > **alarmes (hérité)** > **Configuration messagerie héritée**.
2. Dans le menu E-mail, sélectionnez **Notifications**.
3. Cliquez sur *Modifier* (Ou *Insérer* s'il ne s'agit pas de la première notification).
4. Sous liste de courrier électronique, sélectionnez la liste de diffusion.
5. Sélectionnez un ou plusieurs niveaux de gravité d'alarme et États de service.
6. Cliquez sur **appliquer les modifications**.

   Des notifications sont envoyées à la liste de diffusion lorsque des alarmes avec le niveau de gravité d'alarme ou l'état de service sélectionné sont déclenchées ou modifiées.

Supprimer les notifications d'alarme pour une liste de diffusion (système hérité)

Vous pouvez supprimer les notifications d'alarme pour une liste de diffusion lorsque vous ne souhaitez plus que la liste de diffusion reçoive des notifications relatives aux alarmes. Par exemple, vous pouvez supprimer les notifications relatives aux alarmes existantes après avoir été passé à l'aide des notifications par e-mail d'alerte.

Avant de commencer

- Vous devez être connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous devez disposer d'autorisations d'accès spécifiques.

Utilisez ces paramètres pour supprimer les notifications par e-mail pour l'ancien système d'alarme. Ces paramètres ne s'appliquent pas aux notifications par e-mail d'alerte.

> Bien que le système d'alarme existant continue d'être pris en charge, le système d'alerte offre des avantages significatifs et est plus facile à utiliser.

Étapes

1. Sélectionnez **SUPPORT** > **alarmes (hérité)** > **Configuration messagerie héritée**.
2. Dans le menu E-mail, sélectionnez **Notifications**.
3. Cliquez sur **Modifier** en regard de la liste de diffusion pour laquelle vous souhaitez supprimer les notifications.
4. Sous Supprimer, cochez la case en regard de la liste de diffusion que vous souhaitez supprimer ou sélectionnez **Supprimer** en haut de la colonne pour supprimer toutes les listes de diffusion.
5. Cliquez sur **appliquer les modifications**.

   Les notifications d'alarme héritées sont supprimées pour les listes d'envoi sélectionnées.

Afficher les anciennes alarmes

Les alarmes (système hérité) sont déclenchées lorsque les attributs système atteignent les valeurs de seuil d'alarme. Vous pouvez afficher les alarmes actives à partir de la page alarmes en cours.

> Bien que le système d'alarme existant continue d'être pris en charge, le système d'alerte offre des avantages significatifs et est plus facile à utiliser.

Avant de commencer

- Vous devez être connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".

Étapes

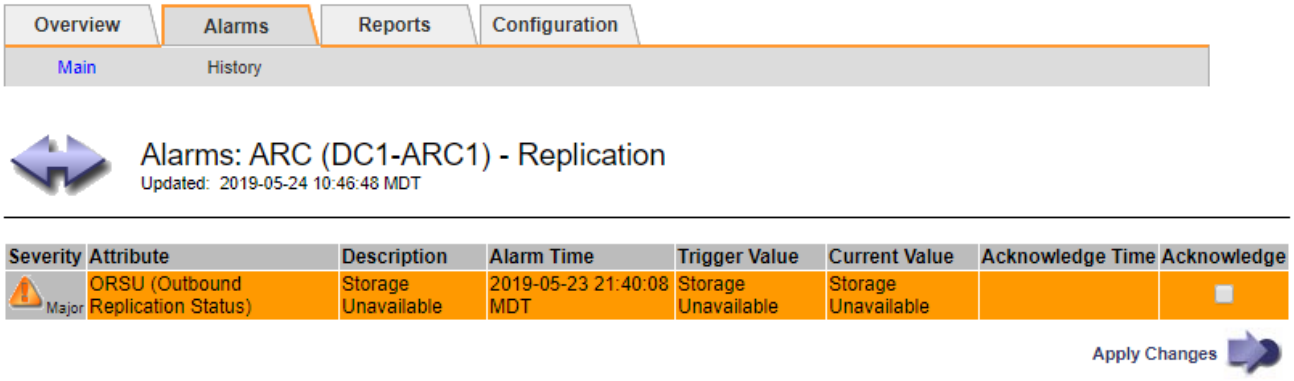
1. Sélectionnez **SUPPORT** > **alarmes (hérité)** > **alarmes actuelles**.

L'icône d'alarme indique la gravité de chaque alarme, comme suit :

Icône	Couleur	Gravité de l'alarme	Signification
	Jaune	Avertissement	Le nœud est connecté à la grille, mais il existe une condition inhabituelle qui n'affecte pas les opérations normales.
	Orange clair	Mineur	Le nœud est connecté à la grille, mais il existe une condition anormale qui pourrait affecter son fonctionnement à l'avenir. Vous devez étudier pour éviter la remontée des problèmes.
	Orange foncé	Majeur	Le nœud est connecté à la grille, mais il existe une condition anormale qui affecte actuellement le fonctionnement. Cela nécessite une attention particulière afin d'éviter la remontée des problèmes.
	Rouge	Primordial	Le nœud est connecté à la grille, mais il existe une condition anormale qui a arrêté des opérations normales. Vous devez résoudre le problème immédiatement.

2. Pour en savoir plus sur l'attribut à l'origine du déclenchement de l'alarme, cliquez avec le bouton droit de la souris sur le nom de l'attribut dans le tableau.
3. Pour afficher des détails supplémentaires sur une alarme, cliquez sur le nom du service dans le tableau.

   L'onglet alarmes du service sélectionné apparaît (**SUPPORT** > **Outils** > **topologie de grille** > ***Grid Node*** > ***Service*** > **alarmes**).



4. Si vous souhaitez effacer le nombre d'alarmes en cours, vous pouvez, en option, procéder comme suit :
   - Accuser réception de l'alarme. Une alarme acquittée n'est plus incluse dans le nombre d'alarmes héritées à moins qu'elle ne soit déclenchée au niveau de gravité suivant ou qu'elle ne soit résolue et se déclenche à nouveau.
   - Désactivez une alarme par défaut particulière ou une alarme personnalisée globale pour l'ensemble du système afin d'éviter qu'elle ne se déclenche à nouveau.

Informations associées

"Référence des alarmes (système hérité)"

"Acquitter les alarmes actuelles (système hérité)"

"Désactiver les alarmes (système hérité)"

Référence des alarmes (système hérité)

Le tableau suivant répertorie toutes les alarmes par défaut héritées. Si une alarme est déclenchée, vous pouvez rechercher le code d'alarme dans ce tableau pour trouver les actions recommandées.

Bien que le système d'alarme existant continue d'être pris en charge, le système d'alerte offre des avantages significatifs et est plus facile à utiliser.

Code	Nom	Service	Action recommandée
ABRL	Relais d'attribut disponibles	BADC, BAMS, BARC, BCLB, BCMN, BLDR, BNMS, BSSM, BDDS	Rétablir la connectivité à un service (un service ADC) exécutant un service de relais d'attribut dès que possible. S'il n'y a pas de relais d'attribut connecté, le nœud de grille ne peut pas signaler les valeurs d'attribut au service NMS. Ainsi, le service NMS ne peut plus surveiller l'état du service ou mettre à jour les attributs du service. Si le problème persiste, contactez le support technique.

Code	Nom	Service	Action recommandée
ACMS	Services de métadonnées disponibles	BARC, BLDR, BCMN	Une alarme se déclenche lorsqu'un service LDR ou ARC perd la connexion à un service DDS. Dans ce cas, les transactions d'ingestion ou de récupération ne peuvent pas être traitées. Si l'indisponibilité des services DDS n'est qu'un bref problème transitoire, les transactions peuvent être retardées. Vérifiez et restaurez les connexions à un service DDS pour effacer cette alarme et rétablir la fonctionnalité complète du service.
ACTES	État du service NetApp Cloud Tiering	ARC	Disponible uniquement pour les nœuds d'archivage avec un type de Tiering cloud cible : simple Storage Service (S3). Si l'attribut ACT pour le nœud d'archivage est défini sur lecture seule activée ou lecture-écriture désactivée, vous devez définir l'attribut sur lecture-écriture activée. Si une alarme majeure est déclenchée en raison d'un échec de l'authentification, vérifiez les informations d'identification associées au compartiment de destination et mettez à jour les valeurs, si nécessaire. Si une alarme majeure est déclenchée pour une autre raison, contactez le support technique.
ADCA	État ADC	ADC	Si une alarme est déclenchée, sélectionnez **SUPPORT** > **Outils** > **topologie de grille**. Sélectionnez ensuite ***site*** > ***grid node*** > **ADC** > **Présentation** > **main** et **ADC** > **alarmes** > **main** pour déterminer la cause de l'alarme. Si le problème persiste, contactez le support technique.
ADCE	État ADC	ADC	Si la valeur de l'état ADC est Veille, continuez à surveiller le service et si le problème persiste, contactez l'assistance technique. Si la valeur de l'état ADC est hors ligne, redémarrez le service. Si le problème persiste, contactez le support technique.

Code	Nom	Service	Action recommandée
AITE	État de récupération	BARC	Disponible uniquement pour les nœuds d'archivage avec un type cible de Tivoli Storage Manager (TSM). Si la valeur de Retrieve State est en attente de la cible, vérifiez le serveur middleware TSM et assurez-vous qu'il fonctionne correctement. Si le nœud d'archivage vient d'être ajouté au système StorageGRID, assurez-vous que la connexion du nœud d'archivage au système de stockage d'archives externe cible est correctement configurée. Si la valeur de l'état de récupération d'archives est hors ligne, essayez de mettre à jour l'état en ligne. Sélectionnez **SUPPORT** > **Outils** > **topologie de grille**. Sélectionnez ensuite ***site*** > ***grid node*** > **ARC** > **Retrieve** > **Configuration** > **main**, sélectionnez **Archive Retrieve State** > **Online**, puis cliquez sur **Apply Changes**. Si le problème persiste, contactez le support technique.
AITU	État de récupération	BARC	Si la valeur de l'état de récupération est erreur cible, recherchez des erreurs dans le système de stockage d'archives externes ciblé. Si la valeur de l'état de récupération d'archives est session perdue, vérifiez le système de stockage d'archives externes ciblé pour vous assurer qu'il est en ligne et qu'il fonctionne correctement. Vérifiez la connexion réseau avec la cible. Si la valeur de l'état de récupération d'archives est erreur inconnue, contactez le support technique.
ALIS	Sessions d'attribut entrant	ADC	Si le nombre de sessions d'attribut entrantes sur un relais d'attribut augmente trop important, cela peut indiquer que le système StorageGRID est devenu déséquilibré. Dans des conditions normales, les sessions d'attribut doivent être réparties de manière uniforme entre les services ADC. Un déséquilibre peut entraîner des problèmes de performances. Si le problème persiste, contactez le support technique.
ALOS	Sessions d'attribut sortant	ADC	Le service ADC a un nombre élevé de sessions d'attribut et est en train de devenir surchargé. Si cette alarme se déclenche, contactez le support technique.

Code	Nom	Service	Action recommandée
ALUR	Référentiels d'attributs inaccessibles	ADC	Vérifiez la connectivité réseau avec le service NMS pour vous assurer que le service peut contacter le référentiel d'attributs. Si cette alarme se déclenche et que la connectivité réseau est correcte, contactez le support technique.
AMQS	Messages d'audit en file d'attente	BADC, BAMS, BARC, BCLB, BCMN, BLDR, BNMS, BDDS	Si les messages d'audit ne peuvent pas être immédiatement transmis à un relais d'audit ou à un référentiel, ils sont stockés dans une file d'attente de disques. Si la file d'attente des disques est saturée, des pannes peuvent se produire. Pour vous permettre de répondre dans le temps afin d'éviter une panne, des alarmes AMQS sont déclenchées lorsque le nombre de messages dans la file d'attente du disque atteint les seuils suivants : • Remarque : plus de 100,000 messages • Mineur : au moins 500,000 messages • Majeur : au moins 2,000,000 messages • Critique : au moins 5,000,000 messages Si une alarme AMQS est déclenchée, vérifiez la charge sur le système --s'il y a eu un nombre important de transactions, l'alarme doit se résoudre au fil du temps. Dans ce cas, vous pouvez ignorer l'alarme. Si l'alarme persiste et augmente la gravité, affichez un graphique de la taille de la file d'attente. Si ce chiffre augmente régulièrement au fil des heures ou des jours, la charge d'audit a probablement dépassé la capacité d'audit du système. Réduisez le taux de fonctionnement du client ou diminuez le nombre de messages d'audit consignés en changeant le niveau d'audit sur erreur ou Désactivé. Voir "Configurez les messages d'audit et les destinations des journaux".

Code	Nom	Service	Action recommandée
AOTE	État du magasin	BARC	Disponible uniquement pour les nœuds d'archivage avec un type cible de Tivoli Storage Manager (TSM). Si la valeur de l'état du magasin attend la cible, vérifiez le système de stockage d'archives externe et assurez-vous qu'il fonctionne correctement. Si le nœud d'archivage vient d'être ajouté au système StorageGRID, assurez-vous que la connexion du nœud d'archivage au système de stockage d'archives externe cible est correctement configurée. Si la valeur de l'état du magasin est hors ligne, vérifiez la valeur de l'état du magasin. Corrigez tout problème avant de remettre l'état du magasin en ligne.
AOTU	État du magasin	BARC	Si la valeur Etat de stockage est session perdue, vérifiez que le système de stockage d'archives externe est connecté et en ligne. Si la valeur erreur cible est définie, recherchez des erreurs dans le système de stockage d'archives externe. Si la valeur de l'état du stockage est erreur inconnue, contactez le support technique.
APMS	Connectivité multivoie du stockage	SSM	Si l'alarme d'état multichemin apparaît en tant que "en mode image" (sélectionnez **SUPPORT** > **Outils** > **topologie de grille**, puis sélectionnez ***site*** > ***grid node*** > **SSM** > **Events**), procédez comme suit : 1. Branchez ou remplacez le câble qui n'affiche aucun voyant. 2. Attendez une à cinq minutes. Ne débranchez pas l'autre câble au moins cinq minutes après avoir branché le premier câble. Un débranchement trop précoce peut entraîner la lecture seule du volume racine, ce qui nécessite le redémarrage du matériel. 3. Retournez à la page **SSM** > **Ressources** et vérifiez que l'état "`Degraded"' Multipath a été modifié en ""nominal" dans la section Storage Hardware.

Code	Nom	Service	Action recommandée
ARCE	État DE L'ARC	ARC	Le service ARC dispose d'un état de veille jusqu'à ce que tous les composants ARC (réplication, stockage, récupération, cible) aient démarré. Il passe ensuite en ligne. Si la valeur de l'état ARC ne passe pas du mode Veille au mode en ligne, vérifier l'état des composants ARC. Si la valeur de l'état ARC est hors ligne, redémarrer le service. Si le problème persiste, contactez le support technique.
AROQ	Objets mis en file d'attente	ARC	Cette alarme peut être déclenchée si le périphérique de stockage amovible fonctionne lentement en raison de problèmes avec le système de stockage d'archives externes ciblé ou si plusieurs erreurs de lecture sont détectées. Vérifiez que le système de stockage d'archives externe ne présente pas d'erreurs et assurez-vous qu'il fonctionne correctement. Dans certains cas, cette erreur peut survenir en raison d'un taux élevé de demandes de données. Surveillez le nombre d'objets mis en file d'attente lorsque l'activité du système diminue.

Code	Nom	Service	Action recommandée
ARRF	Échecs de demande	ARC	Si une récupération à partir du système de stockage d'archives externe cible échoue, le nœud d'archivage retente l'extraction car la défaillance peut être due à un problème transitoire. Cependant, si les données de l'objet sont corrompues ou si elles ont été marquées comme étant définitivement indisponibles, la récupération n'échoue pas. En revanche, le nœud d'archivage tente continuellement la récupération et la valeur des échecs de demande continue d'augmenter. Cette alarme peut indiquer que le support de stockage contenant les données demandées est corrompu. Vérifiez le système de stockage d'archives externe pour diagnostiquer le problème. Si vous déterminez que les données d'objet ne sont plus dans l'archive, l'objet devra être supprimé du système StorageGRID. Pour plus d'informations, contactez le support technique. Une fois le problème qui a déclenché cette alarme résolu, réinitialisez le nombre de défaillances. Sélectionnez **SUPPORT** > **Outils** > **topologie de grille**. Sélectionnez ensuite ***site*** > ***grid node*** > **ARC** > **Retrieve** > **Configuration** > **main**, sélectionnez **Réinitialiser le nombre d'échecs de demande** et cliquez sur **appliquer les modifications**.
ARRV	Échecs de vérification	ARC	Pour diagnostiquer et corriger ce problème, contactez le support technique. Une fois le problème qui a déclenché cette alarme résolu, réinitialisez le nombre de défaillances. Sélectionnez **SUPPORT** > **Outils** > **topologie de grille**. Sélectionnez ensuite ***site*** > ***grid node*** > **ARC** > **Retrieve** > **Configuration** > **main**, sélectionnez **Réinitialiser le nombre d'échecs de vérification** et cliquez sur **appliquer les changements**.

Code	Nom	Service	Action recommandée
ARVF	Échecs de stockage	ARC	Cette alarme peut survenir en raison d'erreurs avec le système de stockage d'archives externes ciblé. Vérifiez que le système de stockage d'archives externe ne présente pas d'erreurs et assurez-vous qu'il fonctionne correctement. Une fois le problème qui a déclenché cette alarme résolu, réinitialisez le nombre de défaillances. Sélectionnez **SUPPORT** > **Outils** > **topologie de grille**. Sélectionnez ensuite ***site*** > ***grid node*** > **ARC** > **Retrieve** > **Configuration** > **main**, sélectionnez **Réinitialiser le nombre d'échecs de stockage** et cliquez sur **appliquer les changements**.
ASXP	Partages d'audit	AMS	Une alarme est déclenchée si la valeur des partages d'audit est inconnue. Cette alarme peut indiquer un problème d'installation ou de configuration du nœud d'administration. Si le problème persiste, contactez le support technique.
AUMA	Statut AMS	AMS	Si la valeur de l'état AMS est erreur de connectivité DB, redémarrez le nœud de la grille. Si le problème persiste, contactez le support technique.
AUME	État AMS	AMS	Si la valeur de l'état AMS est Veille, continuez à surveiller le système StorageGRID. Si le problème persiste, contactez le support technique. Si la valeur de l'état AMS est hors ligne, redémarrez le service. Si le problème persiste, contactez le support technique.
AUXS	Audit de l'état d'exportation	AMS	Si une alarme se déclenche, corrigez le problème sous-jacent, puis redémarrez le service AMS. Si le problème persiste, contactez le support technique.
BADD	Nombre de disques défaillants du contrôleur de stockage	SSM	Cette alarme se déclenche lorsqu'un ou plusieurs disques d'une appliance StorageGRID sont défectueux ou non optimaux. Remplacez les disques si nécessaire.

Code	Nom	Service	Action recommandée
BASF	Identificateurs d'objet disponibles	CMN	Lorsqu'un système StorageGRID est provisionné, le service CMN reçoit un nombre fixe d'identifiants d'objets. Cette alarme se déclenche lorsque le système StorageGRID commence à épuiser sa fourniture d'identifiants d'objets. Pour attribuer davantage d'identifiants, contactez le support technique.
BASSES	Identificateur de l'état d'allocation de bloc	CMN	Par défaut, une alarme est déclenchée lorsque les identificateurs d'objet ne peuvent pas être attribués car le quorum ADC ne peut pas être atteint. L'allocation de bloc d'identificateur sur le service CMN requiert un quorum (50 % + 1) des services ADC pour être connectés et en ligne. Si le quorum n'est pas disponible, le service CMN ne peut pas allouer de nouveaux blocs d'identification tant que le quorum ADC n'est pas rétabli. En cas de perte du quorum ADC, il n'y a généralement aucun impact immédiat sur le système StorageGRID (les clients peuvent toujours récupérer et récupérer le contenu), car la quantité d'identifiants d'un mois environ est mise en cache ailleurs dans le réseau ; Cependant, si la condition persiste, le système StorageGRID perdra la possibilité d'ingérer un nouveau contenu. Si une alarme est déclenchée, recherchez la raison de la perte du quorum ADC (par exemple, il peut s'agir d'une défaillance du réseau ou du nœud de stockage) et prenez des mesures correctives. Si le problème persiste, contactez le support technique.
BRDT	Température du châssis du contrôleur de calcul	SSM	Une alarme est déclenchée si la température du contrôleur de calcul d'une appliance StorageGRID dépasse le seuil nominal. Vérifier si les composants matériels et les problèmes environnementaux sont en surchauffe. Si nécessaire, remplacer l'organe.

Code	Nom	Service	Action recommandée
POINT DE FIN	Décalage	BADC, BLDR, BNMS, BAMS, BCLB, BCMN, BARC	Une alarme se déclenche si l'heure d'entretien (secondes) diffère sensiblement de l'heure du système d'exploitation. Dans des conditions normales, le service doit se resynchroniser. Si le temps d'entretien dépasse trop loin du temps du système d'exploitation, le fonctionnement du système peut être affecté. Vérifiez que la source de temps du système StorageGRID est correcte. Si le problème persiste, contactez le support technique.
BTSE	État de l'horloge	BADC, BLDR, BNMS, BAMS, BCLB, BCMN, BARC	Une alarme se déclenche si l'heure du service n'est pas synchronisée avec l'heure suivie par le système d'exploitation. Dans des conditions normales, le service doit se resynchroniser. Si le temps dérive trop loin du temps du système d'exploitation, le fonctionnement du système peut être affecté. Vérifiez que la source de temps du système StorageGRID est correcte. Si le problème persiste, contactez le support technique.
CAHP	Pourcentage d'utilisation du tas Java	DDS	Une alarme se déclenche si Java ne parvient pas à effectuer la collecte des déchets à un rythme qui permet au système de disposer d'un espace suffisant pour fonctionner correctement. Une alarme peut indiquer une charge de travail d'utilisateur dépassant les ressources disponibles sur le système pour le magasin de métadonnées DDS. Vérifiez l'activité ILM dans le tableau de bord ou sélectionnez **SUPPORT** > **Outils** > **topologie de grille**, puis sélectionnez ***site*** > ***GRID node*** > **DDS** > **Resources** > **Overview** > **main**. Si le problème persiste, contactez le support technique.

Code	Nom	Service	Action recommandée
CASA	État de la banque de données	DDS	Une alarme est déclenchée si le magasin de métadonnées Cassandra n'est plus disponible. Vérifier l'état de Cassandra : 1. Sur le nœud de stockage, connectez-vous en tant qu'administrateur et `su` Pour s'identifier à l'aide du mot de passe indiqué dans le fichier Passwords.txt. 2. Entrez : `service cassandra status` 3. Si Cassandra n'est pas en cours d'exécution, redémarrez-le : `service cassandra restart` Cette alarme peut également indiquer que le magasin de métadonnées (base de données Cassandra) pour un nœud de stockage nécessite une reconstruction. Reportez-vous aux informations relatives au dépannage de l'alarme Services : état - Cassandra (SVST) dans "Diagnostiquez les problèmes liés aux métadonnées". Si le problème persiste, contactez le support technique.
CASSE	État du magasin de données	DDS	Cette alarme est déclenchée lors de l'installation ou de l'extension pour indiquer qu'un nouveau magasin de données rejoint la grille.
CCNE	Matériel de calcul	SSM	Cette alarme est déclenchée si l'état du matériel du contrôleur de calcul d'une appliance StorageGRID nécessite une intervention.

Code	Nom	Service	Action recommandée
CDLP	Espace utilisé pour les métadonnées (en %)	DDS	Cette alarme se déclenche lorsque l'espace effectif des métadonnées (CEMS) atteint 70 % (alarme mineure), 90 % (alarme majeure) et 100 % (alarme critique). Si cette alarme atteint le seuil de 90 %, un avertissement apparaît sur le tableau de bord dans le Gestionnaire de grille. Vous devez effectuer une procédure d'extension pour ajouter de nouveaux nœuds de stockage dès que possible. Voir "Développez votre grille". Si cette alarme atteint le seuil de 100 %, vous devez arrêter d'ingérer immédiatement des objets et ajouter des nœuds de stockage. Cassandra exige un certain espace pour effectuer les opérations essentielles telles que le compactage et la réparation. Ces opérations seront affectées si les métadonnées de l'objet utilisent plus de 100 % de l'espace autorisé. Des résultats indésirables peuvent survenir. **Remarque** : contactez le support technique si vous ne pouvez pas ajouter de nœuds de stockage. Une fois que de nouveaux nœuds de stockage sont ajoutés, le système rééquilibre automatiquement les métadonnées d'objet sur tous les nœuds de stockage, et l'alarme est supprimée. Consultez également les informations relatives au dépannage de l'alerte de stockage de métadonnées faible dans "Diagnostiquez les problèmes liés aux métadonnées". Si le problème persiste, contactez le support technique.
CMNA	État CMN	CMN	Si la valeur de l'état CMN est erreur, sélectionnez **SUPPORT** > **Outils** > **topologie de grille**, puis sélectionnez ***site*** > ***grid node*** > **CMN** > **Présentation** > **main** et **CMN** > **alarmes** > **main** pour déterminer la cause de l'erreur et résoudre le problème. Une alarme est déclenchée et la valeur de l'état CMN est pas de CMN en ligne lors d'une actualisation matérielle du nœud d'administration principal lorsque les CMN sont commutés (la valeur de l'ancien état CMN est en attente et la nouvelle est en ligne). Si le problème persiste, contactez le support technique.

Code	Nom	Service	Action recommandée
CPRC	Capacité restante	NMS	Une alarme se déclenche si la capacité restante (nombre de connexions disponibles pouvant être ouvertes à la base de données NMS) est inférieure à la gravité configurée pour l'alarme. Si une alarme est déclenchée, contactez le support technique.
CPSA	Alimentation a du contrôleur de calcul	SSM	Une alarme est déclenchée en cas de problème au niveau de l'alimentation A du contrôleur de calcul d'une appliance StorageGRID. Si nécessaire, remplacer l'organe.
CPSB	Alimentation B du contrôleur de calcul	SSM	Une alarme est déclenchée en cas de problème au niveau de l'alimentation B du contrôleur de calcul d'une appliance StorageGRID. Si nécessaire, remplacer l'organe.
CPUT	Température du processeur du contrôleur de calcul	SSM	Une alarme est déclenchée si la température du CPU du contrôleur de calcul d'une appliance StorageGRID dépasse le seuil nominal. Si le nœud de stockage est une appliance StorageGRID, le système StorageGRID indique que le contrôleur nécessite une intervention. Vérifier si les composants matériels et les problèmes d'environnement sont en surchauffe. Si nécessaire, remplacer l'organe.
DNST	État DNS	SSM	Une fois l'installation terminée, une alarme DNST est déclenchée dans le service SSM. Une fois que le DNS est configuré et que les nouvelles informations de serveur atteignent tous les nœuds de la grille, l'alarme est annulée.

Code	Nom	Service	Action recommandée
ECCD	Fragments corrompus détectés	LDR	Une alarme se déclenche lorsque le processus de vérification en arrière-plan détecte un fragment codé d'effacement corrompu. Si un fragment corrompu est détecté, une tentative de reconstruction du fragment est effectuée. Réinitialisez les fragments corrompus détectés et copie les attributs perdus à zéro et surveillez-les pour voir si les comptages sont à nouveau affichés. Si le nombre augmente, le stockage sous-jacent du nœud de stockage peut être problématique. Une copie des données d'objet avec code d'effacement n'est pas considérée comme manquante tant que le nombre de fragments perdus ou corrompus n'enfreint pas la tolérance aux pannes du code d'effacement. Il est donc possible d'avoir un fragment corrompu et de pouvoir récupérer l'objet. Si le problème persiste, contactez le support technique.
ECST	État de vérification	LDR	Cette alarme indique l'état actuel du processus de vérification en arrière-plan des données d'objet avec code d'effacement sur ce nœud de stockage. Une alarme majeure est déclenchée en cas d'erreur dans le processus de vérification en arrière-plan.
FONPN	Ouvrez les descripteurs de fichier	BADC, BAMS, BARC, BCLB, BCMN, BLDR, BNMS, BSSM, BDDS	Le FOPN peut devenir grand pendant l'activité de pointe. S'il ne diminue pas pendant des périodes de ralentissement d'activité, contacter le support technique.
HSTE	État HTTP	BLDR	Voir les actions recommandées pour HSTU.

Code	Nom	Service	Action recommandée
HSTU	Statut HTTP	BLDR	HSTE et HSTU sont liés au protocole HTTP pour tout le trafic LDR, y compris S3, Swift et autres trafics StorageGRID internes. Une alarme indique que l'une des situations suivantes s'est produite : • HTTP a été mis hors ligne manuellement. • L'attribut HTTP de démarrage automatique a été désactivé. • Le service LDR est en cours de fermeture. L'attribut Auto-Start HTTP est activé par défaut. Si ce paramètre est modifié, HTTP peut rester hors ligne après un redémarrage. Si nécessaire, attendez que le service LDR redémarre. Sélectionnez **SUPPORT** > **Outils** > **topologie de grille**. Sélectionnez ensuite ***Storage Node*** > **LDR** > **Configuration**. Si HTTP est hors ligne, mettez-le en ligne. Vérifiez que l'attribut Auto-Start HTTP est activé. Si HTTP reste hors ligne, contactez le support technique.
HTA	Démarrage automatique HTTP	LDR	Spécifie si les services HTTP doivent démarrer automatiquement au démarrage. Il s'agit d'une option de configuration spécifiée par l'utilisateur.
IRSU	État de la réplication entrante	BLDR, BARC	Une alarme indique que la réplication entrante a été désactivée. Confirmer les paramètres de configuration : sélectionnez **SUPPORT** > **Outils** > **topologie de grille**. Sélectionnez ensuite ***site*** > ***grid node*** > **LDR** > **Replication** > **Configuration** > **main**.

Code	Nom	Service	Action recommandée
LATA	Latence moyenne	NMS	Vérifiez les problèmes de connectivité. Vérifiez l'activité du système pour confirmer qu'il y a une augmentation de l'activité du système. Une augmentation de l'activité système entraînera une augmentation de l'activité des données d'attribut. Cette augmentation de l'activité entraînera un retard dans le traitement des données d'attribut. Il peut s'agir d'une activité normale du système et se subside. Rechercher des alarmes multiples. Une augmentation des temps de latence moyens peut être indiquée par un nombre excessif d'alarmes déclenchées. Si le problème persiste, contactez le support technique.
LDRE	Etat LDR	LDR	Si la valeur de l'Etat LDR est en attente, continuez à suivre la situation et si le problème persiste, contactez l'assistance technique. Si la valeur de LDR State est hors ligne, redémarrez le service. Si le problème persiste, contactez le support technique.
PERDU	Objets perdus	DDS, LDR	Déclenché lorsque le système StorageGRID ne parvient pas à extraire une copie de l'objet demandé à partir de n'importe quel emplacement du système. Avant le déclenchement d'une alarme PERDUE (objets perdus), le système tente de récupérer et de remplacer un objet manquant ailleurs dans le système. Les objets perdus représentent une perte de données. L'attribut objets perdus est incrémenté chaque fois que le nombre d'emplacements d'un objet passe à zéro sans que le service DDS purge automatiquement le contenu pour satisfaire la stratégie ILM. Rechercher immédiatement les alarmes PERDUES (objets PERDUS). Si le problème persiste, contactez le support technique. "Dépanner les données d'objet perdues ou manquantes"

Code	Nom	Service	Action recommandée
MCEP	Expiration du certificat de l'interface de gestion	CMN	Déclenché lorsque le certificat utilisé pour accéder à l'interface de gestion est sur le point d'expirer. 1. Dans Grid Manager, sélectionnez **CONFIGURATION** > **sécurité** > **certificats**. 2. Dans l'onglet **Global**, sélectionnez **Management interface certificate**. 3. "Télécharger un nouveau certificat d'interface de gestion."
MINQ	Notifications par e-mail en file d'attente	NMS	Vérifiez les connexions réseau des serveurs hébergeant le service NMS et le serveur de messagerie externe. Vérifiez également que la configuration du serveur de messagerie est correcte. "Configuration des paramètres du serveur de messagerie pour les alarmes (système hérité)"
MINUTES	Statut des notifications par e-mail	BNMS	Une alarme mineure se déclenche si le service NMS ne parvient pas à se connecter au serveur de messagerie. Vérifiez les connexions réseau des serveurs hébergeant le service NMS et le serveur de messagerie externe. Vérifiez également que la configuration du serveur de messagerie est correcte. "Configuration des paramètres du serveur de messagerie pour les alarmes (système hérité)"
MLLE	État du moteur d'interface NMS	BNMS	Une alarme se déclenche si le moteur d'interface NMS du nœud d'administration qui collecte et génère du contenu d'interface est déconnecté du système. Cochez Server Manager pour déterminer si l'application individuelle du serveur est en panne.
NANG	Paramètre de négociation automatique du réseau	SSM	Vérifiez la configuration de la carte réseau. Le paramètre doit correspondre aux préférences de vos routeurs et commutateurs réseau. Un réglage incorrect peut avoir un impact important sur les performances du système.
NUP	Paramètre duplex réseau	SSM	Vérifiez la configuration de la carte réseau. Le paramètre doit correspondre aux préférences de vos routeurs et commutateurs réseau. Un réglage incorrect peut avoir un impact important sur les performances du système.

Code	Nom	Service	Action recommandée
NLNK	Détection de la liaison réseau	SSM	Vérifiez les connexions des câbles réseau sur le port et au niveau du commutateur. Vérifiez les configurations du routeur, du commutateur et de la carte réseau. Redémarrez le serveur. Si le problème persiste, contactez le support technique.
NRER	Erreurs de réception	SSM	Les causes suivantes peuvent être des alarmes NRER : • Correction d'erreur de marche avant (FEC) non compatible • Le port du commutateur et la MTU de la carte réseau ne correspondent pas • Taux d'erreur de liaison élevés • Dépassement de la mémoire tampon de la sonnerie NIC Voir les informations sur le dépannage de l'alarme d'erreur de réception réseau (NRER) dans "Résolution des problèmes de réseau, de matériel et de plateforme".
NRLY	Relais d'audit disponibles	BADC, BARC, BCLB, BCMN, BLDR, BNMS, BDDS	Si les relais d'audit ne sont pas connectés aux services ADC, les événements d'audit ne peuvent pas être signalés. Elles sont mises en file d'attente et indisponibles aux utilisateurs jusqu'à ce que la connexion soit restaurée. Rétablir la connectivité avec un service ADC dès que possible. Si le problème persiste, contactez le support technique.
NSCA	Etat NMS	NMS	Si la valeur de NMS Status est DB Connectivity Error, redémarrez le service. Si le problème persiste, contactez le support technique.

Code	Nom	Service	Action recommandée
NSCE	Etat NMS	NMS	Si la valeur de l'état NMS est Veille, continuez à surveiller et si le problème persiste, contactez le support technique. Si la valeur de l'état NMS est hors ligne, redémarrez le service. Si le problème persiste, contactez le support technique.
NSPD	Vitesse	SSM	Cela peut être dû à des problèmes de connectivité réseau ou de compatibilité des pilotes. Si le problème persiste, contactez le support technique.
NTBR	Espace libre	NMS	Si une alarme est déclenchée, vérifiez la rapidité d'utilisation de la base de données. Une chute soudaine (par opposition à un changement progressif dans le temps) indique une condition d'erreur. Si le problème persiste, contactez le support technique. Le réglage du seuil d'alarme vous permet de gérer de manière proactive les besoins de stockage supplémentaire. Si l'espace disponible atteint un seuil bas (voir seuil d'alarme), contactez le support technique pour modifier l'allocation de la base de données.
NTRE	Erreurs de transmission	SSM	Ces erreurs peuvent être résolues sans être réinitialisées manuellement. S'ils ne s'effacent pas, vérifiez le matériel réseau. Vérifiez que le matériel et le pilote de la carte sont correctement installés et configurés pour fonctionner avec vos routeurs et commutateurs réseau. Une fois le problème sous-jacent résolu, réinitialiser le compteur. Sélectionnez **SUPPORT** > **Outils** > **topologie de grille**. Sélectionnez ensuite ***site*** > ***grid node*** > **SSM** > **Resources** > **Configuration** > **main**, sélectionnez **Réinitialiser le nombre d'erreurs de transmission** et cliquez sur **appliquer les modifications**.
NTFQ	Décalage de fréquence NTP	SSM	Si le décalage de fréquence dépasse le seuil configuré, il y a probablement un problème matériel avec l'horloge locale. Si le problème persiste, contactez l'assistance technique pour organiser un remplacement.

Code	Nom	Service	Action recommandée
NTPL	Verrouillage NTP	SSM	Si le démon NTP n'est pas verrouillé sur une source de temps externe, vérifiez la connectivité réseau aux sources de temps externes désignées, leur disponibilité et leur stabilité.
NTOF	Décalage horaire NTP	SSM	Si le décalage dépasse le seuil configuré, il y a probablement un problème matériel avec l'oscillateur de l'horloge locale. Si le problème persiste, contactez l'assistance technique pour organiser un remplacement.
NTSJ	Jitter de la source horaire choisie	SSM	Cette valeur indique la fiabilité et la stabilité de la source de temps que NTP sur le serveur local utilise comme référence. Si une alarme est déclenchée, cela peut indiquer que l'oscillateur de la source de temps est défectueux ou qu'il y a un problème avec la liaison WAN à la source de temps.
NTSU	État NTP	SSM	Si la valeur de l'état NTP n'est pas en cours d'exécution, contactez le support technique.
OPST	État général de l'alimentation	SSM	Une alarme se déclenche si l'alimentation d'un appareil StorageGRID diffère de la tension de fonctionnement recommandée. Vérifier l'état du bloc d'alimentation A ou B pour déterminer quelle alimentation fonctionne normalement. Si nécessaire remplacer l'alimentation.
OQRT	Objets en quarantaine	LDR	Une fois les objets restaurés automatiquement par le système StorageGRID, les objets mis en quarantaine peuvent être supprimés du répertoire de quarantaine. 1. Sélectionnez **SUPPORT** > **Outils** > **topologie de grille**. 2. Sélectionnez **site** > **Storage Node** > **LDR** > **Verification** > **Configuration** > **main**. 3. Sélectionnez **Supprimer les objets en quarantaine**. 4. Cliquez sur **appliquer les modifications**. Les objets mis en quarantaine sont supprimés et le nombre est remis à zéro.

Code	Nom	Service	Action recommandée
ORSU	État de la réplication sortante	BLDR, BARC	Une alarme indique que la réplication sortante n'est pas possible : le stockage est dans un état où les objets ne peuvent pas être récupérés. Une alarme se déclenche si la réplication sortante est désactivée manuellement. Sélectionnez **SUPPORT** > **Outils** > **topologie de grille**. Sélectionnez ensuite ***site*** > ***grid node*** > **LDR** > **Replication** > **Configuration**. Une alarme est déclenchée si le service LDR n'est pas disponible pour la réplication. Sélectionnez **SUPPORT** > **Outils** > **topologie de grille**. Sélectionnez ensuite ***site*** > ***grid node*** > **LDR** > **Storage**.
SLF	État du tiroir	SSM	Une alarme est déclenchée si l'état de l'un des composants du tiroir de stockage d'une appliance de stockage est dégradé. Les composants des tiroirs de stockage incluent les IOM, les ventilateurs, les alimentations et les tiroirs disques.si cette alarme se déclenche, consultez les instructions de maintenance de votre appliance.
PMEM	Utilisation de la mémoire de service (pourcentage)	BADC, BAMS, BARC, BCLB, BCMN, BLDR, BNMS, BSSM, BDDS	Peut avoir une valeur supérieure à y% RAM, où y représente le pourcentage de mémoire utilisé par le serveur. Les chiffres inférieurs à 80 % sont normaux. Plus de 90 % sont considérés comme un problème. Si l'utilisation de la mémoire est élevée pour un seul service, surveillez la situation et recherchez. Si le problème persiste, contactez le support technique.
PSAS	État de l'alimentation Électrique A	SSM	Une alarme se déclenche si l'alimentation A d'un appareil StorageGRID diffère de la tension de fonctionnement recommandée. Si nécessaire remplacer l'alimentation A.
PSB	État de l'alimentation B	SSM	Une alarme se déclenche si l'alimentation B d'un appareil StorageGRID diffère de la tension de fonctionnement recommandée. Si nécessaire remplacer l'alimentation B.

Code	Nom	Service	Action recommandée
RTTD	État de Tivoli Storage Manager	BARC	Disponible uniquement pour les nœuds d'archivage avec un type cible de Tivoli Storage Manager (TSM). Si la valeur de l'état Tivoli Storage Manager est hors ligne, vérifiez l'état de Tivoli Storage Manager et résolvez les problèmes éventuels. Remettre le composant en ligne. Sélectionnez **SUPPORT** > **Outils** > **topologie de grille**. Sélectionnez ensuite ***site*** > ***grid node*** > **ARC** > **cible** > **Configuration** > **main**, sélectionnez **Tivoli Storage Manager State** > **Online**, puis cliquez sur **appliquer les modifications**.
RTU	Statut de Tivoli Storage Manager	BARC	Disponible uniquement pour les nœuds d'archivage avec un type cible de Tivoli Storage Manager (TSM). Si la valeur de l'état de Tivoli Storage Manager est erreur de configuration et que le nœud d'archivage vient d'être ajouté au système StorageGRID, assurez-vous que le serveur middleware TSM est correctement configuré. Si la valeur de l'état de Tivoli Storage Manager est échec de la connexion ou échec de la connexion, essayez de nouveau, vérifiez la configuration réseau sur le serveur middleware TSM et la connexion réseau entre le serveur middleware TSM et le système StorageGRID. Si la valeur de l'état de Tivoli Storage Manager est échec de l'authentification, ou échec de l'authentification, reconnexion, le système StorageGRID peut se connecter au serveur middleware TSM, mais ne peut pas authentifier la connexion. Vérifiez que le serveur middleware TSM est configuré avec l'utilisateur, le mot de passe et les autorisations appropriés, puis redémarrez le service. Si la valeur de Tivoli Storage Manager Status est session Failure (échec de session), une session établie a été perdue de manière inattendue. Vérifiez la connexion réseau entre le serveur middleware TSM et le système StorageGRID. Vérifiez que le serveur middleware ne comporte pas d'erreurs. Si la valeur de l'état de Tivoli Storage Manager est erreur inconnue, contactez l'assistance technique.

Code	Nom	Service	Action recommandée
RRF	Réplications entrantes — échec	BLDR, BARC	Une alarme de répétition entrante — une alarme de défaillance peut se produire pendant des périodes de charge élevée ou de perturbations temporaires du réseau. Une fois l'activité du système réduite, cette alarme doit être déclenchée. Si le nombre de réplications ayant échoué continue à augmenter, recherchez des problèmes réseau et vérifiez que les services LDR et ARC source et destination sont en ligne et disponibles. Pour réinitialiser le nombre, sélectionnez **SUPPORT** > **Outils** > **topologie de grille**, puis sélectionnez ***site*** > ***grid node*** > **LDR** > **Replication** > **Configuration** > **main**. Sélectionnez **Réinitialiser le nombre d'échecs de réplication entrants**, puis cliquez sur **appliquer les modifications**.
RIRQ	Réplications entrantes — en file d'attente	BLDR, BARC	Des alarmes peuvent se produire en cas de charge élevée ou d'interruption temporaire du réseau. Une fois l'activité du système réduite, cette alarme doit être déclenchée. Si le nombre de réplications en file d'attente continue à augmenter, recherchez des problèmes réseau et vérifiez que les services LDR et ARC source et destination sont en ligne et disponibles.
RORQ	Réplications sortantes — en file d'attente	BLDR, BARC	La file d'attente de réplication sortante contient des données d'objet copiées afin de satisfaire les règles ILM et les objets requis par les clients. Une alarme peut se produire suite à une surcharge du système. Attendez que l'alarme s'efface lorsque l'activité du système diminue. Si l'alarme se répète, ajoutez de la capacité en ajoutant des nœuds de stockage.
VICE-PRÉSIDENT SAVP	Espace utilisable total (pourcentage)	LDR	Si l'espace utilisable atteint un seuil minimal, options incluent l'extension du système StorageGRID ou le déplacement des données d'objet vers l'archivage via un nœud d'archivage.

Code	Nom	Service	Action recommandée
SCA	État	CMN	Si la valeur Etat de la tâche de grille active est erreur, recherchez le message de tâche de grille. Sélectionnez **SUPPORT** > **Outils** > **topologie de grille**. Sélectionnez ensuite ***site*** > ***grid node*** > **CMN** > **Grid Tasks** > **Overview** > **main**. Le message de tâche de grille affiche des informations sur l'erreur (par exemple, « échec de la vérification sur le nœud 12130011 »). Après avoir examiné et corrigé le problème, redémarrez la tâche de grille. Sélectionnez **SUPPORT** > **Outils** > **topologie de grille**. Sélectionnez ensuite ***site*** > ***grid node*** > **CMN** > **Grid Tasks** > **Configuration** > **main** et sélectionnez **actions** > **Exécuter**. Si la valeur Etat d'une tâche de grille en cours d'arrêt est erreur, réessayez de mettre fin à la tâche de grille. Si le problème persiste, contactez le support technique.
SCEP	Expiration du certificat des terminaux du service d'API de stockage	CMN	Déclenché lorsque le certificat utilisé pour accéder aux terminaux de l'API de stockage arrive à expiration. 1. Sélectionnez **CONFIGURATION** > **sécurité** > **certificats**. 2. Dans l'onglet **Global**, sélectionnez **S3 et certificat API Swift**. 3. "Téléchargez un nouveau certificat API S3 et Swift."
SCHR	État	CMN	Si la valeur Etat de la tâche de grille historique est abandonnée, recherchez la raison et exécutez à nouveau la tâche si nécessaire. Si le problème persiste, contactez le support technique.
SCSA	Contrôleur de stockage A	SSM	Une alarme est déclenchée en cas de problème au niveau du contrôleur de stockage A dans une appliance StorageGRID. Si nécessaire, remplacer l'organe.

Code	Nom	Service	Action recommandée
SCSB	Contrôleur de stockage B	SSM	Une alarme est déclenchée en cas de problème au niveau du contrôleur de stockage B dans une appliance StorageGRID. Si nécessaire, remplacer l'organe. Certains modèles d'appliance ne disposent pas de contrôleur de stockage B.
SHLH	Santé	LDR	Si la valeur de l'option Santé d'un magasin d'objets est erreur, vérifiez et corrigez : • problèmes avec le volume monté • erreurs du système de fichiers
SLSA	Moyenne de charge CPU	SSM	Plus la valeur est élevée, plus le système est occupé. Si la moyenne de charge CPU persiste à une valeur élevée, le nombre de transactions dans le système doit être examiné afin de déterminer si cela est dû à une charge importante à ce moment-là. Afficher un graphique de la moyenne de charge de la CPU : sélectionnez **SUPPORT** > **Outils** > **topologie de la grille**. Sélectionnez ensuite ***site*** > ***grid node*** > **SSM** > **Ressources** > **Rapports** > **graphiques**. Si la charge du système n'est pas importante et que le problème persiste, contactez le support technique.
SMST	Etat du moniteur de journal	SSM	Si la valeur de l'état de surveillance du journal n'est pas connectée pendant une période prolongée, contactez le support technique.

Code	Nom	Service	Action recommandée
SMTT	Nombre total d'événements	SSM	Si la valeur du total des événements est supérieure à zéro, vérifiez s'il existe des événements connus (tels que des défaillances réseau) pouvant en être la cause. Sauf si ces erreurs ont été effacées (c'est-à-dire que le nombre a été remis à 0), les alarmes Total Events peuvent être déclenchées. Lorsqu'un problème est résolu, réinitialisez le compteur pour effacer l'alarme. Sélectionnez **NODES** > ***site*** > ***grid node*** > **Events** > **Reset Event counts**. Pour réinitialiser le nombre d'événements, vous devez disposer de l'autorisation de configuration de la page de topologie de la grille. Si la valeur de Total Events est égale à zéro ou si le nombre augmente et que le problème persiste, contactez le support technique.
SNST	État	CMN	Une alarme indique qu'il y a un problème de stockage des lots de tâches de la grille. Si la valeur de l'état est erreur de point de contrôle ou si le quorum n'est pas atteint, confirmez qu'une majorité des services ADC sont connectés au système StorageGRID (50 % plus un) et patientez quelques minutes. Si le problème persiste, contactez le support technique.
SOSS	État du système d'exploitation de stockage	SSM	Une alarme est déclenchée si SANtricity OS indique qu'un composant d'une appliance StorageGRID présente un problème « nécessitant une attention particulière ». Sélectionnez **NOEUDS**. Sélectionnez ensuite **appliance Storage Node** > **Hardware**. Faites défiler vers le bas pour afficher l'état de chaque composant. Dans SANtricity OS, vérifiez les autres composants de l'appliance pour isoler le problème.
SSMA	État SSM	SSM	Si la valeur État SSM est erreur, sélectionnez **SUPPORT** > **Outils** > **topologie de grille**, puis sélectionnez ***site*** > ***grid node*** > **SSM** > **Présentation** > **main** et **SSM** > **Présentation** > **Survol** > **alarmes** pour déterminer la cause de l'alarme. Si le problème persiste, contactez le support technique.

Code	Nom	Service	Action recommandée
SSME	État SSM	SSM	Si la valeur de l'état SSM est Veille, continuez à surveiller et si le problème persiste, contactez le support technique. Si la valeur de l'état SSM est hors ligne, redémarrez le service. Si le problème persiste, contactez le support technique.
SST	État du stockage	BLDR	Si la valeur de l'état de stockage est insuffisant espace utilisable, il n'y a plus de stockage disponible sur le nœud de stockage et les ingoses de données sont redirigées vers un autre nœud de stockage disponible. Les demandes de récupération peuvent continuer à être fournies à partir de ce nœud de grille. Un stockage supplémentaire doit être ajouté. Elle n'a aucun impact sur les fonctionnalités de l'utilisateur final, mais l'alarme persiste tant que du stockage supplémentaire n'est pas ajouté. Si la valeur de l'état du stockage est Volume(s) indisponible(s), une partie du stockage est indisponible. Le stockage et la récupération de ces volumes ne sont pas possibles. Pour plus d'informations, sélectionnez **SUPPORT** > **Outils** > **topologie de grille**. Sélectionnez ensuite ***site*** > ***grid node*** > **LDR** > **Storage** > **Présentation** > **main**. L'état de santé du volume est répertorié sous magasins d'objets. Si la valeur de l'état de stockage est erreur, contactez le support technique. "Dépanner l'alarme Storage Status (SSTS)"

Code	Nom	Service	Action recommandée
VST	État	SSM	Cette alarme s'efface lorsque d'autres alarmes liées à un service non opérationnel sont résolues. Suivez les alarmes de service source pour rétablir le fonctionnement. Sélectionnez **SUPPORT** > **Outils** > **topologie de grille**. Sélectionnez ensuite ***site*** > ***grid node*** > **SSM** > **Services** > **Présentation** > **main**. Lorsque l'état d'un service est indiqué comme non en cours d'exécution, son état est désactivé d'un point de vue administratif. L'état du service peut être indiqué comme étant en cours d'exécution pour les raisons suivantes : • Le service a été arrêté manuellement (`/etc/init.d/<service\> stop`). • Il y a un problème avec la base de données MySQL et Server Manager arrête le service MI. • Un nœud de grille a été ajouté, mais pas démarré. • Pendant l'installation, un nœud de grille n'est pas encore connecté au nœud d'administration. Si un service n'est pas en cours d'exécution, redémarrez-le (`/etc/init.d/<service\> restart`). Cette alarme peut également indiquer que le magasin de métadonnées (base de données Cassandra) pour un nœud de stockage nécessite une reconstruction. Si le problème persiste, contactez le support technique. "Dépanner l'alarme Services : Status - Cassandra (SVST)"
TMEM	Mémoire installée	SSM	Les nœuds exécutés avec moins de 24 Gio de mémoire installée peuvent entraîner des problèmes de performances et l'instabilité du système. La quantité de mémoire installée sur le système doit être augmentée à au moins 24 Gio.

Code	Nom	Service	Action recommandée
TPOP	Opérations en attente	ADC	Une file d'attente de messages peut indiquer que le service ADC est surchargé. Trop peu de services ADC peuvent être connectés au système StorageGRID. Dans un déploiement important, le service ADC peut nécessiter l'ajout de ressources de calcul, ou le système peut nécessiter des services ADC supplémentaires.
UMEM	Mémoire disponible	SSM	Si la RAM disponible est faible, déterminez s'il s'agit d'un problème matériel ou logiciel. S'il ne s'agit pas d'un problème matériel ou si la mémoire disponible est inférieure à 50 Mo (seuil d'alarme par défaut), contactez le support technique.
VMFI	Entrées disponibles	SSM	Cela indique que du stockage supplémentaire est nécessaire. Contactez l'assistance technique.
VMFR	Espace disponible	SSM	Si la valeur de l'espace disponible est trop faible (voir seuils d'alarme), il faut examiner si des fichiers journaux ne sont pas proportionnels ou si des objets prennent trop d'espace disque (voir seuils d'alarme) qui doivent être réduits ou supprimés. Si le problème persiste, contactez le support technique.
VMST	État	SSM	Une alarme est déclenchée si la valeur État du volume monté est Inconnu. Une valeur Inconnu ou Offline peut indiquer que le volume ne peut pas être monté ou accessible en raison d'un problème avec le périphérique de stockage sous-jacent.
VPRI	Priorité de vérification	BLDR, BARC	Par défaut, la valeur de la priorité de vérification est adaptative. Si la priorité de vérification est définie sur élevée, une alarme est déclenchée car la vérification du stockage peut ralentir le fonctionnement normal du service.

Code	Nom	Service	Action recommandée
VSTU	État de vérification de l'objet	BLDR	Sélectionnez **SUPPORT** > **Outils** > **topologie de grille**. Sélectionnez ensuite ***site*** > ***grid node*** > **LDR** > **Storage** > **Présentation** > **main**. Vérifiez si le système d'exploitation ne présente aucun signe d'erreur de périphérique de bloc ou de système de fichiers. Si la valeur de l'état de vérification de l'objet est erreur inconnue, elle indique généralement un problème matériel ou système de fichiers de bas niveau (erreur d'E/S) qui empêche la tâche de vérification du stockage d'accéder au contenu stocké. Contactez l'assistance technique.
XAMS	Référentiels d'audit inaccessibles	BADC, BARC, BCLB, BCMN, BLDR, BNMS	Vérifiez la connectivité réseau au serveur hébergeant le nœud d'administration. Si le problème persiste, contactez le support technique.

Référence des fichiers journaux

Référence des fichiers journaux : présentation

StorageGRID fournit des journaux utilisés pour capturer les événements, les messages de diagnostic et les conditions d'erreur. Il se peut que vous soyez invité à collecter les fichiers journaux et à les transférer au support technique pour faciliter le dépannage.

Les journaux sont classés comme suit :

- "Journaux du logiciel StorageGRID"
- "Journaux de déploiement et de maintenance"
- "Journaux de logiciels tiers"
- "Sur le bycast.log"

> Les détails fournis pour chaque type de journal sont fournis à titre de référence uniquement. Les journaux sont destinés au dépannage avancé par le support technique. Les techniques avancées qui impliquent la reconstruction de l'historique des problèmes à l'aide des journaux d'audit et des fichiers journaux de l'application sont hors de portée de ces instructions.

Accéder aux journaux

Pour accéder aux journaux, vous pouvez "collectez les fichiers journaux et les données système" à partir d'un ou plusieurs nœuds sous forme d'archive de fichier journal unique. Si le nœud d'administration principal n'est pas disponible ou ne parvient pas à atteindre un nœud spécifique, vous pouvez accéder à des fichiers journaux individuels pour chaque nœud de la grille comme suit :

1. Saisissez la commande suivante : `ssh admin@grid_node_IP`
2. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
3. Entrez la commande suivante pour passer à la racine : `su -`
4. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

Catégories de fichiers journaux

L'archive du fichier journal StorageGRID contient les journaux décrits pour chaque catégorie et les fichiers supplémentaires contenant des mesures et la sortie de la commande debug.

Emplacement d'archivage	Description
audit	Messages d'audit générés pendant le fonctionnement normal du système.
base-os-logs	Informations sur le système d'exploitation de base, notamment les versions d'images StorageGRID.
packs	Informations de configuration globale (bundles).
cassandra	Informations sur la base de données Cassandra et journaux de réparation de couches.
d'europe	Informations VCS sur le nœud actuel et les informations de groupe EC par ID de profil.
grille	Journaux de grille généraux, y compris le débogage (`bycast.log`) et `servermanager` journaux.
grid.xml	Le fichier de configuration du grid est partagé sur tous les nœuds.
hagroups	Metrics et journaux pour les groupes de haute disponibilité.
installer	`Gdu-server` et installer les journaux.
lumberjack.log	Messages de débogage liés à la collecte de journaux.
Lambda-arbitre	Journaux associés à la demande de proxy S3 Select.
Métriques	Journaux de service pour Grafana, Jaeger, node exportateur et Prometheus.
etcd	Journaux d'accès divers et d'erreurs.
mysql	La configuration de la base de données MariaDB et les journaux associés.
nette	Journaux générés par des scripts de mise en réseau et le service Dynap.

Emplacement d'archivage	Description
nginx	Fichiers et journaux de configuration de l'équilibreur de charge et de la fédération du grid. Inclut également les journaux de trafic Grid Manager et tenant Manager.
nginx-gw	Fichiers et journaux de configuration de l'équilibreur de charge et de la fédération du grid.
ntp	Fichier de configuration et journaux NTP.
os	Fichier d'état du nœud et du grid incluant les services `pid`.
autre	Fichiers journaux sous `/var/local/log` qui ne sont pas collectés dans d'autres dossiers.
diminution des	Informations de performances pour le CPU, la mise en réseau et les E/S de disque
données prometheus	Metrics Prometheus actuels si la collecte des journaux inclut des données Prometheus.
provisionnement	Journaux relatifs au processus de provisionnement de la grille.
radeau	Journaux de grappe raft utilisés dans les services de plate-forme.
ssh	Journaux liés à la configuration et au service SSH.
snmp	Configuration de l'agent SNMP et listes d'autorisation/refus d'alarme utilisées pour envoyer des notifications SNMP.
sockets-données	Données des sockets pour le débogage réseau.
system-commands.txt	Résultat des commandes du conteneur StorageGRID. Contient des informations sur le système, telles que la mise en réseau et l'utilisation du disque.

Journaux du logiciel StorageGRID

Les journaux StorageGRID vous permettent de résoudre les problèmes.

> Si vous souhaitez envoyer vos journaux à un serveur syslog externe ou modifier la destination des informations d'audit telles que `bycast.log` et `nms.log`, voir "Configurez les messages d'audit et les destinations des journaux".

Journaux StorageGRID généraux

Nom du fichier	Remarques	Ci-après
/var/local/log/bycast.log	Fichier de dépannage StorageGRID principal. Sélectionnez **SUPPORT** > **Outils** > **topologie de grille**. Sélectionnez ensuite ***site*** > ***Node*** > **SSM** > **Events**.	Tous les nœuds
/var/local/log/bycast-err.log	Contient un sous-ensemble de `bycast.log` (Messages avec ERREUR de gravité et CRITIQUE). Des messages CRITIQUES sont également affichés dans le système. Sélectionnez **SUPPORT** > **Outils** > **topologie de grille**. Sélectionnez ensuite ***site*** > ***Node*** > **SSM** > **Events**.	Tous les nœuds
/var/local/core/	Contient tous les fichiers core dump créés si le programme se termine anormalement. Les causes possibles sont les échecs d'assertion, les violations ou les retards de thread. **Note**: Le fichier `` `/var/local/core/kexec_cmd `` il existe généralement sur les nœuds d'appliance et n'indique pas d'erreur.	Tous les nœuds

Journaux liés au chiffrement

Nom du fichier	Remarques	Ci-après
/var/local/log/ssh-config-generation.log	Contient des journaux relatifs à la génération de configurations SSH et au rechargement de services SSH.	Tous les nœuds
/var/local/log/nginx/config-generation.log	Contient les journaux relatifs à la génération des configurations nginx et au rechargement des services nginx.	Tous les nœuds
/var/local/log/nginx-gw/config-generation.log	Contient les journaux relatifs à la génération des configurations nginx-gw (et au rechargement des services nginx-gw).	Nœuds d'administration et de passerelle
/var/local/log/update-cipher-configurations.log	Contient des journaux relatifs à la configuration des règles TLS et SSH.	Tous les nœuds

Journaux de fédération du grid

Nom du fichier	Remarques	Ci-après
/var/local/log/update_grid_federation_config.log	Contient les journaux relatifs à la génération des configurations nginx et nginx-gw pour les connexions de fédération de grille.	Tous les nœuds

Journaux NMS

Nom du fichier	Remarques	Ci-après
/var/local/log/nms.log	• Capture des notifications à partir du Grid Manager et du tenant Manager. • Capture les événements liés au fonctionnement du service NMS, par exemple, le traitement des alarmes, les notifications par e-mail et les modifications de configuration. • Contient des mises à jour de bundle XML résultant des modifications de configuration effectuées dans le système. • Contient des messages d'erreur liés au sous-échantillonnage de l'attribut effectué une fois par jour. • Contient les messages d'erreur du serveur Web Java, par exemple les erreurs de génération de page et les erreurs HTTP Status 500.	Nœuds d'administration
/var/local/log/nms.errlog	Contient des messages d'erreur relatifs aux mises à niveau de la base de données MySQL. Contient le flux erreur standard (stderr) des services correspondants. Il y a un fichier journal par service. Ces fichiers sont généralement vides, sauf en cas de problème avec le service.	Nœuds d'administration
/var/local/log/nms.requestlog	Contient des informations sur les connexions sortantes de l'API de gestion vers les services StorageGRID internes.	Nœuds d'administration

Journaux Server Manager

Nom du fichier	Remarques	Ci-après
/var/local/log/servermanager.log	Fichier journal de l'application Server Manager exécutée sur le serveur.	Tous les nœuds
/Var/local/log/GridstatBackend.errlog	Fichier journal de l'application back-end de l'interface utilisateur graphique de Server Manager.	Tous les nœuds
/var/local/log/gridstat.errlog	Fichier journal de l'interface graphique de Server Manager.	Tous les nœuds

Journaux des services StorageGRID

Nom du fichier	Remarques	Ci-après
/var/local/log/acct.errlog		Nœuds de stockage exécutant le service ADC
/var/local/log/adc.errlog	Contient le flux erreur standard (stderr) des services correspondants. Il y a un fichier journal par service. Ces fichiers sont généralement vides, sauf en cas de problème avec le service.	Nœuds de stockage exécutant le service ADC
/var/local/log/ams.errlog		Nœuds d'administration
/var/local/log/arc.errlog		Nœuds d'archivage
/var/local/log/cassandra/system.log	Informations pour le magasin de métadonnées (base de données Cassandra) pouvant être utilisées en cas de problème lors de l'ajout de nouveaux nœuds de stockage ou si la tâche de réparation nodetool cale.	Nœuds de stockage
/var/local/log/cassandra-reaper.log	Informations concernant le service Cassandra Reaper, qui répare les données de la base de données Cassandra.	Nœuds de stockage
/var/local/log/cassandra-reaper.errlog	Informations d'erreur pour le service Cassandra Reaper.	Nœuds de stockage
/var/local/log/chunk.errlog		Nœuds de stockage
/var/local/log/cmn.errlog		Nœuds d'administration

Nom du fichier	Remarques	Ci-après
/var/local/log/cms.errlog	Ce fichier journal peut être présent sur les systèmes qui ont été mis à niveau à partir d'une ancienne version de StorageGRID. Il contient des informations héritées.	Nœuds de stockage
/var/local/log/cts.errlog	Ce fichier journal est créé uniquement si le type cible est **Cloud Tiering - simple Storage Service (S3).**	Nœuds d'archivage
/var/local/log/dds.errlog		Nœuds de stockage
/var/local/log/dmv.errlog		Nœuds de stockage
/var/local/log/dylip*	Contient des journaux liés au service dynap, qui surveille la grille pour les modifications IP dynamiques et met à jour la configuration locale.	Tous les nœuds
/var/local/log/grafana.log	Journal associé au service Grafana, utilisé pour la visualisation des metrics dans Grid Manager.	Nœuds d'administration
/var/local/log/hagroups.log	Journal associé aux groupes haute disponibilité.	Nœuds d'administration et nœuds de passerelle
/var/local/log/hagroups_events.log	Suivi des changements d'état, tels que la transition de LA SAUVEGARDE vers LE MAÎTRE ou LE DÉFAUT.	Nœuds d'administration et nœuds de passerelle
/var/local/log/idnt.errlog		Nœuds de stockage exécutant le service ADC
/var/local/log/jaeger.log	Journal associé au service jaeger, qui est utilisé pour la collecte de traces.	Tous les nœuds
/var/local/log/kstn.errlog		Nœuds de stockage exécutant le service ADC

Nom du fichier	Remarques	Ci-après
/var/local/log/lambda*	Contient les journaux du service S3 Select.	Nœuds d'administration et de passerelle Seuls certains nœuds d'administration et de passerelle contiennent ce journal. Voir la "Exigences et limitations de S3 Select pour les nœuds d'administration et de passerelle".
/var/local/log/ldr.errlog		Nœuds de stockage
/var/local/log/miscd/*.log	Contient des journaux pour le service MISCd (démon de contrôle du service d'information), qui fournit une interface pour interroger et gérer les services sur d'autres nœuds et pour gérer les configurations environnementales sur le nœud, comme interroger l'état des services s'exécutant sur d'autres nœuds.	Tous les nœuds
/var/local/log/nginx/*.log	Contient des journaux pour le service nginx, qui agit comme un mécanisme d'authentification et de communication sécurisée pour divers services de réseau (comme Prometheus et Dynap) pour pouvoir communiquer avec les services sur d'autres nœuds via des API HTTPS.	Tous les nœuds
/var/local/log/nginx-gw/*.log	Contient les journaux généraux relatifs au service nginx-gw, y compris les journaux d'erreurs et les journaux des ports d'administration restreints sur les nœuds d'administration.	Nœuds d'administration et nœuds de passerelle
/var/local/log/nginx-gw/cgr-access.log.gz	Contient des journaux d'accès relatifs au trafic de réplication inter-grid.	Nœuds d'administration, nœuds de passerelle ou les deux, en fonction de la configuration de fédération grid. Uniquement disponible sur la grille de destination pour la réplication inter-grid.

Nom du fichier	Remarques	Ci-après
/var/local/log/nginx-gw/endpoint-access.log.gz	Contient des journaux d'accès pour le service Load Balancer, qui permet l'équilibrage de la charge du trafic S3 et Swift entre les clients et les nœuds de stockage.	Nœuds d'administration et nœuds de passerelle
/var/local/log/persistence*	Contient les journaux du service Persistence, qui gère les fichiers sur le disque racine qui doivent persister au cours d'un redémarrage.	Tous les nœuds
/var/local/log/prometheus.log	Pour tous les nœuds, il contient le journal de service de l'exportateur de nœuds et le journal des services de metrics de l'outil d'exportation de nœuds. Pour les nœuds d'administration, contient également les journaux des services Prometheus et Alert Manager.	Tous les nœuds
/var/local/log/raft.log	Contient la sortie de la bibliothèque utilisée par le service RSM pour le protocole de radeau.	Nœuds de stockage avec service RSM
/var/local/log/rms.errlog	Contient les journaux du service RSM (State machine Service) répliqué, qui est utilisé pour les services de plate-forme S3.	Nœuds de stockage avec service RSM
/var/local/log/ssm.errlog		Tous les nœuds
/var/local/log/update-s3vs-domains.log	Contient des journaux relatifs aux mises à jour de traitement pour la configuration des noms de domaine hébergés sur des serveurs virtuels S3.consultez les instructions d'implémentation des applications client S3.	Nœuds d'administration et de passerelle
/var/local/log/update-snmp-firewall.*	Contiennent des journaux relatifs aux ports de pare-feu gérés pour SNMP.	Tous les nœuds
/var/local/log/update-sysl.log	Contient des journaux relatifs aux modifications apportées à la configuration syslog du système.	Tous les nœuds

Nom du fichier	Remarques	Ci-après
/var/local/log/update-traffic-classes.log	Contient des journaux relatifs aux modifications apportées à la configuration des classificateurs de trafic.	Nœuds d'administration et de passerelle
/var/local/log/update-utcn.log	Contient des journaux liés au mode réseau client non fiable sur ce nœud.	Tous les nœuds

Informations associées

"Sur le bycast.log"

"UTILISEZ L'API REST S3"

Journaux de déploiement et de maintenance

Vous pouvez utiliser les journaux de déploiement et de maintenance pour résoudre les problèmes.

Nom du fichier	Remarques	Ci-après
/var/local/log/install.log	Créé lors de l'installation du logiciel. Contient un enregistrement des événements d'installation.	Tous les nœuds
/var/local/log/expansion-progress.log	Créé pendant les opérations d'extension. Contient un enregistrement des événements d'extension.	Nœuds de stockage
/var/local/log/pa-move.log	Créé lors de l'exécution de `pa-move.sh` script.	Nœud d'administration principal
/var/local/log/pa-move-new_pa.log	Créé lors de l'exécution de `pa-move.sh` script.	Nœud d'administration principal
/var/local/log/pa-move-old_pa.log	Créé lors de l'exécution de `pa-move.sh` script.	Nœud d'administration principal
/var/local/log/gdu-server.log	Créé par le service GDU. Contient les événements liés aux procédures d'approvisionnement et de maintenance gérées par le nœud d'administration principal.	Nœud d'administration principal
/var/local/log/send_admin_hw.log	Créé lors de l'installation. Contient des informations de débogage liées aux communications d'un nœud avec le nœud d'administration principal.	Tous les nœuds

Nom du fichier	Remarques	Ci-après
/var/local/log/upgrade.log	Créé lors de la mise à niveau logicielle. Contient un enregistrement des événements de mise à jour du logiciel.	Tous les nœuds

Journaux de logiciels tiers

Vous pouvez utiliser les journaux de logiciels tiers pour résoudre les problèmes.

Catégorie	Nom du fichier	Remarques	Ci-après
Archivage	/var/local/log/dsierror.log	Informations d'erreur pour les API client TSM.	Nœuds d'archivage
MySQL	/var/local/log/mysql.err /var/local/log/mysql-slow.log	Fichiers journaux générés par MySQL. `mysql.err` capture les erreurs de base de données et les événements tels que les démarrages et arrêts de service. `mysql-slow.log` (Le journal de requête lent) capture les instructions SQL qui ont pris plus de 10 secondes à exécuter.	Nœuds d'administration
Système d'exploitation	/var/local/log/messages	Ce répertoire contient les fichiers journaux du système d'exploitation. Les erreurs contenues dans ces journaux s'affichent également dans Grid Manager. Sélectionnez **SUPPORT** > **Outils** > **topologie de grille**. Sélectionnez ensuite **Topology** > ***site*** > ***Node*** > **SSM** > **Events**.	Tous les nœuds
NTP	/var/local/log/ntp.log /var/lib/ntp/var/log/ntpstats/	`/var/local/log/ntp.log` Contient le fichier journal des messages d'erreur NTP. `/var/lib/ntp/var/log/ntpstats/` Le répertoire contient les statistiques de synchronisation NTP. `loopstats` enregistre les informations statistiques de filtre en boucle. `peerstats` enregistre les statistiques homologues.	Tous les nœuds

Sur le bycast.log

Le fichier `/var/local/log/bycast.log` Est le fichier de dépannage principal du logiciel StorageGRID. Il y a un `bycast.log` fichier pour chaque nœud de grid. Le fichier contient des messages spécifiques à ce nœud de grille.

Le fichier `/var/local/log/bycast-err.log` est un sous-ensemble de `bycast.log`. Il contient des messages D'ERREUR de gravité et D'ERREUR CRITIQUE.

Vous pouvez également modifier la destination des journaux d'audit et envoyer des informations d'audit à un serveur syslog externe. Les journaux locaux des enregistrements d'audit continuent à être générés et stockés lorsqu'un serveur syslog externe est configuré. Voir "Configurez les messages d'audit et les destinations des journaux".

Rotation des fichiers pour bycast.log

Lorsque le `bycast.log` Le fichier atteint 1 Go, le fichier existant est enregistré et un nouveau fichier journal est démarré.

Le fichier enregistré est renommé `bycast.log.1`, et le nouveau fichier est nommé `bycast.log`. Lorsque le nouveau `bycast.log` Atteint 1 Go, `bycast.log.1` est renommé et compressé pour devenir `bycast.log.2.gz`, et `bycast.log` est renommé `bycast.log.1`.

La limite de rotation pour `bycast.log` est de 21 fichiers. Lorsque la 22e version du `bycast.log` le fichier est créé, le fichier le plus ancien est supprimé.

La limite de rotation pour `bycast-err.log` est sept fichiers.

> ⓘ Si un fichier journal a été compressé, vous ne devez pas le décompresser au même emplacement que celui dans lequel il a été écrit. La décompression du fichier au même emplacement peut interférer avec les scripts de rotation du journal.

Vous pouvez également modifier la destination des journaux d'audit et envoyer des informations d'audit à un serveur syslog externe. Les journaux locaux des enregistrements d'audit continuent à être générés et stockés lorsqu'un serveur syslog externe est configuré. Voir "Configurez les messages d'audit et les destinations des journaux".

Informations associées

"Collecte de fichiers journaux et de données système"

Messages en bycast.log

Messages dans `bycast.log` Sont écrits par l'ADE (ADE). ADE est l'environnement d'exécution utilisé par les services de chaque nœud de la grille.

Exemple de message ADE :

```
May 15 14:07:11 um-sec-rg1-agn3 ADE: |12455685    0357819531
SVMR EVHR 2019-05-05T27T17:10:29.784677| ERROR 0906 SVMR: Health
check on volume 3 has failed with reason 'TOUT'
```

Les messages ADE contiennent les informations suivantes :

Segment de message	Valeur dans l'exemple
ID de nœud	12455685

Segment de message	Valeur dans l'exemple
ID processus ADE	0357819531
Nom du module	SVMR
Identifiant du message	EVHR
Heure système UTC	2019-05-05T27T17:10:29.784677 (AAAA-MM-DDTHH:MM:SS.UUUUUUUU)
Niveau de gravité	ERREUR
Numéro de suivi interne	0906
Messagerie	SVMR : le bilan de santé du volume 3 a échoué avec la raison « tout »

Gravité des messages en bycast.log

Les messages dans `bycast.log` des niveaux de sévérité sont attribués.

Par exemple :

- **AVIS** — un événement qui devrait être enregistré s'est produit. La plupart des messages du journal sont à ce niveau.
- **AVERTISSEMENT** — une condition inattendue s'est produite.
- **ERREUR** — Une erreur majeure s'est produite qui aura une incidence sur les opérations.
- **CRITIQUE** — une condition anormale s'est produite qui a arrêté les opérations normales. Vous devez immédiatement corriger la condition sous-jacente. Les messages critiques sont également affichés dans le Grid Manager. Sélectionnez **SUPPORT** > **Outils** > **topologie de grille**. Sélectionnez ensuite **site** > **nœud** > **SSM** > **événements**.

Codes d'erreur dans `bycast.log`

La plupart des messages d'erreur dans `bycast.log` contient des codes d'erreur.

Le tableau suivant répertorie les codes non numériques courants dans `bycast.log`. La signification exacte d'un code non numérique dépend du contexte dans lequel il est signalé.

Code d'erreur	Signification
CAN	Pas d'erreur
GERR	Inconnu
ANNUL	Annulée

Code d’erreur	Signification
ABRT	Abandonné
TOUT	Délai dépassé
INVL	Non valide
NFND	Introuvable
VERS	Version
CONF	Configuration
ECHEC	Échec
CIPD	Incomplet
L’A FAIT	L’a fait
SUNV	Service indisponible

Le tableau suivant répertorie les codes d’erreur numériques dans `bycast.log`.

Numéro de l’erreur	Code d’erreur	Signification
001	EPERM	Opération non autorisée
002	RÉF	Ce fichier ou répertoire n’est pas disponible
003	ESRCH	Pas de tel processus
004	EINTA	Appel système interrompu
005	EIO	Erreur d’E/S.
006	ENXIO	Ce périphérique ou cette adresse n’est pas disponible
007	E2BIG	Liste d’arguments trop longue
008	ENOEXEC	Erreur de format Exec
009	EBADF	Numéro de fichier incorrect

Numéro de l’erreur	Code d’erreur	Signification
010	ECHILD	Aucun processus enfant
011	EAGAIN	Réessayez
012	ENOMEM	Mémoire insuffisante
013	EACCES	Autorisation refusée
014	PAR DÉFAUT	Adresse incorrecte
015	ENOTBLK	Dispositif de blocage requis
016	EBUSY	Périphérique ou ressource occupé
017	EEXIST	Le fichier existe déjà
018	EXDEV	Liaison interpériphérique
019	ENV	Aucun appareil de ce type
020	ENOTDIR	Pas un répertoire
021	EISDIR	Est un répertoire
022	EINVAL	Argument non valide
023	PAGE D’ACCUEIL	Dépassement de la table de fichiers
024	EMFILE	Trop de fichiers ouverts
025	EN COURS	Pas une machine à écrire
026	ETXTBBY	Fichier texte occupé
027	EFBIG	Fichier trop volumineux
028	ENOSPC	Il n’y a plus d’espace sur l’appareil
029	ESPIPE	Recherche illégale
030	EROFS	Système de fichiers en lecture seule

Numéro de l'erreur	Code d'erreur	Signification
031	ALINK	Trop de liens
032	EPIPE	Tuyau cassé
033	ÉDOM	Argument mathématique hors domaine de la fonction
034	ERANGE	Résultat mathématique non représentativité
035	EDEADLE	L'impasse de la ressource se produirait
036	ENAMETOOLONG	Nom de fichier trop long
037	ENOLCK	Aucun verrouillage d'enregistrement disponible
038	ENOSYS	Fonction non implémentée
039	ENOTEMPTY	Répertoire non vide
040	ELOP	Trop de liens symboliques rencontrés
041		
042	ENOMSG	Aucun message du type souhaité
043	EIDRM	Identificateur supprimé
044	ECHNG	Numéro de canal hors plage
045	EL2NSYNC	Niveau 2 non synchronisé
046	EL3HLT	Niveau 3 arrêté
047	EL3RST	Remise à zéro du niveau 3
048	ELNRNG	Numéro de liaison hors plage
049	EUNATCH	Pilote de protocole non connecté
050	ENOCSI	Aucune structure CSI disponible
051	EL2HLT	Niveau 2 arrêté

Numéro de l'erreur	Code d'erreur	Signification
052	EBADE	Échange non valide
053	ADR	Descripteur de demande non valide
054	EXFULL	Exchange complet
055	ENOANO	Pas d'anode
056	EBADRQC	Code de demande non valide
057	EBADSLT	Emplacement non valide
058		
059	EBFONT	Format de fichier de police incorrect
060	ENOSTR	Le périphérique n'est pas un flux
061	ENODATA	Aucune donnée disponible
062	ETIME	Temporisation expirée
063	ENOSR	Ressources hors flux
064	ENONET	La machine n'est pas sur le réseau
065	ENOPKG	Package non installé
066	EREMOTE	L'objet est distant
067	LIAISON	Le lien a été rompu
068	EADV	Erreur de publicité
069	ESRMNT	Erreur Srmount
070	ECOMM	Erreur de communication sur l'envoi
071	EPROTO	Erreur de protocole
072	EMULTIIHOP	Multihop tenté

Numéro de l'erreur	Code d'erreur	Signification
073	EDOTTDOT	Erreur spécifique RFS
074	EBADMSG	Pas un message de données
075	EOVERFLOW	Valeur trop élevée pour le type de données défini
076	ENOTUNIQ	Nom non unique sur le réseau
077	EDFD	Descripteur de fichier dans un état incorrect
078	SOUS-GROUPE	Adresse distante modifiée
079	ELIBACC	Impossible d'accéder à une bibliothèque partagée nécessaire
080	ELIBBAD	Accès à une bibliothèque partagée endommagée
081	ELIBSCN	
082	ELIBMAX	Tentative de liaison dans trop de bibliothèques partagées
083	ELIBEXEC	impossible d'exécuter directement une bibliothèque partagée
084	EILSEQ	Séquence d'octets non autorisée
085	SYSTÈME	L'appel système interrompu doit être redémarré
086	ESTRPIPE	Erreur de tuyau de flux
087	EUSERS	Trop d'utilisateurs
088	ENOTSOCK	Fonctionnement de la prise femelle sur non prise femelle
089	EDESTADDRREQ	Adresse de destination requise
090	EMSGSIZE	Message trop long
091	EPROTOTYPE	Type de protocole incorrect pour le socket
092	EN OPTION	Protocole non disponible

Numéro de l'erreur	Code d'erreur	Signification
093	EPROTONOSUPPORT	Protocole non pris en charge
094	ESOCKNOSUPPORT	Type de socket non pris en charge
095	EOPNOTSUPP	Opération non prise en charge sur le terminal de transport
096	EPFNOSUPPORT	Famille de protocoles non prise en charge
097	EAFNOSUPPORT	Famille d'adresses non prise en charge par le protocole
098	EADDDRINUSE	Adresse déjà utilisée
099	EADDRNOTAVAIL	Impossible d'attribuer l'adresse demandée
100	EN-TÊTE	Le réseau ne fonctionne pas
101	ENETUNREACH	Le réseau est inaccessible
102	ENETRESET	La connexion au réseau a été interrompue en raison d'une réinitialisation
103	ECONNABORTED	Le logiciel a provoqué l'arrêt de la connexion
104	ECONRESET	Réinitialisation de la connexion par poste
105	ENOBUFS	Aucun espace tampon disponible
106	EISCONN	Terminal de transport déjà connecté
107	ENOTCONN	Le terminal de transport n'est pas connecté
108	ESHUTDOWN	Impossible d'envoyer après l'arrêt du terminal de transport
109	ETOONYREFS	Trop de références : impossible d'épisser
110	ETIMDOUT	La connexion a expiré
111	ECONREFUSED	Connexion refusée
112	EHOSTDOWN	L'hôte n'est pas en panne

Numéro de l'erreur	Code d'erreur	Signification
113	EHOSTUNREACH	Aucune route vers l'hôte
114	EALREADY	Opération déjà en cours
115	EINPROGRESS	Opération en cours
116		
117	EUCLEAN	La structure doit être nettoyée
118	ENOTNAM	Pas un fichier de type nommé XENIX
119	ENAVAIL	Aucun sémaphores XENIX n'est disponible
120	EISNAM	Est un fichier de type nommé
121	EREMOTIO	Erreur d'E/S distante
122	EDUQUOT	Quota dépassé
123	ENOMEDIUM	Aucun support trouvé
124	EMEDIUMTYPE	Type de support incorrect
125	ECANCELED	Opération annulée
126	ENOKAY	Clé requise non disponible
127	EKEYEXPIRED	La clé a expiré
128	EKEYREVOKED	La clé a été révoquée
129	EKEYREJECTED	La clé a été rejetée par le service
130	EOWNERDEAD	Pour des mutexes robustes : le propriétaire est mort
131	ENOTREOVERABLE	Pour les mutexes robustes : état non récupérable

Configurez les messages d'audit et les destinations des journaux

Les messages d'audit et les journaux enregistrent les activités du système et les événements de sécurité. Ils constituent les outils essentiels de surveillance et de

dépannage. Vous pouvez régler les niveaux d'audit pour augmenter ou diminuer le type et le nombre de messages d'audit enregistrés. Vous pouvez éventuellement définir les en-têtes de requête HTTP que vous souhaitez inclure dans les messages d'audit client en lecture et écriture. Vous pouvez également configurer un serveur syslog externe et modifier la destination des informations d'audit.

Pour plus d'informations sur les messages d'audit, reportez-vous à la section "Examiner les journaux d'audit".

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous disposez d'autorisations d'accès à la racine ou à la maintenance.

Description de la tâche

Tous les nœuds StorageGRID génèrent des messages d'audit et des journaux pour suivre l'activité et les événements du système. Par défaut, les informations d'audit sont envoyées au journal d'audit des nœuds d'administration. Vous pouvez régler les niveaux d'audit pour augmenter ou diminuer le type et le nombre de messages d'audit enregistrés dans le journal d'audit. Vous pouvez également configurer des informations d'audit qui seront stockées temporairement sur les nœuds d'origine pour une collecte manuelle.

> Si vous disposez d'une grande grille, utilisez plusieurs types d'applications S3 ou souhaitez conserver toutes les données d'audit, configurez un serveur syslog externe et enregistrez les informations d'audit à distance. L'utilisation d'un serveur externe réduit l'impact sur les performances de la journalisation des messages d'audit sans réduire l'exhaustivité des données d'audit. Voir "Considérations relatives au serveur syslog externe" pour plus d'informations.

Modifier les niveaux de messages d'audit dans le journal d'audit

Vous pouvez définir un niveau d'audit différent pour chacune des catégories de messages suivantes dans le journal d'audit :

Catégorie de vérification	Description
Système	Par défaut, ce niveau est défini sur Normal. Voir "Messages d'audit système".
Stockage	Par défaut, ce niveau est défini sur erreur. Voir "Messages d'audit du stockage objet".
Gestion	Par défaut, ce niveau est défini sur Normal. Voir "Message d'audit de gestion".
Lectures du client	Par défaut, ce niveau est défini sur Normal. Voir "Messages d'audit de lecture du client".
Écritures des clients	Par défaut, ce niveau est défini sur Normal. Voir "Écrire des messages d'audit client".
Les opérations ILM	Par défaut, ce niveau est défini sur Normal. Voir "Messages d'audit des opérations ILM".

Ces valeurs par défaut s'appliquent si vous avez installé StorageGRID à l'origine à l'aide de la version 10.3 ou ultérieure. Si vous avez mis à niveau à partir d'une version antérieure de StorageGRID, la valeur par défaut pour toutes les catégories est Normal.

Durant les mises à niveau, les configurations des niveaux d'audit ne seront pas effectives immédiatement.

Étapes

1. Sélectionnez **CONFIGURATION** > **surveillance** > **serveur d'audit et syslog**.
2. Pour chaque catégorie de message d'audit, sélectionnez un niveau d'audit dans la liste déroulante :

Niveau d'audit	Description
Éteint	Aucun message d'audit de la catégorie n'est enregistré.
Erreur	Seuls les messages d'erreur sont consignés—les messages d'audit pour lesquels le code de résultat n'a pas été « réussi » (CMC).
Normale	Les messages transactionnels standard sont consignés—les messages répertoriés dans ces instructions pour la catégorie.
Débogage	Obsolète. Ce niveau se comporte de la même manière que le niveau d'audit normal.

Les messages inclus pour tout niveau particulier incluent ceux qui seraient consignés aux niveaux supérieurs. Par exemple, le niveau Normal inclut tous les messages d'erreur.

Si vous n'avez pas besoin d'un enregistrement détaillé des opérations de lecture du client pour vos applications S3, vous pouvez éventuellement définir le paramètre **lecture du client** sur **erreur** pour diminuer le nombre de messages d'audit enregistrés dans le journal d'audit.

3. Éventuellement, sous **en-têtes de protocole d'audit**, définissez les en-têtes de requête HTTP que vous souhaitez inclure dans les messages d'audit de lecture et d'écriture du client. Utilisez un astérisque (*) comme caractère générique pour qu'il corresponde à zéro ou à plusieurs caractères. Utilisez la séquence d'échappement (*) pour faire correspondre un astérisque littéral.

   Les en-têtes de protocole d'audit ne s'appliquent qu'aux demandes S3 et Swift.

4. Sélectionnez **Ajouter un autre en-tête** pour créer des en-têtes supplémentaires, si nécessaire.

   Lorsque des en-têtes HTTP sont trouvés dans une requête, ils sont inclus dans le message d'audit sous le champ HTRH.

   Les en-têtes de requête de protocole d'audit ne sont consignés que si le niveau d'audit pour **lecture client** ou **écriture client** n'est pas **off**.

5. Sélectionnez **Enregistrer**

Une bannière verte indique que votre configuration a été enregistrée avec succès.

Utiliser un serveur syslog externe

Vous pouvez configurer un serveur syslog externe si vous souhaitez enregistrer les informations d'audit à distance.

- Pour enregistrer les informations d'audit sur un serveur syslog externe, accédez à "Configurer un serveur syslog externe".
- Si vous n'utilisez pas de serveur syslog externe, accédez à Sélectionnez les destinations des informations d'audit.

Sélectionnez les destinations des informations d'audit

Vous pouvez spécifier l'emplacement d'envoi des journaux d'audit, des journaux d'événements de sécurité et des journaux d'application.

Certaines destinations sont disponibles uniquement si vous utilisez un serveur syslog externe. Voir "Configurer un serveur syslog externe" pour configurer un serveur syslog externe.

Pour plus d'informations sur les journaux du logiciel StorageGRID, reportez-vous à la section "Journaux du logiciel StorageGRID".

1. Sur la page Audit and syslog Server, sélectionnez la destination des informations d'audit dans les options répertoriées :

Option	Description
Par défaut (nœuds d'administration/nœuds locaux)	Les messages d'audit sont envoyés au journal d'audit (`audit.log`) Sur le nœud d'administration, les journaux d'événements de sécurité et les journaux d'applications sont stockés sur les nœuds où ils ont été générés (également appelés « nœud local »).
Serveur syslog externe	Les informations d'audit sont envoyées à un serveur syslog externe et enregistrées sur le nœud local. Le type d'information envoyée dépend de la façon dont vous avez configuré le serveur syslog externe. Cette option n'est activée qu'après avoir configuré un serveur syslog externe.
Nœud d'administration et serveur syslog externe	Les messages d'audit sont envoyés au journal d'audit (`audit.log`) Sur le nœud d'administration, les informations d'audit sont envoyées au serveur syslog externe et enregistrées sur le nœud local. Le type d'information envoyée dépend de la façon dont vous avez configuré le serveur syslog externe. Cette option n'est activée qu'après avoir configuré un serveur syslog externe.

Option	Description
Nœuds locaux uniquement	Aucune information d'audit n'est envoyée à un nœud d'administration ou à un serveur syslog distant. Les informations d'audit sont enregistrées uniquement sur les nœuds qui les ont générées. **Remarque**: StorageGRID supprime périodiquement ces journaux locaux dans une rotation pour libérer de l'espace. Lorsque le fichier journal d'un nœud atteint 1 Go, le fichier existant est enregistré et un nouveau fichier journal est démarré. La limite de rotation du journal est de 21 fichiers. Lorsque la 22e version du fichier journal est créée, le fichier journal le plus ancien est supprimé. En moyenne, environ 20 Go de données de journalisation sont stockés sur chaque nœud.

Les informations d'audit générées sur chaque nœud local sont stockées dans `/var/local/log/localaudit.log`

2. Sélectionnez **Enregistrer**.

   Un message d'avertissement s'affiche.

3. Sélectionnez **OK** pour confirmer que vous souhaitez modifier la destination des informations d'audit.

   Une bannière verte s'affiche pour vous informer que votre configuration d'audit a été enregistrée.

   Les nouveaux journaux sont envoyés aux destinations que vous avez sélectionnées. Les journaux existants restent à leur emplacement actuel.

Informations associées

"Considérations relatives au serveur syslog externe"

"Administrer StorageGRID"

"Dépanner le serveur syslog externe"

Utiliser un serveur syslog externe

Considérations relatives au serveur syslog externe

Utilisez les consignes suivantes pour estimer la taille du serveur syslog externe dont vous avez besoin.

Qu'est-ce qu'un serveur syslog externe ?

Un serveur syslog externe est un serveur hors de StorageGRID que vous pouvez utiliser pour collecter les informations d'audit système sur un emplacement unique. L'utilisation d'un serveur syslog externe vous permet de configurer les destinations de vos informations d'audit afin de réduire le trafic réseau sur vos nœuds d'administration et de gérer ces informations de manière plus efficace. Les types d'informations d'audit que vous pouvez envoyer au serveur syslog externe sont les suivants :

- Journaux d'audit contenant les messages d'audit générés pendant le fonctionnement normal du système

- Événements liés à la sécurité tels que les connexions et la remontée à la racine
- Fichiers journaux d'application pouvant être demandés s'il est nécessaire d'ouvrir un dossier d'assistance pour résoudre un problème rencontré

Comment estimer la taille du serveur syslog externe

En principe, la taille de la grille est adaptée au débit requis, défini en termes d'opérations S3 par seconde ou d'octets par seconde. Par exemple, votre grid peut être capable de gérer 1,000 opérations S3 par seconde ou 2,000 Mo par seconde, d'ingales et de récupérations d'objets. Il est conseillé de dimensionner votre serveur syslog externe en fonction des besoins de votre grid.

Cette section fournit des formules heuristiques qui vous aident à estimer le taux et la taille moyenne des messages de journal de différents types requis par votre serveur syslog externe en termes de caractéristiques de performance connues ou souhaitées de la grille (opérations S3 par seconde).

Utilisez des opérations S3 par seconde dans les formules d'estimation

Si votre grille a été dimensionnée pour un débit exprimé en octets par seconde, vous devez convertir ce dimensionnement en opérations S3 par seconde afin d'utiliser les formules d'estimation. Pour convertir le débit du grid, vous devez d'abord déterminer la taille d'objet moyenne que vous pouvez utiliser les informations des journaux d'audit et des mesures existants (le cas échéant), ou en utilisant vos connaissances des applications qui utilisent StorageGRID. Par exemple, si la taille du grid a été dimensionnée pour atteindre un débit de 2,000 Mo/seconde, et que la taille d'objet moyenne est de 2 Mo, votre grille a été dimensionnée pour traiter 1,000 opérations S3 par seconde (2,000 Mo/2 Mo).

> ⓘ Les formules de dimensionnement externe du serveur syslog présentées dans les sections suivantes fournissent des estimations communes (plutôt que des estimations de cas les plus défavorables). Selon votre configuration et votre charge de travail, un taux plus élevé ou moins élevé de messages syslog ou de données syslog peut être constaté que les formules le prévoient. Les formules sont destinées à être utilisées uniquement comme directives.

Formules d'estimation pour les journaux d'audit

Si vous ne disposez d'aucune information concernant votre charge de travail S3 autre que le nombre d'opérations S3 par seconde que votre grille doit prendre en charge, vous pouvez estimer le volume des journaux d'audit que votre serveur syslog externe devra gérer à l'aide des formules suivantes : Dans l'hypothèse où vous laissez les niveaux d'audit définis sur les valeurs par défaut (toutes les catégories sont définies sur Normal, sauf Storage, qui est défini sur erreur) :

```
Audit Log Rate = 2 x S3 Operations Rate
Audit Log Average Size = 800 bytes
```

Par exemple, si le grid est dimensionné pour 1,000 opérations S3 par seconde, votre serveur syslog externe doit être dimensionné pour prendre en charge 2,000 messages syslog par seconde et doit être capable de recevoir (et généralement stocker) les données du journal d'audit à un taux de 1.6 Mo par seconde.

Si vous en savez plus sur votre charge de travail, des estimations plus précises sont possibles. Pour les journaux d'audit, les variables supplémentaires les plus importantes sont le pourcentage d'opérations S3 PUT (par rapport à) et la taille moyenne, en octets, des champs S3 suivants (les abréviations de 4 caractères utilisées dans le tableau sont des noms de champs du journal d'audit) :

Code	Champ	Description
CCUA	Nom du compte de locataire S3 (expéditeur de la demande)	Nom du compte de tenant pour l'utilisateur qui a envoyé la demande. Vide pour les demandes anonymes.
SBAC	Nom de compte de locataire S3 (propriétaire du compartiment)	Nom du compte du locataire pour le propriétaire du compartiment. Permet d'identifier les accès inter-comptes ou anonymes.
S3BK	Compartiment S3	Nom du compartiment S3.
S3KY	Clé S3	Le nom de la clé S3 n'inclut pas le nom du compartiment. Les opérations sur les compartiments n'incluent pas ce champ.

Nous allons utiliser P pour représenter le pourcentage d'opérations S3 qui sont PUT, où 0 ≤ P ≤ 1 (pour une charge de travail PUT de 100 %, P = 1, et pour une charge DE travail GET de 100 %, P = 0).

Utilisons K pour représenter la taille moyenne de la somme des noms de comptes S3, du compartiment S3 et de la clé S3. Supposons que le nom de compte S3 soit toujours mon compte s3 (13 octets), que les compartiments ont des noms de longueur fixe comme /my/application/catg-12345 (28 octets) et que les objets ont des clés à longueur fixe comme 5733a5d7-f069-41ef-8fbd-132449c69c (36 octets). La valeur de K est alors de 90 (13+13+28+36).

Si vous pouvez déterminer les valeurs P et K, vous pouvez estimer le volume des journaux d'audit que votre serveur syslog externe doit traiter à l'aide des formules suivantes, en supposant que vous laissez les niveaux d'audit par défaut (toutes les catégories définies sur Normal, sauf Storage, Qui est défini sur erreur) :

```
Audit Log Rate = ((2 x P) + (1 - P)) x S3 Operations Rate
Audit Log Average Size = (570 + K) bytes
```

Par exemple, si le grid est dimensionné pour 1,000 opérations S3 par seconde, le workload est PUT à 50 %, et les noms de compte S3, les noms de compartiment, Et les noms d'objet utilisent une moyenne de 90 octets. Votre serveur syslog externe doit être dimensionné pour prendre en charge 1,500 messages syslog par seconde et doit être capable de recevoir (et généralement stocker) les données du journal d'audit à un taux d'environ 1 Mo par seconde.

Formules d'estimation pour les niveaux d'audit non par défaut

Les formules fournies pour les journaux d'audit supposent l'utilisation des paramètres par défaut du niveau d'audit (toutes les catégories sont définies sur Normal, sauf Storage, qui est défini sur erreur). Les formules détaillées d'estimation du taux et de la taille moyenne des messages d'audit pour les paramètres de niveau d'audit non par défaut ne sont pas disponibles. Toutefois, le tableau suivant peut être utilisé pour faire une estimation approximative du taux; vous pouvez utiliser la formule de taille moyenne fournie pour les journaux d'audit, mais sachez qu'elle risque de générer une surestimation car les messages d'audit « supplémentaires » sont, en moyenne, inférieurs aux messages d'audit par défaut.

Condition	Formule
Réplication : niveaux d'audit tous définis sur débogage ou Normal	Taux du journal d'audit = 8 x taux d'opérations S3
Codage d'effacement : les niveaux d'audit sont tous définis sur débogage ou Normal	Utiliser la même formule que pour les paramètres par défaut

Formules d'estimation pour les événements de sécurité

Les événements de sécurité ne sont pas corrélés avec les opérations S3 et produisent généralement un volume négligeable de journaux et de données. Pour ces raisons, aucune formule d'estimation n'est fournie.

Formules d'estimation pour les journaux d'application

Si vous ne disposez d'aucune information concernant votre charge de travail S3 autre que le nombre d'opérations S3 par seconde que que votre grid est censé prendre en charge, vous pouvez estimer le volume des journaux d'applications que votre serveur syslog externe devra gérer à l'aide des formules suivantes :

```
Application Log Rate = 3.3 x S3 Operations Rate
Application Log Average Size = 350 bytes
```

Par exemple, si le grid est dimensionné pour 1,000 opérations S3 par seconde, votre serveur syslog externe doit être dimensionné pour prendre en charge 3,300 journaux d'application par seconde et être capable de recevoir (et de stocker) les données de journaux d'application à un taux de 1.2 Mo par seconde environ.

Si vous en savez plus sur votre charge de travail, des estimations plus précises sont possibles. Pour les journaux d'application, les variables supplémentaires les plus importantes sont la stratégie de protection des données (réplication contre Le code d'effacement), le pourcentage d'opérations S3 PUT (par rapport à Et la taille moyenne, en octets, des champs S3 suivants (les abréviations de 4 caractères utilisées dans le tableau sont des noms de champs du journal d'audit) :

Code	Champ	Description
CCUA	Nom du compte de locataire S3 (expéditeur de la demande)	Nom du compte de tenant pour l'utilisateur qui a envoyé la demande. Vide pour les demandes anonymes.
SBAC	Nom de compte de locataire S3 (propriétaire du compartiment)	Nom du compte du locataire pour le propriétaire du compartiment. Permet d'identifier les accès inter-comptes ou anonymes.
S3BK	Compartiment S3	Nom du compartiment S3.

Code	Champ	Description
S3KY	Clé S3	Le nom de la clé S3 n'inclut pas le nom du compartiment. Les opérations sur les compartiments n'incluent pas ce champ.

Exemples d'estimations de dimensionnement

Cette section explique des exemples d'utilisation des formules d'estimation pour les grilles avec les méthodes de protection des données suivantes :

- La réplication
- Codage d'effacement

Si vous utilisez la réplication pour la protection des données

La p représente le pourcentage d'opérations S3 qui sont PUT, 0 ≤ P ≤ 1 (pour une charge de travail PUT de 100 %, P = 1 et POUR une charge DE travail GET de 100 %, P = 0).

Imaginons que K représente la taille moyenne de la somme des noms de compte S3, du compartiment S3 et de la clé S3. Supposons que le nom de compte S3 soit toujours mon compte s3 (13 octets), que les compartiments ont des noms de longueur fixe comme /my/application/catg-12345 (28 octets) et que les objets ont des clés à longueur fixe comme 5733a5d7-f069-41ef-8fbd-132449c69c (36 octets). Ensuite K a une valeur de 90 (13+13+28+36).

Si vous pouvez déterminer des valeurs pour P et K, vous pouvez estimer le volume des journaux d'application que votre serveur syslog externe devra traiter à l'aide des formules suivantes.

```
Application Log Rate = ((1.1 x P) + (2.5 x (1 - P))) x S3 Operations Rate
Application Log Average Size = (P x (220 + K)) + ((1 - P) x (240 + (0.2 x
K))) Bytes
```

Par exemple, si le grid est dimensionné pour 1,000 opérations S3 par seconde, le workload est utilisé à 50 % et les noms de comptes S3, de compartiments et de noms d'objet moyenne à 90 octets, votre serveur syslog externe doit être dimensionné pour prendre en charge 1800 journaux d'applications par seconde. Et sera en mesure de recevoir (et de stocker en général) des données d'application à un taux de 0.5 Mo par seconde.

Si vous utilisez le code d'effacement pour la protection des données

La p représente le pourcentage d'opérations S3 qui sont PUT, 0 ≤ P ≤ 1 (pour une charge de travail PUT de 100 %, P = 1 et POUR une charge DE travail GET de 100 %, P = 0).

Imaginons que K représente la taille moyenne de la somme des noms de compte S3, du compartiment S3 et de la clé S3. Supposons que le nom de compte S3 soit toujours mon compte s3 (13 octets), que les compartiments ont des noms de longueur fixe comme /my/application/catg-12345 (28 octets) et que les objets ont des clés à longueur fixe comme 5733a5d7-f069-41ef-8fbd-132449c69c (36 octets). Ensuite K a une valeur de 90 (13+13+28+36).

Si vous pouvez déterminer des valeurs pour P et K, vous pouvez estimer le volume des journaux d'application que votre serveur syslog externe devra traiter à l'aide des formules suivantes.

```
Application Log Rate = ((3.2 x P) + (1.3 x (1 - P))) x S3 Operations Rate
Application Log Average Size = (P x (240 + (0.4 x K))) + ((1 - P) x (185 +
(0.9 x K))) Bytes
```

Par exemple, si le grid est dimensionné pour 1,000 opérations S3 par seconde, le workload est utilisé à 50 % et les noms de comptes S3, les noms de compartiment, Et les noms d'objet en moyenne de 90 octets, votre serveur syslog externe doit être dimensionné pour prendre en charge 2,250 journaux d'application par seconde. Il doit alors être capable de recevoir et de stocker les données de l'application à un taux de 0.6 Mo par seconde.

Pour plus d'informations sur la configuration des niveaux de messages d'audit et d'un serveur syslog externe, reportez-vous aux sections suivantes :

- "Configurer un serveur syslog externe"
- "Configurez les messages d'audit et les destinations des journaux"

Configurer un serveur syslog externe

Si vous souhaitez enregistrer les journaux d'audit, les journaux d'application et les journaux d'événements de sécurité dans un emplacement en dehors de votre grille, utilisez cette procédure pour configurer un serveur syslog externe.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous disposez d'autorisations d'accès à la racine ou à la maintenance.
- Vous disposez d'un serveur syslog avec la capacité de recevoir et stocker les fichiers journaux. Pour plus d'informations, voir "Considérations relatives au serveur syslog externe".
- Vous disposez des certifications serveur et client appropriées si vous prévoyez d'utiliser TLS ou RELP/TLS.

Description de la tâche

Si vous souhaitez envoyer des informations d'audit à un serveur syslog externe, vous devez d'abord configurer le serveur externe.

L'envoi d'informations d'audit à un serveur syslog externe vous permet de :

- Collectez et gérez plus efficacement les informations d'audit, telles que les messages d'audit, les journaux d'application et les événements de sécurité
- Réduisez le trafic réseau sur vos nœuds d'administration car les informations d'audit sont transférées directement des différents nœuds de stockage vers le serveur syslog externe, sans passer par un nœud d'administration

> Lorsque les journaux sont envoyés à un serveur syslog externe, les journaux uniques supérieurs à 8192 octets sont tronqués à la fin du message pour se conformer aux limitations communes dans les implémentations de serveur syslog externes.

Pour optimiser les options de restauration complète des données en cas de défaillance du serveur syslog externe, jusqu'à 20 Go de journaux locaux d'enregistrements d'audit (localaudit.log) sont conservés sur chaque nœud.

Si les options de configuration disponibles dans cette procédure ne sont pas suffisamment flexibles pour répondre à vos besoins, des options de configuration supplémentaires peuvent être appliquées à l'aide de l'API privée `audit-destinations` terminaux. Par exemple, il est possible d'utiliser différents serveurs syslog pour différents groupes de nœuds.

Configurez le serveur externe

Accéder à l'assistant

Pour démarrer, accédez à l'assistant configurer le serveur syslog externe.

Étapes

1. Sélectionnez **CONFIGURATION** > **surveillance** > **serveur d'audit et syslog**.
2. Sur la page Audit and syslog Server, sélectionnez **Configure External syslog Server**. Si vous avez déjà configuré un serveur syslog externe, sélectionnez **Modifier serveur syslog externe**.

   L'assistant configurer le serveur syslog externe s'affiche.

Entrez les informations du journal système

Vous devez fournir les informations dont StorageGRID a besoin pour accéder au serveur syslog externe.

Étapes

1. Pour l'étape **Entrez les informations syslog** de l'assistant, entrez un nom de domaine complet valide ou une adresse IPv4 ou IPv6 pour le serveur syslog externe dans le champ **Host**.
2. Entrez le port de destination sur le serveur syslog externe (doit être un entier compris entre 1 et 65535). Le port par défaut est 514.
3. Sélectionnez le protocole utilisé pour envoyer les informations d'audit au serveur syslog externe.

   Il est recommandé d'utiliser **TLS** ou **RELP/TLS**. Vous devez télécharger un certificat de serveur pour utiliser l'une de ces options. L'utilisation de certificats permet de sécuriser les connexions entre votre grille et le serveur syslog externe. Pour plus d'informations, voir "Gérer les certificats de sécurité".

   Toutes les options de protocole requièrent la prise en charge par le serveur syslog externe ainsi que sa configuration. Vous devez choisir une option compatible avec le serveur syslog externe.

   Le protocole RELP (fiable Event Logging Protocol) étend la fonctionnalité du protocole syslog afin de fournir des messages d'événement fiables. L'utilisation de RELP peut aider à éviter la perte d'informations d'audit si votre serveur syslog externe doit redémarrer.

4. Sélectionnez **Continuer**.
5. si vous avez sélectionné **TLS** ou **RELP/TLS**, téléchargez les certificats suivants :
   - **Certificats CA serveur** : un ou plusieurs certificats CA de confiance pour la vérification du serveur syslog externe (dans le codage PEM). Si omis, le certificat d'autorité de certification de la grille par

défaut sera utilisé. Le fichier que vous téléchargez ici peut être un bundle CA.

- **Certificat client** : certificat client pour l'authentification sur le serveur syslog externe (dans le codage PEM).
- **Clé privée client** : clé privée pour le certificat client (dans le codage PEM).

> Si vous utilisez un certificat client, vous devez également utiliser une clé privée client. Si vous fournissez une clé privée chiffrée, vous devez également fournir la phrase de passe. L'utilisation d'une clé privée chiffrée n'est pas un avantage majeur en matière de sécurité, car la clé et la phrase de passe doivent être stockées. Si elles sont disponibles, il est recommandé de recourir à une clé privée non chiffrée pour plus de simplicité.

i. Sélectionnez **Parcourir** pour le certificat ou la clé que vous souhaitez utiliser.
ii. Sélectionnez le fichier de certificat ou le fichier de clé.
iii. Sélectionnez **Ouvrir** pour charger le fichier.

Une coche verte s'affiche en regard du nom du fichier de certificat ou de clé, vous informant qu'il a été téléchargé avec succès.

6. Sélectionnez **Continuer**.

Gérer le contenu du journal système

Vous pouvez sélectionner les informations à envoyer au serveur syslog externe.

Étapes

1. Pour l'étape **gérer le contenu syslog** de l'assistant, sélectionnez chaque type d'informations d'audit que vous souhaitez envoyer au serveur syslog externe.
   - **Envoyer les journaux d'audit** : envoie les événements StorageGRID et les activités système
   - **Envoyer des événements de sécurité** : envoie des événements de sécurité tels qu'une tentative d'ouverture de session par un utilisateur non autorisé ou une ouverture de session par un utilisateur en tant que root
   - **Envoyer les journaux d'application** : envoie les fichiers journaux utiles pour le dépannage, notamment :
     - `bycast-err.log`
     - `bycast.log`
     - `jaeger.log`
     - `nms.log` (Nœuds d'administration uniquement)
     - `prometheus.log`
     - `raft.log`
     - `hagroups.log`
2. Utilisez les menus déroulants pour sélectionner la gravité et l'installation (type de message) de la catégorie d'informations d'audit que vous souhaitez envoyer.

   Si vous sélectionnez **Passthrough** pour la gravité et l'installation, les informations envoyées au serveur syslog distant recevront la même gravité et les mêmes fonctions qu'lorsqu'il est connecté localement au nœud. La définition de l'installation et de la gravité peut vous aider à agréger les journaux de manière

personnalisable pour faciliter l'analyse.

> Pour plus d'informations sur les journaux du logiciel StorageGRID, reportez-vous à la section "Journaux du logiciel StorageGRID".

a. Pour **gravité**, sélectionnez **passe-système** si vous souhaitez que chaque message envoyé au syslog externe ait la même valeur de gravité que dans le syslog local.

   Pour les journaux d'audit, si vous sélectionnez **Passthrough**, la gravité est 'info'.

   Pour les événements de sécurité, si vous sélectionnez **Passthrough**, les valeurs de gravité sont générées par la distribution Linux sur les nœuds.

   Pour les journaux d'application, si vous sélectionnez **Passthrough**, les niveaux de gravité varient entre 'info' et 'avis', selon le problème. Par exemple, l'ajout d'un serveur NTP et la configuration d'un groupe HA donnent la valeur « INFO », tandis que l'arrêt délibéré du service SSM ou RSM donne la valeur « notification ».

b. Si vous ne souhaitez pas utiliser la valeur passthrough, sélectionnez une valeur de gravité comprise entre 0 et 7.

   La valeur sélectionnée sera appliquée à tous les messages de ce type. Les informations sur les différents niveaux de gravité seront perdues lorsque vous choisissez de remplacer la gravité par une valeur fixe.

Gravité	Description
0	Urgence : le système est inutilisable
1	Alerte : une action doit être effectuée immédiatement
2	Critique : conditions critiques
3	Erreur : conditions d'erreur
4	Avertissement : conditions d'avertissement
5	Remarque : condition normale mais significative
6	Information : messages d'information
7	Débogage : messages de niveau débogage

c. Pour **Facility**, sélectionnez **Passthrough** si vous souhaitez que chaque message envoyé au syslog externe ait la même valeur que dans le syslog local.

   Pour les journaux d'audit, si vous sélectionnez **Passthrough**, la fonction envoyée au serveur syslog externe est « local7 ».

   Pour les événements de sécurité, si vous sélectionnez **passe-système**, les valeurs de l'établissement sont générées par la distribution linux sur les nœuds.

Pour les journaux d'application, si vous sélectionnez **passe-système**, les journaux d'application envoyés au serveur syslog externe ont les valeurs d'installation suivantes :

Journal de l'application	Valeur passe-système
bycast.log	utilisateur ou démon
bycast-err.log	utilisateur, démon, local3 ou local4
jaeger.log	localis2
nms.log	local3
prometheus.log	local4
raft.log	local5
hagroups.log	local6

d. Si vous ne souhaitez pas utiliser la valeur passthrough, sélectionnez la valeur de l'installation comprise entre 0 et 23.

   La valeur sélectionnée sera appliquée à tous les messages de ce type. Les informations sur les différentes installations seront perdues lorsque vous choisissez de remplacer l'établissement par une valeur fixe.

Installation	Description
0	kern (messages du noyau)
1	utilisateur (messages de niveau utilisateur)
2	e-mail
3	démon (démons système)
4	auth (messages de sécurité/d'autorisation)
5	syslog (messages générés en interne par syslogd)
6	lpr (sous-système d'imprimante ligne)
7	news (sous-système d'informations réseau)
8	UCP
9	cron (démon d'horloge)

Installation	Description
10	sécurité (messages de sécurité/d'autorisation)
11	FTP
12	NTP
13	audit journal (audit du journal)
14	alerte journal (alerte de journal)
15	horloge (démon d'horloge)
16	localis0
17	local1
18	localis2
19	local3
20	local4
21	local5
22	local6
23	localis7

3. Sélectionnez **Continuer**.

Envoyer des messages de test

Avant de commencer à utiliser un serveur syslog externe, vous devez demander à tous les nœuds de votre grille d'envoyer des messages de test au serveur syslog externe. Ces messages de test vous aideront à valider l'intégralité de votre infrastructure de collecte de journaux avant de vous engager à envoyer des données au serveur syslog externe.

> N'utilisez pas la configuration du serveur syslog externe tant que vous n'avez pas confirmé que le serveur syslog externe a reçu un message test de chaque nœud de votre grille et que le message a été traité comme prévu.

Étapes

1. Si vous ne souhaitez pas envoyer de messages de test parce que vous êtes certain que votre serveur syslog externe est correctement configuré et peut recevoir des informations d'audit de tous les nœuds de votre grille, sélectionnez **Ignorer et terminer**.

Une bannière verte s'affiche, indiquant que votre configuration a été correctement enregistrée.

2. Sinon, sélectionnez **Envoyer les messages de test** (recommandé).

   Les résultats de test apparaissent en permanence sur la page jusqu'à ce que vous arrêiez le test. Pendant que le test est en cours, vos messages d'audit continuent d'être envoyés à vos destinations précédemment configurées.

3. Si vous recevez des erreurs, corrigez-les et sélectionnez à nouveau **Envoyer des messages de test**.

   Voir "Dépannage du serveur syslog externe" pour vous aider à résoudre toutes les erreurs.

4. Attendez qu'une bannière verte indique que tous les nœuds ont réussi le test.
5. Vérifiez votre serveur syslog pour déterminer si les messages de test sont reçus et traités comme prévu.

   > Si vous utilisez UDP, vérifiez l'ensemble de votre infrastructure de collecte de journaux. Le protocole UDP ne permet pas une détection d'erreur aussi rigoureuse que les autres protocoles.

6. Sélectionnez **Arrêter et Terminer**.

   Vous revenez à la page **Audit and syslog Server**. Une bannière verte s'affiche pour vous informer que la configuration de votre serveur syslog a bien été enregistrée.

   > Vos informations d'audit StorageGRID ne sont pas envoyées au serveur syslog externe tant que vous n'avez pas sélectionné une destination qui inclut le serveur syslog externe.

Sélectionnez les destinations des informations d'audit

Vous pouvez spécifier l'emplacement d'envoi des journaux d'événements de sécurité, des journaux d'application et des journaux de messages d'audit.

> Pour plus d'informations sur les journaux du logiciel StorageGRID, reportez-vous à la section "Journaux du logiciel StorageGRID".

Étapes

1. Sur la page Audit and syslog Server, sélectionnez la destination des informations d'audit dans les options répertoriées :

Option	Description
Par défaut (nœuds d'administration/nœuds locaux)	Les messages d'audit sont envoyés au journal d'audit (`audit.log`) Sur le nœud d'administration, les journaux d'événements de sécurité et les journaux d'applications sont stockés sur les nœuds où ils ont été générés (également appelés « nœud local »).
Serveur syslog externe	Les informations d'audit sont envoyées à un serveur syslog externe et enregistrées sur le nœud local. Le type d'information envoyée dépend de la façon dont vous avez configuré le serveur syslog externe. Cette option n'est activée qu'après avoir configuré un serveur syslog externe.

Option	Description
Nœud d'administration et serveur syslog externe	Les messages d'audit sont envoyés au journal d'audit (`audit.log`) Sur le nœud d'administration, les informations d'audit sont envoyées au serveur syslog externe et enregistrées sur le nœud local. Le type d'information envoyée dépend de la façon dont vous avez configuré le serveur syslog externe. Cette option n'est activée qu'après avoir configuré un serveur syslog externe.
Nœuds locaux uniquement	Aucune information d'audit n'est envoyée à un nœud d'administration ou à un serveur syslog distant. Les informations d'audit sont enregistrées uniquement sur les nœuds qui les ont générées. **Remarque**: StorageGRID supprime périodiquement ces journaux locaux dans une rotation pour libérer de l'espace. Lorsque le fichier journal d'un nœud atteint 1 Go, le fichier existant est enregistré et un nouveau fichier journal est démarré. La limite de rotation du journal est de 21 fichiers. Lorsque la 22e version du fichier journal est créée, le fichier journal le plus ancien est supprimé. En moyenne, environ 20 Go de données de journalisation sont stockés sur chaque nœud.

Les informations d'audit générées sur chaque nœud local sont stockées dans `/var/local/log/localaudit.log`

2. Sélectionnez **Enregistrer**. Ensuite, sélectionnez **OK** pour accepter la modification de la destination du journal.
3. Si vous avez sélectionné **serveur syslog externe** ou **nœuds Admin et serveur syslog externe** comme destination pour les informations d'audit, un avertissement supplémentaire s'affiche. Passez en revue le texte d'avertissement.

Vous devez confirmer que le serveur syslog externe peut recevoir des messages StorageGRID de test.

4. Sélectionnez **OK** pour confirmer que vous souhaitez modifier la destination des informations d'audit.

   Une bannière verte s'affiche pour vous informer que la configuration de votre audit a bien été enregistrée.

   Les nouveaux journaux sont envoyés aux destinations que vous avez sélectionnées. Les journaux existants restent à leur emplacement actuel.

Informations associées

"Présentation du message d'audit"

"Configurez les messages d'audit et les destinations des journaux"

"Messages d'audit système"

"Messages d'audit du stockage objet"

"Message d'audit de gestion"

"Messages d'audit de lecture du client"

"Administrer StorageGRID"

Utiliser la surveillance SNMP

Utiliser la surveillance SNMP : présentation

Si vous souhaitez surveiller StorageGRID à l'aide du protocole SNMP (simple Network Management Protocol), vous devez configurer l'agent SNMP inclus avec StorageGRID.

- "Configurez l'agent SNMP"
- "Mettez à jour l'agent SNMP"

Capacités

Chaque nœud StorageGRID exécute un agent SNMP, ou démon, qui fournit une MIB. La MIB StorageGRID contient des définitions de tableau et de notification pour les alertes et les alarmes. La base MIB contient également des informations de description du système, telles que la plateforme et le numéro de modèle pour chaque nœud. Chaque nœud StorageGRID supporte également un sous-ensemble d'objets MIB-II.

Voir "Accéder aux fichiers MIB" Si vous souhaitez télécharger les fichiers MIB sur vos nœuds grid.

Au départ, le protocole SNMP est désactivé sur tous les nœuds. Lorsque vous configurez l'agent SNMP, tous les nœuds StorageGRID reçoivent la même configuration.

L'agent SNMP StorageGRID prend en charge les trois versions du protocole SNMP. Il fournit un accès MIB en lecture seule pour les requêtes et il peut envoyer deux types de notifications événementielle à un système de gestion :

- **Traps** sont des notifications envoyées par l'agent SNMP qui ne nécessitent pas d'acquittement par le système de gestion. Les interruptions servent à signaler au système de gestion qu'une alerte s'est produite au sein de StorageGRID, par exemple.

  Les traps sont pris en charge dans les trois versions de SNMP.

- **Inform** sont similaires aux pièges, mais ils exigent une reconnaissance du système de gestion. Si l'agent SNMP ne reçoit pas d'accusé de réception dans un certain temps, il renvoie l'information jusqu'à ce qu'un accusé de réception soit reçu ou que la valeur de nouvelle tentative maximale ait été atteinte.

  Les informations sont prises en charge dans SNMPv2c et SNMPv3.

Les notifications d'interruption et d'information sont envoyées dans les cas suivants :

- Une alerte par défaut ou personnalisée est déclenchée à tout niveau de gravité. Pour supprimer les notifications SNMP pour une alerte, vous devez configurer un silence pour l'alerte. Les notifications d'alerte sont envoyées par "Nœud d'administration de l'expéditeur préféré".

  Chaque alerte est associée à l'un des trois types de déroutement en fonction du niveau de gravité de l'alerte : activeMinorAlert, activeMajorAlert et activeCriticalAlert. Pour obtenir la liste des alertes pouvant déclencher ces interruptions, reportez-vous au "Référence des alertes".

- Certaines alarmes (système hérité) sont déclenchées à des niveaux de gravité spécifiés ou plus.

> Les notifications SNMP ne sont pas envoyées pour chaque alarme ou chaque gravité d'alarme.

Prise en charge de la version SNMP

Le tableau fournit un résumé détaillé des éléments pris en charge pour chaque version de SNMP.

	SNMPv1	SNMPv2c	SNMPv3
Requêtes	Requêtes MIB en lecture seule	Requêtes MIB en lecture seule	Requêtes MIB en lecture seule
Authentification par requête	Chaîne de communauté	Chaîne de communauté	Utilisateur USM (User Security Model)
Notifications	Traps uniquement	Pièges et information	Pièges et information
Authentification des notifications	Communauté d'interruptions par défaut ou chaîne de communauté personnalisée pour chaque destination d'interruption	Communauté d'interruptions par défaut ou chaîne de communauté personnalisée pour chaque destination d'interruption	Utilisateur USM pour chaque destination d'interruption

Limites

- StorageGRID supporte l'accès MIB en lecture seule. L'accès en lecture/écriture n'est pas pris en charge.
- Tous les nœuds de la grille reçoivent la même configuration.
- SNMPv3 : StorageGRID ne prend pas en charge le mode support transport (TSM).
- SNMPv3 : le seul protocole d'authentification pris en charge est SHA (HMAC-SHA-96).
- SNMPv3 : le seul protocole de confidentialité pris en charge est AES.

Informations associées

- "Référence des alertes"
- "Référence des alarmes (système hérité)"
- "Notifications d'alerte de silence"

Configurez l'agent SNMP

Vous pouvez configurer l'agent SNMP StorageGRID si vous souhaitez utiliser un système de gestion SNMP tiers pour l'accès MIB en lecture seule et les notifications.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous disposez de l'autorisation d'accès racine.

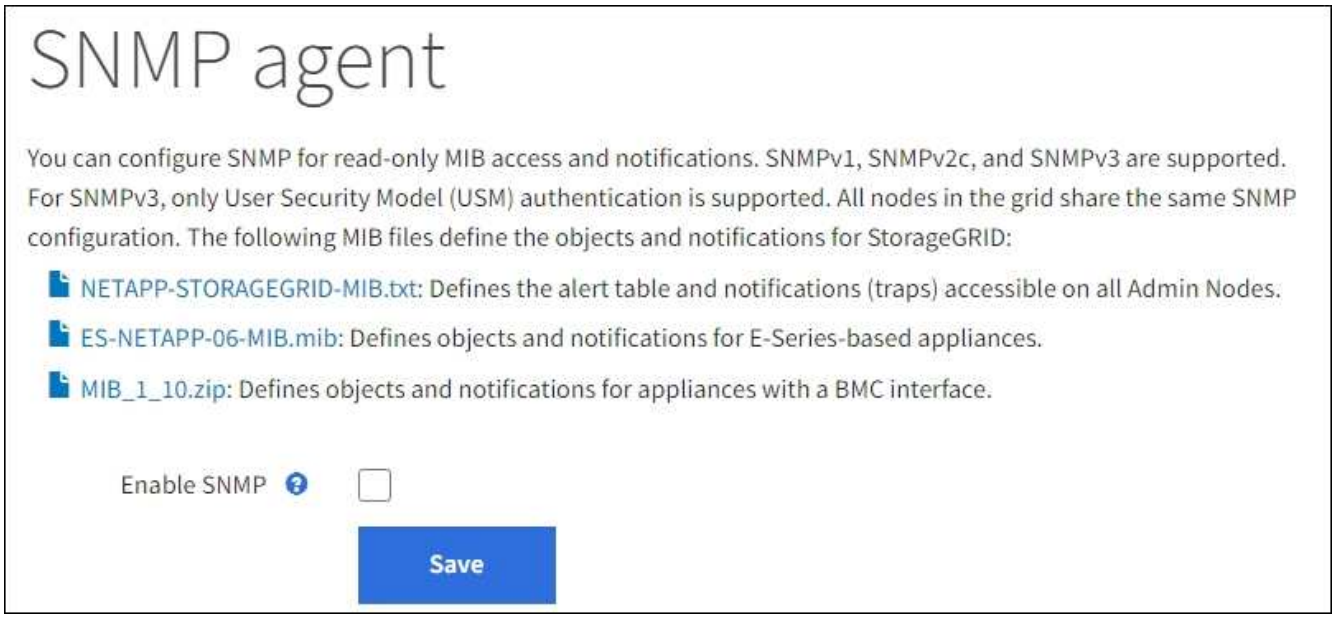
Description de la tâche

L'agent SNMP StorageGRID prend en charge les trois versions du protocole SNMP. Vous pouvez configurer l'agent pour une ou plusieurs versions.

Étapes

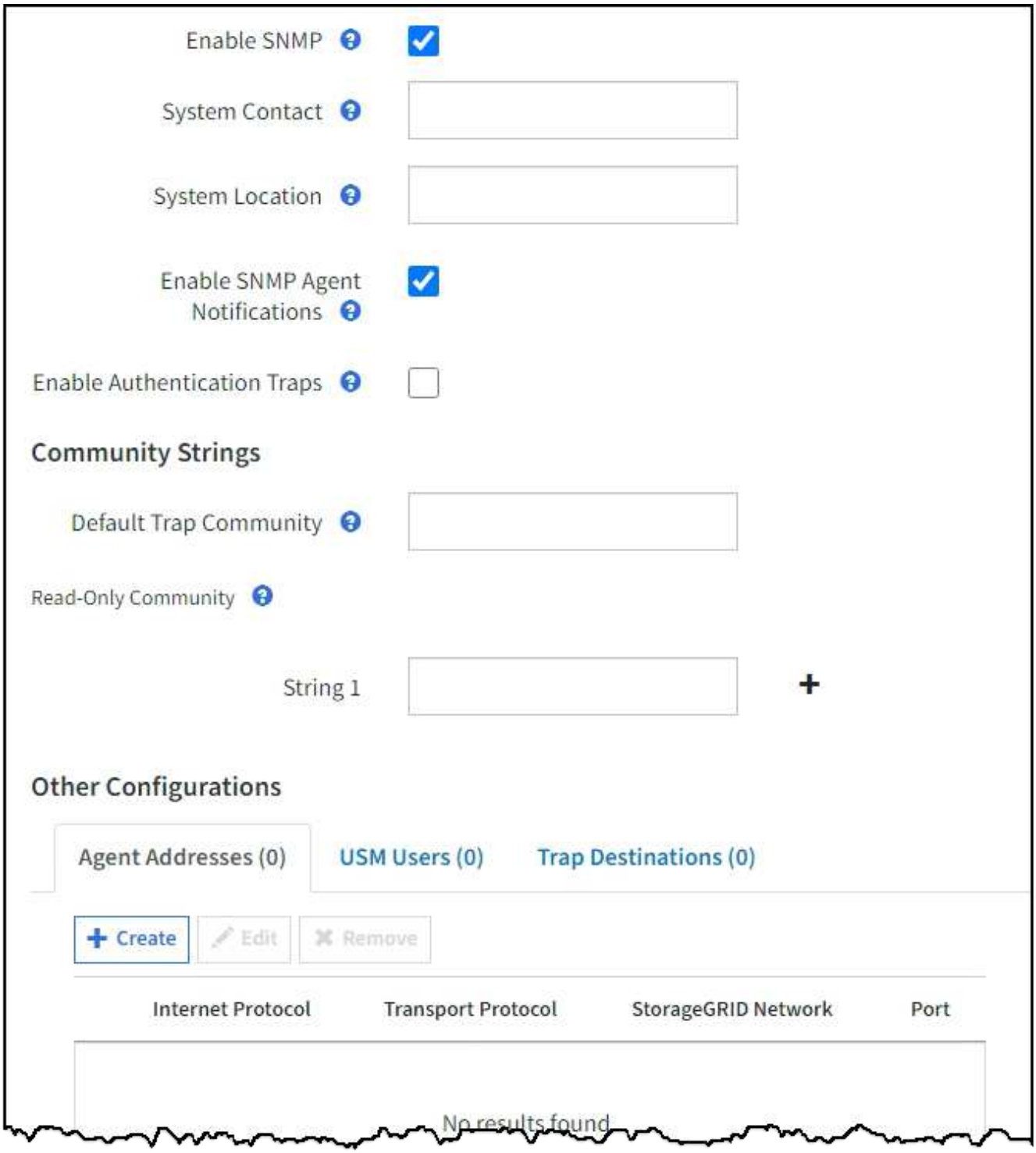
1. Sélectionnez **CONFIGURATION** > **surveillance** > **agent SNMP**.

   La page agent SNMP s'affiche.



2. Pour activer l'agent SNMP sur tous les nœuds de la grille, cochez la case **Activer SNMP**.

   Les champs de configuration d'un agent SNMP s'affichent.



3. Dans le champ **Contact système**, entrez la valeur que vous souhaitez que StorageGRID vous apporte dans les messages SNMP pour sysContact.

   Le contact système est généralement une adresse e-mail. La valeur indiquée s'applique à tous les nœuds du système StorageGRID. **Contact système** peut comporter un maximum de 255 caractères.

4. Dans le champ **emplacement du système**, entrez la valeur que vous souhaitez que StorageGRID vous apporte dans les messages SNMP pour sysLocation.

   L'emplacement du système peut être toute information utile pour identifier l'emplacement de votre système StorageGRID. Par exemple, vous pouvez utiliser l'adresse d'un établissement. La valeur indiquée

s'applique à tous les nœuds du système StorageGRID. **Emplacement du système** peut comporter un maximum de 255 caractères.

5. Laissez la case **Activer les notifications d'agent SNMP** cochée si vous souhaitez que l'agent SNMP StorageGRID envoie des notifications d'interruption et d'information.

   Si cette case est décochée, l'agent SNMP prend en charge l'accès MIB en lecture seule, mais n'envoie pas de notifications SNMP.

6. Cochez la case **Activer les interruptions d'authentification** si vous souhaitez que l'agent SNMP StorageGRID envoie une interruption d'authentification s'il reçoit un message de protocole authentifié de façon incorrecte.
7. Si vous utilisez SNMPv1 ou SNMPv2c, complétez la section chaînes de communauté.

   Les champs de cette section sont utilisés pour l'authentification communautaire dans SNMPv1 ou SNMPv2c. Ces champs ne s'appliquent pas au protocole SNMPv3.

   a. Dans le champ **Default Trap Community**, vous pouvez également saisir la chaîne de communauté par défaut que vous souhaitez utiliser pour les destinations de déroutement.

      Selon les besoins, vous pouvez fournir une autre chaîne de communauté (« personnalisée ») lorsque vous définir une destination de recouvrement spécifique.

      Default Trap Community peut comporter un maximum de 32 caractères et ne peut pas contenir de caractères d'espace.

   b. Pour **Read-Only Community**, entrez une ou plusieurs chaînes de communauté pour autoriser l'accès MIB en lecture seule sur les adresses d'agent IPv4 et IPv6. Sélectionnez le signe plus ➕ pour ajouter plusieurs chaînes.

      Lorsque le système de gestion interroge la MIB StorageGRID, il envoie une chaîne de communauté. Si la chaîne de communauté correspond à l'une des valeurs spécifiées ici, l'agent SNMP envoie une réponse au système de gestion.

      Chaque chaîne de communauté peut comporter un maximum de 32 caractères et ne peut pas contenir de caractères d'espace. Jusqu'à cinq chaînes sont autorisées.

      ⓘ Pour assurer la sécurité de votre système StorageGRID, n'utilisez pas « public » comme chaîne de communauté. Si vous n'entrez pas de chaîne de communauté, l'agent SNMP utilise l'ID de grille de votre système StorageGRID comme chaîne de communauté.

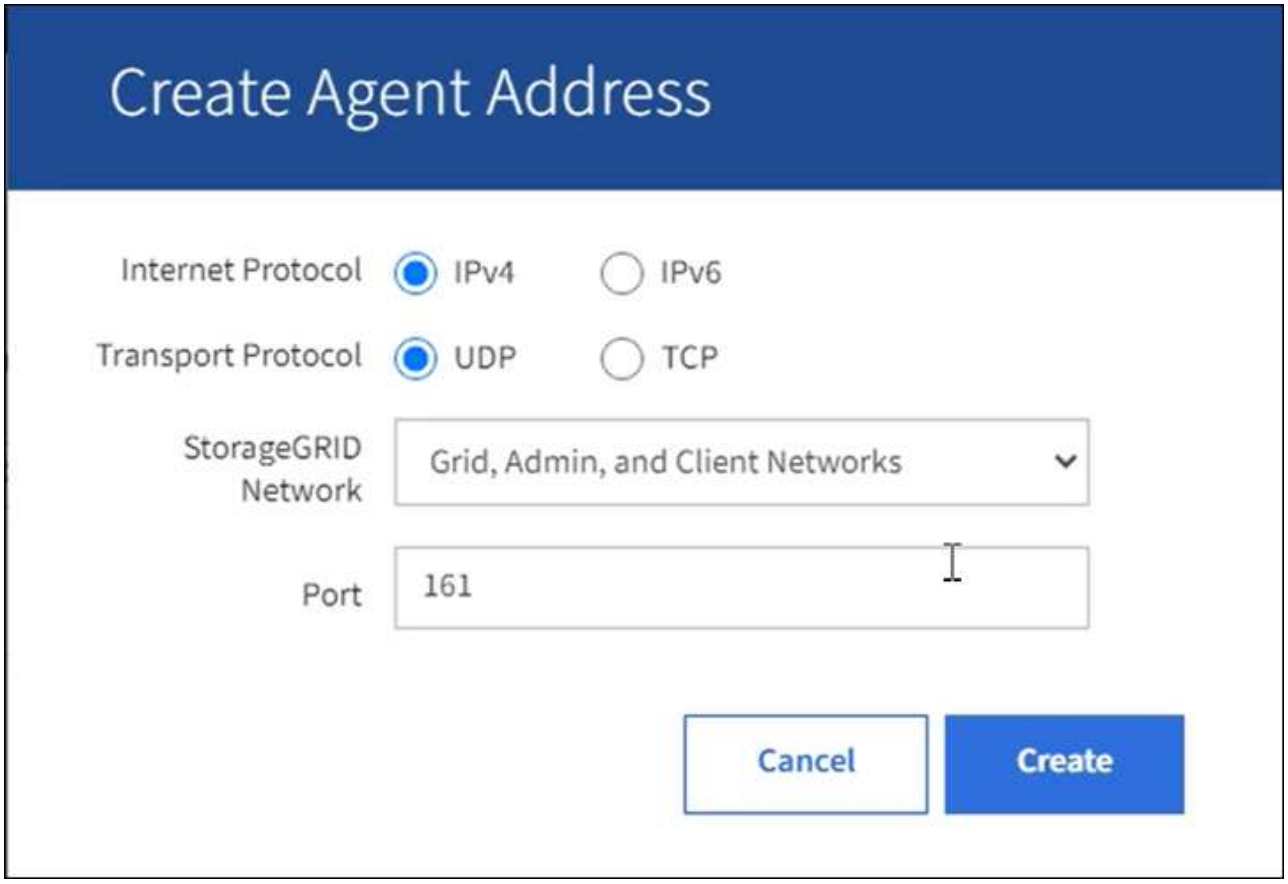
8. Vous pouvez également sélectionner l'onglet adresses d'agent dans la section autres configurations.

   Utilisez cet onglet pour spécifier une ou plusieurs « adresses d'écoute ». Ce sont les adresses StorageGRID sur lesquelles l'agent SNMP peut recevoir des requêtes. Chaque adresse de l'agent inclut un protocole Internet, un protocole de transport, un réseau StorageGRID et éventuellement un port.

   Si vous ne configurez pas d'adresse d'agent, l'adresse d'écoute par défaut est le port UDP 161 sur tous les réseaux StorageGRID.

   a. Sélectionnez **Créer**.

      La boîte de dialogue Créer une adresse d'agent s'affiche.



b. Pour **Internet Protocol**, indiquez si cette adresse doit utiliser IPv4 ou IPv6.

   Par défaut, SNMP utilise IPv4.

c. Pour **transport Protocol**, sélectionnez si cette adresse utilisera UDP ou TCP.

   Par défaut, SNMP utilise UDP.

d. Dans le champ **réseau StorageGRID**, sélectionnez le réseau StorageGRID sur lequel la requête sera reçue.

   - Réseau Grid, Admin et client : StorageGRID doit écouter les requêtes SNMP sur les trois réseaux.
   - Réseau Grid
   - Réseau d'administration
   - Réseau client

   > Pour vous assurer que les communications client avec StorageGRID restent sécurisées, vous ne devez pas créer d'adresse d'agent pour le réseau client.

e. Dans le champ **Port**, saisissez éventuellement le numéro de port que l'agent SNMP doit écouter.

   Le port UDP par défaut d'un agent SNMP est 161, mais vous pouvez entrer n'importe quel numéro de port inutilisé.

Lorsque vous enregistrez l'agent SNMP, StorageGRID ouvre automatiquement les ports d'adresse de l'agent sur le pare-feu interne. Vous devez vous assurer que tous les pare-feu externes autorisent l'accès à ces ports.

f. Sélectionnez **Créer**.

L'adresse de l'agent est créée et ajoutée à la table.

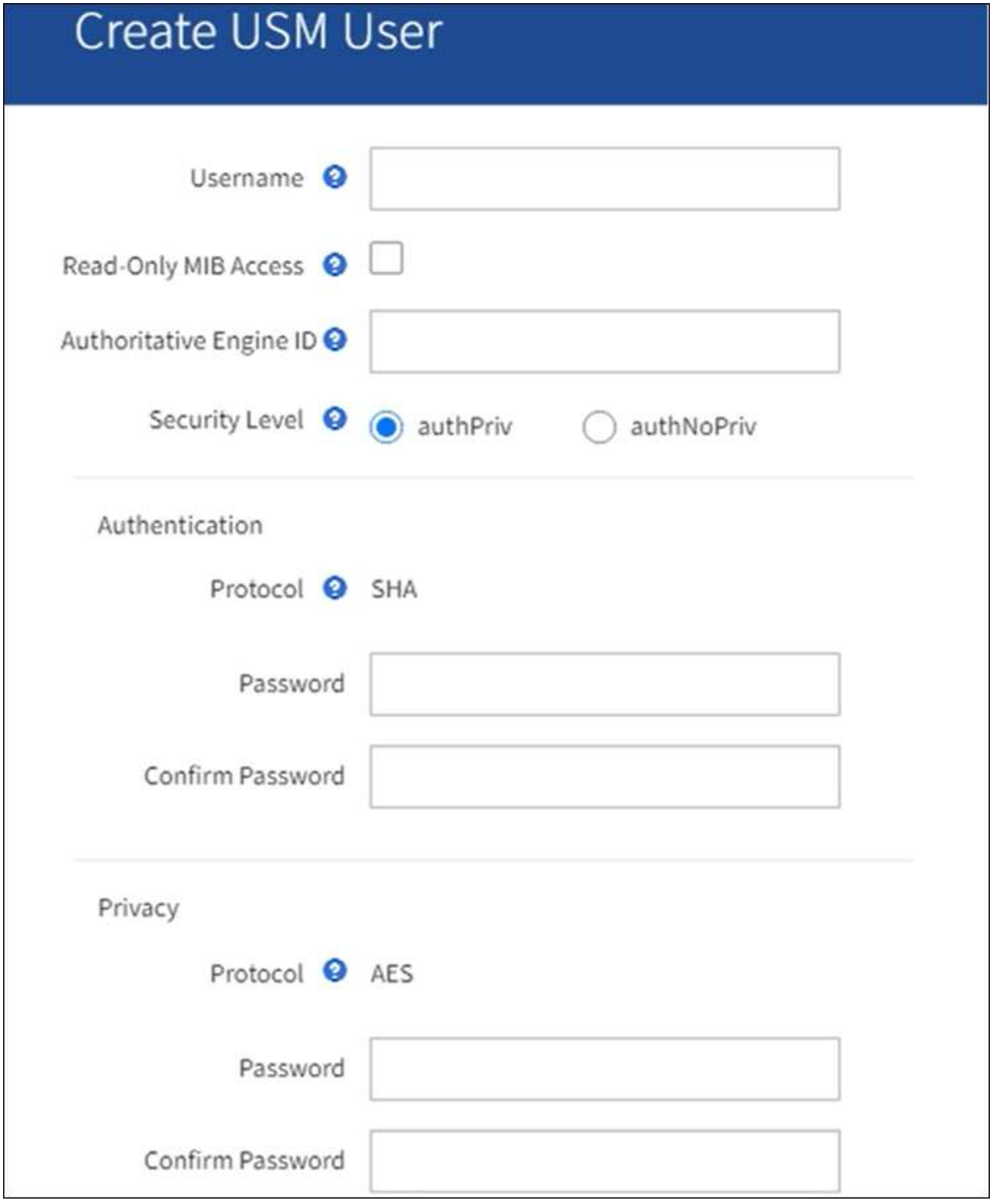
9. Si vous utilisez SNMPv3, sélectionnez l'onglet utilisateurs USM dans la section autres configurations.

Utilisez cet onglet pour définir les utilisateurs USM autorisés à interroger la MIB ou à recevoir des interruptions et des informations.

Cette étape ne s'applique pas si vous utilisez uniquement SNMPv1 ou SNMPv2c.

a. Sélectionnez **Créer**.

La boîte de dialogue Créer un utilisateur USM s'affiche.



b. Saisissez un **Nom d'utilisateur** unique pour cet utilisateur USM.

   Les noms d'utilisateur ont un maximum de 32 caractères et ne peuvent pas contenir de caractères d'espace. Le nom d'utilisateur ne peut pas être modifié après la création de l'utilisateur.

c. Cochez la case **accès MIB en lecture seule** si cet utilisateur doit avoir un accès en lecture seule à la MIB.

   Si vous sélectionnez **accès MIB en lecture seule**, le champ **ID moteur autorisée** est désactivé.

Les utilisateurs USM disposant d'un accès MIB en lecture seule ne peuvent pas avoir d'ID de moteur.

d. Si cet utilisateur sera utilisé dans une destination INFORM, saisissez l'ID de moteur * faisant autorité pour cet utilisateur.

Les destinations SNMPv3 INFORM doivent avoir des utilisateurs avec des ID de moteur. La destination d'interruption SNMPv3 ne peut pas avoir d'utilisateurs avec des ID de moteur.

L'ID de moteur faisant autorité peut être de 5 à 32 octets en hexadécimal.

e. Sélectionnez un niveau de sécurité pour l'utilisateur USM.

- **AuthPriv** : cet utilisateur communique avec l'authentification et la confidentialité (cryptage). Vous devez spécifier un protocole d'authentification et un mot de passe ainsi qu'un protocole de confidentialité et un mot de passe.
- **AuthNoPriv**: Cet utilisateur communique avec l'authentification et sans confidentialité (pas de cryptage). Vous devez spécifier un protocole d'authentification et un mot de passe.

f. Entrez et confirmez le mot de passe que cet utilisateur utilisera pour l'authentification.

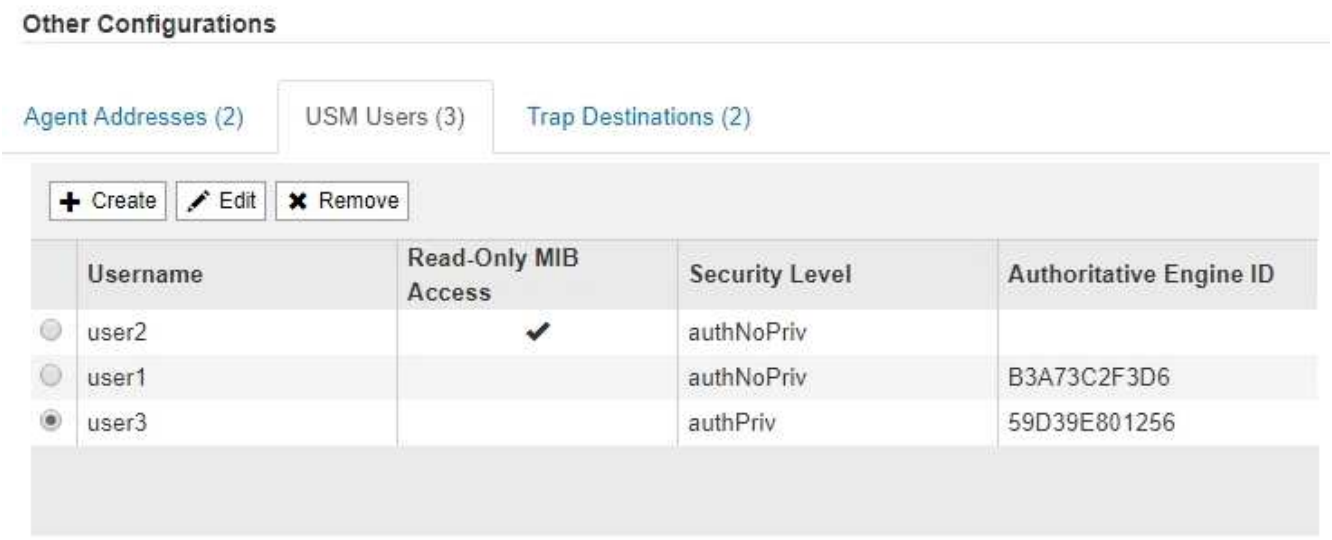
Le seul protocole d'authentification pris en charge est SHA (HMAC-SHA-96).

g. Si vous avez sélectionné **authPriv**, entrez et confirmez le mot de passe que cet utilisateur utilisera pour la confidentialité.

Le seul protocole de confidentialité pris en charge est AES.

h. Sélectionnez **Créer**.

L'utilisateur USM est créé et ajouté à la table.



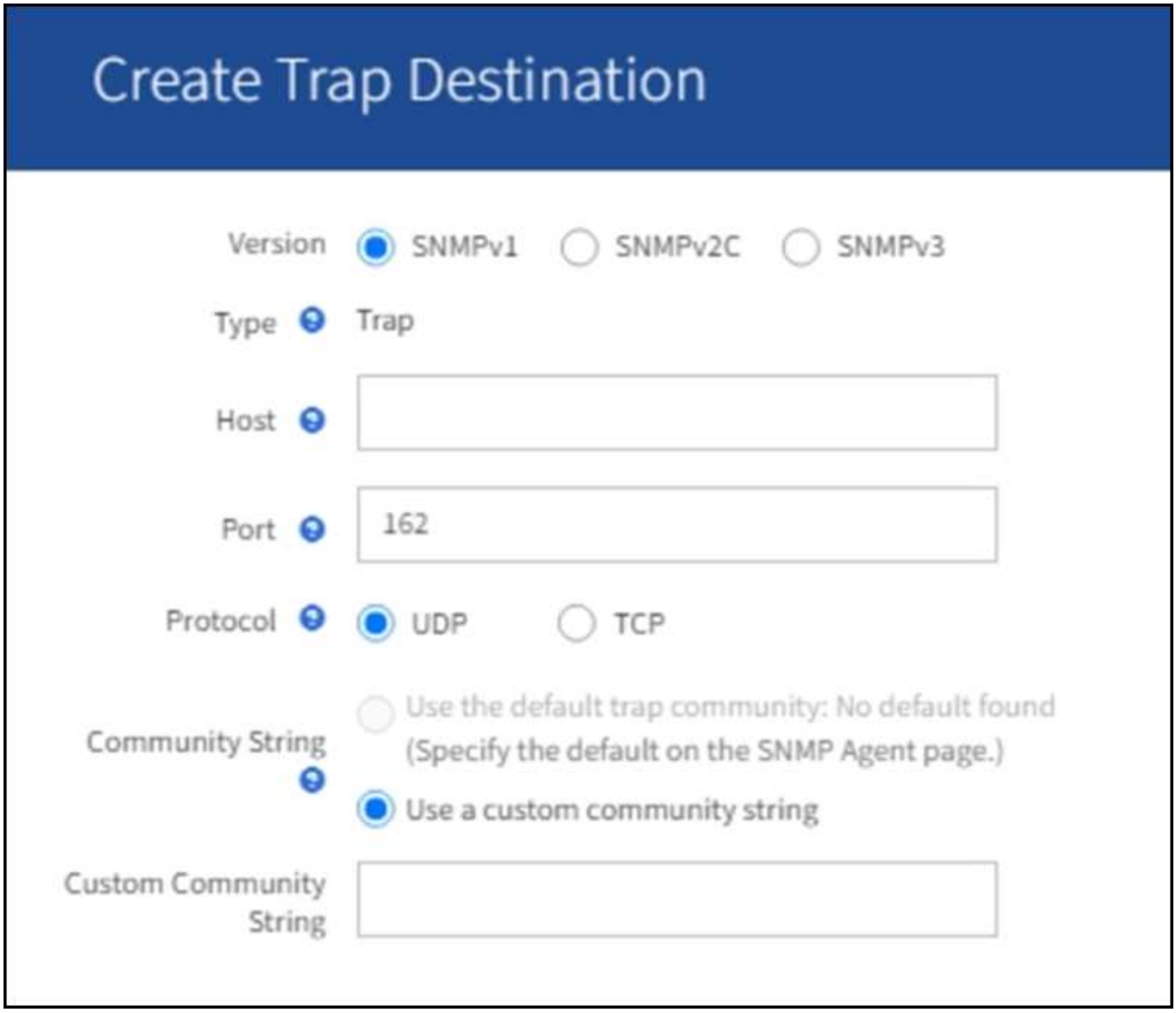
10. dans la section autres configurations, sélectionnez l'onglet destinations de recouvrement.

L'onglet destinations de recouvrement permet de définir une ou plusieurs destinations pour les notifications

d’interruption StorageGRID ou d’information. Lorsque vous activez l’agent SNMP et sélectionnez **Enregistrer**, StorageGRID commence à envoyer des notifications à chaque destination définie. Des notifications sont envoyées lorsque des alertes sont déclenchées. Les notifications standard sont également envoyées pour les entités MIB-II prises en charge (par exemple, ifdown et coldStart).

a. Sélectionnez **Créer**.

   La boîte de dialogue Créer une destination de recouvrement s’affiche.



a. Dans le champ **version**, sélectionnez la version SNMP à utiliser pour cette notification.
b. Remplissez le formulaire en fonction de la version que vous avez sélectionnée

Version	Spécifiez ces informations
SNMPv1 (Pour SNMPv1, l'agent SNMP ne peut envoyer que des interruptions. Les informations ne sont pas prises en charge.)	i. Dans le champ **Host**, entrez une adresse IPv4 ou IPv6 (ou FQDN) pour recevoir l'interruption. ii. Pour **Port**, utilisez la valeur par défaut (162), sauf si vous devez utiliser une autre valeur. (162 est le port standard des traps SNMP.) iii. Pour **Protocol**, utilisez la valeur par défaut (UDP). TCP est également pris en charge. (UDP est le protocole standard d'interruption SNMP.) iv. Utilisez la communauté d'interruptions par défaut, si l'une d'entre elles a été spécifiée sur la page agent SNMP, ou entrez une chaîne de communauté personnalisée pour cette destination d'interruption. La chaîne de communauté personnalisée peut comporter jusqu'à 32 caractères et ne peut pas contenir d'espace.
SNMPv2c	i. Indiquez si la destination sera utilisée pour les interruptions ou pour les informations. ii. Dans le champ **Host**, entrez une adresse IPv4 ou IPv6 (ou FQDN) pour recevoir l'interruption. iii. Pour **Port**, utilisez la valeur par défaut (162), sauf si vous devez utiliser une autre valeur. (162 est le port standard des traps SNMP.) iv. Pour **Protocol**, utilisez la valeur par défaut (UDP). TCP est également pris en charge. (UDP est le protocole standard d'interruption SNMP.) v. Utilisez la communauté d'interruptions par défaut, si l'une d'entre elles a été spécifiée sur la page agent SNMP, ou entrez une chaîne de communauté personnalisée pour cette destination d'interruption. La chaîne de communauté personnalisée peut comporter jusqu'à 32 caractères et ne peut pas contenir d'espace.

Version	Spécifiez ces informations
SNMPv3	i. Indiquez si la destination sera utilisée pour les interruptions ou pour les informations. ii. Dans le champ **Host**, entrez une adresse IPv4 ou IPv6 (ou FQDN) pour recevoir l'interruption. iii. Pour **Port**, utilisez la valeur par défaut (162), sauf si vous devez utiliser une autre valeur. (162 est le port standard des traps SNMP.) iv. Pour **Protocol**, utilisez la valeur par défaut (UDP). TCP est également pris en charge. (UDP est le protocole standard d'interruption SNMP.) v. Sélectionnez l'utilisateur USM qui sera utilisé pour l'authentification. ◦ Si vous avez sélectionné **Trap**, seuls les utilisateurs d'USM sans ID de moteur faisant autorité sont affichés. ◦ Si vous avez sélectionné **INFORM**, seuls les utilisateurs d'USM avec des ID de moteur faisant autorité sont affichés.

c. Sélectionnez **Créer**.

La destination de la trappe est créée et ajoutée à la table.

11. Une fois la configuration de l'agent SNMP terminée, sélectionnez **Enregistrer**.

La nouvelle configuration de l'agent SNMP devient active.

Informations associées

"Notifications d'alerte de silence"

Mettez à jour l'agent SNMP

Vous pouvez désactiver les notifications SNMP, mettre à jour les chaînes de communauté ou ajouter ou supprimer des adresses d'agent, des utilisateurs USM et des destinations d'interruption.

Avant de commencer

- Vous devez être connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous devez disposer de l'autorisation d'accès racine.

Description de la tâche

Chaque fois que vous mettez à jour le "Configuration de l'agent SNMP", N'oubliez pas que vous devez sélectionner **Enregistrer** en bas de la page Agent SNMP pour valider les modifications que vous avez apportées à chaque onglet.

Étapes

1. Sélectionnez **CONFIGURATION** > **surveillance** > **agent SNMP**.

La page agent SNMP s'affiche.

2. Si vous souhaitez désactiver l'agent SNMP sur tous les nœuds de la grille, décochez la case **Activer SNMP** et sélectionnez **Enregistrer**.

   L'agent SNMP est désactivé pour tous les nœuds de la grille. Si vous réactivez ultérieurement l'agent, tous les paramètres de configuration SNMP précédents sont conservés.

3. Vous pouvez également mettre à jour les valeurs saisies pour **Contact système** et **emplacement système**.
4. Vous pouvez également décocher la case **Activer les notifications d'agent SNMP** si vous ne souhaitez plus que l'agent SNMP StorageGRID envoie des notifications d'interruption et d'information.

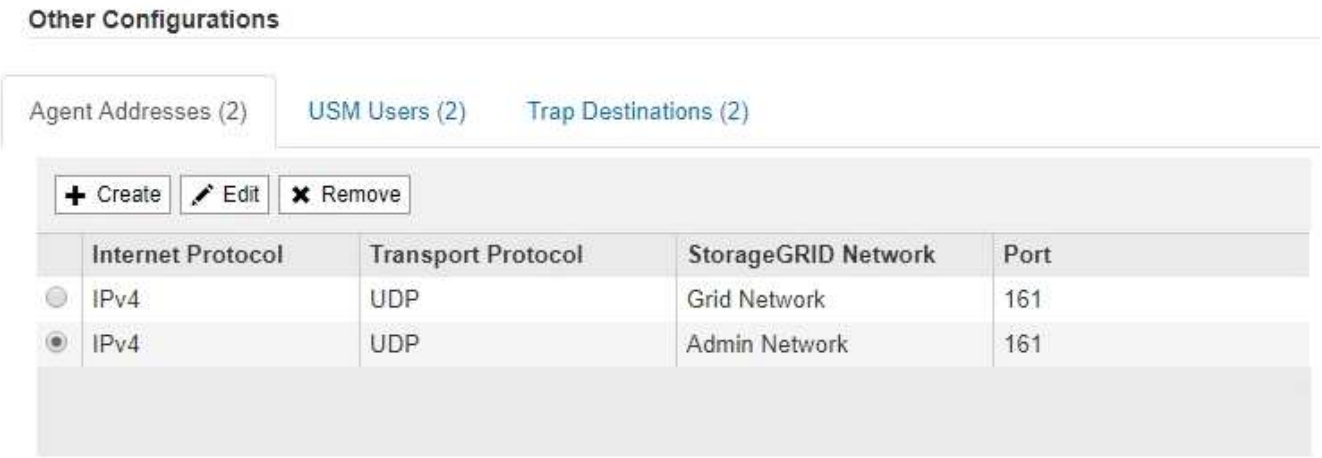
   Lorsque cette case est décochée, l'agent SNMP prend en charge l'accès MIB en lecture seule, mais n'envoie pas de notifications SNMP.

5. Vous pouvez également décocher la case **Activer les interruptions d'authentification** si vous ne souhaitez plus que l'agent SNMP StorageGRID envoie une interruption d'authentification lorsqu'il reçoit un message de protocole authentifié de manière incorrecte.
6. Si vous utilisez SNMPv1 ou SNMPv2c, vous pouvez mettre à jour la section chaînes de communauté.

   Les champs de cette section sont utilisés pour l'authentification communautaire dans SNMPv1 ou SNMPv2c. Ces champs ne s'appliquent pas au protocole SNMPv3.

   > Si vous souhaitez supprimer la chaîne de communauté par défaut, vous devez d'abord vous assurer que toutes les destinations de déroutement utilisent une chaîne de communauté personnalisée.

7. Pour mettre à jour les adresses des agents, sélectionnez l'onglet adresses des agents dans la section autres configurations.



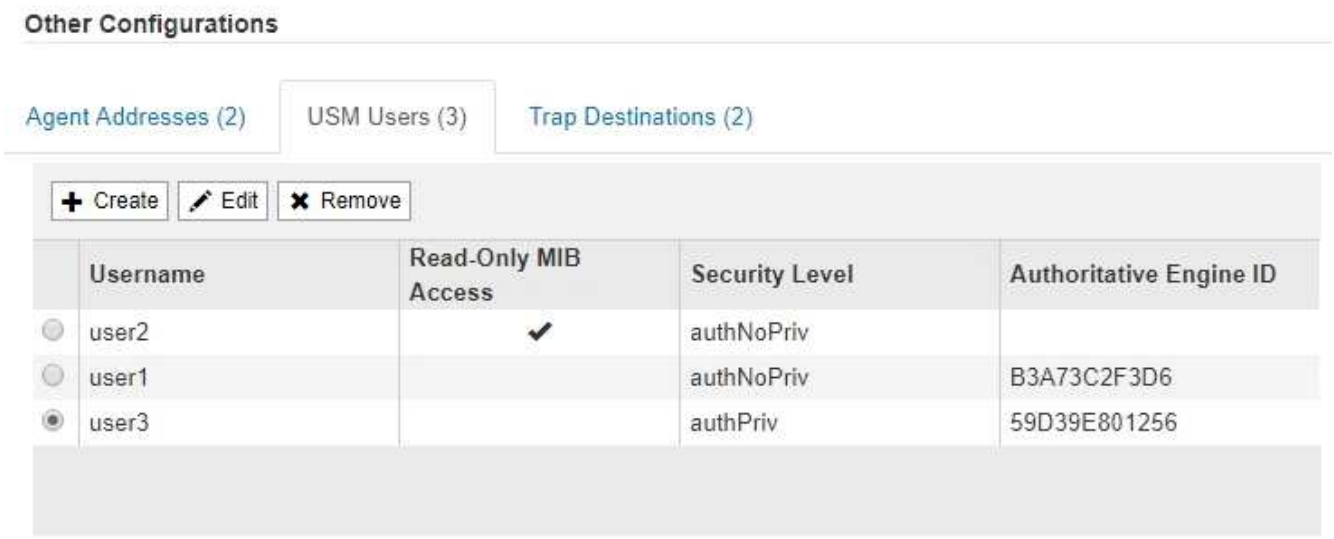
   Utilisez cet onglet pour spécifier une ou plusieurs « adresses d'écoute ». Ce sont les adresses StorageGRID sur lesquelles l'agent SNMP peut recevoir des requêtes. Chaque adresse de l'agent inclut un protocole Internet, un protocole de transport, un réseau StorageGRID et un port.

   a. Pour ajouter une adresse d'agent, sélectionnez **Créer**. Ensuite, reportez-vous à l'étape pour connaître les adresses des agents dans les instructions de configuration de l'agent SNMP.
   b. Pour modifier une adresse d'agent, sélectionnez le bouton radio correspondant à l'adresse et sélectionnez **Modifier**. Ensuite, reportez-vous à l'étape pour connaître les adresses des agents dans les instructions de configuration de l'agent SNMP.

c. Pour supprimer une adresse d'agent, sélectionnez le bouton radio correspondant à l'adresse et sélectionnez **Supprimer**. Ensuite, sélectionnez **OK** pour confirmer que vous souhaitez supprimer cette adresse.

d. Pour valider vos modifications, sélectionnez **Enregistrer** en bas de la page agent SNMP.

8. Pour mettre à jour les utilisateurs USM, sélectionnez l'onglet utilisateurs USM dans la section autres configurations.



Utilisez cet onglet pour définir les utilisateurs USM autorisés à interroger la MIB ou à recevoir des interruptions et des informations.

a. Pour ajouter un utilisateur USM, sélectionnez **Create**. Reportez-vous ensuite à l'étape pour les utilisateurs d'USM dans les instructions de configuration de l'agent SNMP.

b. Pour modifier un utilisateur USM, sélectionnez le bouton radio de l'utilisateur et sélectionnez **Modifier**. Reportez-vous ensuite à l'étape pour les utilisateurs d'USM dans les instructions de configuration de l'agent SNMP.

   Le nom d'utilisateur d'un utilisateur USM existant ne peut pas être modifié. Si vous devez modifier un nom d'utilisateur, vous devez le supprimer et en créer un nouveau.

> Si vous ajoutez ou supprimez l'ID moteur faisant autorité d'un utilisateur et que cet utilisateur est actuellement sélectionné pour une destination, vous devez modifier ou supprimer la destination, comme indiqué à l'étape Destination du trap SNMP. Sinon, une erreur de validation se produit lorsque vous enregistrez la configuration de l'agent SNMP.

a. Pour supprimer un utilisateur USM, sélectionnez le bouton radio de l'utilisateur et sélectionnez **Supprimer**. Ensuite, sélectionnez **OK** pour confirmer que vous souhaitez supprimer cet utilisateur.

> Si l'utilisateur que vous avez supprimé est actuellement sélectionné pour une destination de recouvrement, vous devez modifier ou supprimer la destination, comme indiqué à l'étape Destination du trap SNMP. Sinon, une erreur de validation se produit lorsque vous enregistrez la configuration de l'agent SNMP.

b. Pour valider vos modifications, sélectionnez **Enregistrer** en bas de la page agent SNMP.

9. si vous souhaitez mettre à jour les destinations d'interruption, sélectionnez l'onglet Trap destinations (destinations d'interruption) dans la section Other configurations.

L'onglet destinations de recouvrement permet de définir une ou plusieurs destinations pour les notifications d'interruption StorageGRID ou d'information. Lorsque vous activez l'agent SNMP et sélectionnez **Enregistrer**, StorageGRID commence à envoyer des notifications à chaque destination définie. Des notifications sont envoyées lorsque des alertes et des alarmes sont déclenchées. Les notifications standard sont également envoyées pour les entités MIB-II prises en charge (par exemple, ifdown et coldStart).

   a. Pour ajouter une destination d'interruption, sélectionnez **Créer**. Reportez-vous ensuite à l'étape pour connaître les destinations de déroutement dans les instructions de configuration de l'agent SNMP.
   b. Pour modifier une destination d'interruption, sélectionnez le bouton radio de l'utilisateur et sélectionnez **Modifier**. Reportez-vous ensuite à l'étape pour connaître les destinations de déroutement dans les instructions de configuration de l'agent SNMP.
   c. Pour supprimer une destination d'interruption, sélectionnez le bouton radio de la destination et sélectionnez **Supprimer**. Ensuite, sélectionnez **OK** pour confirmer que vous souhaitez supprimer cette destination.
   d. Pour valider vos modifications, sélectionnez **Enregistrer** en bas de la page agent SNMP.

10. Lorsque vous avez mis à jour la configuration de l'agent SNMP, sélectionnez **Enregistrer**.

Accéder aux fichiers MIB

Les fichiers MIB contiennent des définitions et des informations sur les propriétés des ressources et services gérés pour les nœuds de votre grille. Vous pouvez accéder aux fichiers MIB qui définissent les objets et les notifications pour StorageGRID. Ces fichiers peuvent être utiles pour la surveillance de votre grille.

Voir "Utiliser la surveillance SNMP" Pour plus d'informations sur les fichiers SNMP et MIB.

Accéder aux fichiers MIB

Étapes

1. Sélectionnez **CONFIGURATION** > **surveillance** > **agent SNMP**.
2. Sur la page agent SNMP, sélectionnez le fichier à télécharger :
   - **NETAPP-STORAGEGRID-MIB.txt** : définit la table d'alertes et les notifications (traps) accessibles sur tous les noeuds d'administration.
   - **ES-NETAPP-06-MIB.mib** : définit les objets et les notifications pour les appliances basées sur E-Series.
   - **MIB_1_10.zip** : définit les objets et les notifications pour les appareils dotés d'une interface BMC.
3. Vous pouvez également accéder aux fichiers MIB à l'emplacement suivant sur n'importe quel nœud StorageGRID :
   `/usr/share/snmp/mibs`
4. Pour extraire le `storagegrid` OID du fichier MIB :

   a. Obtenir l'OID de la racine de la MIB StorageGRID :

   ```
   root@user-adm1:~ # snmptranslate -On -IR storagegrid
   ```

   Résultat : `.1.3.6.1.4.1.789.28669` (`28669` Est toujours l'OID pour StorageGRID)

a. Puis grep pour l'OID StorageGRID dans toute l'arborescence (en utilisant le collage pour joindre les lignes) :

```
root@user-adm1:~ # snmptranslate -Tso | paste -d " " - - | grep 28669
```

Le `snmptranslate` Command a de nombreuses options qui sont utiles pour explorer la MIB. Cette commande est disponible sur n'importe quel nœud StorageGRID.

Contenu du fichier MIB

Tous les objets se trouvent sous l'OID StorageGRID.

Nom de l'objet	ID objet (OID)	Description
		Le module MIB pour les entités NetApp StorageGRID.

Objets MIB

Nom de l'objet	ID objet (OID)	Description
ActiveAlertCount		Nombre d'alertes actives dans activeAlertTable.
ActiveAlertTable		Tableau des alertes actives dans StorageGRID.
ActiveAlertId		ID de l'alerte. Uniquement unique dans l'ensemble actuel d'alertes actives.
ActiveAlertName		Nom de l'alerte.
ActiveAlertInstance		Nom de l'entité qui a généré l'alerte, en général le nom du nœud.
ActiveAlertSeverity		Gravité de l'alerte.
ActiveAlertStartTime		Date et heure du déclenchement de l'alerte.

Types de notification (interruptions)

Toutes les notifications incluent les variables suivantes en tant que variables :

- ActiveAlertId
- ActiveAlertName
- ActiveAlertInstance
- ActiveAlertSeverity
- ActiveAlertStartTime

Type de notification	ID objet (OID)	Description
ActiveMinorAlert		Alerte avec gravité mineure
ActiveMajorAlert		Alerte de gravité majeure
ActiveCriticalAlert		Alerte avec gravité critique

Collecte de données StorageGRID supplémentaires

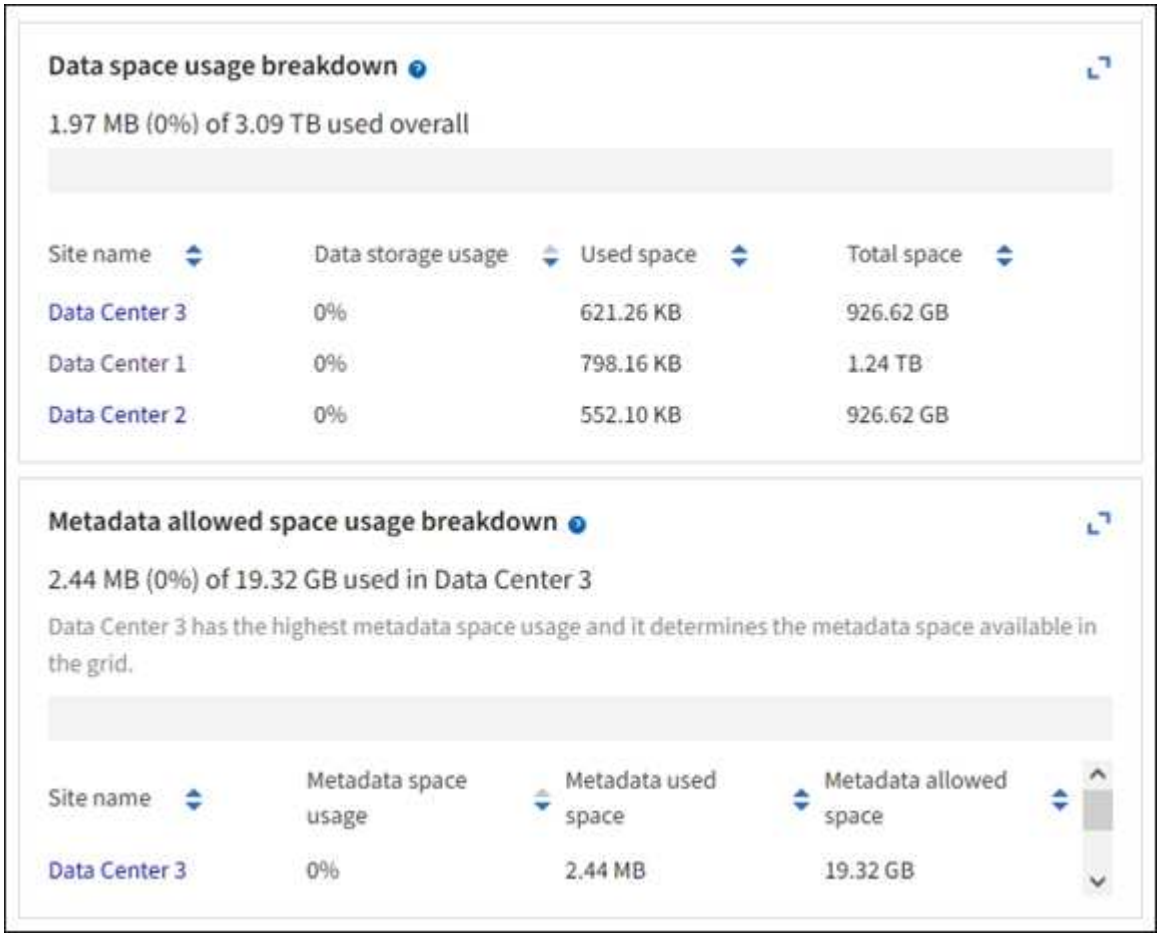
Utilisez des graphiques et des graphiques

Vous pouvez utiliser des graphiques et des rapports pour surveiller l'état du système StorageGRID et résoudre les problèmes.

Types de graphiques

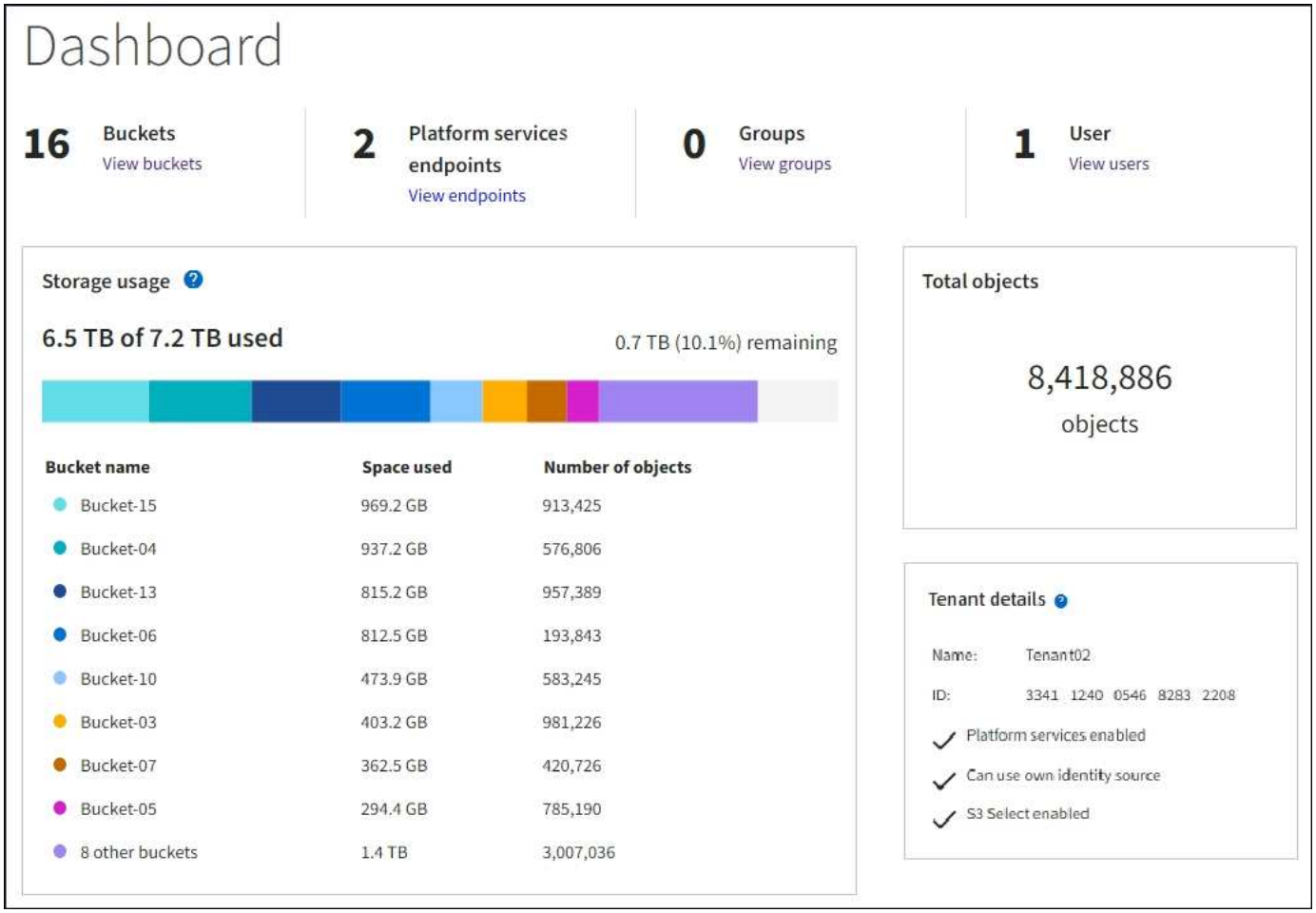
Les graphiques et les graphiques résument les valeurs des mesures et des attributs StorageGRID spécifiques.

Le tableau de bord Grid Manager inclut des cartes qui résument le stockage disponible pour la grille et chaque site.



Le panneau Storage usage (utilisation du stockage) du tableau de bord du gestionnaire de locataires affiche les informations suivantes :

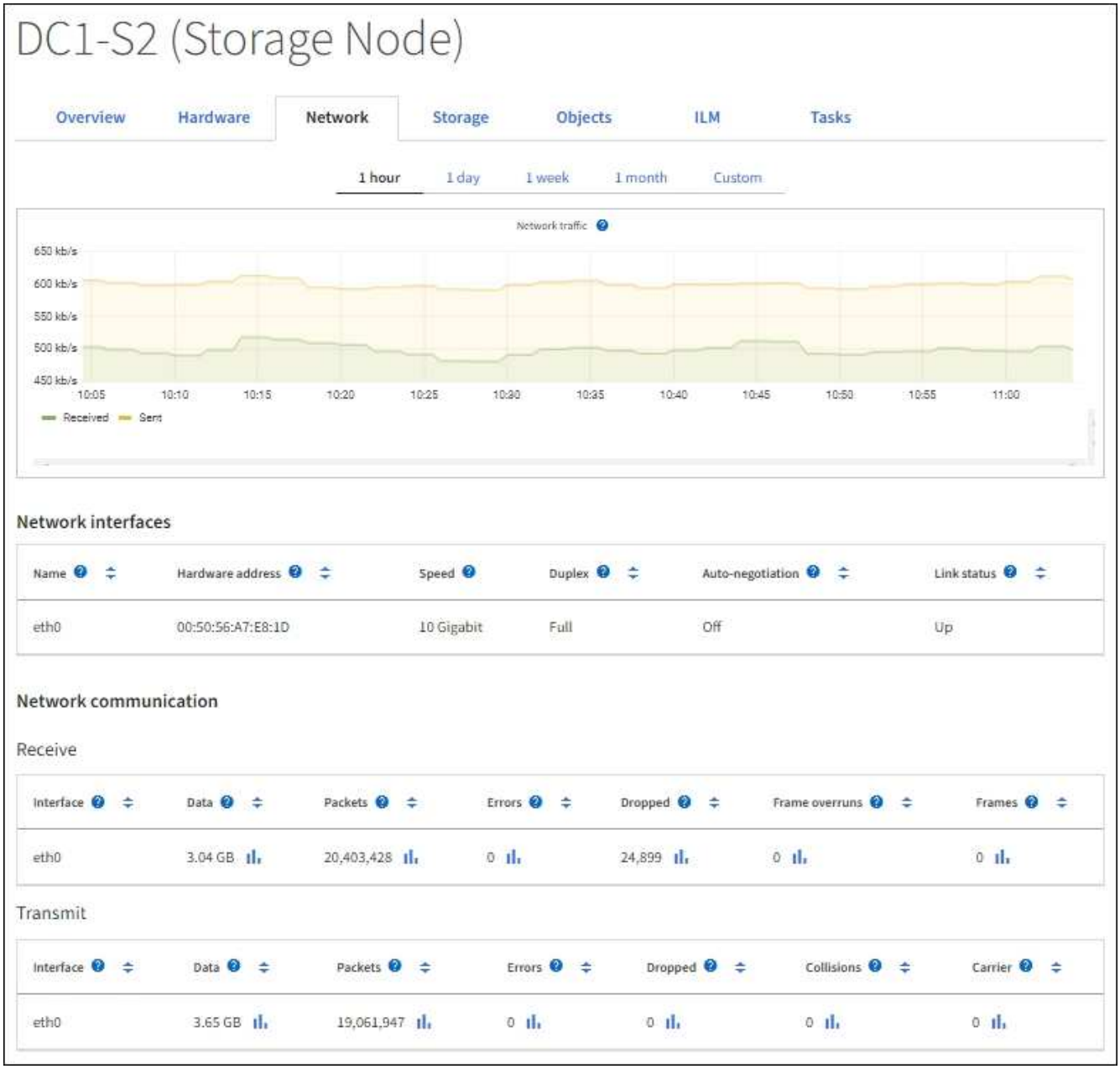
- Liste des compartiments les plus grands (S3) ou des conteneurs (Swift) du locataire
- Un graphique à barres qui représente les tailles relatives des grands godets ou conteneurs
- La quantité totale d'espace utilisé et, si un quota est défini, la quantité et le pourcentage d'espace restant



De plus, les graphiques qui montrent comment les mesures et les attributs StorageGRID changent au fil du temps sont disponibles à partir de la page nœuds et de la page **SUPPORT** > **Outils** > **topologie de grille**.

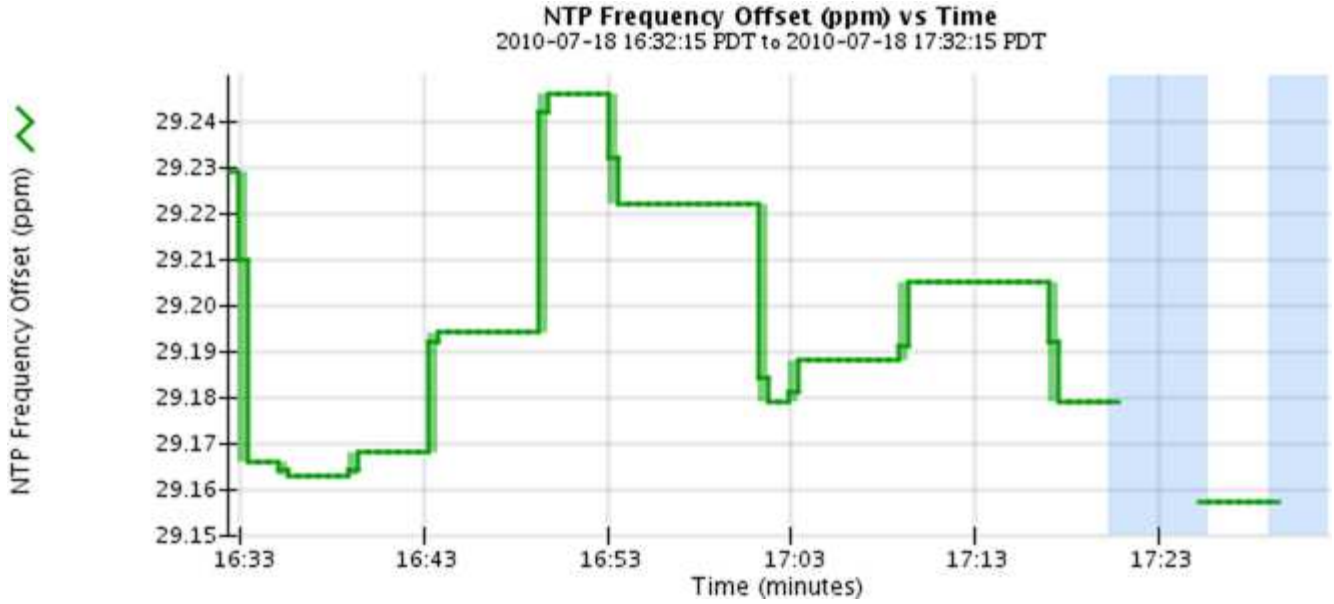
Il existe quatre types de graphiques :

- **Graphiques Grafana** : affichés sur la page nœuds, les graphiques Grafana sont utilisés pour tracer les valeurs des metrics Prometheus dans le temps. Par exemple, l'onglet **NOEUDS** > **réseau** d'un noeud de stockage comprend un tableau Grafana pour le trafic réseau.

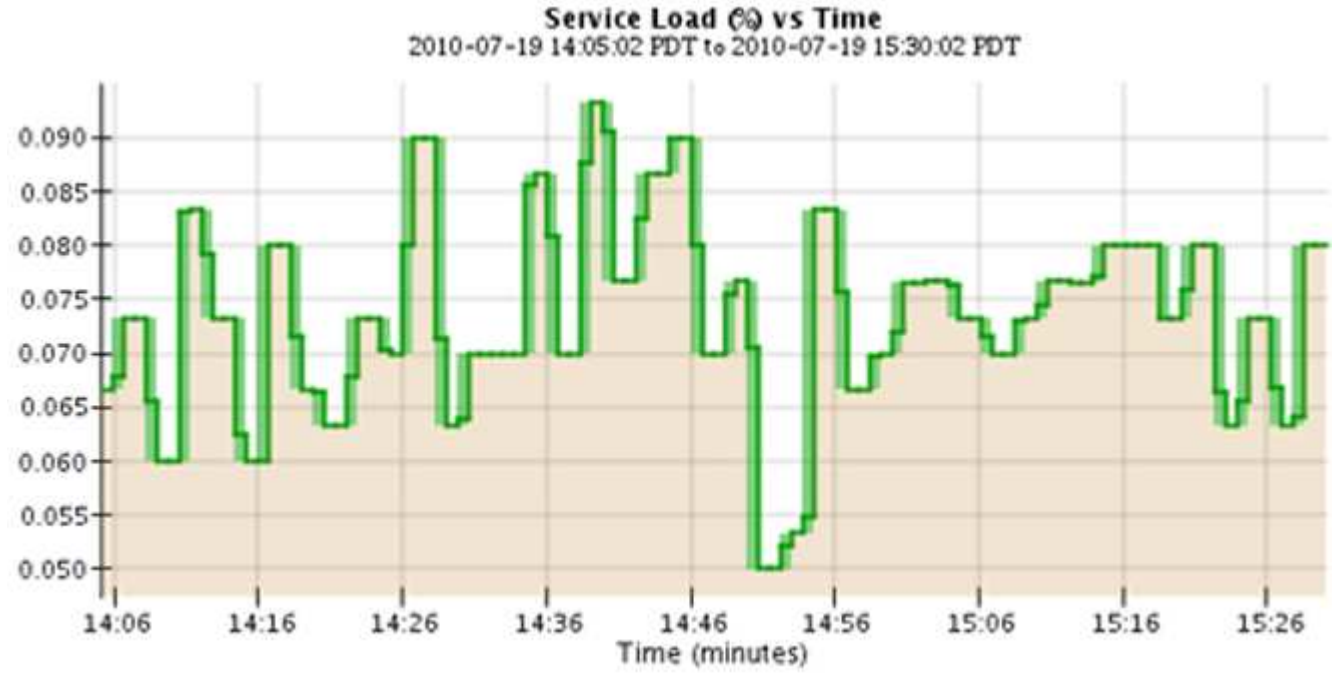


Les graphiques Grafana sont également inclus dans les tableaux de bord pré-construits disponibles à partir de la page **SUPPORT** > **Tools** > **Metrics**.

- **Graphes linéaires** : disponible à partir de la page nœuds et de la page **SUPPORT** > **Outils** > **topologie de grille** (sélectionnez l'icône de graphique Après une valeur de données), des graphes linéaires sont utilisés pour tracer les valeurs des attributs StorageGRID qui ont une valeur unitaire (tels que le décalage de fréquence NTP, en ppm). Les modifications de la valeur sont tracées dans des intervalles de données réguliers (bacs) au fil du temps.

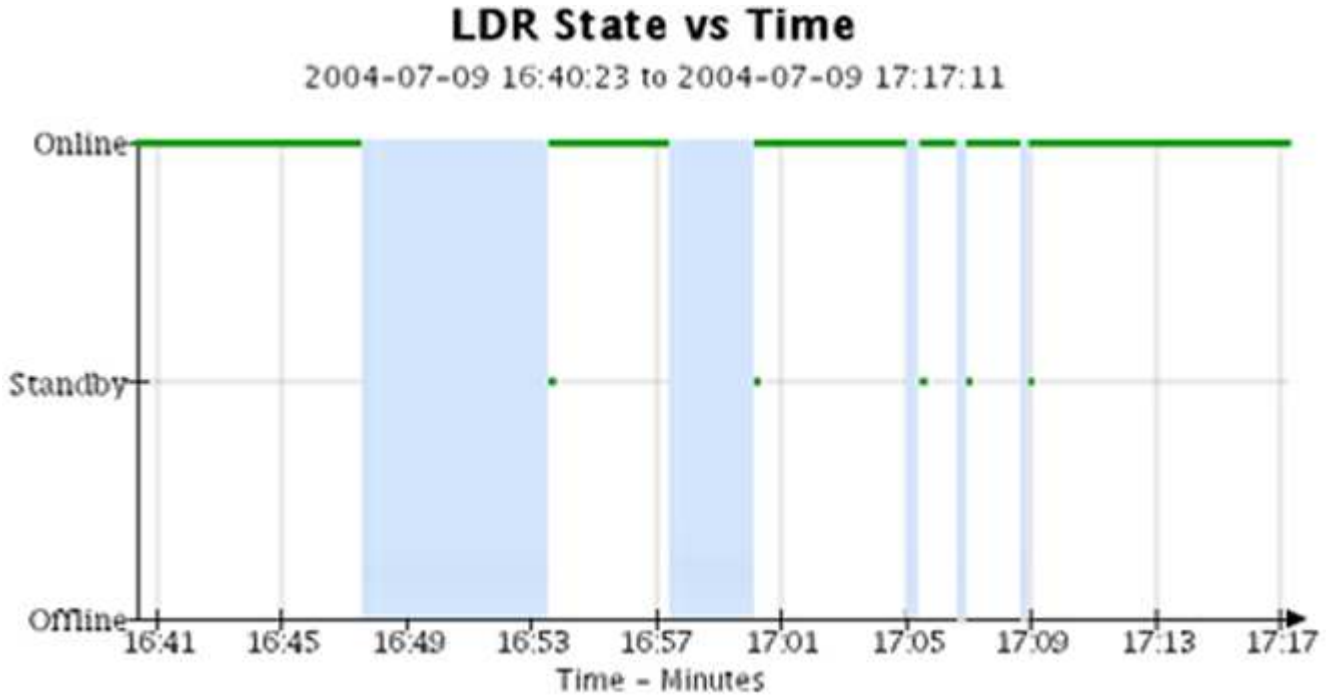


- **Graphes de zone** : disponible à partir de la page nœuds et de la page **SUPPORT** > **Outils** > **topologie de grille** (sélectionnez l'icône de graphique après une valeur de données), les graphes de zone sont utilisés pour tracer les quantités d'attributs volumétriques, telles que les nombres d'objets ou les valeurs de charge de service. Les graphiques de zone sont similaires aux graphiques de ligne, mais incluent un ombrage marron clair en dessous de la ligne. Les modifications de la valeur sont tracées dans des intervalles de données réguliers (bacs) au fil du temps.



- Certains graphiques sont signalés par un autre type d'icône de graphique et ont un format différent :

- **Graphique d'état** : disponible à partir de la page **SUPPORT** > **Outils** > **topologie de grille** (sélectionnez l'icône de graphique après une valeur de données), les graphiques d'état sont utilisés pour tracer les valeurs d'attribut représentant des états distincts tels qu'un état de service qui peut être en ligne, en attente ou hors ligne. Les graphiques d'état sont similaires aux graphiques linéaires, mais la transition est discontinue. En d'autres termes, la valeur passe d'une valeur d'état à une autre.



Informations associées

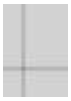
"Afficher la page nœuds"

"Afficher l'arborescence de la grille topologique"

"Examinez les metrics de support"

Légende du graphique

Les lignes et les couleurs utilisées pour dessiner des graphiques ont une signification spécifique.

Échantillon	Signification
	Les valeurs des attributs signalés sont tracées à l'aide de lignes vert foncé.
	Un ombrage vert clair autour des lignes vert foncé indique que les valeurs réelles de cette plage de temps varient et ont été « binning » pour un tracé plus rapide. La ligne foncée représente la moyenne pondérée. La plage en vert clair indique les valeurs maximum et minimum dans le bac. L'ombrage marron clair est utilisé pour les graphiques de zone pour indiquer les données volumétriques.
	Les zones vierges (aucune donnée tracée) indiquent que les valeurs d'attribut ne sont pas disponibles. L'arrière-plan peut être bleu, gris ou un mélange de gris et de bleu, selon l'état du service signalant l'attribut.
	L'ombrage bleu clair indique que certaines ou toutes les valeurs d'attribut à ce moment étaient indéterminées ; l'attribut n'a pas signalé de valeurs parce que le service était dans un état inconnu.
	L'ombrage gris indique que certaines ou toutes les valeurs d'attribut à ce moment n'étaient pas connues car le service signalant les attributs était administrativement en panne.
	Un mélange d'ombrage gris et bleu indique que certaines des valeurs d'attribut au moment étaient indéterminées (parce que le service était dans un état inconnu), tandis que d'autres n'étaient pas connus car le service signalant les attributs était administrativement en panne.

Affichez des graphiques et des graphiques

La page nœuds contient les graphiques et les graphiques auxquels vous devez accéder régulièrement pour surveiller les attributs tels que la capacité de stockage et le débit. Dans certains cas, en particulier lorsque vous travaillez avec le support technique, vous pouvez utiliser la page **SUPPORT** > **Outils** > **topologie de grille** pour accéder à des graphiques supplémentaires.

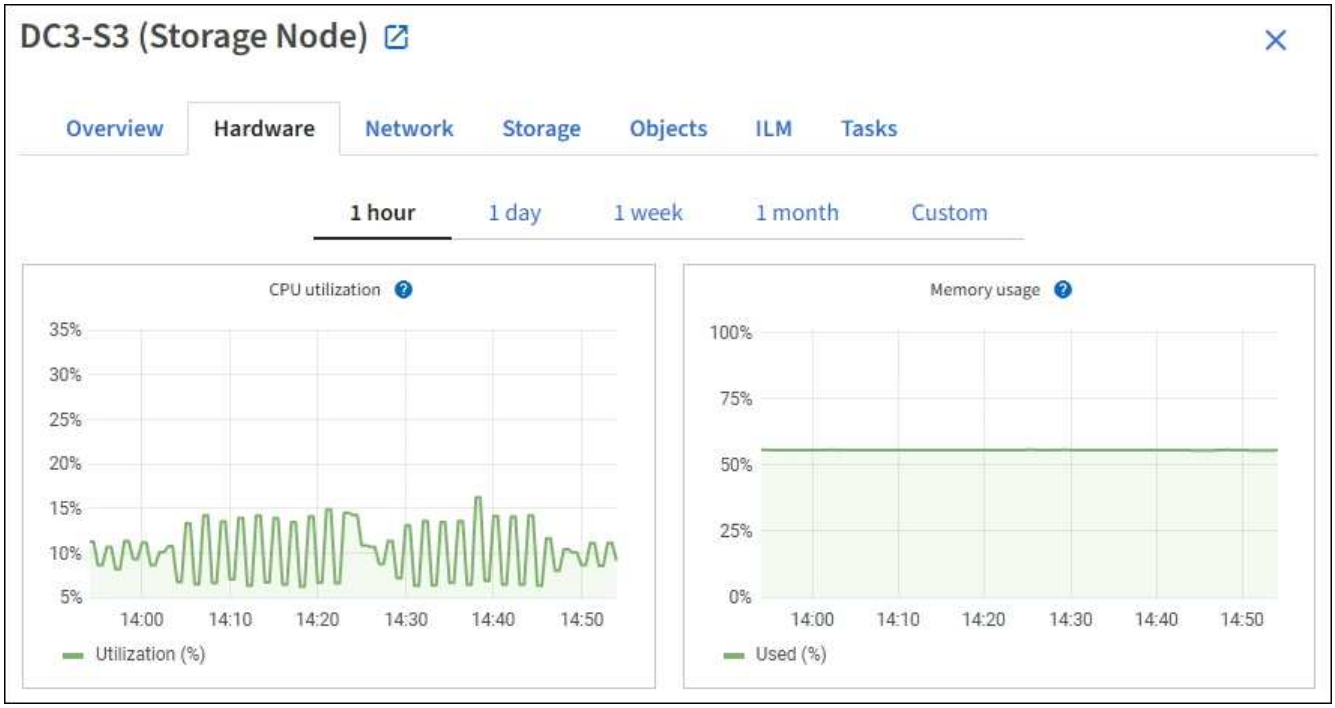
Avant de commencer

Vous devez être connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".

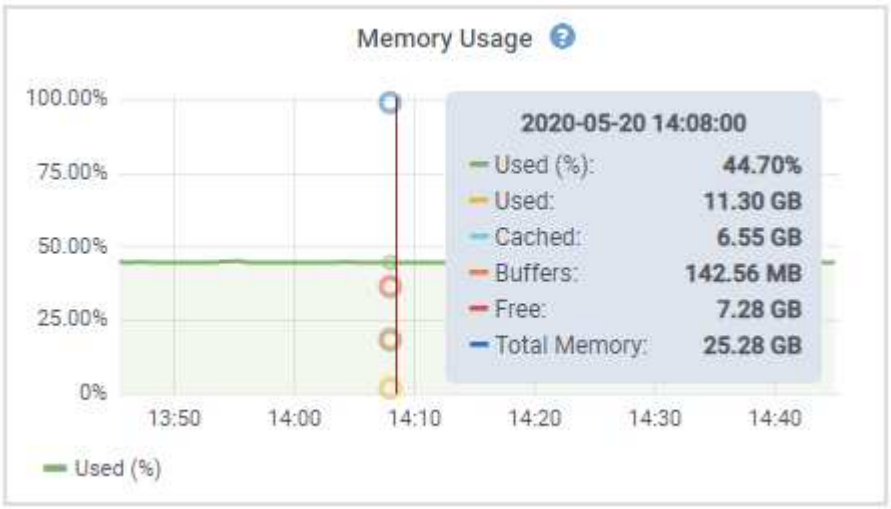
Étapes

1. Sélectionnez **NOEUDS**. Ensuite, sélectionnez un nœud, un site ou la grille entière.
2. Sélectionnez l'onglet pour lequel vous souhaitez afficher les informations.

Certains onglets comprennent un ou plusieurs graphiques Grafana, qui sont utilisés pour tracer les valeurs des metrics Prometheus dans le temps. Par exemple, l'onglet **NODES** > **Hardware** d'un noeud comprend deux diagrammes Grafana.



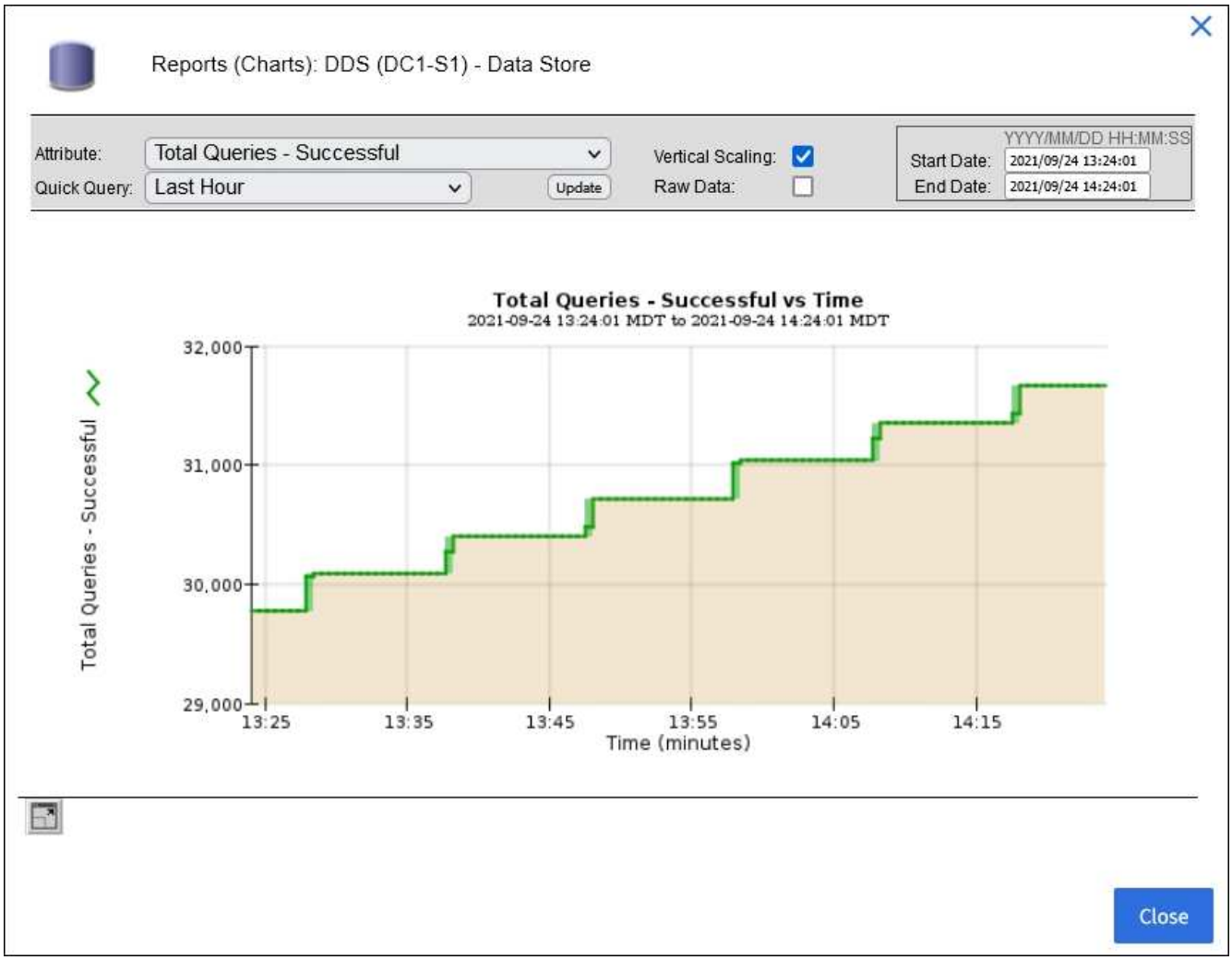
3. Si vous le souhaitez, placez votre curseur sur le graphique pour afficher des valeurs plus détaillées pour un point particulier dans le temps.

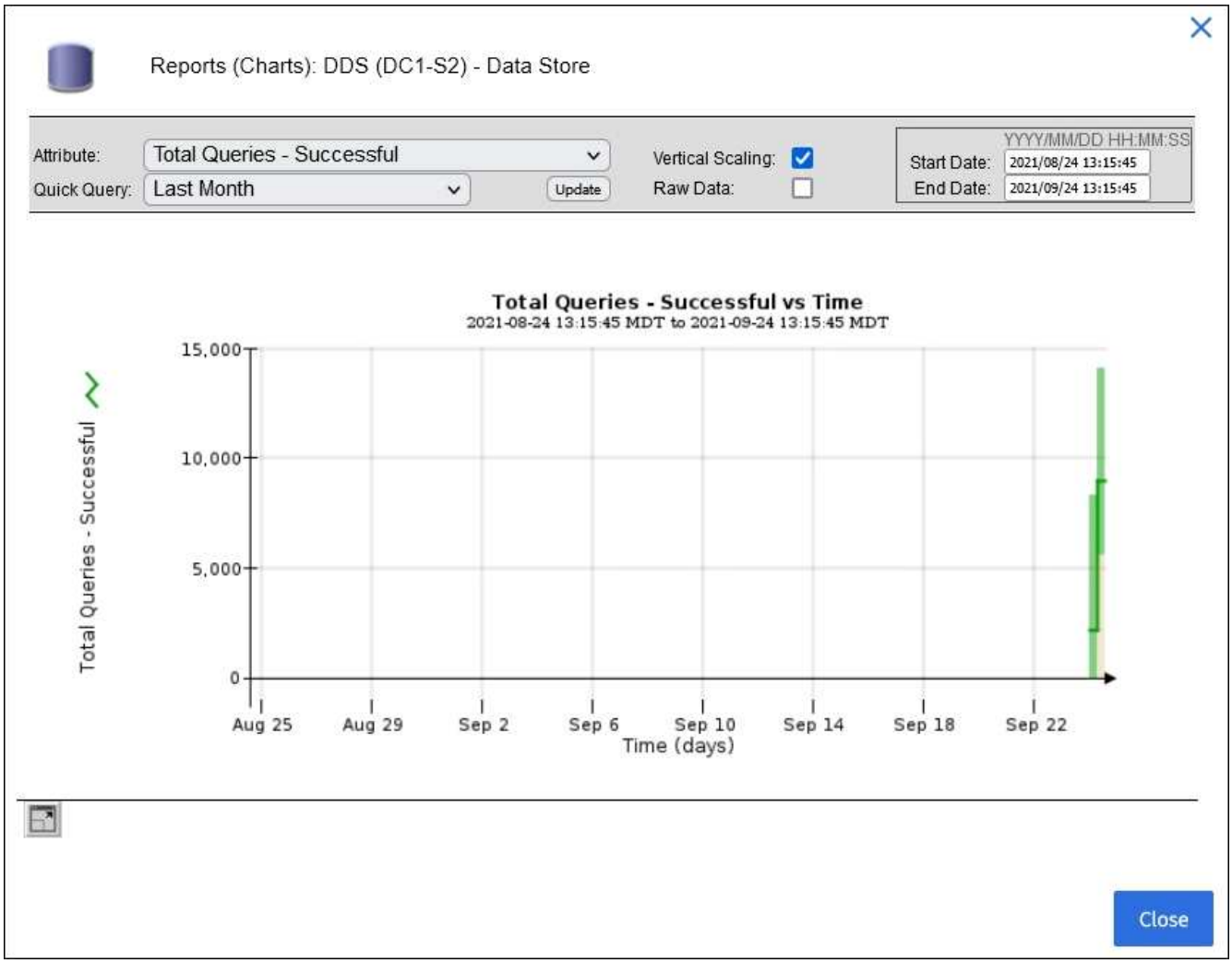


4. Si nécessaire, vous pouvez souvent afficher un graphique pour un attribut ou une mesure spécifique. Dans le tableau de la page nœuds, sélectionnez l'icône du graphique à droite du nom de l'attribut.

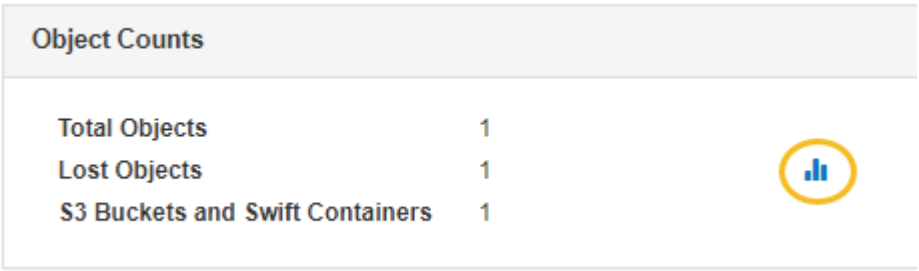
> Les graphiques ne sont pas disponibles pour toutes les mesures et tous les attributs.

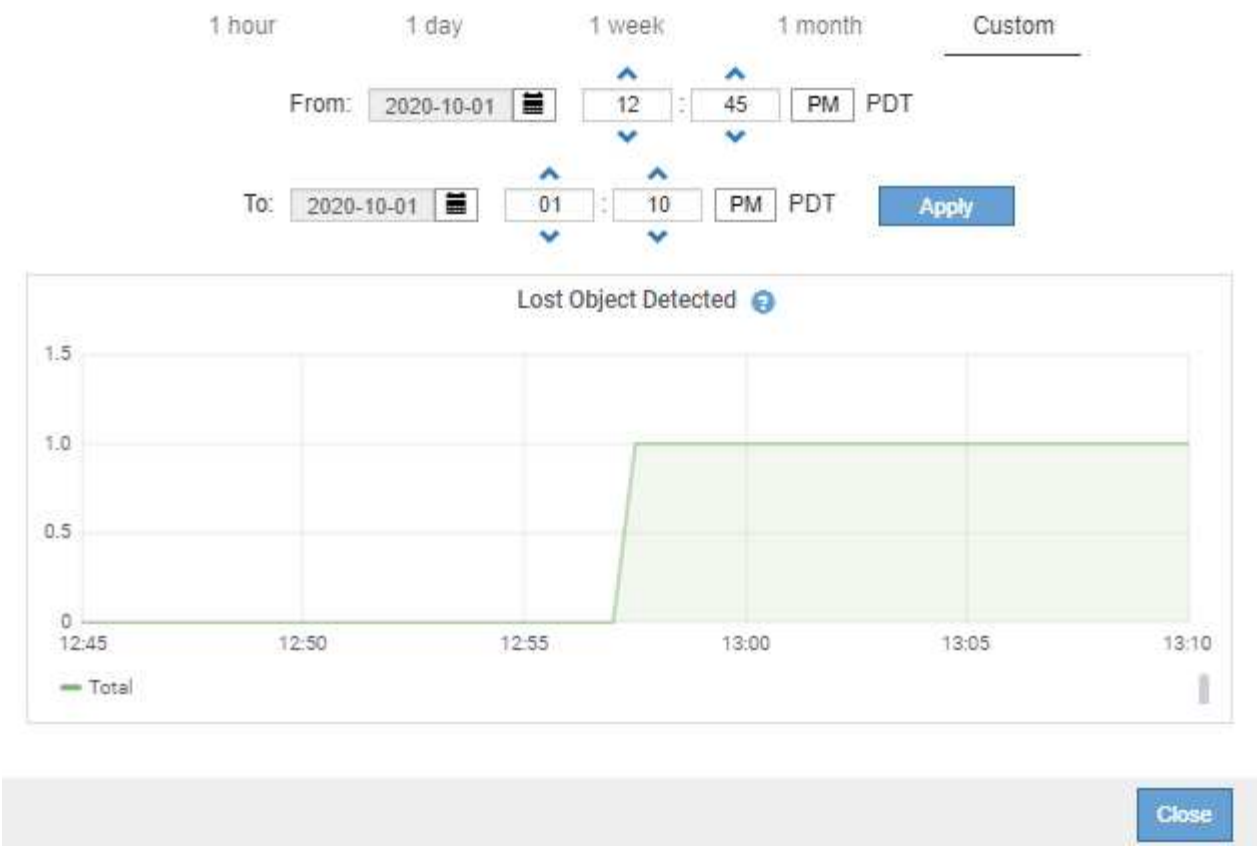
Exemple 1 : dans l'onglet objets d'un noeud de stockage, vous pouvez sélectionner l'icône du graphique Pour afficher le nombre total de requêtes de stockage de métadonnées réussies pour le noeud de stockage.


Reports (Charts): DDS (DC1-S1) - Data Store
Attribute:
Total Queries - Successful
Quick Query:
Last Hour
Update
Vertical Scaling:
Raw Data:
YYYY/MM/DD HH:MM:SS
Start Date:
2021/09/24 13:24:01
End Date:
2021/09/24 14:24:01
Total Queries - Successful vs Time
2021-09-24 13:24:01 MDT to 2021-09-24 14:24:01 MDT
Total Queries - Successful
32,000
31,000
30,000
29,000
13:25
13:35
13:45
13:55
14:05
14:15
Time (minutes)
Close

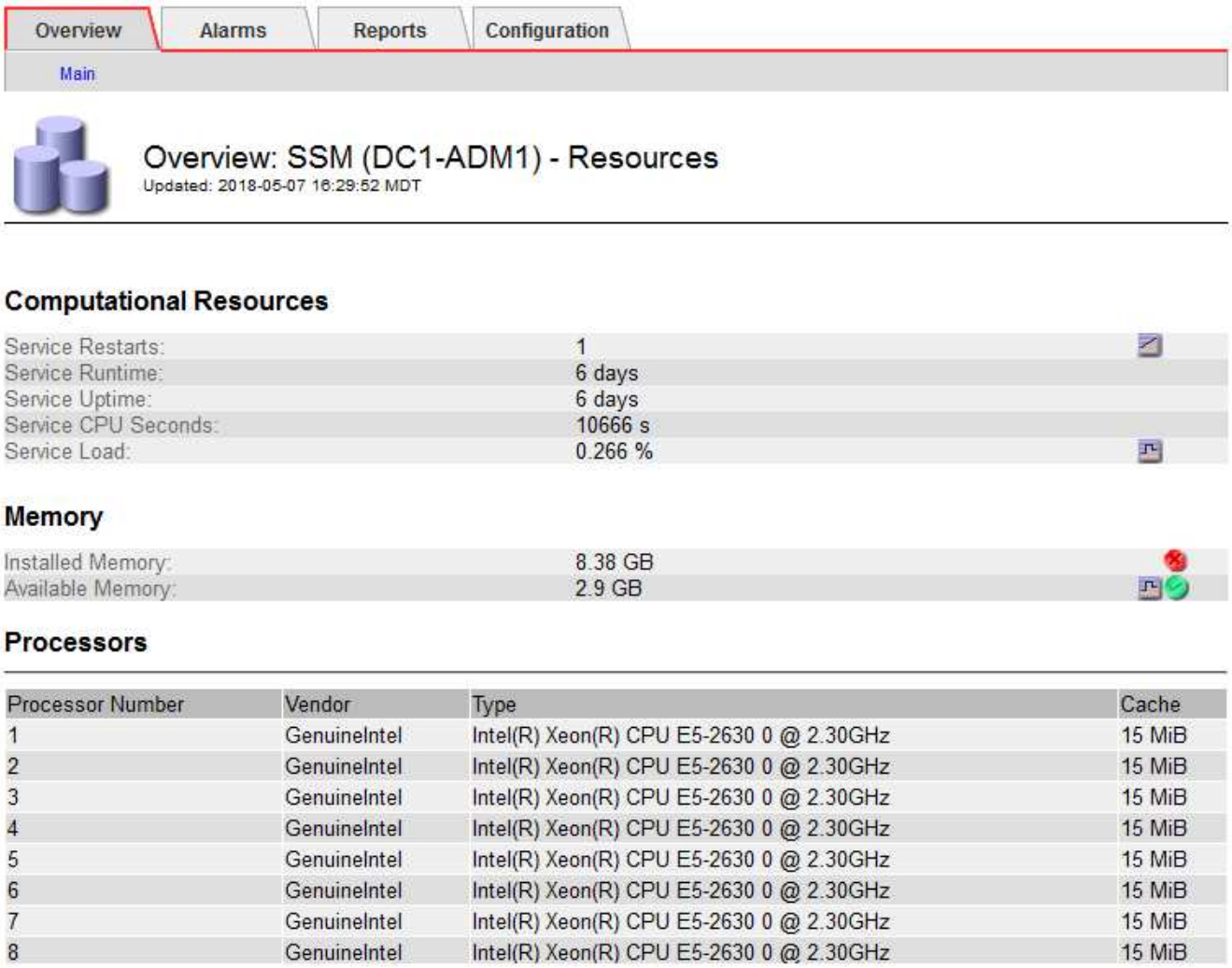


Exemple 2 : dans l'onglet objets d'un noeud de stockage, vous pouvez sélectionner l'icône du graphique Pour afficher le graphique Grafana du nombre d'objets perdus détectés au fil du temps.





5. Pour afficher les graphiques des attributs qui ne sont pas affichés sur la page nœud, sélectionnez **SUPPORT** > **Outils** > **topologie de grille**.
6. Sélectionnez ***grid node*** > ***component ou service*** > **Présentation** > **main**.



7. Sélectionnez l'icône du graphique à côté de l'attribut.

   L'affichage passe automatiquement à la page **Rapports** > **graphiques**. Le graphique affiche les données de l'attribut au cours du dernier jour.

Générer des graphiques

Les graphiques affichent une représentation graphique des valeurs de données d'attribut. Vous pouvez générer des rapports sur un site de data Center, un nœud grid, un composant ou un service.

Avant de commencer

- Vous devez être connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous devez disposer d'autorisations d'accès spécifiques.

Étapes

1. Sélectionnez **SUPPORT** > **Outils** > **topologie de grille**.
2. Sélectionnez ***grid node*** > ***component ou service*** > **Rapports** > **diagrammes**.
3. Sélectionnez l'attribut à rapporter dans la liste déroulante **attribut**.
4. Pour forcer l'axe y à commencer à zéro, décochez la case **mise à l'échelle verticale**.
5. Pour afficher les valeurs avec une précision maximale, cochez la case **données brutes** ou pour arrondir

les valeurs à un maximum de trois décimales (par exemple, pour les attributs signalés en pourcentage), décochez la case **données brutes**.

6. Sélectionnez la période à laquelle effectuer le rapport dans la liste déroulante **requête rapide**.

   Sélectionnez l'option requête personnalisée pour sélectionner une plage de temps spécifique.

   Le graphique apparaît après quelques instants. Prévoir plusieurs minutes pour la totalisation de longues plages de temps.

7. Si vous avez sélectionné requête personnalisée, personnalisez la période de temps du graphique en saisissant **Date de début** et **Date de fin**.

   Utiliser le format *YYYY/MM/DDHH:MM:SS* en heure locale. Des zéros non significatifs sont nécessaires pour correspondre au format. Par exemple, la validation a échoué dans 2017/4/6 7:30:00. Le format correct est: 2017/04/06 07:30:00.

8. Sélectionnez **mettre à jour**.

   Un graphique est généré après quelques secondes. Prévoir plusieurs minutes pour la totalisation de longues plages de temps. En fonction de la durée définie pour la requête, un rapport texte brut ou texte agrégé s'affiche.

Utilisez les rapports texte

Les rapports texte affichent une représentation textuelle des valeurs de données d'attribut traitées par le service NMS. Il existe deux types de rapports générés selon la période de temps sur laquelle vous vous signalez : des rapports de texte brut pour des périodes inférieures à une semaine et des rapports de texte agrégés pour des périodes supérieures à une semaine.

Rapports de texte brut

Un rapport en texte brut affiche des détails sur l'attribut sélectionné :

- Heure de réception : date et heure locales auxquelles une valeur d'échantillon des données d'un attribut a été traitée par le service NMS.
- Heure de l'échantillon : date et heure locales auxquelles une valeur d'attribut a été échantillonnée ou modifiée à la source.
- Valeur : valeur d'attribut au moment de l'échantillon.

Text Results for Services: Load - System Logging

2010-07-18 15:58:39 PDT To 2010-07-19 15:58:39 PDT

Time Received	Sample Time	Value
2010-07-19 15:58:09	2010-07-19 15:58:09	0.016 %
2010-07-19 15:56:06	2010-07-19 15:56:06	0.024 %
2010-07-19 15:54:02	2010-07-19 15:54:02	0.033 %
2010-07-19 15:52:00	2010-07-19 15:52:00	0.016 %
2010-07-19 15:49:57	2010-07-19 15:49:57	0.008 %
2010-07-19 15:47:54	2010-07-19 15:47:54	0.024 %
2010-07-19 15:45:50	2010-07-19 15:45:50	0.016 %
2010-07-19 15:43:47	2010-07-19 15:43:47	0.024 %
2010-07-19 15:41:43	2010-07-19 15:41:43	0.032 %
2010-07-19 15:39:40	2010-07-19 15:39:40	0.024 %
2010-07-19 15:37:37	2010-07-19 15:37:37	0.008 %
2010-07-19 15:35:34	2010-07-19 15:35:34	0.016 %
2010-07-19 15:33:31	2010-07-19 15:33:31	0.024 %
2010-07-19 15:31:27	2010-07-19 15:31:27	0.032 %
2010-07-19 15:29:24	2010-07-19 15:29:24	0.032 %
2010-07-19 15:27:21	2010-07-19 15:27:21	0.049 %
2010-07-19 15:25:18	2010-07-19 15:25:18	0.024 %
2010-07-19 15:21:12	2010-07-19 15:21:12	0.016 %
2010-07-19 15:19:09	2010-07-19 15:19:09	0.008 %
2010-07-19 15:17:07	2010-07-19 15:17:07	0.016 %

Agréger les rapports de texte

Un rapport texte agrégé affiche des données sur une période plus longue (généralement une semaine) qu'un rapport texte brut. Chaque entrée est le résultat d'un résumé de plusieurs valeurs d'attribut (un ensemble de valeurs d'attribut) par le service NMS dans le temps en une seule entrée avec des valeurs moyennes, maximales et minimales dérivées de l'agrégation.

Chaque entrée affiche les informations suivantes :

- Heure d'agrégation : dernière date et heure locales que le service NMS a agrégées (recueillies) un ensemble de valeurs d'attribut modifiées.
- Valeur moyenne : moyenne de la valeur de l'attribut sur la période de temps agrégée.
- Valeur minimale : valeur minimale sur la période de temps agrégée.
- Valeur maximale : valeur maximale sur la période de temps agrégée.

Text Results for Attribute Send to Relay Rate

2010-07-11 16:02:46 PDT To 2010-07-19 16:02:46 PDT

Aggregate Time	Average Value	Minimum Value	Maximum Value
2010-07-19 15:59:52	0.271072196 Messages/s	0.266649743 Messages/s	0.274983464 Messages/s
2010-07-19 15:53:52	0.275585378 Messages/s	0.266562352 Messages/s	0.283302736 Messages/s
2010-07-19 15:49:52	0.279315709 Messages/s	0.233318712 Messages/s	0.333313579 Messages/s
2010-07-19 15:43:52	0.28181323 Messages/s	0.241651024 Messages/s	0.374976601 Messages/s
2010-07-19 15:39:52	0.284233141 Messages/s	0.249982001 Messages/s	0.324971987 Messages/s
2010-07-19 15:33:52	0.325752083 Messages/s	0.266641993 Messages/s	0.358306197 Messages/s
2010-07-19 15:29:52	0.278531507 Messages/s	0.274984766 Messages/s	0.283320999 Messages/s
2010-07-19 15:23:52	0.281437642 Messages/s	0.274981961 Messages/s	0.291577735 Messages/s
2010-07-19 15:17:52	0.261563307 Messages/s	0.258318006 Messages/s	0.266655787 Messages/s
2010-07-19 15:13:52	0.265159147 Messages/s	0.258318557 Messages/s	0.26663986 Messages/s

Générer des rapports texte

Les rapports texte affichent une représentation textuelle des valeurs de données d'attribut traitées par le service NMS. Vous pouvez générer des rapports sur un site de data Center, un nœud grid, un composant ou un service.

Avant de commencer

- Vous devez être connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous devez disposer d'autorisations d'accès spécifiques.

Description de la tâche

Pour les données d'attribut qui devraient changer en permanence, ces données d'attribut sont échantillonnées par le service NMS (à la source) à intervalles réguliers. Pour les données d'attribut qui changent rarement (par exemple, les données en fonction d'événements tels que les changements d'état ou d'état), une valeur d'attribut est envoyée au service NMS lorsque la valeur change.

Le type de rapport affiché dépend de la période configurée. Par défaut, les rapports de texte agrégés sont générés pour les périodes de plus d'une semaine.

Le texte gris indique que le service a été désactivé administrativement au cours de l'échantillonnage. Le texte bleu indique que le service était dans un état inconnu.

Étapes

1. Sélectionnez **SUPPORT** > **Outils** > **topologie de grille**.
2. Sélectionnez ***grid node*** > ***component ou service*** > **Reports** > **Text**.
3. Sélectionnez l'attribut à rapporter dans la liste déroulante **attribut**.
4. Sélectionnez le nombre de résultats par page dans la liste déroulante **Résultats par page**.
5. Pour arrondir les valeurs à un maximum de trois décimales (par exemple, pour les attributs signalés en pourcentage), décochez la case **données brutes**.
6. Sélectionnez la période à laquelle effectuer le rapport dans la liste déroulante **requête rapide**.

   Sélectionnez l'option requête personnalisée pour sélectionner une plage de temps spécifique.

Le rapport apparaît après quelques instants. Prévoir plusieurs minutes pour la totalisation de longues plages de temps.

7. Si vous avez sélectionné requête personnalisée, vous devez personnaliser la période de rapport en entrant **Date de début** et **Date de fin**.

   Utiliser le format `YYYY/MM/DDHH:MM:SS` en heure locale. Des zéros non significatifs sont nécessaires pour correspondre au format. Par exemple, la validation a échoué dans 2017/4/6 7:30:00. Le format correct est: 2017/04/06 07:30:00.

8. Cliquez sur **mettre à jour**.

   Un rapport texte est généré au bout de quelques instants. Prévoir plusieurs minutes pour la totalisation de longues plages de temps. En fonction de la durée définie pour la requête, un rapport texte brut ou texte agrégé s'affiche.

Exporter les rapports texte

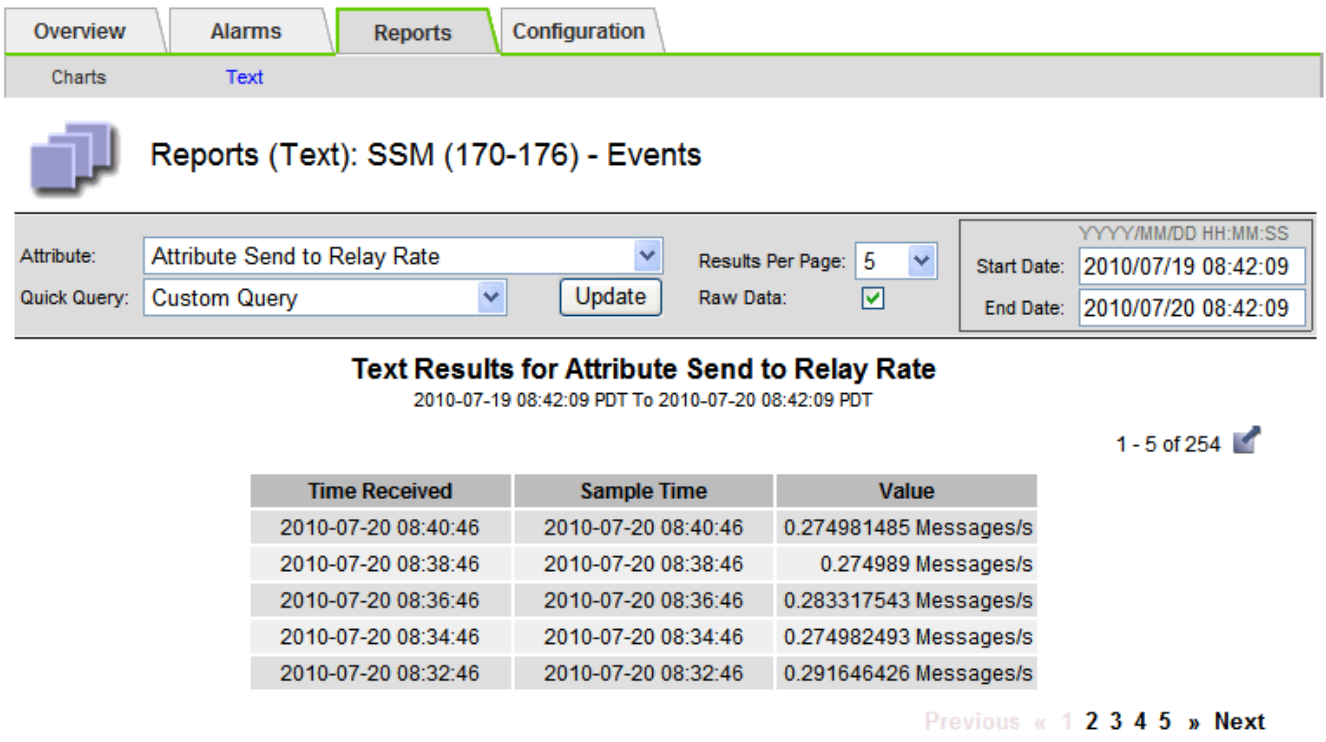
Les rapports texte exportés ouvrent un nouvel onglet de navigateur, qui vous permet de sélectionner et de copier les données.

Description de la tâche

Les données copiées peuvent ensuite être enregistrées dans un nouveau document (par exemple, une feuille de calcul) et utilisées pour analyser les performances du système StorageGRID.

Étapes

1. Sélectionnez **SUPPORT** > **Outils** > **topologie de grille**.
2. Créer un rapport texte.
3. Cliquez sur *Exporter*.



La fenêtre Exporter un rapport texte s'ouvre et affiche le rapport.

```
Grid ID: 000 000
OID: 2.16.124.113590.2.1.400019.1.1.1.16996732.200
Node Path: Site/170-176/SSM/Events
Attribute: Attribute Send to Relay Rate (ABSR)
Query Start Date: 2010-07-19 08:42:09 PDT
Query End Date: 2010-07-20 08:42:09 PDT
Time Received,Time Received (Epoch),Sample Time,Sample Time (Epoch),Value,Type
2010-07-20 08:40:46,1279640446559000,2010-07-20 08:40:46,1279640446537209,0.274981485 Messages/s,U
2010-07-20 08:38:46,1279640326561000,2010-07-20 08:38:46,1279640326529124,0.274989 Messages/s,U
2010-07-20 08:36:46,1279640206556000,2010-07-20 08:36:46,1279640206524330,0.283317543 Messages/s,U
2010-07-20 08:34:46,1279640086540000,2010-07-20 08:34:46,1279640086517645,0.274982493 Messages/s,U
2010-07-20 08:32:46,1279639966543000,2010-07-20 08:32:46,1279639966510022,0.291646426 Messages/s,U
2010-07-20 08:30:46,1279639846561000,2010-07-20 08:30:46,1279639846501672,0.308315369 Messages/s,U
2010-07-20 08:28:46,1279639726527000,2010-07-20 08:28:46,1279639726494673,0.291657509 Messages/s,U
2010-07-20 08:26:46,1279639606526000,2010-07-20 08:26:46,1279639606490890,0.266627739 Messages/s,U
2010-07-20 08:24:46,1279639486495000,2010-07-20 08:24:46,1279639486473368,0.258318523 Messages/s,U
2010-07-20 08:22:46,1279639366480000,2010-07-20 08:22:46,1279639366466497,0.274985902 Messages/s,U
2010-07-20 08:20:46,1279639246469000,2010-07-20 08:20:46,1279639246460346,0.283253871 Messages/s,U
2010-07-20 08:18:46,1279639126469000,2010-07-20 08:18:46,1279639126426669,0.274982804 Messages/s,U
2010-07-20 08:16:46,1279639006437000,2010-07-20 08:16:46,1279639006419168,0.283315503 Messages/s,U
```

4. Sélectionnez et copiez le contenu de la fenêtre Exporter un rapport texte.

   Ces données peuvent maintenant être collées dans un document tiers, tel qu'une feuille de calcul.

Surveillez L'PUT et OBTENEZ des performances

Vous pouvez surveiller les performances de certaines opérations, telles que le stockage et la récupération d'objets, afin de faciliter l'identification des modifications qui pourraient nécessiter une investigation plus poussée.

Description de la tâche

Pour contrôler LES PUT et GET, vous pouvez exécuter les commandes S3 et Swift directement depuis un poste de travail ou à l'aide de l'application open source S3tester. Ces méthodes vous permettent d'évaluer la performance indépendamment des facteurs externes à StorageGRID, tels que les problèmes liés à une application client ou à un réseau externe.

Lorsque vous effectuez des tests de MISE EN PLACE et D'OBTENTION d'opérations, suivez les instructions suivantes :

- Utilisez des tailles d'objet comparables aux objets que vous ingérer dans votre grid.
- Exécutez vos opérations sur des sites locaux et distants.

Messages dans "journal d'audit" indiquez le temps total nécessaire à l'exécution de certaines opérations. Par exemple, pour déterminer le temps de traitement total d'une demande GET S3, vous pouvez vérifier la valeur de l'attribut TIME dans le message d'audit SGET. Vous pouvez également trouver l'attribut HEURE dans les messages d'audit pour les opérations suivantes :

- **S3**: SUPPRIMER, OBTENIR, TÊTE, métadonnées mises à jour, POST, EN
- **SWIFT**: SUPPRIMER, OBTENIR, TÊTE, METTRE

Lors de l'analyse des résultats, examinez le temps moyen requis pour répondre à une demande, ainsi que le

débit global que vous pouvez atteindre. Répétez régulièrement les mêmes tests et notez les résultats afin d'identifier les tendances qui pourraient nécessiter une enquête.

- C'est possible "Téléchargez S3Tester sur github".

Surveiller les opérations de vérification d'objets

Le système StorageGRID peut vérifier l'intégrité des données d'objet sur les nœuds de stockage en vérifiant la présence d'objets corrompus et manquants.

Avant de commencer

- Vous devez être connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous devez disposer de l'autorisation Maintenance ou accès racine.

Description de la tâche

Deux "processus de vérification" collaborez pour assurer l'intégrité des données :

- **Vérification de l'arrière-plan** s'exécute automatiquement, en vérifiant continuellement l'exactitude des données de l'objet.

  La vérification en arrière-plan vérifie automatiquement et en continu tous les nœuds de stockage pour déterminer s'il existe des copies corrompues des données d'objet répliquées et codées par effacement. Si un problème est détecté, le système StorageGRID tente automatiquement de remplacer les données d'objet corrompues à partir des copies stockées ailleurs dans le système. La vérification en arrière-plan ne s'exécute pas sur les nœuds d'archivage ou sur les objets d'un pool de stockage cloud.

  > ⓘ L'alerte **objet corrompu non identifié détecté** est déclenchée si le système détecte un objet corrompu qui ne peut pas être corrigé automatiquement.

- **La vérification de l'existence d'objet** peut être déclenchée par un utilisateur pour vérifier plus rapidement l'existence (mais pas l'exactitude) des données d'objet.

  Le contrôle d'existence d'objet vérifie si toutes les copies répliquées attendues d'objets et de fragments avec code d'effacement existent sur un nœud de stockage. La vérification de l'existence d'un objet permet de vérifier l'intégrité des périphériques de stockage, en particulier si un problème matériel récent peut avoir une incidence sur l'intégrité des données.

Vous devez consulter régulièrement les résultats des vérifications de fond et des contrôles d'existence d'objet. Recherchez immédiatement toute instance de données d'objet corrompues ou manquantes afin de déterminer la cause première.

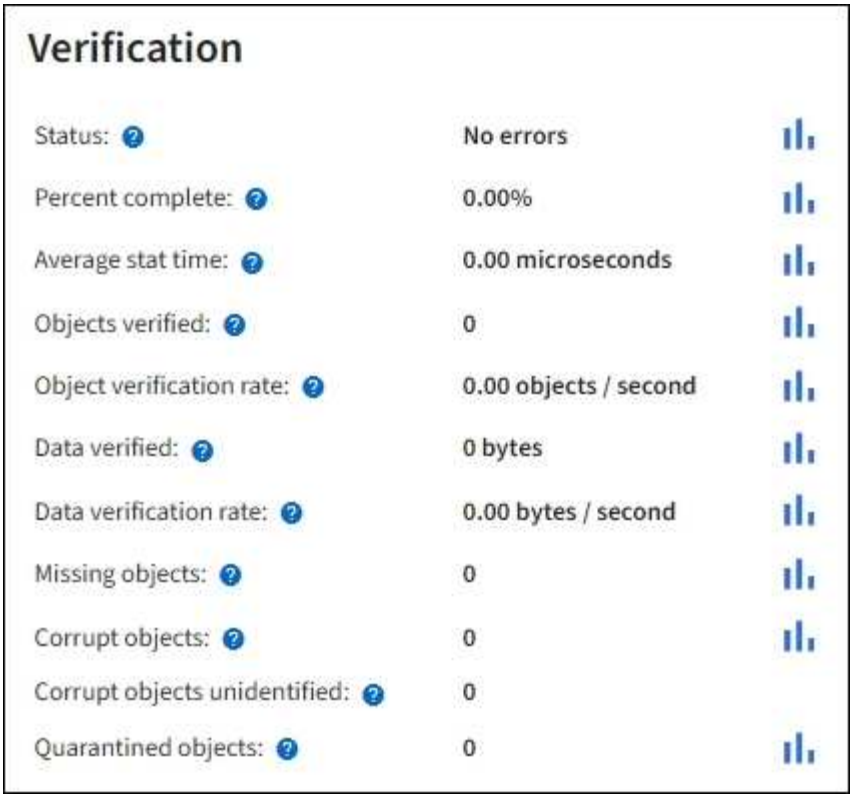
Étapes

1. Examiner les résultats des vérifications de base :

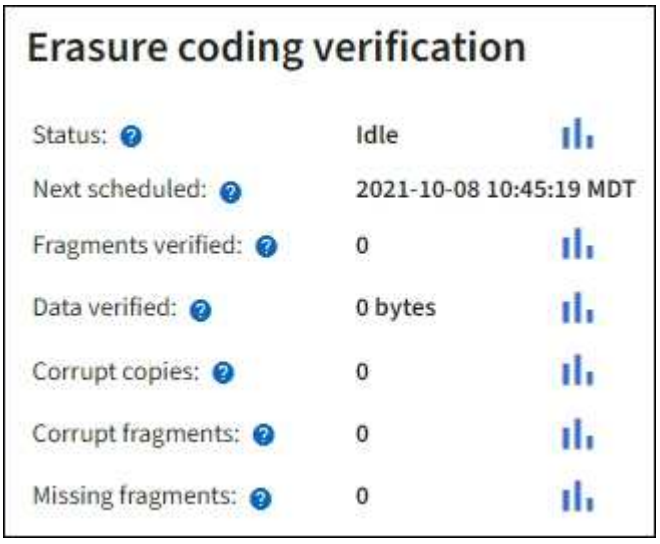
   a. Sélectionnez **NODES** > ***Storage Node*** > **Objects**.

   b. Vérifier les résultats de la vérification :

      - Pour vérifier la vérification des données d'objet répliqué, consultez les attributs de la section Vérification.

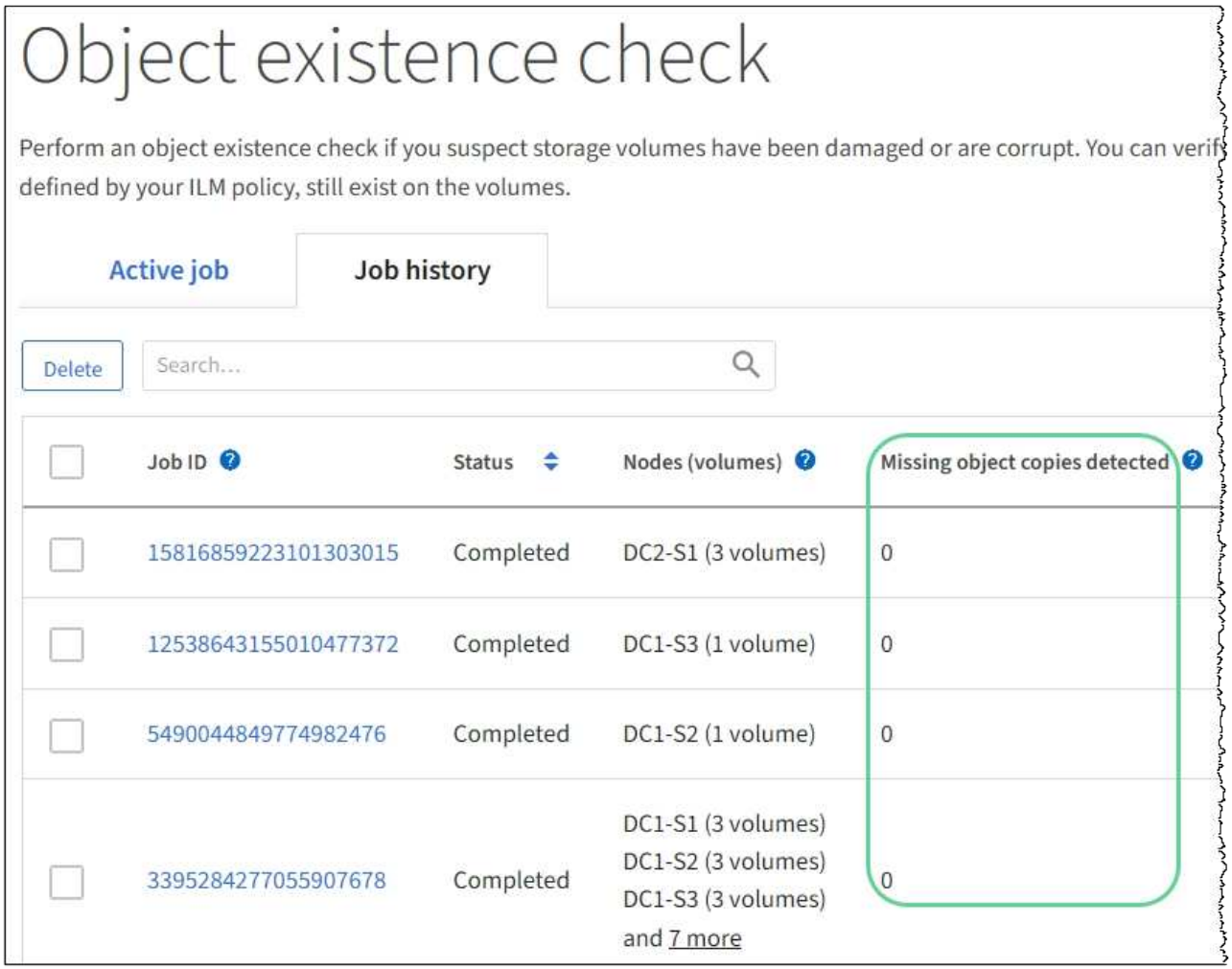


- Pour vérifier la vérification du fragment avec code d'effacement, sélectionnez ***Storage Node*** > **ILM** et examinez les attributs de la section Vérification du code d'effacement.



Sélectionnez le point d'interrogation à côté du nom d'un attribut pour afficher le texte d'aide.

2. Examinez les résultats des travaux de vérification de l'existence d'un objet :
   a. Sélectionnez **MAINTENANCE** > **Vérification de l'existence d'objet** > **Historique du travail**.
   b. Scannez la colonne copies d'objet manquantes détectées. Si des travaux ont entraîné 100 copies d'objets manquantes ou plus et que l'alerte **objets perdus** a été déclenchée, contactez le support technique.



Contrôle des événements

Vous pouvez surveiller les événements détectés par un nœud de grille, y compris les événements personnalisés que vous avez créés pour suivre les événements qui sont consignés sur le serveur syslog. Le message dernier événement affiché dans Grid Manager fournit plus d'informations sur l'événement le plus récent.

Les messages d'événement sont également répertoriés dans le `/var/local/log/bycast-err.log` fichier journal. Voir la "Référence des fichiers journaux".

L'alarme SMTT (Total Events) peut être déclenchée à plusieurs reprises par des problèmes tels que des problèmes de réseau, des pannes de courant ou des mises à niveau. Cette section contient des informations sur l'investigation des événements afin que vous puissiez mieux comprendre pourquoi ces alarmes se sont produites. Si un événement s'est produit à cause d'un problème connu, il est possible de réinitialiser les compteurs d'événements.

Étapes

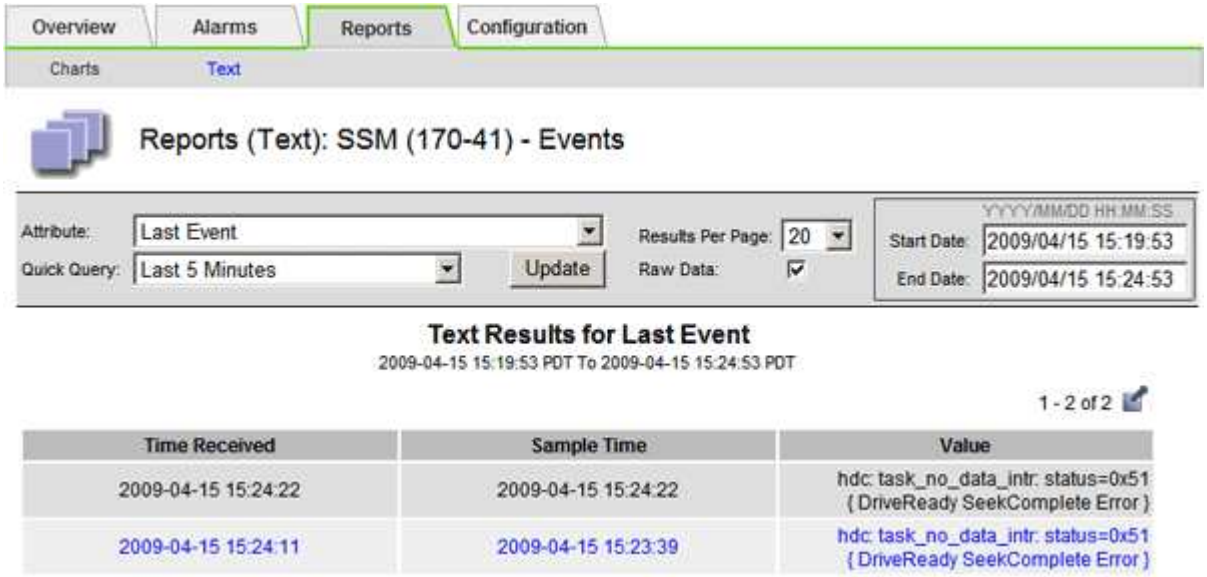
1. Examinez les événements du système pour chaque nœud du grid :
   a. Sélectionnez **SUPPORT** > **Outils** > **topologie de grille**.
   b. Sélectionnez ***site*** > ***grid node*** > **SSM** > **Events** > **Overview** > **main**.
2. Générer une liste de messages d'événement précédents pour vous aider à isoler les problèmes qui se

sont produits auparavant :

a. Sélectionnez **SUPPORT** > **Outils** > **topologie de grille**.
b. Sélectionnez ***site*** > ***grid node*** > **SSM** > **Events** > **Reports**.
c. Sélectionnez **texte**.

   L'attribut **dernier événement** n'est pas affiché dans le "affichage des graphiques". Pour l'afficher :

d. Remplacez **attribut** par **dernier événement**.
e. Vous pouvez également sélectionner une période pour **requête rapide**.
f. Sélectionnez **mettre à jour**.



Créer des événements syslog personnalisés

Les événements personnalisés vous permettent de suivre tous les événements utilisateur du noyau, du démon, de l'erreur et du niveau critique consignés sur le serveur syslog. Un événement personnalisé peut être utile pour surveiller l'occurrence des messages du journal système (et donc les événements de sécurité réseau et les défaillances matérielles).

Description de la tâche

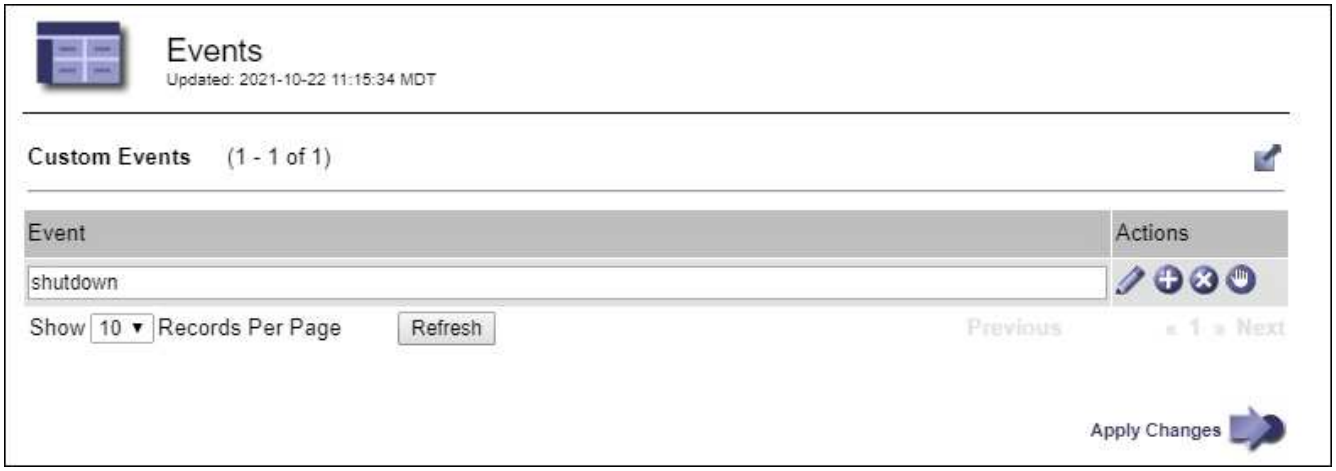
Pensez à créer des événements personnalisés pour surveiller les problèmes récurrents. Les considérations suivantes s'appliquent aux événements personnalisés.

- Après la création d'un événement personnalisé, chaque occurrence de celui-ci est surveillée.
- Pour créer un événement personnalisé basé sur des mots-clés dans `/var/local/log/messages` les fichiers journaux de ces fichiers doivent être :
  - Généré par le noyau
  - Généré par un démon ou un programme utilisateur au niveau d'erreur ou critique

Remarque : toutes les entrées du `/var/local/log/messages` les fichiers seront mis en correspondance à moins qu'ils ne satisfassent aux exigences indiquées ci-dessus.

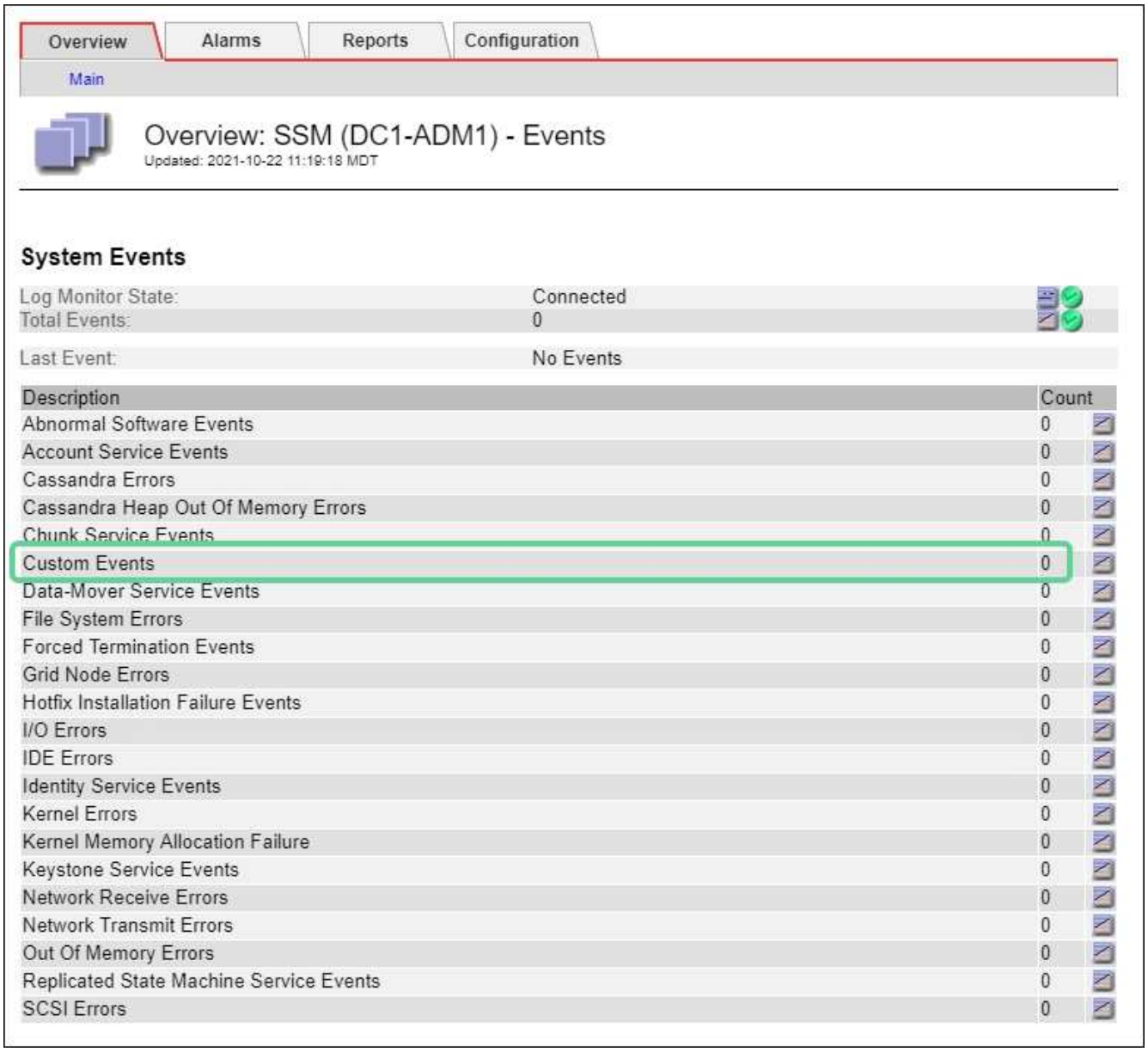
Étapes

1. Sélectionnez **SUPPORT** > **alarmes (hérité)** > **événements personnalisés**.
2. Cliquez sur **Modifier** (Ou **Insérer** si ce n'est pas le premier événement).
3. Entrez une chaîne d'événement personnalisée, par exemple, l'arrêt



4. Sélectionnez **appliquer les modifications**.
5. Sélectionnez **SUPPORT** > **Outils** > **topologie de grille**.
6. Sélectionnez ***GRID node*** > **SSM** > **Events**.
7. Localisez l'entrée événements personnalisés dans le tableau Evénements et surveillez la valeur de **Count**.

   Si le nombre augmente, un événement personnalisé que vous surveillez est déclenché sur ce nœud de la grille.



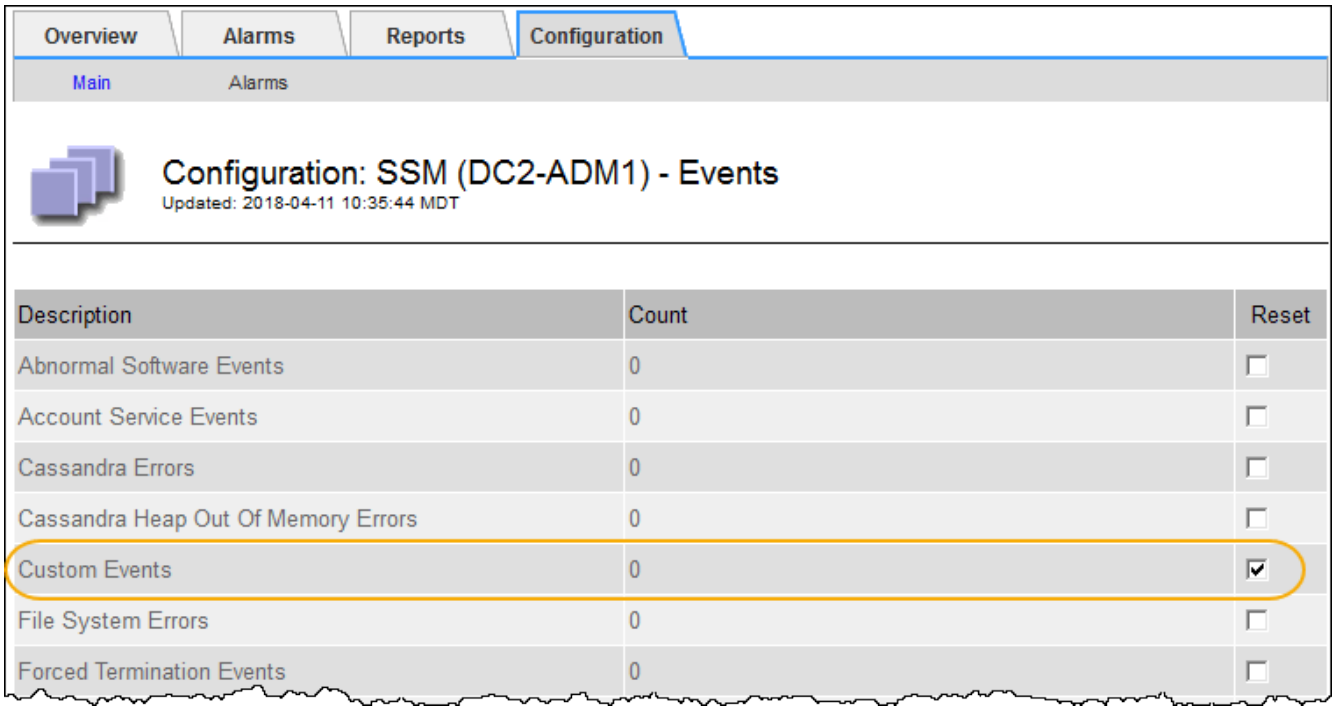
Réinitialisez le nombre d'événements personnalisés

Si vous souhaitez réinitialiser le compteur uniquement pour les événements personnalisés, vous devez utiliser la page topologie de la grille dans le menu support.

La réinitialisation d'un compteur entraîne le déclenchement de l'alarme par l'événement suivant. En revanche, lorsque vous reconnaissez une alarme, celle-ci n'est déclenchée que si le niveau de seuil suivant est atteint.

Étapes

1. Sélectionnez **SUPPORT** > **Outils** > **topologie de grille**.
2. Sélectionnez ***GRID node*** > **SSM** > **Events** > **Configuration** > **main**.
3. Cochez la case **Réinitialiser** pour les événements personnalisés.



4. Sélectionnez **appliquer les modifications**.

Examiner les messages d'audit

Les messages d'audit vous permettent de mieux comprendre le fonctionnement détaillé de votre système StorageGRID. Vous pouvez utiliser les journaux d'audit pour résoudre les problèmes et évaluer les performances.

Pendant le fonctionnement normal du système, tous les services StorageGRID génèrent des messages d'audit comme suit :

- Les messages d'audit système sont liés au système d'audit lui-même, à l'état du nœud de la grille, à l'activité des tâches à l'échelle du système et aux opérations de sauvegarde du service.
- Les messages d'audit du stockage objet sont liés au stockage et à la gestion des objets dans StorageGRID, notamment le stockage objet et les récupérations, les transferts entre nœuds de grille et nœuds de grille, et les vérifications.
- Les messages d'audit de lecture et d'écriture du client sont consignés lorsqu'une application client S3 ou Swift demande de créer, de modifier ou de récupérer un objet.
- Les messages d'audit de gestion consigne les demandes des utilisateurs vers l'API de gestion.

Chaque nœud d'administration stocke les messages d'audit dans des fichiers texte. Le partage d'audit contient le fichier actif (audit.log) ainsi que les journaux d'audit compressés des jours précédents. Chaque nœud de la grille stocke également une copie des informations d'audit générées sur le nœud.

Pour accéder facilement aux journaux d'audit, vous pouvez le faire "Configurer l'accès client d'audit pour NFS". Vous pouvez également accéder aux fichiers journaux d'audit directement à partir de la ligne de commande du nœud d'administration.

Vous pouvez également modifier la destination des journaux d'audit et envoyer des informations d'audit à un serveur syslog externe. Les journaux locaux des enregistrements d'audit continuent à être générés et stockés lorsqu'un serveur syslog externe est configuré. Voir "Configurez les messages d'audit et les destinations des

journaux".

Pour plus de détails sur le fichier journal d'audit, le format des messages d'audit, les types de messages d'audit et les outils disponibles pour analyser les messages d'audit, reportez-vous à la section "Examiner les journaux d'audit".

Collecte de fichiers journaux et de données système

Vous pouvez utiliser le Gestionnaire de grille pour récupérer les fichiers journaux et les données système (y compris les données de configuration) de votre système StorageGRID.

Avant de commencer

- Vous devez être connecté au gestionnaire de grille sur le nœud d'administration principal à l'aide d'un "navigateur web pris en charge".
- Vous devez disposer d'autorisations d'accès spécifiques.
- Vous devez disposer de la phrase secrète pour le provisionnement.

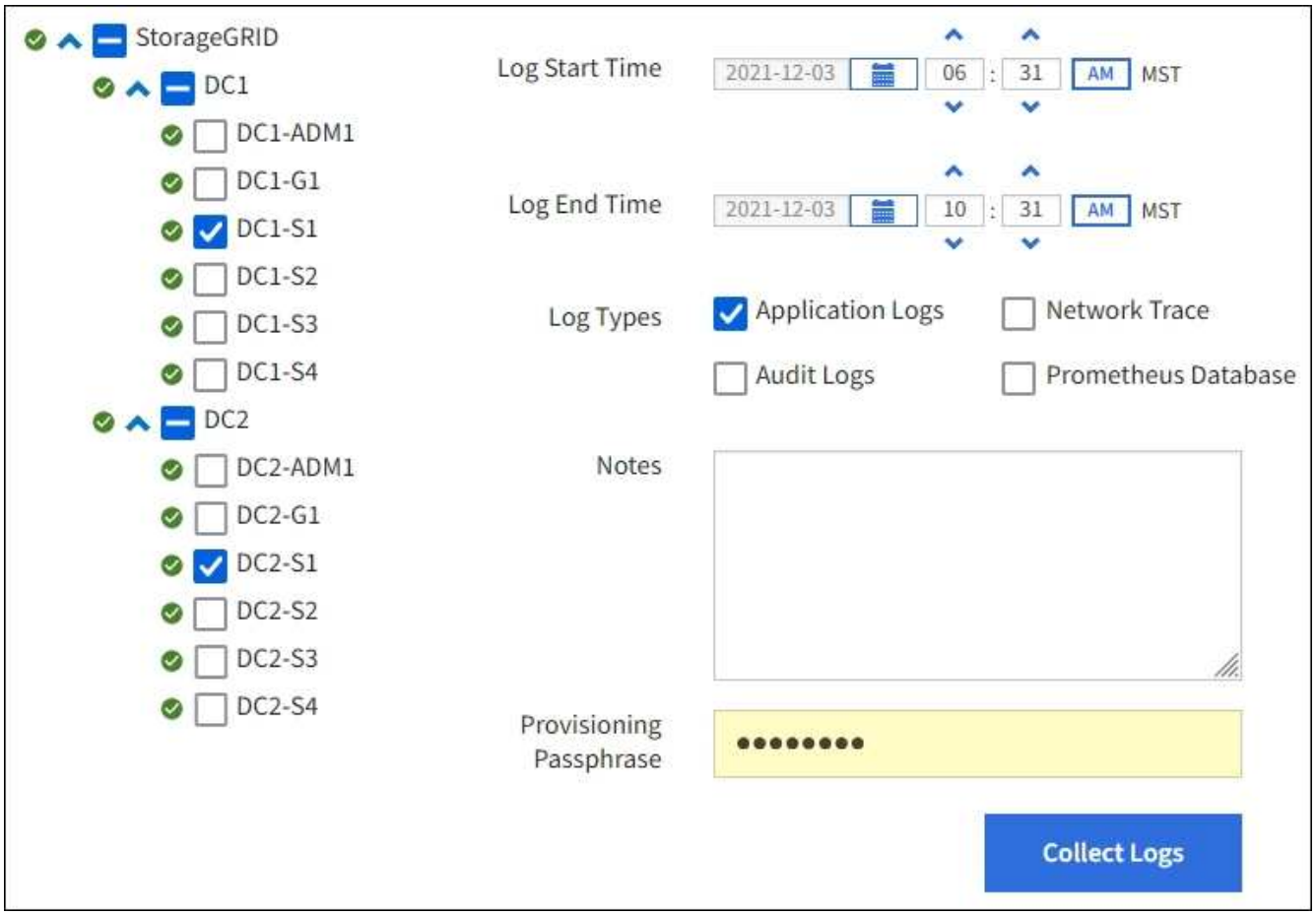
Description de la tâche

Vous pouvez utiliser le gestionnaire de grille pour rassembler "fichiers journaux", données système et données de configuration de n'importe quel nœud de grille pour la période sélectionnée. Les données sont collectées et archivées dans un fichier .tar.gz que vous pouvez ensuite télécharger sur votre ordinateur local.

Vous pouvez également modifier la destination des journaux d'audit et envoyer des informations d'audit à un serveur syslog externe. Les journaux locaux des enregistrements d'audit continuent à être générés et stockés lorsqu'un serveur syslog externe est configuré. Voir "Configurez les messages d'audit et les destinations des journaux".

Étapes

1. Sélectionnez **SUPPORT** > **Outils** > **journaux**.



2. Sélectionnez les nœuds de grille pour lesquels vous souhaitez collecter les fichiers journaux.

   Si nécessaire, vous pouvez collecter des fichiers journaux pour l'intégralité de la grille ou un site de data Center.

3. Sélectionnez une **heure de début** et **heure de fin** pour définir la plage horaire des données à inclure dans les fichiers journaux.

   Si vous sélectionnez une période très longue ou que vous collectez des journaux de tous les nœuds d'un grand grid, l'archivage des journaux risque de devenir trop volumineux pour être stocké sur un nœud, ou trop volumineux pour être collecté sur le nœud d'administration principal pour le téléchargement. Dans ce cas, vous devez redémarrer la collecte de journaux avec un jeu de données plus petit.

4. Sélectionnez les types de journaux que vous souhaitez collecter.
   - **Journaux d'applications** : journaux spécifiques à l'application que le support technique utilise le plus fréquemment pour le dépannage. Les journaux collectés sont un sous-ensemble des journaux d'application disponibles.
   - **Journaux d'audit** : journaux contenant les messages d'audit générés pendant le fonctionnement normal du système.
   - **Trace réseau** : journaux utilisés pour le débogage réseau.
   - **Base de données Prometheus** : indicateurs de séries chronologiques des services sur tous les nœuds.
5. Vous pouvez également saisir des notes concernant les fichiers journaux que vous recueillez dans la zone de texte **Notes**.

Vous pouvez utiliser ces notes pour fournir des informations de support technique sur le problème qui vous a demandé de collecter les fichiers journaux. Vos notes sont ajoutées à un fichier appelé `info.txt`, avec d'autres informations sur la collecte de fichier journal. Le `info.txt` le fichier est enregistré dans le package d'archivage du fichier journal.

6. Saisissez le mot de passe de provisionnement de votre système StorageGRID dans la zone de texte **phrase de passe de provisionnement**.
7. Sélectionnez **collecter les journaux**.

   Lorsque vous soumettez une nouvelle demande, la collection précédente de fichiers journaux est supprimée.

   Vous pouvez utiliser la page journaux pour surveiller la progression de la collecte des fichiers journaux pour chaque nœud de la grille.

   Si vous recevez un message d'erreur sur la taille du journal, essayez de collecter les journaux pour une période plus courte ou pour moins de nœuds.

8. Sélectionnez **Download** lorsque la collecte des fichiers journaux est terminée.

   Le fichier *.tar.gz* contient tous les fichiers journaux de tous les nœuds de la grille où la collecte des journaux a réussi. Dans le fichier combiné *.tar.gz*, il y a une archive de fichier journal pour chaque nœud de la grille.

Une fois que vous avez terminé

Vous pouvez télécharger à nouveau le package d'archivage des fichiers journaux ultérieurement si nécessaire.

Vous pouvez également sélectionner **Supprimer** pour supprimer le paquet d'archive de fichier journal et libérer de l'espace disque. Le progiciel d'archivage du fichier journal actuel est automatiquement supprimé lors de la prochaine collecte de fichiers journaux.

Déclencher manuellement un message AutoSupport

Pour aider le support technique à résoudre les problèmes liés à votre système StorageGRID, vous pouvez déclencher manuellement un message AutoSupport à envoyer.

Avant de commencer

- Vous devez être connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous devez disposer de l'accès racine ou d'une autre autorisation de configuration de grille.

Étapes

1. Sélectionnez **SUPPORT** > **Outils** > **AutoSupport**.
2. Dans l'onglet **Paramètres**, sélectionnez **Envoyer AutoSupport** déclenché par l'utilisateur.

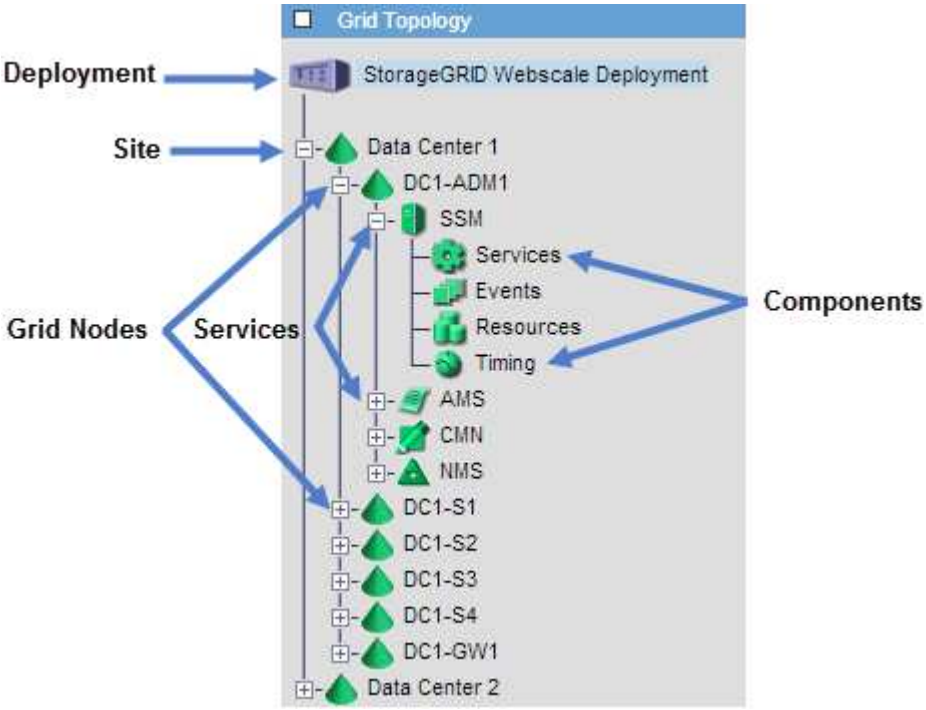
   StorageGRID tente d'envoyer un message AutoSupport au support technique. Si la tentative réussit, les valeurs **résultat le plus récent** et **dernier temps** réussi dans l'onglet **Résultats** sont mises à jour. En cas de problème, la valeur **résultat** la plus récente est mise à jour sur "échec" et StorageGRID n'essaie pas d'envoyer à nouveau le message AutoSupport.

Après avoir envoyé un message AutoSupport déclenché par l'utilisateur, actualisez la page AutoSupport de votre navigateur après 1 minute pour accéder aux résultats les plus récents.

Afficher l'arborescence de la grille topologique

L'arborescence de la grille topologie permet d'accéder à des informations détaillées sur les éléments du système StorageGRID, notamment les sites, les nœuds de la grille, les services et les composants. Dans la plupart des cas, il vous suffit d'accéder à l'arborescence de la grille topologique lorsque vous y êtes invité ou lorsque vous collaborez avec le support technique.

Pour accéder à l'arborescence de la topologie de grille, sélectionnez **SUPPORT** > **Outils** > **topologie de grille**.



Pour développer ou réduire l'arborescence de la topologie de la grille, cliquez sur ⊞ ou ⊟ au niveau site, nœud ou service. Pour développer ou réduire tous les éléments du site entier ou de chaque nœud, maintenez la touche **<Ctrl>** enfoncée et cliquez sur.

Attributs des StorageGRID

Attributs valeurs et États du rapport pour la plupart des fonctions du système StorageGRID. Des valeurs d'attribut sont disponibles pour chaque nœud de grille, chaque site et la grille entière.

Les attributs StorageGRID sont utilisés à plusieurs endroits dans le Gestionnaire de grille :

- **Page noeuds** : la plupart des valeurs affichées sur la page noeuds sont des attributs StorageGRID. (Les metrics de Prometheus sont également affichés sur les pages nœuds.)
- **Alarmes** : lorsque les attributs atteignent des valeurs de seuil définies, les alarmes StorageGRID (système hérité) sont déclenchées à des niveaux de gravité spécifiques.
- **Grid Topology Tree** : les valeurs d'attribut sont affichées dans l'arborescence de la topologie de la grille

(**SUPPORT** > **Outils** > **topologie de la grille**).

- **Evénements** : les événements système se produisent lorsque certains attributs enregistrent une condition d'erreur ou de panne pour un nœud, y compris des erreurs telles que des erreurs réseau.

Valeurs d'attribut

Les attributs sont rapportés sur la base du meilleur effort et sont approximativement corrects. Les mises à jour d'attributs peuvent être perdues dans certains cas, comme la panne d'un service ou la panne et la reconstruction d'un nœud de la grille.

En outre, les retards de propagation peuvent ralentir le reporting des attributs. Les valeurs mises à jour pour la plupart des attributs sont envoyées au système StorageGRID à intervalles fixes. Plusieurs minutes peuvent être nécessaires avant qu'une mise à jour soit visible dans le système et deux attributs qui changent plus ou moins simultanément peuvent être signalés à des moments légèrement différents.

Examinez les metrics de support

Lorsque vous dépannez un problème, vous pouvez consulter les graphiques et les metrics détaillés de votre système StorageGRID en collaboration avec le support technique.

Avant de commencer

- Vous devez être connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous devez disposer d'autorisations d'accès spécifiques.

Description de la tâche

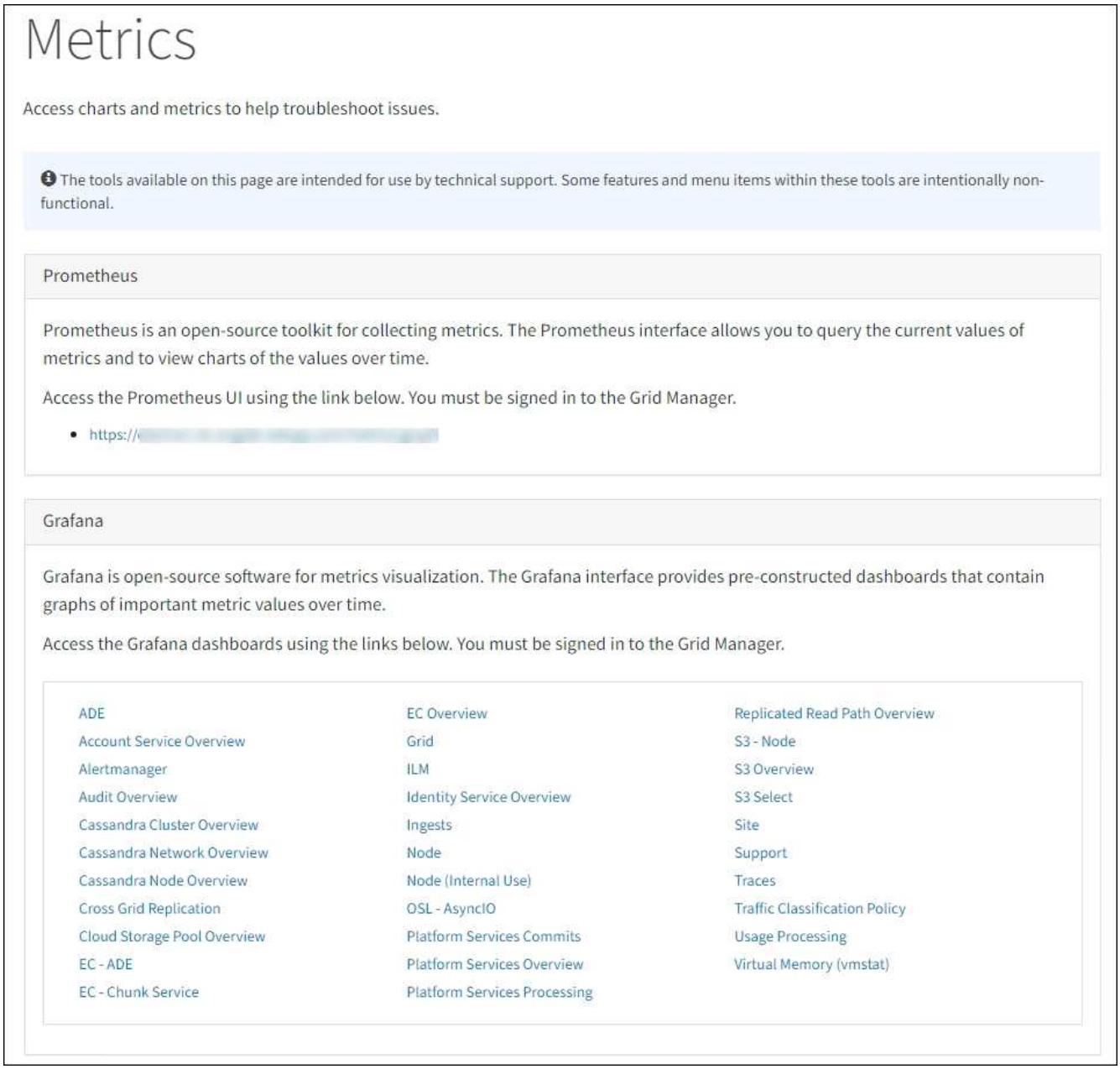
La page Metrics vous permet d'accéder aux interfaces utilisateur de Prometheus et Grafana. Prometheus est un logiciel open source qui permet de collecter des metrics. Grafana est un logiciel open source permettant de visualiser les metrics.

> Les outils disponibles sur la page métriques sont destinés au support technique. Certaines fonctions et options de menu de ces outils sont intentionnellement non fonctionnelles et peuvent faire l'objet de modifications. Voir la liste des "Metrics Prometheus couramment utilisés".

Étapes

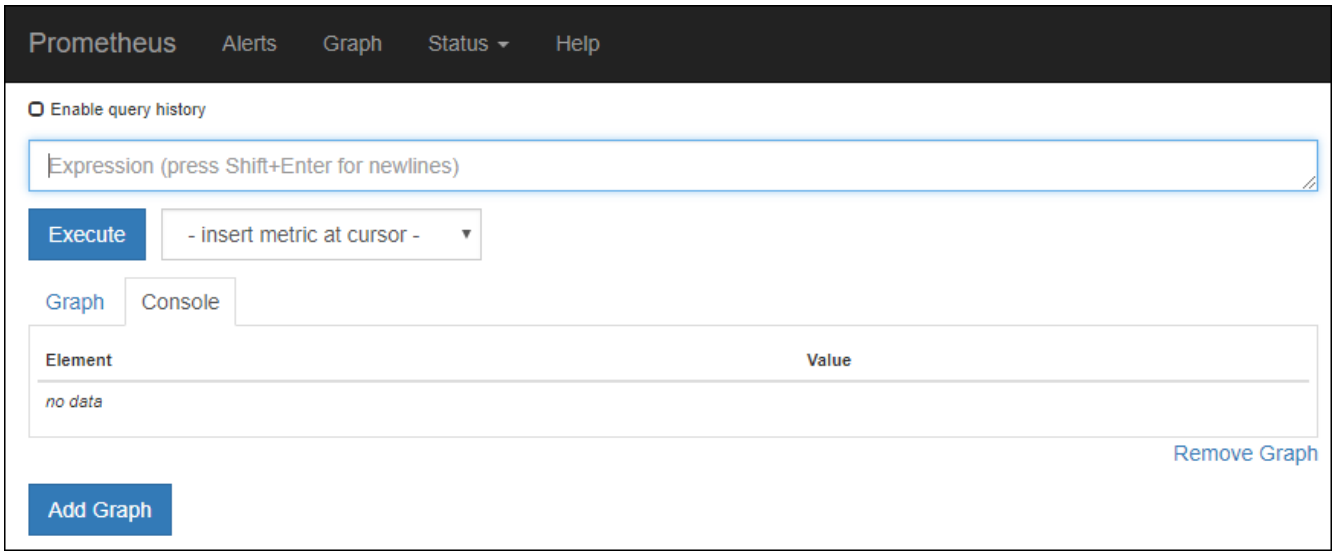
1. Comme indiqué par le support technique, sélectionnez **SUPPORT** > **Outils** > **métriques**.

   Voici un exemple de la page métriques :



2. Pour interroger les valeurs actuelles des metrics StorageGRID et afficher les graphiques des valeurs dans le temps, cliquez sur le lien de la section Prometheus.

   L'interface Prometheus s'affiche. Vous pouvez utiliser cette interface pour exécuter des requêtes sur les mesures StorageGRID disponibles et pour générer des graphiques sur les mesures StorageGRID au fil du temps.



Les indicateurs qui incluent *private* dans leurs noms sont destinés à un usage interne uniquement et peuvent être modifiés sans préavis entre les versions de StorageGRID.

3. Pour accéder aux tableaux de bord pré-construits contenant des graphiques des mesures StorageGRID au fil du temps, cliquez sur les liens de la section Grafana.

   L'interface Grafana pour le lien que vous avez sélectionné s'affiche.

Exécuter les diagnostics

Lors du dépannage d'un problème, vous pouvez vous aider avec le support technique à exécuter des diagnostics sur votre système StorageGRID et examiner les résultats.

- "Examinez les metrics de support"
- "Metrics Prometheus couramment utilisés"

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous disposez d'autorisations d'accès spécifiques.

Description de la tâche

La page Diagnostics effectue un ensemble de contrôles de diagnostic sur l'état actuel de la grille. Chaque vérification de diagnostic peut avoir l'un des trois États suivants :

-

- **Normal** : toutes les valeurs sont comprises dans la plage normale.
- **Attention** : une ou plusieurs valeurs sont hors de la plage normale.
- **Attention** : une ou plusieurs valeurs sont significativement en dehors de la plage normale.

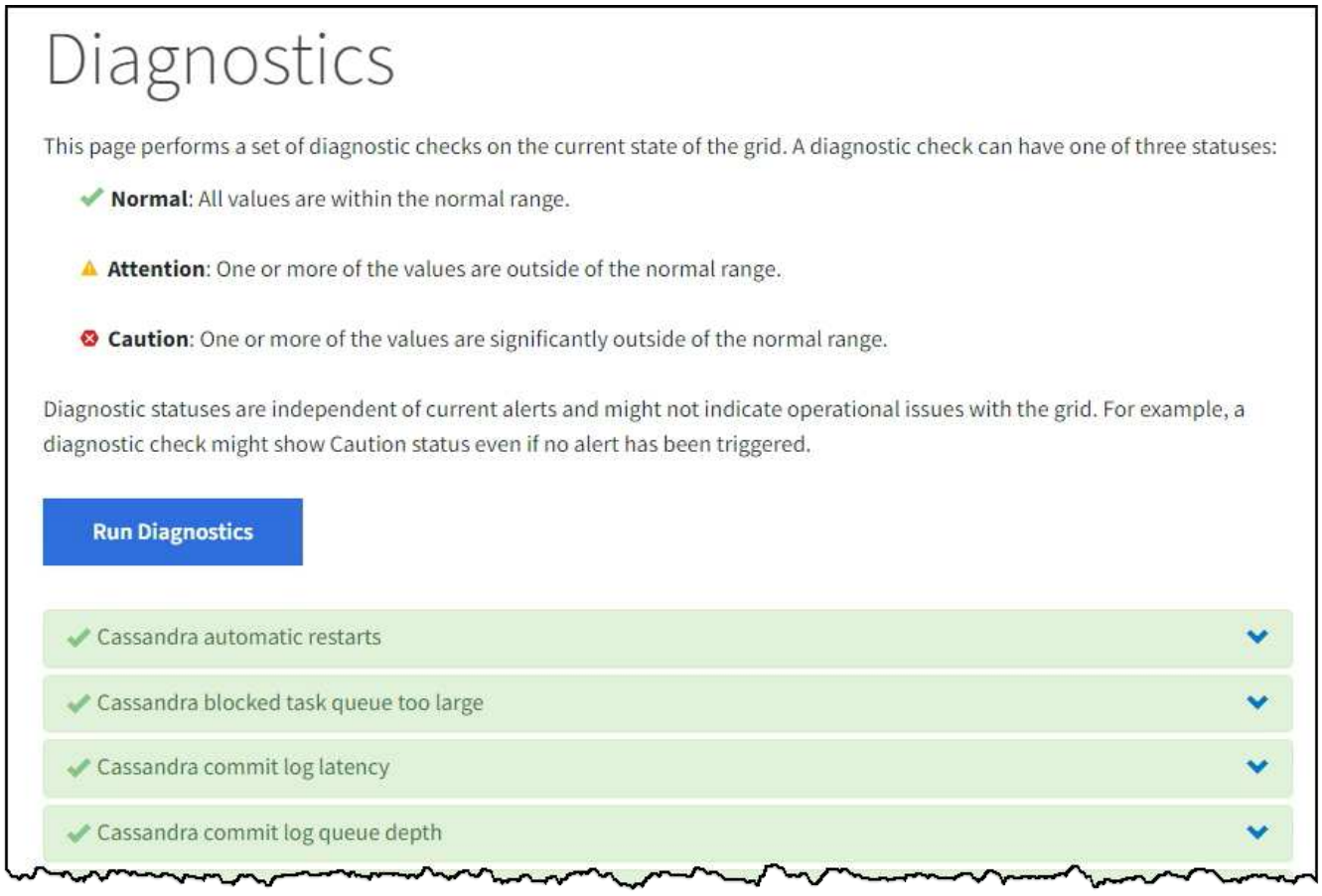
Les États de diagnostic sont indépendants des alertes en cours et peuvent ne pas indiquer de problèmes opérationnels dans la grille. Par exemple, une vérification de diagnostic peut afficher l'état de mise en garde même si aucune alerte n'a été déclenchée.

Étapes

1. Sélectionnez **SUPPORT** > **Outils** > **Diagnostics**.

   La page Diagnostics s'affiche et répertorie les résultats de chaque vérification de diagnostic. Les résultats sont triés par gravité (attention, attention, puis normale). Dans chaque gravité, les résultats sont triés par ordre alphabétique.

   Dans cet exemple, tous les diagnostics ont un état Normal.



2. Pour en savoir plus sur un diagnostic spécifique, cliquez n'importe où dans la ligne.

   Des détails sur le diagnostic et ses résultats actuels s'affichent. Les informations suivantes sont répertoriées :

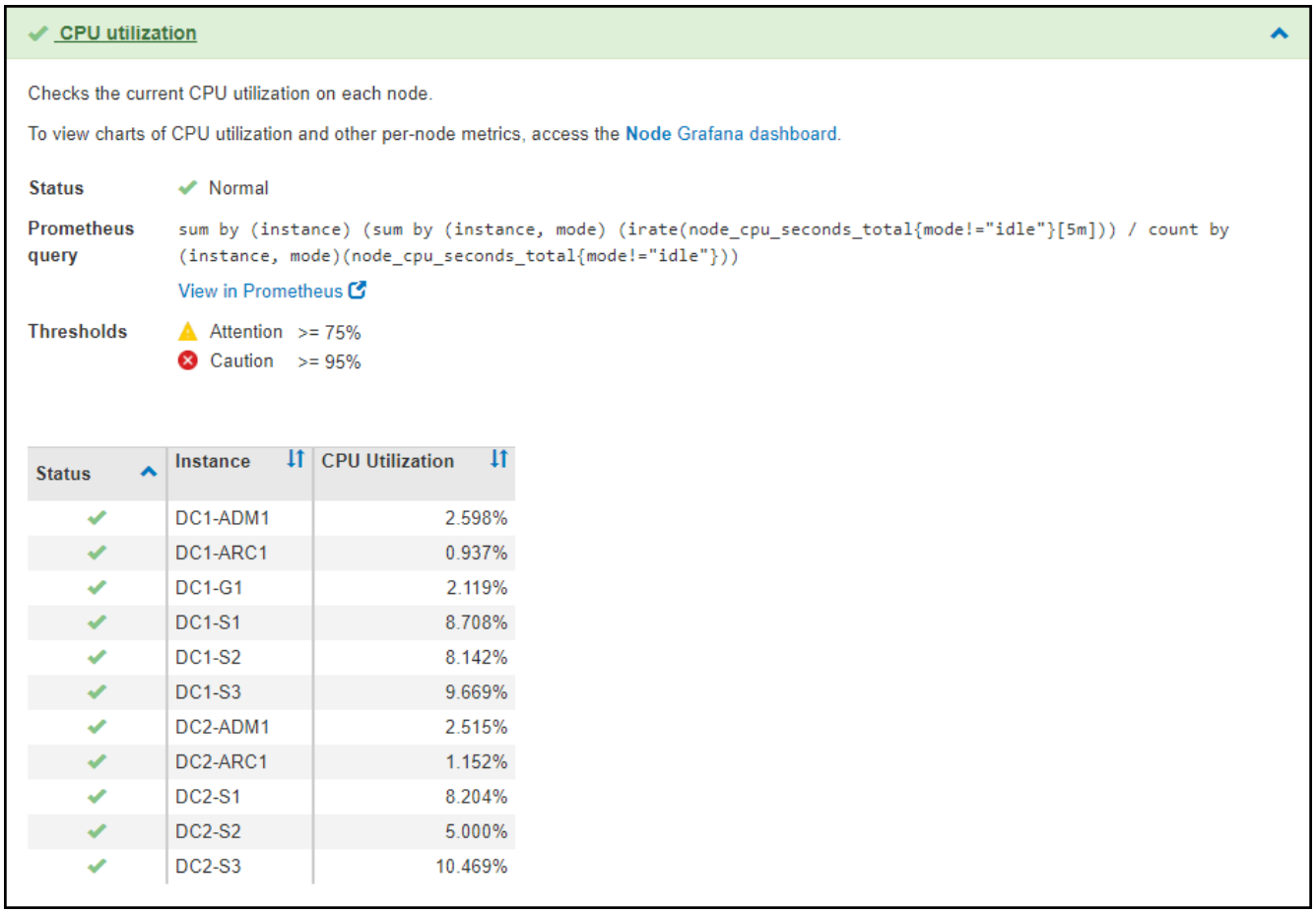
   - **Etat** : état actuel de ce diagnostic : normal, attention ou attention.
   - **Requête Prometheus** : si utilisé pour le diagnostic, l'expression Prometheus qui a été utilisée pour

générer les valeurs d'état. (Une expression Prometheus n'est pas utilisée pour tous les diagnostics.)

- **Seuils** : si disponibles pour le diagnostic, les seuils définis par le système pour chaque état de diagnostic anormal. (Les valeurs de seuil ne sont pas utilisées pour tous les diagnostics.)

  Vous ne pouvez pas modifier ces seuils.

- **Valeurs d'état** : tableau indiquant l'état et la valeur du diagnostic dans l'ensemble du système StorageGRID. Dans cet exemple, l'utilisation actuelle du processeur pour chaque nœud d'un système StorageGRID est indiquée. Toutes les valeurs de nœud sont inférieures aux seuils attention et mise en garde, de sorte que l'état général du diagnostic est Normal.



3. **Facultatif** : pour afficher les graphiques Grafana relatifs à ce diagnostic, cliquez sur le lien **Dashboard**.

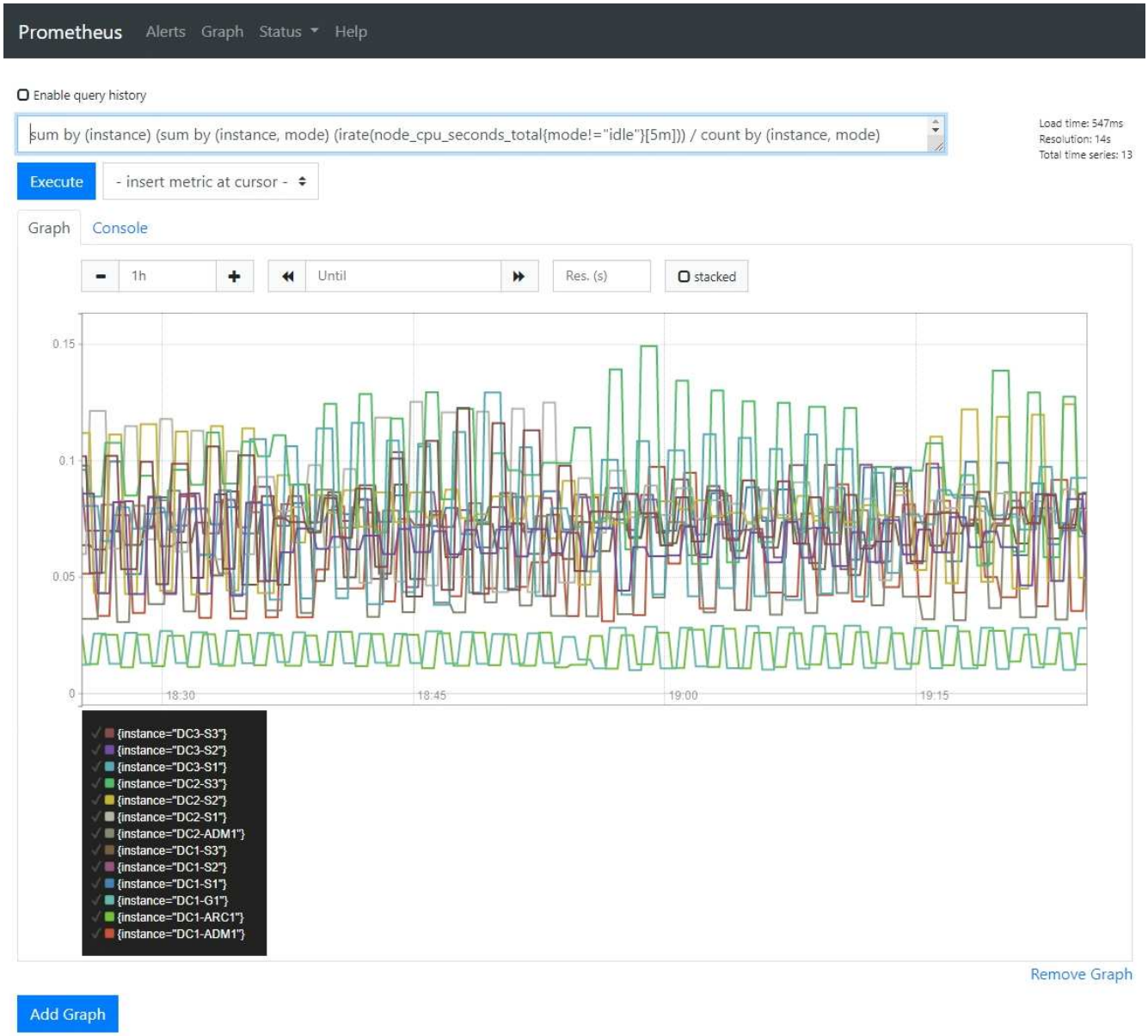
   Ce lien ne s'affiche pas pour tous les diagnostics.

   Le tableau de bord associé à Grafana s'affiche. Dans cet exemple, le tableau de bord des nœuds apparaît et affiche l'utilisation des CPU dans le temps pour ce nœud, ainsi que d'autres graphiques Grafana pour le nœud.

   Vous pouvez également accéder aux tableaux de bord pré-construits Grafana à partir de la section **SUPPORT** > **Tools** > **Metrics**.

4. **Facultatif** : pour afficher un graphique de l'expression Prometheus au fil du temps, cliquez sur **Afficher dans Prometheus**.

   Un graphique Prometheus de l'expression utilisée dans le diagnostic s'affiche.



Créer des applications de surveillance personnalisées

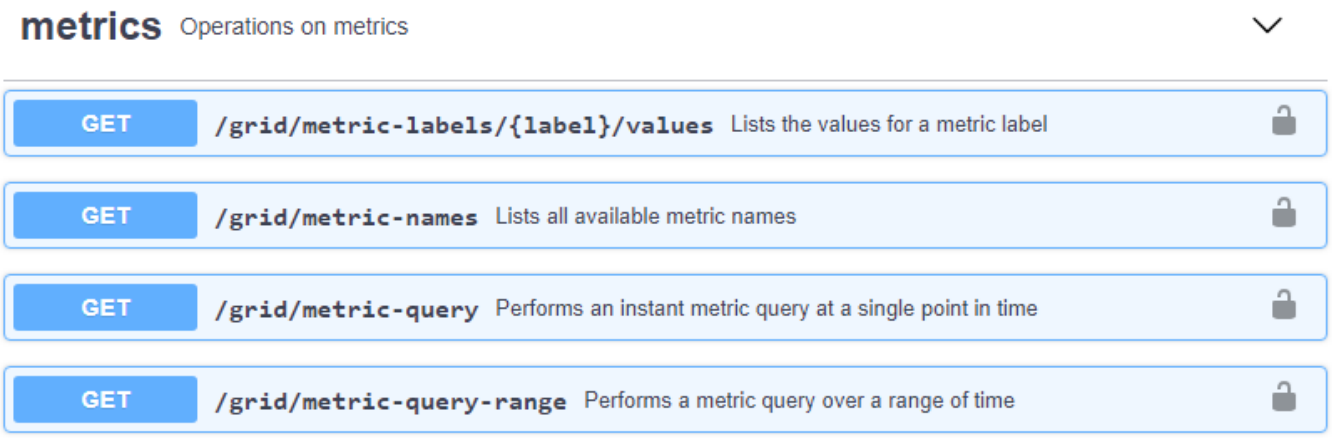
Vous pouvez créer des applications et des tableaux de bord de surveillance personnalisés à l'aide des metrics StorageGRID disponibles dans l'API de gestion du grid.

Si vous souhaitez surveiller des mesures qui ne s'affichent pas sur une page existante du Gestionnaire de grille ou si vous souhaitez créer des tableaux de bord personnalisés pour StorageGRID, vous pouvez utiliser l'API de gestion de grille pour interroger les mesures StorageGRID.

Vous pouvez également accéder directement à des metrics Prometheus à l'aide d'un outil de surveillance externe tel que Grafana. Pour utiliser un outil externe, vous devez télécharger ou générer un certificat de client d'administration afin de permettre à StorageGRID d'authentifier l'outil pour la sécurité. Voir la "Instructions d'administration de StorageGRID".

Pour afficher les opérations de l'API de metrics, y compris la liste complète des metrics disponibles, rendez-vous sur Grid Manager. En haut de la page, sélectionnez l'icône d'aide et sélectionnez **documentation API** >

metrics.



Les détails de la mise en œuvre d'une application de surveillance personnalisée dépassent le champ d'application de cette documentation.

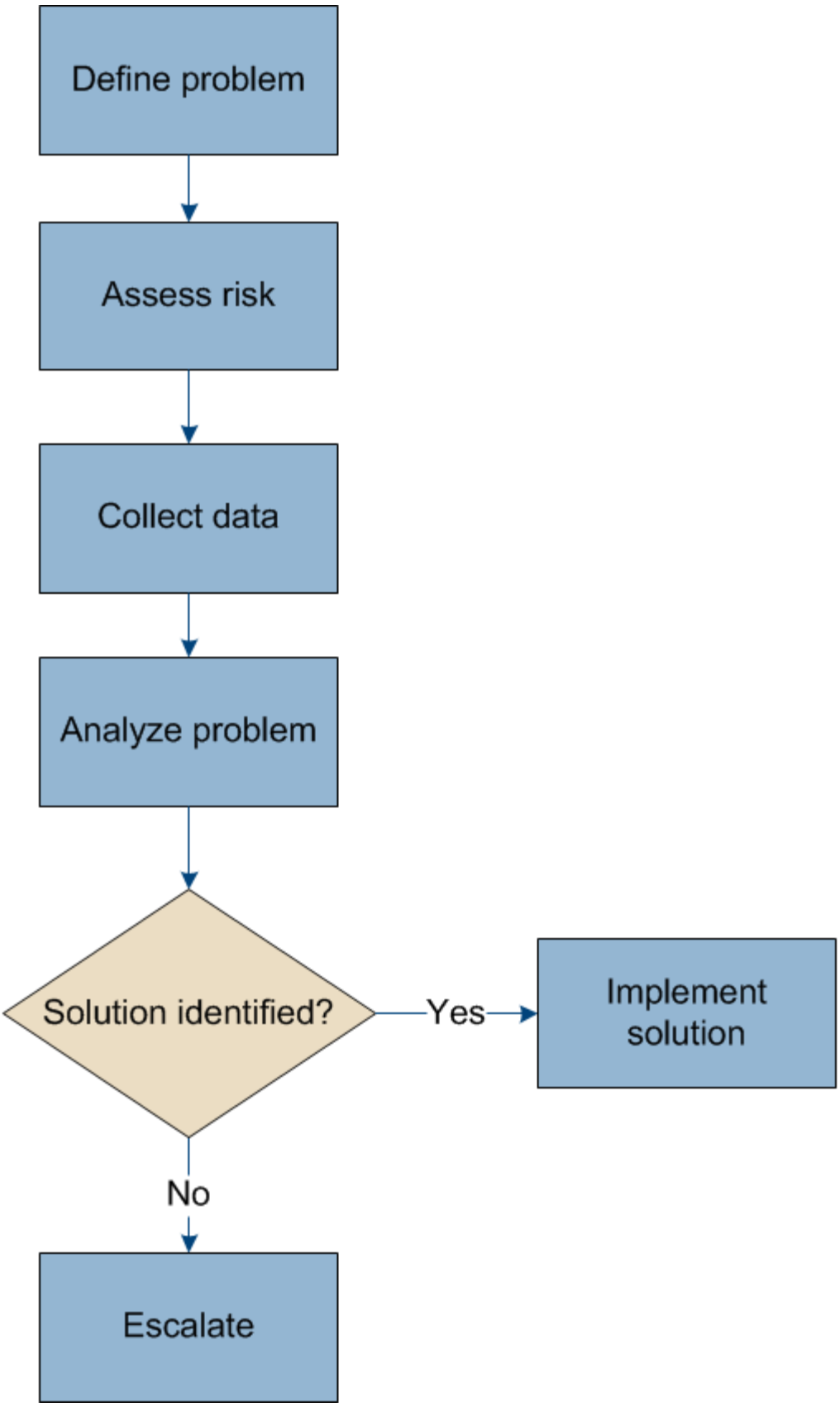
Dépanner le système StorageGRID

Dépannage d'un système StorageGRID : présentation

Si vous rencontrez un problème avec un système StorageGRID, consultez les conseils et les instructions de cette section pour déterminer et résoudre le problème.

Présentation de la détection des problèmes

Si vous rencontrez un problème quand "Administration d'un système StorageGRID", vous pouvez utiliser le processus décrit dans cette figure pour identifier et analyser le problème. Vous pouvez souvent résoudre vous-même certains problèmes, mais vous devrez peut-être les faire remonter au support technique.



définir le problème

La première étape pour résoudre un problème est de définir clairement le problème.

Ce tableau fournit des exemples de types d'informations que vous pouvez collecter pour définir un problème :

Question	Exemple de réponse
Que fait ou ne fait pas le système StorageGRID ? Quels sont ses symptômes ?	Les applications client signalent que les objets ne peuvent pas être ingérés dans StorageGRID.
Quand le problème a-t-il démarré ?	L'ingestion d'objet a d'abord été refusée à environ 14:50 le 8 janvier 2020.
Comment avez-vous remarqué le problème pour la première fois ?	Notifié par la demande du client. Vous avez également reçu des notifications par e-mail d'alerte.
Le problème se produit-il de manière cohérente ou seulement parfois ?	Le problème est en cours.
Si le problème se produit régulièrement, quelles sont les étapes à suivre	Un problème se produit à chaque fois qu'un client tente d'ingérer un objet.
Si le problème se produit par intermittence, quand cela se produit-il? Notez l'heure de chaque incident que vous connaissez.	Le problème n'est pas intermittent.
Avez-vous déjà vu ce problème ? À quelle fréquence avez-vous eu ce problème par le passé ?	C'est la première fois que j'ai vu cette question.

Évaluez les risques et l'impact sur le système

Une fois le problème défini, évaluez les risques et l'impact sur le système StorageGRID. Par exemple, la présence d'alertes critiques ne signifie pas nécessairement que le système ne fournit pas de services de base.

Ce tableau récapitule l'impact du problème exemple sur les opérations du système :

Question	Exemple de réponse
Le système StorageGRID est-il en mesure d'ingérer du contenu ?	Non
Les applications client peuvent-elles récupérer du contenu ?	Certains objets peuvent être récupérés et d'autres ne le peuvent pas.
Les données sont-elles menacées ?	Non
La capacité à mener des activités est-elle gravement affectée ?	Oui, car les applications client ne peuvent pas stocker d'objets sur le système StorageGRID et les données ne peuvent pas être récupérées de manière cohérente.

Collecte de données

Une fois que vous avez défini le problème et évalué ses risques et son impact, collectez des données pour analyse. Le type de données les plus utiles à recueillir dépend de la nature du problème.

Type de données à collecter	Pourquoi recueillir ce dat	Instructions
Créer le calendrier des modifications récentes	Toute modification de votre système StorageGRID, de sa configuration ou de son environnement peut provoquer un nouveau comportement.	• Créer un calendrier des modifications récentes
Examinez les alertes et les alarmes	Les alertes et les alarmes peuvent vous aider à déterminer rapidement la cause première d'un problème en fournissant des indications importantes sur les problèmes sous-jacents qui pourraient l'être. Consultez la liste des alertes et alarmes en cours pour voir si StorageGRID a identifié la cause principale d'un problème pour vous. Pour en savoir plus, consultez les alertes et les alarmes déclenchées par le passé.	• "Afficher les alertes actuelles et résolues" • "Gestion des alarmes (système hérité)"
Contrôle des événements	Les événements incluent les événements d'erreur système ou de panne pour un nœud, y compris les erreurs telles que les erreurs réseau. Surveiller les événements pour en savoir plus sur les problèmes ou obtenir de l'aide pour les résoudre.	• "Contrôle des événements"
Identifier les tendances à l'aide de graphiques et de rapports texte	Les tendances peuvent donner des indications précieuses sur le moment où les problèmes sont apparus et vous aider à comprendre la rapidité à laquelle les choses évoluent.	• "Utilisez des graphiques et des graphiques" • "Utilisez les rapports texte"
Établir les lignes de base	Collectez des informations sur les niveaux normaux de différentes valeurs opérationnelles. Ces valeurs de référence, ainsi que les écarts par rapport à ces lignes de base, peuvent fournir des indices précieux.	• Établir les lignes de base
Tests d'entrée et de récupération	Pour résoudre les problèmes de performance liés à l'entrée et à la récupération, utilisez un poste de travail pour stocker et récupérer des objets. Comparez les résultats obtenus avec ceux observés lors de l'utilisation de l'application client.	• "Surveillez L'PUT et OBTENEZ des performances"

Type de données à collecter	Pourquoi recueillir ce dat	Instructions
Examiner les messages d'audit	Examinez les messages d'audit afin de suivre les opérations StorageGRID en détail. Les détails dans les messages d'audit peuvent être utiles pour le dépannage de nombreux types de problèmes, y compris les problèmes de performance.	• "Examiner les messages d'audit"
Vérifier l'emplacement des objets et l'intégrité du stockage	En cas de problèmes de stockage, vérifiez que les objets sont placés à l'endroit où vous vous attendez. Vérifiez l'intégrité des données d'objet sur un nœud de stockage.	• "Surveiller les opérations de vérification d'objets" • "Confirmer l'emplacement des données d'objet" • "Vérifiez l'intégrité de l'objet"
Collecte de données pour le support technique	L'assistance technique peut vous demander de collecter des données ou de passer en revue des informations spécifiques pour résoudre les problèmes.	• "Collecte de fichiers journaux et de données système" • "Déclencher manuellement un message AutoSupport" • "Examinez les metrics de support"

Créez un calendrier des modifications récentes

En cas de problème, vous devriez considérer ce qui a changé récemment et quand ces changements se sont produits.

- Toute modification de votre système StorageGRID, de sa configuration ou de son environnement peut provoquer un nouveau comportement.
- Un calendrier des modifications peut vous aider à identifier les changements susceptibles d'être responsables d'un problème, ainsi que la manière dont chaque changement pourrait avoir affecté son développement.

Créez un tableau des dernières modifications apportées à votre système, qui contient des informations sur la date à laquelle chaque modification a eu lieu, ainsi que des informations pertinentes sur la modification, telles que les autres événements survenus pendant que la modification a été en cours :

Heure de la modification	Type de modification	Détails
Par exemple : • Quand avez-vous démarré la restauration du nœud ? • Quand la mise à niveau logicielle s'est-elle terminée ? • Avez-vous interrompu le processus ?	Que s'est-il passé ? Qu'avez-vous fait ?	Documentez toute information pertinente concernant la modification. Par exemple : • Détails des modifications du réseau. • Quel correctif a été installé. • Changement des workloads clients. Assurez-vous de noter si plusieurs changements ont eu lieu en même temps. Par exemple, ce changement a-t-il été effectué pendant qu'une mise à niveau était en cours ?

Exemples de changements récents importants

Voici quelques exemples de changements potentiellement importants :

- Le système StorageGRID a-t-il été récemment installé, étendu ou récupéré ?
- Le système a-t-il été mis à niveau récemment ? Un correctif a-t-il été appliqué ?
- Du matériel a-t-il été réparé ou modifié récemment ?
- La règle ILM a-t-elle été mise à jour ?
- La charge de travail client a-t-elle changé ?
- L'application client ou son comportement a-t-il changé ?
- Avez-vous modifié des équilibreurs de charge, ou ajouté ou supprimé un groupe haute disponibilité de nœuds d'administration ou de nœuds de passerelle ?
- Certaines tâches lancées peuvent-elles prendre un certain temps ? Voici quelques exemples :
  - Récupération d'un noeud de stockage défaillant
  - Désaffectation des nœuds de stockage
- Des modifications ont-elles été apportées à l'authentification utilisateur, par exemple l'ajout d'un locataire ou la modification de la configuration LDAP ?
- La migration des données a-t-elle lieu ?
- Les services de plateforme ont-ils été récemment activés ou modifiés ?
- La conformité a-t-elle été activée récemment ?
- Les pools de stockage cloud ont-ils été ajoutés ou supprimés ?
- La compression du stockage ou le chiffrement ont-ils été modifiés ?
- L'infrastructure réseau a-t-elle été modifiée ? Par exemple, VLAN, routeurs ou DNS.
- Des modifications ont-elles été apportées aux sources NTP ?
- Des modifications ont-elles été apportées aux interfaces réseau Grid, Admin ou client ?
- Des modifications de configuration ont-elles été apportées au nœud d'archivage ?
- Le système StorageGRID ou son environnement a-t-il subi d'autres modifications ?

Établir les lignes de base

Vous pouvez établir des lignes de base pour votre système en enregistrant les niveaux normaux de différentes valeurs opérationnelles. À l'avenir, vous pourrez comparer les valeurs actuelles à ces lignes de base afin de détecter et de résoudre les valeurs anormales.

Propriété	Valeur	Comment obtenir
Consommation de stockage moyenne	Go utilisés/jour Pourcentage consommé/jour	Accédez à Grid Manager. Sur la page nœuds, sélectionnez la totalité de la grille ou d'un site et accédez à l'onglet stockage. Dans le graphique stockage utilisé - données d'objet, recherchez une période où la ligne est assez stable. Positionnez le curseur de votre souris sur le graphique pour estimer la quantité de stockage consommée chaque jour Vous pouvez collecter ces informations pour l'intégralité du système ou pour un data Center spécifique.
Consommation moyenne des métadonnées	Go utilisés/jour Pourcentage consommé/jour	Accédez à Grid Manager. Sur la page nœuds, sélectionnez la totalité de la grille ou d'un site et accédez à l'onglet stockage. Dans le graphique stockage utilisé - métadonnées d'objet, recherchez une période où la ligne est assez stable. Positionnez le curseur de votre souris sur le graphique pour estimer la quantité de stockage de métadonnées consommée chaque jour Vous pouvez collecter ces informations pour l'intégralité du système ou pour un data Center spécifique.
Vitesse des opérations S3/Swift	Opérations/seconde	Sur le tableau de bord Grid Manager, sélectionnez **Performance** > **S3 Operations** ou **Performance** > **Swift Operations**. Pour afficher les taux d'entrée et de récupération et les nombres pour un site ou un nœud spécifique, sélectionnez **NODES** > ***site ou nœud de stockage*** > **objets**. Placez le curseur sur le graphique Ingest and Retrieve pour S3 ou Swift.
Échec des opérations S3/Swift	Exploitation	Sélectionnez **SUPPORT** > **Outils** > **topologie de grille**. Dans l'onglet Présentation de la section opérations d'API, affichez la valeur des opérations S3 - FAILED ou opérations Swift - FAILED.

Propriété	Valeur	Comment obtenir
Évaluation des règles ILM	Objets/seconde	Dans la page noeuds, sélectionnez ***grid*** > **ILM**. Dans le graphique ILM Queue, recherchez une période où la ligne est assez stable. Placez votre curseur sur le graphique pour estimer la valeur de référence du **taux d'évaluation** pour votre système.
Taux d'analyse ILM	Objets/seconde	Sélectionnez **NODES** > ***grid*** > **ILM**. Dans le graphique ILM Queue, recherchez une période où la ligne est assez stable. Placez le curseur sur le graphique pour estimer la valeur de référence de **Scan Rate** pour votre système.
Objets mis en file d'attente à partir des opérations client	Objets/seconde	Sélectionnez **NODES** > ***grid*** > **ILM**. Dans le graphique ILM Queue, recherchez une période où la ligne est assez stable. Placez votre curseur sur le graphique pour estimer la valeur de base des **objets mis en file d'attente (à partir des opérations client)** pour votre système.
Latence moyenne des requêtes	Millisecondes	Sélectionnez **NODES** > ***Storage Node*** > **Objects**. Dans le tableau requêtes, affichez la valeur de la latence moyenne.

Analysez les données

Utilisez les informations que vous recueillez pour déterminer la cause du problème et les solutions potentielles.

L'analyse dépend du problème, mais en général :

- Localiser les points de défaillance et les goulets d'étranglement à l'aide des alarmes.
- Reconstruire l'historique des problèmes à l'aide de l'historique des alarmes et des graphiques.
- Utiliser les tableaux pour rechercher des anomalies et comparer la situation du problème avec le fonctionnement normal.

Liste de contrôle des informations de réaffectation

Si vous ne parvenez pas à résoudre le problème par vous-même, contactez le support technique. Avant de contacter le support technique, collectez les informations du tableau ci-dessous pour faciliter la résolution de votre problème.

✔	Élément	Remarques
	Énoncé du problème	Quels sont les symptômes du problème ? Quand le problème a-t-il démarré ? Cela se produit-il de manière cohérente ou intermittente ? Si elle est intermittente, à quelle heure s'est-elle produite ? Définissez le problème
	Évaluation de l'impact	Quelle est la gravité du problème ? Quel est l'impact sur l'application client ? • Le client a-t-il déjà été connecté avec succès ? • Le client est-il en mesure d'ingérer, de récupérer et de supprimer des données ?
	ID du système StorageGRID	Sélectionnez **MAINTENANCE** > **système** > **Licence**. L'ID système StorageGRID s'affiche dans le cadre de la licence actuelle.
	Version logicielle	Dans la partie supérieure du Gestionnaire de grille, sélectionnez l'icône d'aide et sélectionnez **About** pour afficher la version StorageGRID.
	Personnalisation	Résumez le mode de configuration de votre système StorageGRID. Par exemple, énumérez les éléments suivants : • La grille utilise-t-elle la compression du stockage, le chiffrement du stockage ou la conformité ? • ILM effectue-t-il des objets répliqués ou soumis à un code d'effacement ? La ILM permet-elle la redondance des sites ? Les règles ILM utilisent-elles des comportements d'ingestion équilibrés, stricts ou Double validation ?
	Fichiers journaux et données système	Collecte des fichiers journaux et des données système pour votre système. Sélectionnez **SUPPORT** > **Outils** > **journaux**. Vous pouvez collecter les journaux pour toute la grille ou pour certains nœuds. Si vous ne recueillez des journaux que pour les nœuds sélectionnés, veillez à inclure au moins un nœud de stockage disposant du service ADC. (Les trois premiers nœuds de stockage d'un site incluent le service ADC.) "Collecte de fichiers journaux et de données système"

✔	Élément	Remarques
	Informations de base	Collectez les informations de base relatives aux opérations d'entrée, aux opérations de récupération et à la consommation du stockage. Établir les lignes de base
	Chronologie des modifications récentes	Créez un calendrier qui résume les modifications récentes apportées au système ou à son environnement. Créer un calendrier des modifications récentes
	Historique des efforts déployés pour diagnostiquer le problème	Si vous avez pris des mesures pour diagnostiquer ou résoudre vous-même le problème, assurez-vous d'enregistrer les mesures que vous avez prises et les résultats obtenus.

Résoudre les problèmes liés au stockage et aux objets

Confirmer l'emplacement des données d'objet

Selon le problème, vous pouvez vouloir le faire "confirmez l'emplacement de stockage des données d'objet". Par exemple, vous pouvez vérifier que la règle ILM fonctionne comme prévu et que les données d'objet sont stockées à l'emplacement prévu.

Avant de commencer

- Vous devez disposer d'un identifiant d'objet, qui peut être l'un des suivants :
  - **UUID** : identifiant unique universel de l'objet. Saisissez l'UUID en majuscules.
  - **CBID** : identifiant unique de l'objet dans StorageGRID . Vous pouvez obtenir le CBID d'un objet à partir du journal d'audit. Saisissez le CBID en majuscules.
  - **S3 bucket et clé d'objet** : lorsqu'un objet est ingéré via le "Interface S3", l'application client utilise une combinaison de clé de compartiment et d'objet pour stocker et identifier l'objet.
  - **Nom du conteneur et de l'objet Swift** : lorsqu'un objet est ingéré via le "Interface Swift", l'application client utilise une combinaison de nom de conteneur et d'objet pour stocker et identifier l'objet.

Étapes

1. Sélectionnez **ILM** > **Object metadata Lookup**.
2. Saisissez l'identifiant de l'objet dans le champ **Identificateur**.

   Vous pouvez entrer un UUID, un CBID, un compartiment S3/une clé-objet ou un nom-objet/conteneur Swift.

3. Si vous souhaitez rechercher une version spécifique de l'objet, saisissez l'ID de version (facultatif).

4. Sélectionnez **rechercher**.

   Le "résultats de la recherche de métadonnées d'objet" apparaît. Cette page répertorie les types d'informations suivants :

   - Les métadonnées système, y compris l'ID d'objet (UUID), l'ID de version (facultatif), le nom de l'objet, le nom du conteneur, le nom ou l'ID du compte de locataire, la taille logique de l'objet, la date et l'heure de la première création de l'objet, ainsi que la date et l'heure de la dernière modification de l'objet.
   - Toutes les paires de clé-valeur de métadonnées utilisateur personnalisées associées à l'objet.
   - Pour les objets S3, toutes les paires de clé-valeur de balise d'objet associées à l'objet.
   - Pour les copies d'objet répliquées, emplacement de stockage actuel de chaque copie.
   - Pour les copies d'objets avec code d'effacement, l'emplacement de stockage actuel de chaque fragment.
   - Pour les copies d'objet dans Cloud Storage Pool, l'emplacement de l'objet, notamment le nom du compartiment externe et l'identifiant unique de l'objet.
   - Pour les objets segmentés et les objets multisegments, une liste de segments d'objet, y compris les identificateurs de segments et la taille des données. Pour les objets de plus de 100 segments, seuls les 100 premiers segments sont affichés.
   - Toutes les métadonnées d'objet dans le format de stockage interne non traité. Ces métadonnées brutes incluent les métadonnées du système interne qui ne sont pas garanties de la version à la version.

     L'exemple suivant présente les résultats de la recherche de métadonnées d'objet pour un objet de test S3 stocké sous forme de deux copies répliquées.

System Metadata

Object ID	A12E96FF-B13F-4905-9E9E-45373F6E7DA8
Name	testobject
Container	source
Account	t-1582139188
Size	5.24 MB
Creation Time	2020-02-19 12:15:59 PST
Modified Time	2020-02-19 12:15:59 PST

Replicated Copies

Node	Disk Path
99-97	/var/local/rangedb/2/p/06/0B/00nM8H$|TFbnQQ}|CV2E
99-99	/var/local/rangedb/1/p/12/0A/00nM8H$|TFboW28|CXG%

Raw Metadata


```
{
    "TYPE": "CTNT",
    "CHND": "A12E96FF-B13F-4905-9E9E-45373F6E7DA8",
    "NAME": "testobject",
    "CBID": "0x8823DE7EC7C10416",
    "PHND": "FEA0AE51-534A-11EA-9FCD-31FF00C36D56",
    "PPTH": "source",
    "META": {
        "BASE": {
            "PAWS": "2",
```


Défaillances de stockage d'objets (volume de stockage)

Le stockage sous-jacent d'un nœud de stockage est divisé en magasins d'objets. Les magasins d'objets sont également appelés volumes de stockage.

Vous pouvez afficher les informations de magasin d'objets pour chaque nœud de stockage. Les magasins d'objets sont affichés en bas de la page **NOEUDS** > ***Storage Node*** > **Storage**.

Disk devices

Name	World Wide Name	I/O load	Read rate	Write rate
sdc(8:16,sdb)	N/A	0.05%	0 bytes/s	4 KB/s
sde(8:48,sdd)	N/A	0.00%	0 bytes/s	82 bytes/s
sdf(8:64,sde)	N/A	0.00%	0 bytes/s	82 bytes/s
sdg(8:80,sdf)	N/A	0.00%	0 bytes/s	82 bytes/s
sdd(8:32,sdc)	N/A	0.00%	0 bytes/s	82 bytes/s
croot(8:1,sda1)	N/A	0.04%	0 bytes/s	4 KB/s
cvloc(8:2,sda2)	N/A	0.95%	0 bytes/s	52 KB/s

Volumes

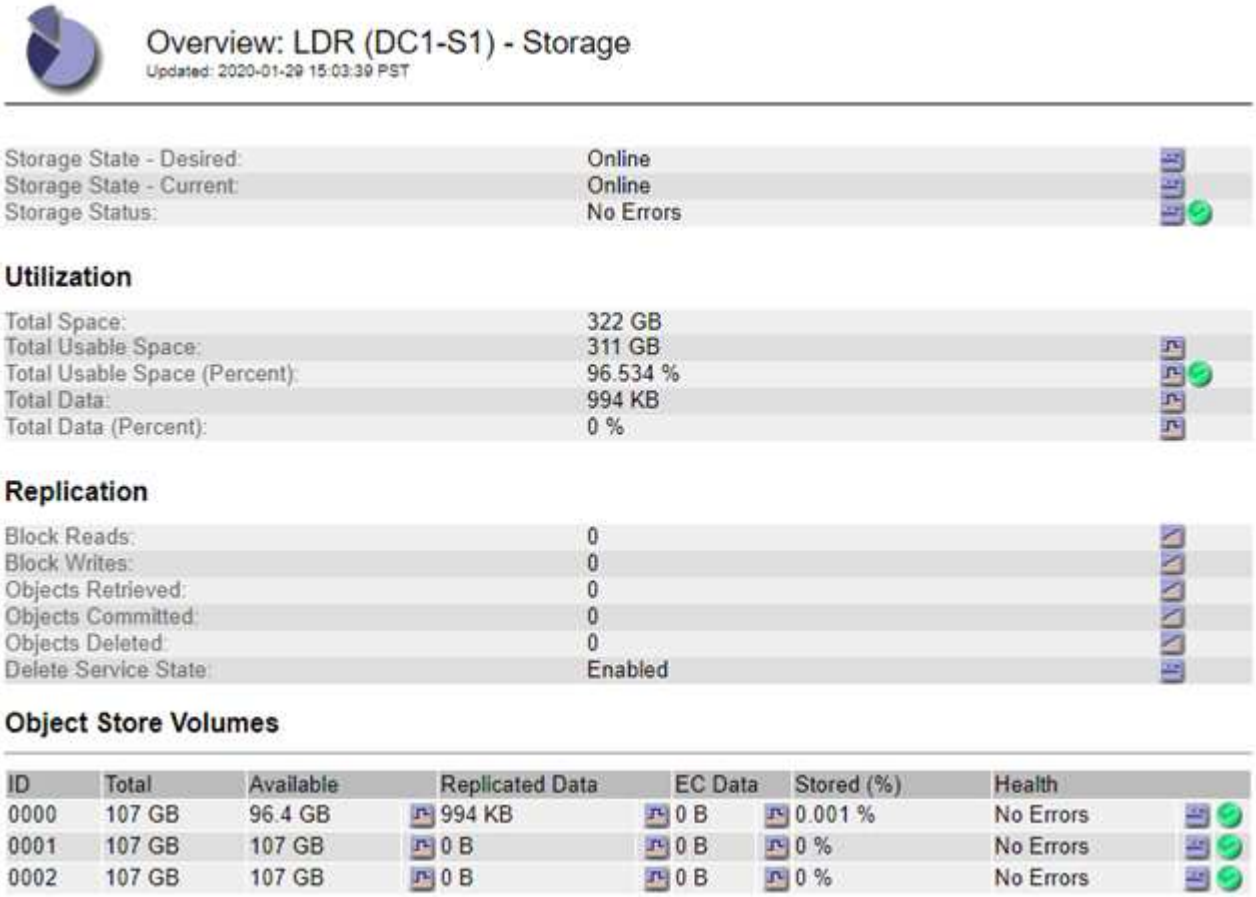
Mount point	Device	Status	Size	Available	Write cache status
/	croot	Online	21.00 GB	14.73 GB	Unknown
/var/local	cvloc	Online	85.86 GB	80.94 GB	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.17 GB	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/2	sde	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/3	sdf	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/4	sdg	Online	107.32 GB	107.18 GB	Enabled

Object stores

ID	Size	Available	Replicated data	EC data	Object data (%)	Health
0000	107.32 GB	96.44 GB	1.55 MB	0 bytes	0.00%	No Errors
0001	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0002	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0003	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0004	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors

Pour en savoir plus "Détails sur chaque nœud de stockage", procédez comme suit :

1. Sélectionnez **SUPPORT** > **Outils** > **topologie de grille**.
2. Sélectionnez ***site*** > ***Storage Node*** > **LDR** > **Storage** > **Présentation** > **main**.



Selon la nature de la défaillance, des défaillances liées à un volume de stockage peuvent se refléter dans une alarme indiquant l'état du stockage ou l'état de santé d'un magasin d'objets. En cas de défaillance d'un volume de stockage, réparez le volume de stockage défectueux pour restaurer le nœud de stockage à son plein fonctionnement dès que possible. Si nécessaire, vous pouvez accéder à l'onglet **Configuration** et "Placez le nœud de stockage en lecture seule" Afin que le système StorageGRID puisse l'utiliser pour la récupération des données tout en vous préparant à une récupération complète du serveur.

Vérifiez l'intégrité de l'objet

Le système StorageGRID vérifie l'intégrité des données d'objet sur les nœuds de stockage, en vérifiant la présence d'objets corrompus et manquants.

Il existe deux processus de vérification : la vérification des antécédents et la vérification de l'existence des objets (anciennement appelée vérification de premier plan). Elles travaillent ensemble pour assurer l'intégrité des données. La vérification en arrière-plan s'exécute automatiquement et vérifie en continu l'exactitude des données d'objet. La vérification de l'existence d'un objet peut être déclenchée par un utilisateur pour vérifier plus rapidement l'existence (mais pas l'exactitude) d'objets.

Qu'est-ce que la vérification des antécédents ?

Le processus de vérification en arrière-plan vérifie automatiquement et en continu les nœuds de stockage pour

détecter des copies corrompues de données d'objet et tente automatiquement de résoudre les problèmes qu'il trouve.

La vérification en arrière-plan vérifie l'intégrité des objets répliqués et des objets avec code d'effacement, comme suit :

- **Objets répliqués** : si le processus de vérification en arrière-plan trouve un objet répliqué corrompu, la copie corrompue est supprimée de son emplacement et mise en quarantaine ailleurs sur le noeud de stockage. Une nouvelle copie non corrompue est ensuite générée et placée pour satisfaire la politique ILM active. Il se peut que la nouvelle copie ne soit pas placée sur le nœud de stockage utilisé pour la copie d'origine.

> Les données d'objet corrompues sont mises en quarantaine au lieu d'être supprimées du système, de sorte qu'elles soient toujours accessibles. Pour plus d'informations sur l'accès aux données d'objet en quarantaine, contactez le support technique.

- **Objets avec code d'effacement** : si le processus de vérification en arrière-plan détecte qu'un fragment d'un objet avec code d'effacement est corrompu, StorageGRID tente automatiquement de reconstruire le fragment manquant en place sur le même nœud de stockage, en utilisant les données restantes et les fragments de parité. Si le fragment corrompu ne peut pas être reconstruit, une tentative est faite pour extraire une autre copie de l'objet. Lorsque la récupération réussit, une évaluation du ILM est effectuée pour créer une copie de remplacement de l'objet avec code d'effacement.

  Le processus de vérification en arrière-plan vérifie uniquement les objets sur les nœuds de stockage. Elle ne vérifie pas les objets sur les nœuds d'archivage ou dans un pool de stockage cloud. Les objets doivent être âgés de plus de quatre jours pour être admissibles à la vérification des antécédents.

La vérification des antécédents s'exécute à un taux continu conçu pour ne pas interférer avec les activités ordinaires du système. Impossible d'arrêter la vérification en arrière-plan. Toutefois, vous pouvez augmenter le taux de vérification en arrière-plan pour vérifier plus rapidement le contenu d'un nœud de stockage si vous soupçonnez un problème.

Alertes et alarmes (anciennes) liées à la vérification des antécédents

Si le système détecte un objet corrompu qu'il ne peut pas corriger automatiquement (parce que la corruption empêche l'objet d'être identifié), l'alerte **objet corrompu non identifié détecté** est déclenchée.

Si la vérification en arrière-plan ne peut pas remplacer un objet corrompu car il ne peut pas localiser une autre copie, l'alerte **objets perdus** est déclenchée.

Modifier le taux de vérification des antécédents

Vous pouvez modifier la vitesse à laquelle la vérification en arrière-plan vérifie les données d'objet répliquées sur un nœud de stockage si vous avez des problèmes d'intégrité des données.

Avant de commencer

- Vous devez être connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous devez disposer d'autorisations d'accès spécifiques.

Description de la tâche

Vous pouvez modifier le taux de vérification pour la vérification en arrière-plan sur un nœud de stockage :

- Adaptatif : paramètre par défaut. La tâche est conçue pour vérifier à un maximum de 4 Mo/s ou 10 objets/s

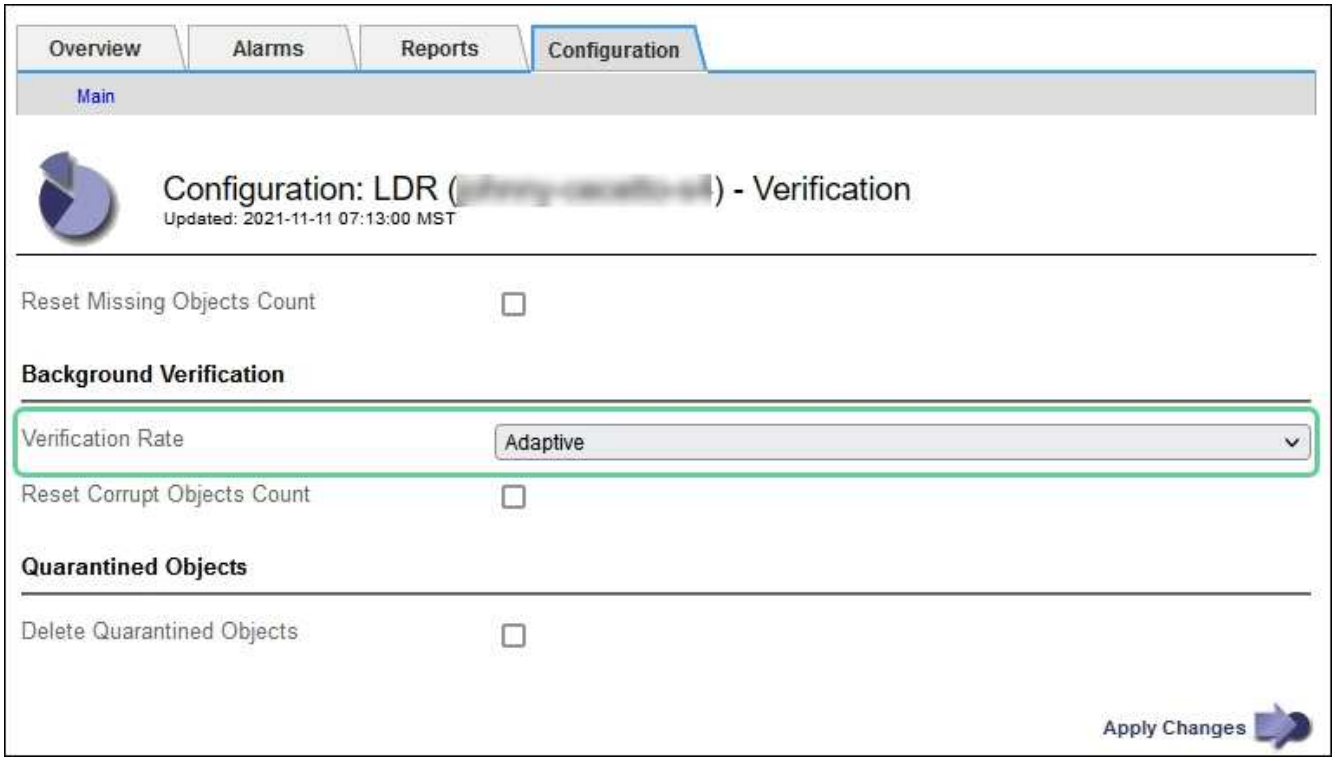
(selon la première limite dépassée).

- Élevé : la vérification du stockage s'effectue rapidement, à une vitesse qui peut ralentir les activités ordinaires des systèmes.

Utilisez le taux de vérification élevé uniquement si vous soupçonnez qu'une erreur matérielle ou logicielle pourrait avoir des données d'objet corrompues. Une fois la vérification de l'arrière-plan de priorité élevée terminée, le taux de vérification se réinitialise automatiquement sur Adaptive.

Étapes

1. Sélectionnez **SUPPORT** > **Outils** > **topologie de grille**.
2. Sélectionnez ***Storage Node*** > **LDR** > **Verification**.
3. Sélectionnez **Configuration** > **main**.
4. Accédez à **LDR** > **Verification** > **Configuration** > **main**.
5. Sous Vérification de l'arrière-plan, sélectionnez **taux de vérification** > **taux élevé** ou **taux de vérification** > **adaptatif**.



Le réglage du taux de vérification sur élevé déclenche l'alarme VPRI (taux de vérification) héritée au niveau des notifications.

6. Cliquez sur **appliquer les modifications**.
7. Surveiller les résultats de la vérification en arrière-plan des objets répliqués.
   a. Accédez à **NOEUDS** > ***Storage Node*** > **objets**.
   b. Dans la section Vérification, surveillez les valeurs de **objets corrompus** et **objets corrompus non identifiés**.

      Si la vérification en arrière-plan trouve des données d'objet répliqué corrompues, la mesure **objets corrompus** est incrémentée et StorageGRID tente d'extraire l'identificateur d'objet des données, comme suit :

- Si l'identifiant d'objet peut être extrait, StorageGRID crée automatiquement une nouvelle copie des données de l'objet. La nouvelle copie peut être effectuée à tout emplacement du système StorageGRID conformément à la politique ILM active.
- Si l'identifiant de l'objet ne peut pas être extrait (car il a été corrompu), la mesure **objets corrompus non identifiés** est incrémentée et l'alerte **objet corrompu non identifié détecté** est déclenchée.

c. Si des données d'objet répliqué corrompues sont trouvées, contactez le support technique pour déterminer la cause première de la corruption.

8. Surveillez les résultats de la vérification en arrière-plan des objets avec code d'effacement.

   Si la vérification en arrière-plan détecte des fragments corrompus de données d'objet codées par effacement, l'attribut fragments corrompus détectés est incrémenté. StorageGRID restaure en reconstruisant le fragment corrompu sur le même nœud de stockage.

   a. Sélectionnez **SUPPORT** > **Outils** > **topologie de grille**.
   b. Sélectionnez ***Storage Node*** > **LDR** > **codage d'effacement**.
   c. Dans le tableau Résultats de la vérification, surveillez l'attribut fragments corrompus détectés (ECCD).

9. Une fois les objets corrompus automatiquement restaurés par le système StorageGRID, réinitialisez le nombre d'objets corrompus.
   a. Sélectionnez **SUPPORT** > **Outils** > **topologie de grille**.
   b. Sélectionnez ***Storage Node*** > **LDR** > **Verification** > **Configuration**.
   c. Sélectionnez **Réinitialiser le nombre d'objets corrompus**.
   d. Cliquez sur **appliquer les modifications**.

10. Si vous êtes sûr que les objets mis en quarantaine ne sont pas nécessaires, vous pouvez les supprimer.

    > Si l'alerte **objets perdus** ou L'alarme héritée PERDUS (objets perdus) a été déclenchée, le support technique peut vouloir accéder aux objets mis en quarantaine pour aider à déboguer le problème sous-jacent ou à tenter la récupération des données.

    a. Sélectionnez **SUPPORT** > **Outils** > **topologie de grille**.
    b. Sélectionnez ***Storage Node*** > **LDR** > **Verification** > **Configuration**.
    c. Sélectionnez **Supprimer les objets en quarantaine**.
    d. Sélectionnez **appliquer les modifications**.

Qu'est-ce que la vérification de l'existence d'objet ?

Le contrôle d'existence d'objet vérifie si toutes les copies répliquées attendues d'objets et de fragments avec code d'effacement existent sur un nœud de stockage. La vérification de l'existence des objets ne vérifie pas les données de l'objet lui-même (la vérification en arrière-plan le fait) ; elle permet plutôt de vérifier l'intégrité des périphériques de stockage, en particulier si un problème matériel récent pouvait affecter l'intégrité des données.

Contrairement à la vérification de l'arrière-plan, qui se produit automatiquement, vous devez démarrer manuellement un travail de vérification de l'existence d'un objet.

Le contrôle d'existence des objets lit les métadonnées de chaque objet stocké dans StorageGRID et vérifie l'existence de copies d'objet répliquées et de fragments d'objet avec code d'effacement. Les données manquantes sont traitées comme suit :

- **Copies répliquées** : si une copie des données d'objet répliqué est manquante, StorageGRID tente automatiquement de remplacer la copie d'une autre copie stockée dans le système. Le nœud de stockage exécute une copie existante via une évaluation ILM. Elle détermine que la politique ILM actuelle n'est plus respectée pour cet objet, car une autre copie est manquante. Une nouvelle copie est générée et placée pour satisfaire à la politique ILM active du système. Cette nouvelle copie peut ne pas être placée au même endroit où la copie manquante a été stockée.
- **Fragments codés par effacement** : si un fragment d'un objet codé par effacement est manquant, StorageGRID tente automatiquement de reconstruire le fragment manquant sur le même nœud de stockage en utilisant les fragments restants. Si le fragment manquant ne peut pas être reconstruit (en raison de la perte d'un trop grand nombre de fragments), ILM tente de trouver une autre copie de l'objet, qu'il peut utiliser pour générer un nouveau fragment avec code d'effacement.

Exécutez la vérification de l'existence d'objet

Vous créez et exécutez un travail de vérification de l'existence d'un objet à la fois. Lorsque vous créez un travail, vous sélectionnez les nœuds de stockage et les volumes à vérifier. Vous sélectionnez également le contrôle de cohérence du travail.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous disposez de l'autorisation Maintenance ou accès racine.
- Vous avez vérifié que les nœuds de stockage à vérifier sont en ligne. Sélectionnez **NOEUDS** pour afficher la table des noeuds. Assurez-vous qu'aucune icône d'alerte n'apparaît en regard du nom du nœud pour les nœuds que vous souhaitez vérifier.
- Vous avez vérifié que les procédures suivantes sont **non** exécutées sur les nœuds que vous voulez vérifier :
  - Extension de la grille pour ajouter un nœud de stockage
  - Désaffectation du nœud de stockage
  - Restauration d'un volume de stockage défaillant
  - Récupération d'un nœud de stockage avec un lecteur système défaillant
  - Rééquilibrage EC
  - Clone du nœud d'appliance

Le contrôle d'existence d'objet ne fournit pas d'informations utiles pendant que ces procédures sont en cours.

Description de la tâche

L'exécution d'une tâche de vérification de l'existence d'un objet peut prendre plusieurs jours ou plusieurs semaines, selon le nombre d'objets de la grille, les nœuds de stockage et les volumes sélectionnés et le contrôle de cohérence sélectionné. Vous ne pouvez exécuter qu'une seule tâche à la fois, mais vous pouvez sélectionner plusieurs nœuds de stockage et volumes en même temps.

Étapes

1. Sélectionnez **MAINTENANCE** > **tâches** > **Vérification d'existence d'objet**.
2. Sélectionnez **Créer un travail**. L'assistant création d'un objet Vérification de l'existence s'affiche.
3. Sélectionnez les nœuds contenant les volumes à vérifier. Pour sélectionner tous les nœuds en ligne, cochez la case **Node name** dans l'en-tête de colonne.

   Vous pouvez effectuer vos recherches par nom de nœud ou site.

Vous ne pouvez pas sélectionner de nœuds qui ne sont pas connectés à la grille.

4. Sélectionnez **Continuer**.
5. Sélectionnez un ou plusieurs volumes pour chaque nœud de la liste. Vous pouvez rechercher des volumes à l'aide du numéro du volume de stockage ou du nom du nœud.

   Pour sélectionner tous les volumes pour chaque nœud sélectionné, cochez la case **Storage volume** dans l'en-tête de colonne.

6. Sélectionnez **Continuer**.
7. Sélectionnez le contrôle de cohérence du travail.

   Le contrôle de cohérence détermine le nombre de copies de métadonnées d'objet utilisées pour la vérification de l'existence de l'objet.

   - **Site fort** : deux copies de métadonnées sur un seul site.
   - **Fort-global**: Deux copies de métadonnées à chaque site.
   - **Tout** (par défaut) : les trois copies des métadonnées de chaque site.

     Pour plus d'informations sur le contrôle de cohérence, reportez-vous aux descriptions de l'assistant.

8. Sélectionnez **Continuer**.
9. Vérifiez et vérifiez vos sélections. Vous pouvez sélectionner **Précédent** pour passer à l'étape précédente de l'assistant afin de mettre à jour vos sélections.

   Un travail de vérification de l'existence d'un objet est généré et exécuté jusqu'à ce que l'un des événements suivants se produise :

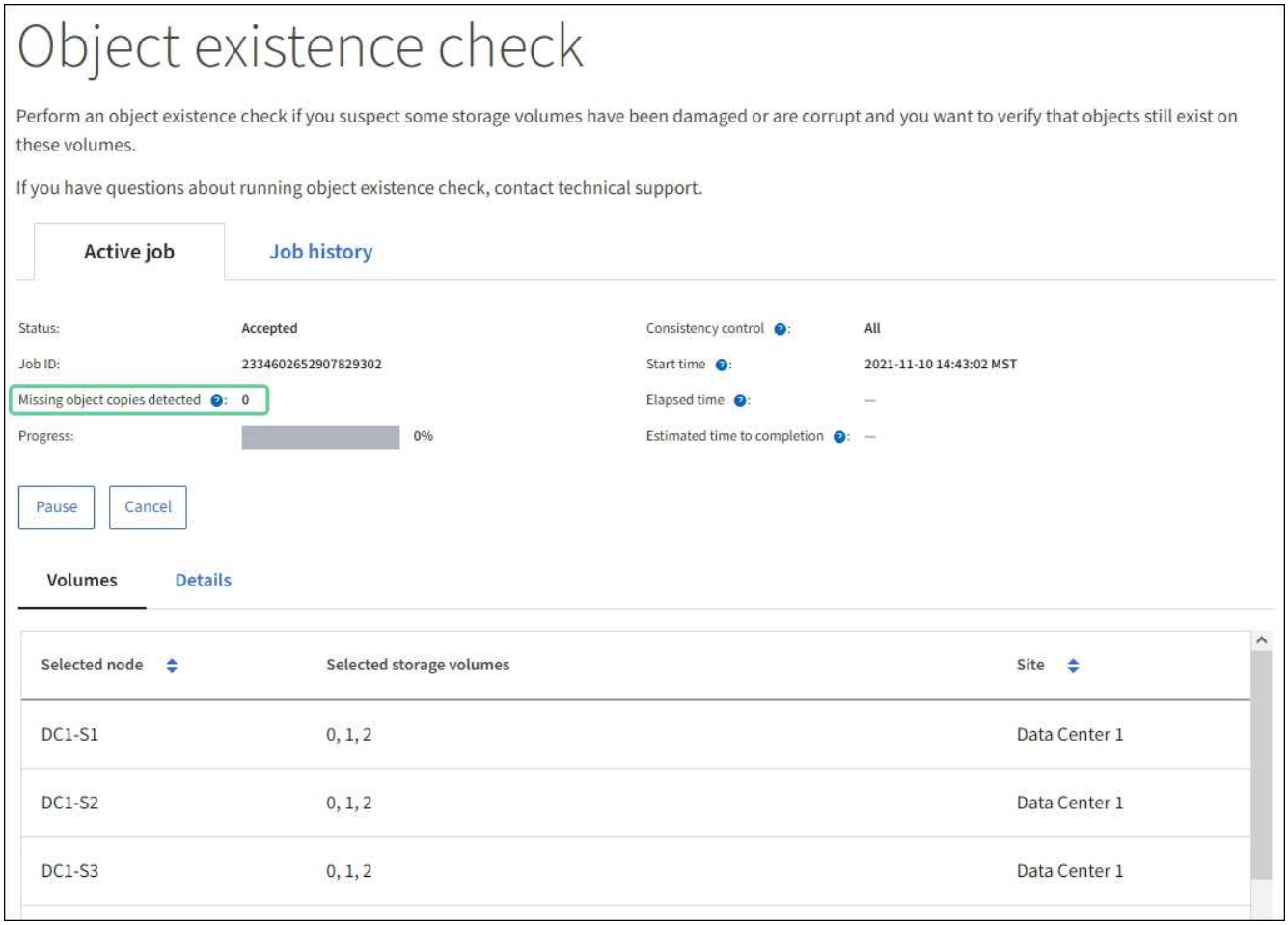
   - Le travail se termine.
   - Vous mettez en pause ou annulez le travail. Vous pouvez reprendre un travail que vous avez interrompu, mais vous ne pouvez pas reprendre un travail que vous avez annulé.
   - Le travail se bloque. L'alerte * Vérification de l'existence de l'objet a calé* est déclenchée. Suivez les actions correctives spécifiées pour l'alerte.
   - Le travail échoue. L'alerte **échec de la vérification de l'existence de l'objet** est déclenchée. Suivez les actions correctives spécifiées pour l'alerte.
   - Un message "Service indisponible" ou "erreur de serveur interne" s'affiche. Au bout d'une minute, actualisez la page pour continuer à surveiller le travail.

   > Si nécessaire, vous pouvez naviguer hors de la page de vérification de l'existence d'un objet et revenir à la page de suivi du travail.

10. Pendant l'exécution du travail, affichez l'onglet **travail actif** et notez la valeur des copies d'objet manquantes détectées.

    Cette valeur représente le nombre total de copies manquantes d'objets répliqués et d'objets avec code d'effacement avec un ou plusieurs fragments manquants.

    Si le nombre de copies d'objet manquantes détectées est supérieur à 100, il peut y avoir un problème avec le stockage du nœud de stockage.



11. Une fois le travail terminé, prenez les mesures supplémentaires requises :
    - Si les copies d'objet manquantes détectées sont nulles, aucun problème n'a été trouvé. Aucune action n'est requise.
    - Si les copies d'objet manquantes détectées sont supérieures à zéro et que l'alerte **objets perdus** n'a pas été déclenchée, toutes les copies manquantes ont été réparées par le système. Vérifiez que tout problème matériel a été corrigé pour éviter d'endommager ultérieurement les copies d'objet.
    - Si les copies d'objet manquantes détectées sont supérieures à zéro et que l'alerte **objets perdus** a été déclenchée, l'intégrité des données pourrait être affectée. Contactez l'assistance technique.
    - Vous pouvez étudier les copies d'objet perdues en utilisant grep pour extraire les messages d'audit LLST : `grep LLST audit_file_name`.

      Cette procédure est similaire à celle pour "analyse des objets perdus", bien que pour les copies d'objet que vous recherchez `LLST` au lieu de `OLST`.

12. Si vous avez sélectionné le contrôle de cohérence fort site ou fort global pour le travail, attendez environ trois semaines pour la cohérence des métadonnées, puis relancez le travail sur les mêmes volumes.

    Lorsque StorageGRID a eu le temps d'assurer la cohérence des métadonnées pour les nœuds et les volumes inclus dans le travail, réexécuter ce travail peut effacer les copies d'objet manquantes, ou faire vérifier d'autres copies d'objet si elles ne sont pas prises en compte.

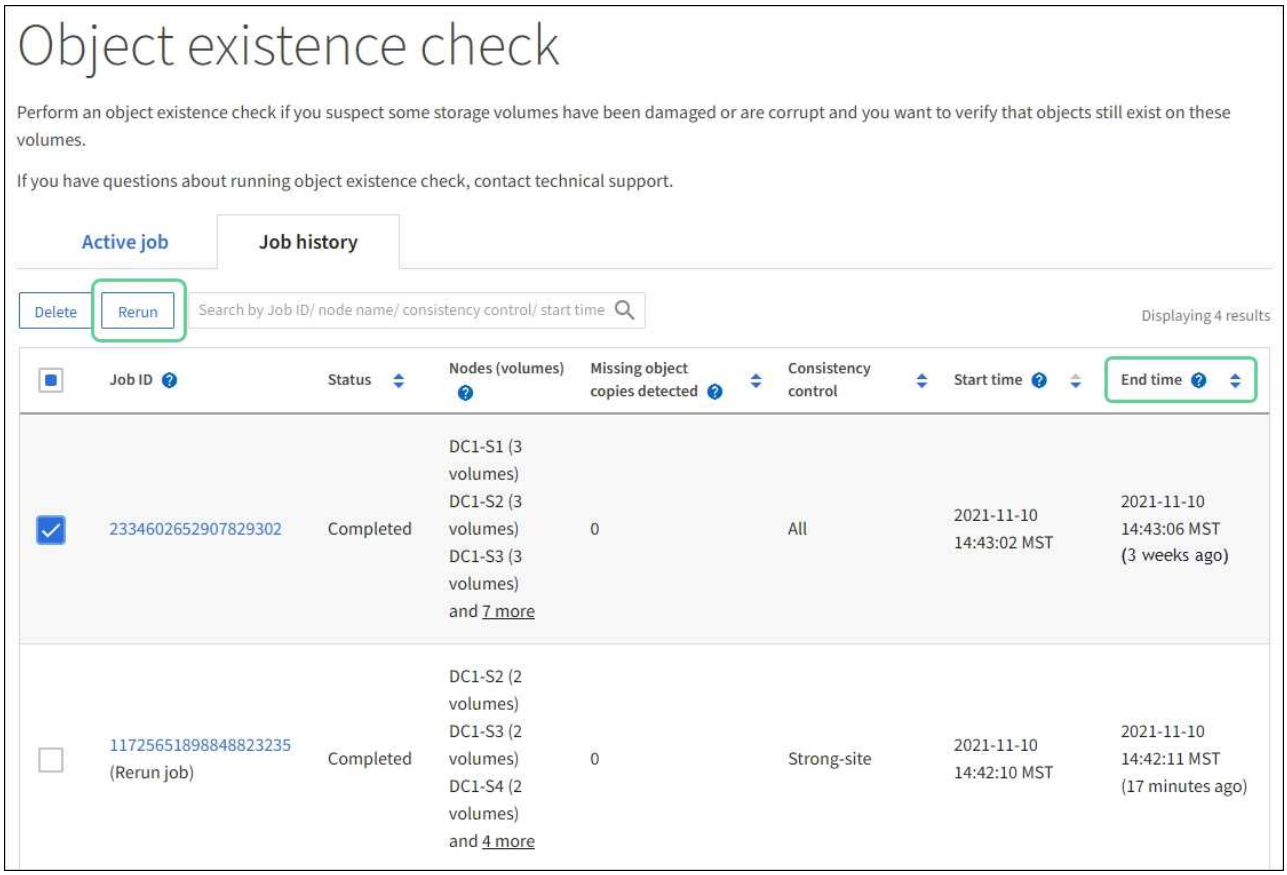
    a. Sélectionnez **MAINTENANCE** > **Vérification de l'existence d'objet** > **Historique du travail**.

    b. Déterminez les travaux prêts à être réexécutés :

i. Consultez la colonne **end Time** pour déterminer les tâches qui ont été exécutées il y a plus de trois semaines.

ii. Pour ces travaux, scannez la colonne de contrôle de cohérence pour obtenir un site fort ou fort-global.

c. Cochez la case de chaque travail à repasser, puis sélectionnez **repassage**.



d. Dans l'assistant repassage de travaux, vérifiez les nœuds et volumes sélectionnés et le contrôle de cohérence.

e. Lorsque vous êtes prêt à réexécuter les travaux, sélectionnez **repassage**.

L'onglet travail actif s'affiche. Tous les travaux que vous avez sélectionnés sont réexécutés comme un travail au niveau d'un contrôle de cohérence du site fort. Un champ **travaux connexes** de la section Détails répertorie les ID des travaux d'origine.

Une fois que vous avez terminé

Si vous avez toujours des problèmes d'intégrité des données, accédez à **SUPPORT** > **Outils** > **topologie de grille** > ***site*** > ***Storage Node*** > **LDR** > **Verification** > **Configuration** > **main** et augmentez le taux de vérification en arrière-plan. La vérification en arrière-plan vérifie l'exactitude de toutes les données d'objet stockées et répare tout problème détecté. Trouver et réparer les problèmes le plus rapidement possible réduit le risque de perte de données.

Dépannez l'alerte de taille d'objet PUT S3 trop grande

L'alerte S3 PUT Object size too large est déclenchée si un locataire tente une opération PUT Object en plusieurs parties qui dépasse la taille limite S3 de 5 Gio.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous avez "autorisations d'accès spécifiques".

Déterminez les locataires qui utilisent des objets supérieurs à 5 Gio. Vous pouvez donc les informer.

Étapes

1. Accédez à **CONFIGURATION** > **surveillance** > **Audit et serveur syslog**.
2. Si les écritures client sont normales, accédez au journal d'audit :

   a. Entrez `ssh admin@primary_Admin_Node_IP`

   b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

   c. Entrez la commande suivante pour passer à la racine : `su -`

   d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

   Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

   e. Entrez `cd /var/local/audit/export`

   f. Identifiez les locataires qui utilisent des objets de plus de 5 Gio.

      i. Entrez `zgrep SPUT * | egrep "CSIZ\(UI64\):[0-9]*[5-9][0-9]{9}"`

      ii. Pour chaque message d'audit dans les résultats, consultez `S3AI` Pour déterminer l'ID de compte de locataire. Utilisez les autres champs du message pour déterminer l'adresse IP utilisée par le client, le compartiment et l'objet :

Code	Description
SAIP	Adresse IP source
S3AI	ID locataire
S3BK	Godet
S3KY	Objet
CSIZ	Taille (octets)

Exemple de résultats du journal d'audit

```
audit.log:2023-01-05T18:47:05.525999
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1672943621106262][TIME(UI64):80431733
3][SAIP(IPAD):"10.96.99.127"][S3AI(CSTR):"93390849266154004343"][SACC(CS
TR):"bhavna"][S3AK(CSTR):"06OX85M40Q90Y280B7YT"][SUSR(CSTR):"urn:sgws:id
entity::93390849266154004343:root"][SBAI(CSTR):"93390849266154004343"][S
BAC(CSTR):"bhavna"][S3BK(CSTR):"test"][S3KY(CSTR):"large-
object"][CBID(UI64):0x077EA25F3B36C69A][UUID(CSTR):"A80219A2-CD1E-466F-
9094-
B9C0FDE2FFA3"][CSIZ(UI64):6040000000][MTME(UI64):1672943621338958][AVER(
UI32):10][ATIM(UI64):1672944425525999][ATYP(FC32):SPUT][ANID(UI32):12220
829][AMID(FC32):S3RQ][ATID(UI64):4333283179807659119]]
```

3. Si les écritures du client ne sont pas normales, utilisez l'ID de locataire de l'alerte pour identifier le locataire :

   a. Accédez à **SUPPORT** > **Outils** > **journaux**. Collectez les journaux d'application du nœud de stockage dans l'alerte. Spécifiez 15 minutes avant et après l'alerte.

   b. Extrayez le fichier et accédez à `bycast.log`:

      ```
      /GID<grid_id>_<time_stamp>/<site_node>/<time_stamp>/grid/bycast.log
      ```

   c. Rechercher dans le journal `method=PUT` et identifier le client dans `clientIP` légale.

      Exemple bycast.log

```
Jan  5 18:33:41 BHAVNAJ-DC1-S1-2-65 ADE: |12220829 1870864574 S3RQ %CEA
2023-01-05T18:33:41.208790| NOTICE   1404 af23cb66b7e3efa5 S3RQ:
EVENT_PROCESS_CREATE - connection=1672943621106262 method=PUT
name=</test/4MiB-0> auth=<V4> clientIP=<10.96.99.127>
```

4. Indiquez aux locataires que la taille maximale de l'objet PUT est de 5 Gio et que vous devez utiliser des téléchargements partitionnés pour les objets supérieurs à 5 Gio.
5. Ignorez l'alerte pendant une semaine si l'application a été modifiée.

Dépanner les données d'objet perdues ou manquantes

Dépannage des données d'objet perdues ou manquantes : présentation

Les objets peuvent être récupérés pour plusieurs raisons, y compris les demandes de lecture provenant d'une application client, les vérifications en arrière-plan des données d'objet répliquées, les réévaluations ILM et la restauration des données d'objet lors de la restauration d'un nœud de stockage.

Le système StorageGRID utilise les informations d'emplacement dans les métadonnées d'un objet pour déterminer l'emplacement à partir duquel vous souhaitez récupérer l'objet. Si une copie de l'objet n'est pas trouvée à l'emplacement prévu, le système tente de récupérer une autre copie de l'objet à partir d'un autre emplacement du système, en supposant que la règle ILM contient une règle permettant de créer au moins

deux copies de l'objet.

Si cette récupération réussit, le système StorageGRID remplace la copie manquante de l'objet. Sinon, l'alerte **objets perdus** est déclenchée comme suit :

- Pour les copies répliquées, si une autre copie ne peut pas être récupérée, l'objet est considéré comme perdu et l'alerte est déclenchée.
- Pour les copies avec code d'effacement, si une copie ne peut pas être récupérée à partir de l'emplacement attendu, l'attribut copies corrompues détectées (ECOR) est incrémenté d'une copie avant qu'une tentative de récupération d'une copie ne soit effectuée à partir d'un autre emplacement. Si aucune autre copie n'est trouvée, l'alerte est déclenchée.

Vous devez examiner immédiatement toutes les alertes **objets perdus** pour déterminer la cause principale de la perte et déterminer si l'objet peut toujours exister dans un nœud hors ligne ou actuellement indisponible, un nœud de stockage ou un nœud d'archivage. Voir "Rechercher les objets perdus".

Dans le cas où les données d'objet sans copie sont perdues, il n'y a pas de solution de récupération. Cependant, vous devez réinitialiser le compteur d'objets perdus pour empêcher les objets perdus connus de masquer les nouveaux objets perdus. Voir "Réinitialiser le nombre d'objets perdus et manquants".

Rechercher les objets perdus

Lorsque l'alerte « Objets perdus » est déclenchée, vous devez enquêter immédiatement. Collectez des informations sur les objets concernés et contactez le support technique.

Avant de commencer

- Vous devez être connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous devez disposer d'autorisations d'accès spécifiques.
- Vous devez avoir le `Passwords.txt` fichier.

Description de la tâche

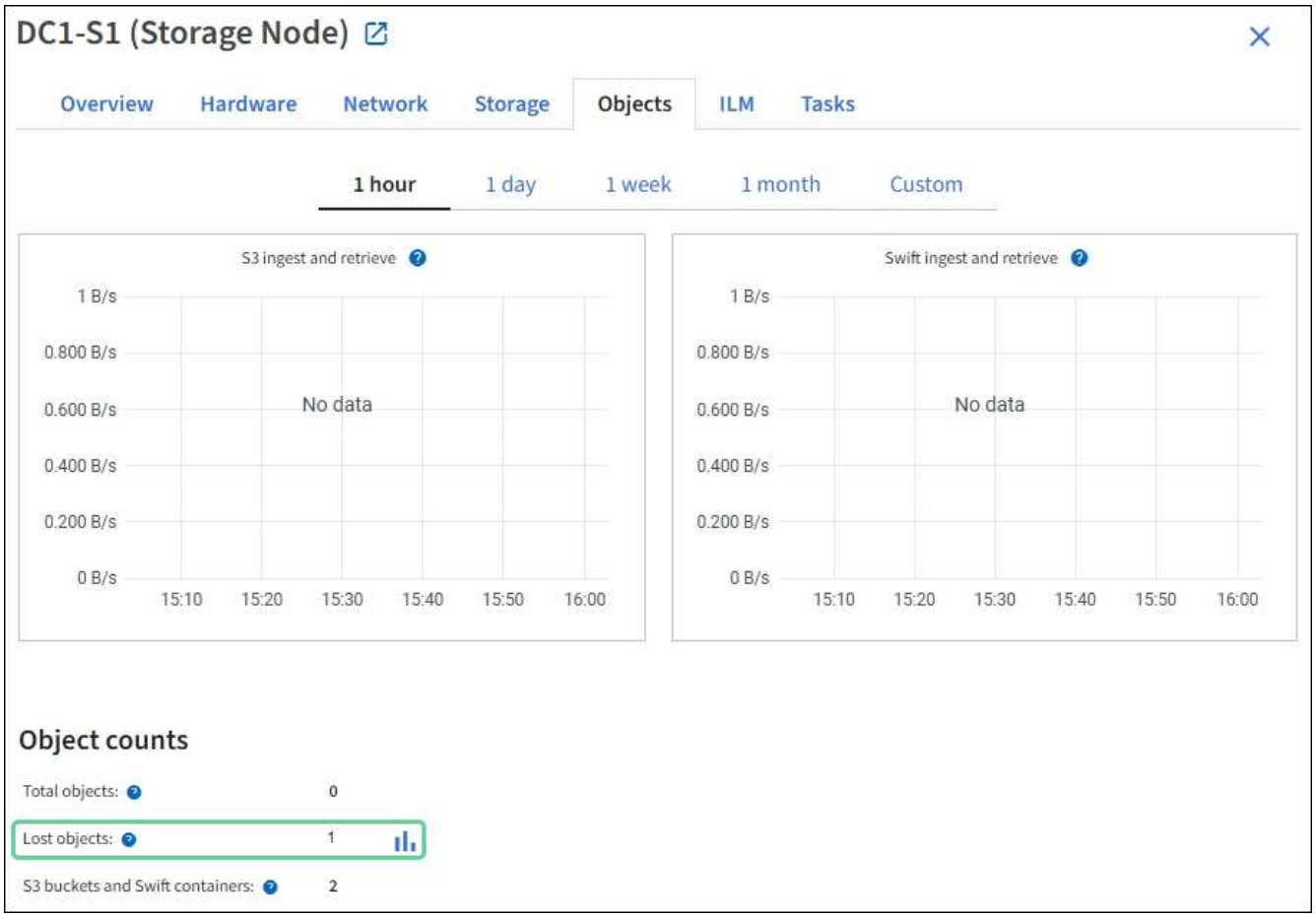
L'alerte **objets perdus** indique que StorageGRID estime qu'il n'y a pas de copie d'un objet dans la grille. Les données ont peut-être été définitivement perdues.

Recherchez immédiatement les alertes relatives à la perte d'objet. Vous devrez peut-être prendre des mesures pour éviter d'autres pertes de données. Dans certains cas, vous pourrez peut-être restaurer un objet perdu si vous prenez une action d'invite.

Étapes

1. Sélectionnez **NOEUDS**.
2. Sélectionnez ***Storage Node*** > **objets**.
3. Vérifiez le nombre d'objets perdus affichés dans le tableau nombres d'objets.

   Ce nombre indique le nombre total d'objets que ce nœud de grille détecte comme manquant dans l'ensemble du système StorageGRID. La valeur est la somme des compteurs d'objets perdus du composant de stockage de données dans les services LDR et DDS.



4. À partir d'un nœud d'administration, "accédez au journal d'audit" Pour déterminer l'identifiant unique (UUID) de l'objet qui a déclenché l'alerte **objets perdus** :
   a. Connectez-vous au nœud grid :
      i. Saisissez la commande suivante : `ssh admin@grid_node_IP`
      ii. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
      iii. Entrez la commande suivante pour passer à la racine : `su -`
      iv. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier. Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.
   b. Accédez au répertoire dans lequel se trouvent les journaux d'audit. Entrez : `cd /var/local/audit/export/`
   c. Utilisez grep pour extraire les messages d'audit objet perdu (OLST). Entrez : `grep OLST audit_file_name`
   d. Notez la valeur UUID incluse dans le message.

```
>Admin: # grep OLST audit.log
2020-02-12T19:18:54.780426
[AUDT:[CBID(UI64):0x38186FE53E3C49A5][UUID(CSTR):926026C4-00A4-449B-
AC72-BCCA72DD1311]
[PATH(CSTR):"source/cats"][NOID(UI32):12288733][VOLI(UI64):3222345986
][RSLT(FC32):NONE][AVER(UI32):10]
[ATIM(UI64):1581535134780426][ATYP(FC32):OLST][ANID(UI32):12448208][A
MID(FC32):ILMX][ATID(UI64):7729403978647354233]]
```

5. Utilisez le `ObjectByUUID` Commande permettant de rechercher l'objet par son identificateur (UUID), puis de déterminer si les données sont à risque.

   a. Telnet vers localhost 1402 pour accéder à la console LDR.

   b. Entrez : `/proc/OBRP/ObjectByUUID UUID_value`

   Dans ce premier exemple, l'objet avec `UUID 926026C4-00A4-449B-AC72-BCCA72DD1311` comporte deux emplacements répertoriés.

```
ade 12448208: /proc/OBRP > ObjectByUUID 926026C4-00A4-449B-AC72-
BCCA72DD1311

{
    "TYPE(Object Type)": "Data object",
    "CHND(Content handle)": "926026C4-00A4-449B-AC72-BCCA72DD1311",
    "NAME": "cats",
    "CBID": "0x38186FE53E3C49A5",
    "PHND(Parent handle, UUID)": "221CABD0-4D9D-11EA-89C3-
ACBB00BB82DD",
    "PPTH(Parent path)": "source",
    "META": {
        "BASE(Protocol metadata)": {
            "PAWS(S3 protocol version)": "2",
            "ACCT(S3 account ID)": "44084621669730638018",
            "*ctp(HTTP content MIME type)": "binary/octet-stream"
        },
        "BYCB(System metadata)": {
            "CSIZ(Plaintext object size)": "5242880",
            "SHSH(Supplementary Plaintext hash)": "MD5D
0xBAC2A2617C1DFF7E959A76731E6EAF5E",
            "BSIZ(Content block size)": "5252084",
            "CVER(Content block version)": "196612",
            "CTME(Object store begin timestamp)": "2020-02-
12T19:16:10.983000",
            "MTME(Object store modified timestamp)": "2020-02-
12T19:16:10.983000",
```

```
            "ITME": "1581534970983000"
        },
        "CMSM": {
            "LATM(Object last access time)": "2020-02-
12T19:16:10.983000"
        },
        "AWS3": {
            "LOCC": "us-east-1"
        }
    },
    "CLCO\(Locations\)": \[
        \{
            "Location Type": "CLDI\(Location online\)",
            "NOID\(Node ID\)": "12448208",
            "VOLI\(Volume ID\)": "3222345473",
            "Object File Path":
"/var/local/rangedb/1/p/17/11/00rH0%DkRt78Ila\#3udu",
            "LTIM\(Location timestamp\)": "2020-02-
12T19:36:17.880569"
        \},
        \{
            "Location Type": "CLDI\(Location online\)",
            "NOID\(Node ID\)": "12288733",
            "VOLI\(Volume ID\)": "3222345984",
            "Object File Path":
"/var/local/rangedb/0/p/19/11/00rH0%DkRt78Rrb\#3s;L",
            "LTIM\(Location timestamp\)": "2020-02-
12T19:36:17.934425"
        }
    ]
}
```

Dans le second exemple, l'objet avec `UUID 926026C4-00A4-449B-AC72-BCCA72DD1311` n'a aucun emplacement répertorié.

```
ade 12448208: / > /proc/OBRP/ObjectByUUID 926026C4-00A4-449B-AC72-
BCCA72DD1311

{
    "TYPE(Object Type)": "Data object",
    "CHND(Content handle)": "926026C4-00A4-449B-AC72-BCCA72DD1311",
    "NAME": "cats",
    "CBID": "0x38186FE53E3C49A5",
    "PHND(Parent handle, UUID)": "221CABD0-4D9D-11EA-89C3-ACBB00BB82DD",
    "PPTH(Parent path)": "source",
    "META": {
        "BASE(Protocol metadata)": {
            "PAWS(S3 protocol version)": "2",
            "ACCT(S3 account ID)": "44084621669730638018",
            "*ctp(HTTP content MIME type)": "binary/octet-stream"
        },
        "BYCB(System metadata)": {
            "CSIZ(Plaintext object size)": "5242880",
            "SHSH(Supplementary Plaintext hash)": "MD5D
0xBAC2A2617C1DFF7E959A76731E6EAF5E",
            "BSIZ(Content block size)": "5252084",
            "CVER(Content block version)": "196612",
            "CTME(Object store begin timestamp)": "2020-02-
12T19:16:10.983000",
            "MTME(Object store modified timestamp)": "2020-02-
12T19:16:10.983000",
            "ITME": "1581534970983000"
        },
        "CMSM": {
            "LATM(Object last access time)": "2020-02-
12T19:16:10.983000"
        },
        "AWS3": {
            "LOCC": "us-east-1"
        }
    }
}
```

a. Examinez le résultat de /proc/OBRP/ObjectByUUID et prenez les mesures appropriées :

Les métadonnées	Conclusion
Aucun objet trouvé ("ERREUR":")	Si l'objet n'est pas trouvé, le message "ERREUR":" est renvoyé. Si l'objet est introuvable, vous pouvez réinitialiser le nombre d'objets perdus* pour effacer l'alerte. L'absence d'objet indique que l'objet a été supprimé intentionnellement.
Emplacements > 0	Si des emplacements sont répertoriés dans la sortie, l'alerte **objets perdus** peut être un faux positif. Vérifiez que les objets existent. Utilisez l'ID de nœud et le chemin du fichier indiqués dans la sortie pour confirmer que le fichier objet se trouve à l'emplacement indiqué. (La procédure pour "recherche d'objets potentiellement perdus" Explique comment utiliser l'ID de nœud pour trouver le nœud de stockage approprié.) Si les objets existent, vous pouvez réinitialiser le nombre d'objets perdus* pour effacer l'alerte.
Emplacements = 0	Si aucun emplacement n'est répertorié dans le résultat, l'objet est potentiellement manquant. Vous pouvez essayer "recherchez et restaurez l'objet" vous pouvez aussi contacter le support technique. L'assistance technique peut vous demander si une procédure de restauration du stockage est en cours. Voir les informations sur "Restauration des données d'objet à l'aide de Grid Manager" et "restauration des données d'objet vers un volume de stockage".

Recherche et restauration d'objets potentiellement perdus

Il est possible de trouver et de restaurer des objets qui ont déclenché une alarme objets perdus (PERDUS) et une alerte **objet perdu** et que vous avez identifié comme potentiellement perdus.

Avant de commencer

- Vous disposez de l'UUID de tout objet perdu, tel qu'identifié dans "Rechercher les objets perdus".
- Vous avez le `Passwords.txt` fichier.

Description de la tâche

Vous pouvez suivre cette procédure pour rechercher les copies répliquées de l'objet perdu ailleurs dans la grille. Dans la plupart des cas, l'objet perdu est introuvable. Toutefois, dans certains cas, vous pouvez trouver et restaurer un objet répliqué perdu si vous prenez une action rapide.

Pour obtenir de l'aide sur cette procédure, contactez le support technique.

Étapes

1. À partir d'un nœud d'administration, recherchez dans les journaux d'audit les emplacements d'objets

possibles :

a. Connectez-vous au nœud grid :

   i. Saisissez la commande suivante : `ssh admin@grid_node_IP`

   ii. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

   iii. Entrez la commande suivante pour passer à la racine : `su -`

   iv. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier. Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

b. Accédez au répertoire dans lequel se trouvent les journaux d'audit : `cd /var/local/audit/export/`

c. Utilisez grep pour extraire le "messages d'audit associés à l'objet potentiellement perdu" et envoyez-les à un fichier de sortie. Entrez : `grep uuid-valueaudit_file_name > output_file_name`

   Par exemple :

```
Admin: # grep 926026C4-00A4-449B-AC72-BCCA72DD1311 audit.log >
messages_about_lost_object.txt
```

d. Utilisez grep pour extraire les messages d'audit emplacement perdu (LLST) de ce fichier de sortie. Entrez : `grep LLST output_file_name`

   Par exemple :

```
Admin: # grep LLST messages_about_lost_objects.txt
```

   Un message d'audit LLST ressemble à cet exemple de message.

```
[AUDT:\[NOID\(UI32\):12448208\][CBIL(UI64):0x38186FE53E3C49A5]
[UUID(CSTR):"926026C4-00A4-449B-AC72-BCCA72DD1311"][LTYP(FC32):CLDI]
[PCLD\(CSTR\):"/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%\#3tN6"\]
[TSRC(FC32):SYST][RSLT(FC32):NONE][AVER(UI32):10][ATIM(UI64):
1581535134379225][ATYP(FC32):LLST][ANID(UI32):12448208][AMID(FC32):CL
SM]
[ATID(UI64):7086871083190743409]]
```

e. Recherchez le champ PCLD et LE champ NOID dans le message LLST.

   Le cas échéant, la valeur de PCLD correspond au chemin complet du disque vers la copie de l'objet répliqué manquante. La valeur de NOID est l'ID de nœud du LDR dans lequel une copie de l'objet peut être trouvée.

Si vous trouvez un emplacement d'objet, vous pourrez peut-être restaurer l'objet.

a. Recherchez le nœud de stockage associé à cet ID de nœud LDR. Dans le Gestionnaire de grille, sélectionnez **SUPPORT** > **Outils** > **topologie de grille**. Sélectionnez ensuite ***Data Center*** > ***Storage***

Node > **LDR**.

L'ID de nœud du service LDR se trouve dans le tableau informations sur le nœud. Vérifiez les informations pour chaque nœud de stockage jusqu'à ce que vous trouviez celui qui héberge ce LDR.

2. Déterminez si l'objet existe sur le nœud de stockage indiqué dans le message d'audit :
   a. Connectez-vous au nœud grid :
      i. Saisissez la commande suivante : `ssh admin@grid_node_IP`
      ii. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
      iii. Entrez la commande suivante pour passer à la racine : `su -`
      iv. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

      Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

   b. Déterminez si le chemin du fichier de l'objet existe.

      Pour le chemin du fichier de l'objet, utilisez la valeur PCLD du message d'audit LLST.

      Par exemple, entrez :

      ```
      ls '/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6'
      ```

      > Placez toujours le chemin d'accès au fichier d'objet entre guillemets simples dans des commandes pour échapper à tout caractère spécial.

      - Si le chemin d'accès à l'objet est introuvable, l'objet est perdu et ne peut pas être restauré à l'aide de cette procédure. Contactez l'assistance technique.
      - Si le chemin d'accès à l'objet est trouvé, passez à l'étape suivante. Vous pouvez essayer de restaurer à nouveau l'objet trouvé dans StorageGRID.

3. Si le chemin d'accès à l'objet a été trouvé, essayez de restaurer l'objet sur StorageGRID :
   a. À partir du même nœud de stockage, modifiez la propriété du fichier objet afin qu'il puisse être géré par StorageGRID. Entrez : `chown ldr-user:bycast 'file_path_of_object'`
   b. Telnet vers localhost 1402 pour accéder à la console LDR. Entrez : `telnet 0 1402`
   c. Entrez : `cd /proc/STOR`
   d. Entrez : `Object_Found 'file_path_of_object'`

      Par exemple, entrez :

      ```
      Object_Found '/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6'
      ```

      Émission du `Object\_Found` commande informe la grille de l'emplacement de l'objet. Il déclenche également la règle ILM active, qui crée des copies supplémentaires, comme spécifié dans la règle.

Si le nœud de stockage sur lequel vous avez trouvé l'objet est hors ligne, vous pouvez le copier sur n'importe quel nœud de stockage en ligne. Placez l'objet dans un répertoire /var/local/rangedb du noeud de stockage en ligne. Ensuite, émettez le `Object\_Found` commande utilisant ce chemin de fichier pour l'objet.

- Si l'objet ne peut pas être restauré, le `Object\_Found` échec de la commande. Contactez l'assistance technique.
- Si l'objet a été restauré avec succès dans StorageGRID, un message de réussite s'affiche. Par exemple :

```
ade 12448208: /proc/STOR > Object_Found
'/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6'

ade 12448208: /proc/STOR > Object found succeeded.
First packet of file was valid. Extracted key: 38186FE53E3C49A5
Renamed '/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6' to
'/var/local/rangedb/1/p/17/11/00rH0%DkRt78Ila#3udu'
```

Passez à l'étape suivante.

4. Si l'objet a été restauré dans StorageGRID, vérifiez que de nouveaux emplacements ont été créés.
   a. Entrez : `cd /proc/OBRP`
   b. Entrez : `ObjectByUUID UUID_value`

   L'exemple suivant montre qu'il existe deux emplacements pour l'objet avec l'UUID 926026C4-00A4-449B-AC72-BCCA72DD1311.

```
ade 12448208: /proc/OBRP > ObjectByUUID 926026C4-00A4-449B-AC72-
BCCA72DD1311

{
    "TYPE(Object Type)": "Data object",
    "CHND(Content handle)": "926026C4-00A4-449B-AC72-BCCA72DD1311",
    "NAME": "cats",
    "CBID": "0x38186FE53E3C49A5",
    "PHND(Parent handle, UUID)": "221CABD0-4D9D-11EA-89C3-ACBB00BB82DD",
    "PPTH(Parent path)": "source",
    "META": {
        "BASE(Protocol metadata)": {
            "PAWS(S3 protocol version)": "2",
            "ACCT(S3 account ID)": "44084621669730638018",
            "*ctp(HTTP content MIME type)": "binary/octet-stream"
        },
        "BYCB(System metadata)": {
            "CSIZ(Plaintext object size)": "5242880",
```

```
            "SHSH(Supplementary Plaintext hash)": "MD5D
0xBAC2A2617C1DFF7E959A76731E6EAF5E",
            "BSIZ(Content block size)": "5252084",
            "CVER(Content block version)": "196612",
            "CTME(Object store begin timestamp)": "2020-02-
12T19:16:10.983000",
            "MTME(Object store modified timestamp)": "2020-02-
12T19:16:10.983000",
            "ITME": "1581534970983000"
        },
        "CMSM": {
            "LATM(Object last access time)": "2020-02-
12T19:16:10.983000"
        },
        "AWS3": {
            "LOCC": "us-east-1"
        }
    },
    "CLCO\(Locations\)": \[
        \{
            "Location Type": "CLDI\(Location online\)",
            "NOID\(Node ID\)": "12448208",
            "VOLI\(Volume ID\)": "3222345473",
            "Object File Path":
"/var/local/rangedb/1/p/17/11/00rH0%DkRt78Ila\#3udu",
            "LTIM\(Location timestamp\)": "2020-02-12T19:36:17.880569"
        \},
        \{
            "Location Type": "CLDI\(Location online\)",
            "NOID\(Node ID\)": "12288733",
            "VOLI\(Volume ID\)": "3222345984",
            "Object File Path":
"/var/local/rangedb/0/p/19/11/00rH0%DkRt78Rrb\#3s;L",
            "LTIM\(Location timestamp\)": "2020-02-12T19:36:17.934425"
        }
    ]
}
```

a. Se déconnecter de la console LDR. Entrez : `exit`

5. À partir d'un nœud d'administration, recherchez dans les journaux d'audit le message d'audit ORLM correspondant à cet objet pour vous assurer que la gestion du cycle de vie des informations (ILM) a placé des copies, si nécessaire.

   a. Connectez-vous au nœud grid :

      i. Saisissez la commande suivante : `ssh admin@grid_node_IP`

ii. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

iii. Entrez la commande suivante pour passer à la racine : `su -`

iv. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier. Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

b. Accédez au répertoire dans lequel se trouvent les journaux d'audit : `cd /var/local/audit/export/`

c. Utilisez grep pour extraire les messages d'audit associés à l'objet dans un fichier de sortie. Entrez : `grep uuid-valueaudit_file_name > output_file_name`

Par exemple :

```
Admin: # grep 926026C4-00A4-449B-AC72-BCCA72DD1311 audit.log >
messages_about_restored_object.txt
```

d. Utilisez grep pour extraire les messages d'audit règles objet met (ORLM) de ce fichier de sortie. Entrez : `grep ORLM output_file_name`

Par exemple :

```
Admin: # grep ORLM messages_about_restored_object.txt
```

Un message d'audit ORLM ressemble à cet exemple de message.

```
[AUDT:[CBID(UI64):0x38186FE53E3C49A5][RULE(CSTR):"Make 2 Copies"]
[STAT(FC32):DONE][CSIZ(UI64):0][UUID(CSTR):"926026C4-00A4-449B-AC72-
BCCA72DD1311"]
[LOCS(CSTR):"**CLDI 12828634 2148730112**, CLDI 12745543 2147552014"]
[RSLT(FC32):SUCS][AVER(UI32):10][ATYP(FC32):ORLM][ATIM(UI64):15633982306
69]
[ATID(UI64):15494889725796157557][ANID(UI32):13100453][AMID(FC32):BCMS]]
```

a. Recherchez le champ EMPLACEMENTS dans le message d'audit.

Le cas échéant, la valeur de CLDI dans LES EMPLACEMENTS est l'ID de nœud et l'ID de volume sur lequel une copie d'objet a été créée. Ce message indique que la ILM a été appliquée et que deux copies d'objet ont été créées à deux emplacements dans la grille.

6. "Réinitialise le nombre d'objets perdus et manquants" Dans le Gestionnaire de grille.

Réinitialiser le nombre d'objets perdus et manquants

Après avoir examiné le système StorageGRID et vérifié que tous les objets perdus enregistrés sont définitivement perdus ou qu'il s'agit d'une fausse alarme, vous pouvez réinitialiser la valeur de l'attribut objets perdus sur zéro.

Avant de commencer

- Vous devez être connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous devez disposer d'autorisations d'accès spécifiques.

Description de la tâche

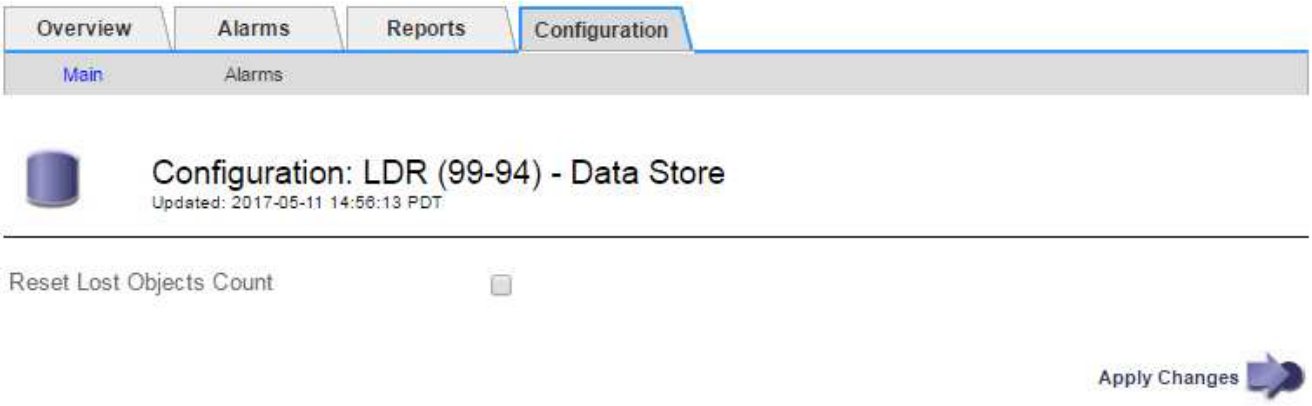
Vous pouvez réinitialiser le compteur objets perdus à partir de l'une des pages suivantes :

- **SUPPORT** > **Outils** > **topologie Grid** > ***site*** > ***Storage Node*** > **LDR** > **Data Store** > **Présentation** > **main**
- **SUPPORT** > **Outils** > **topologie Grid** > ***site*** > ***Storage Node*** > **DDS** > **Data Store** > **Présentation** > **main**

Ces instructions montrent la réinitialisation du compteur à partir de la page **LDR** > **Data Store**.

Étapes

1. Sélectionnez **SUPPORT** > **Outils** > **topologie de grille**.
2. Sélectionnez ***site*** > ***Storage Node*** > **LDR** > **Data Store** > **Configuration** pour le nœud de stockage qui a l'alerte **objets perdus** ou L'alarme PERDUE.
3. Sélectionnez **Réinitialiser le nombre d'objets perdus**.



4. Cliquez sur **appliquer les modifications**.

   L'attribut objets perdus est réinitialisé à 0 et l'alerte **objets perdus** et l'effacement de l'alarme PERDUE, qui peut prendre quelques minutes.

5. Si vous le souhaitez, réinitialisez d'autres valeurs d'attribut associées qui auraient pu être incrémentées en cours d'identification de l'objet perdu.

   a. Sélectionnez ***site*** > ***Storage Node*** > **LDR** > **codage d'effacement** > **Configuration**.
   b. Sélectionnez **Réinitialiser les lectures nombre d'échecs** et **Réinitialiser les copies corrompues nombre d'échecs détectés**.
   c. Cliquez sur **appliquer les modifications**.
   d. Sélectionnez ***site*** > ***Storage Node*** > **LDR** > **Verification** > **Configuration**.
   e. Sélectionnez **Réinitialiser le nombre d'objets manquants** et **Réinitialiser le nombre d'objets corrompus**.
   f. Si vous êtes sûr que les objets mis en quarantaine ne sont pas requis, vous pouvez sélectionner **Supprimer les objets mis en quarantaine**.

      Des objets mis en quarantaine sont créés lorsque la vérification en arrière-plan identifie une copie

d'objet répliquée corrompue. Dans la plupart des cas, StorageGRID remplace automatiquement l'objet corrompu, et il est sûr de supprimer les objets mis en quarantaine. Cependant, si l'alerte **objets perdus** ou L'alarme PERDUE est déclenchée, le support technique peut vouloir accéder aux objets mis en quarantaine.

g. Cliquez sur **appliquer les modifications**.

La réinitialisation des attributs peut prendre quelques instants après avoir cliqué sur **appliquer les modifications**.

Dépanner l'alerte de stockage de données d'objet faible

L'alerte **mémoire de données d'objet faible** surveille la quantité d'espace disponible pour le stockage de données d'objet sur chaque nœud de stockage.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous avez "autorisations d'accès spécifiques".

Description de la tâche

L'alerte **stockage de données d'objet faible** est déclenchée lorsque la quantité totale de données d'objet répliquées et codées d'effacement sur un nœud de stockage correspond à l'une des conditions configurées dans la règle d'alerte.

Par défaut, une alerte majeure est déclenchée lorsque cette condition est évaluée comme vrai :

```
(storagegrid_storage_utilization_data_bytes/
(storagegrid_storage_utilization_data_bytes +
storagegrid_storage_utilization_usable_space_bytes)) >=0.90
```

Dans cette condition :

- `storagegrid_storage_utilization_data_bytes` Est une estimation de la taille totale des données d'objet répliquées et codées d'effacement pour un nœud de stockage.
- `storagegrid_storage_utilization_usable_space_bytes` Correspond à la quantité totale d'espace de stockage objet restant pour un nœud de stockage.

Si une alerte majeure ou mineure **stockage de données d'objet bas** est déclenchée, vous devez exécuter une procédure d'extension dès que possible.

Étapes

1. Sélectionnez **ALERTES** > **actuel**.

   La page alertes s'affiche.

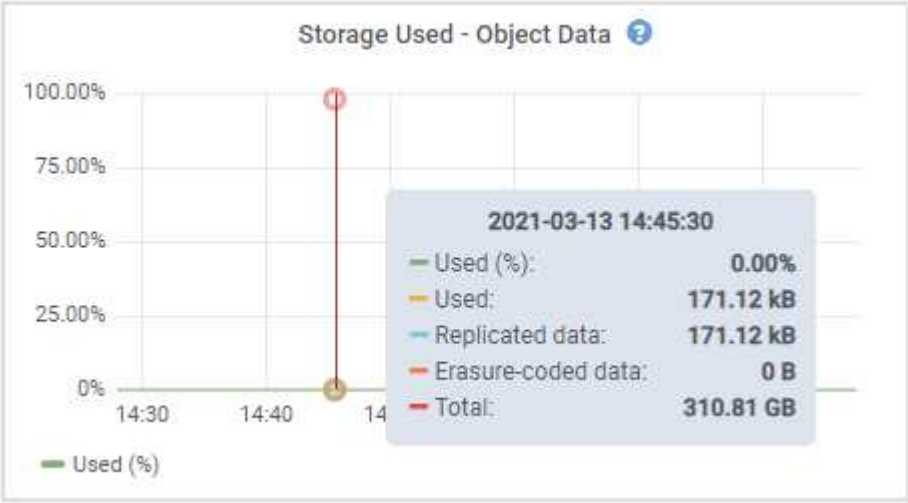
2. Dans le tableau des alertes, développez le groupe d'alertes **stockage de données d'objet bas**, si nécessaire, et sélectionnez l'alerte que vous souhaitez afficher.

   Sélectionnez l'alerte, et non l'en-tête d'un groupe d'alertes.

3. Vérifiez les détails dans la boîte de dialogue et notez ce qui suit :
   - Temps déclenché
   - Le nom du site et du noeud
   - Valeurs actuelles des mesures de cette alerte
4. Sélectionnez **NOEUDS** > ***Storage Node ou site*** > **Storage**.
5. Positionnez le curseur sur le graphique stockage utilisé - données d'objet.

   Les valeurs suivantes sont affichées :

   - **Utilisé (%)** : pourcentage de l'espace utilisable total qui a été utilisé pour les données d'objet.
   - **Used** : quantité de l'espace utilisable total qui a été utilisé pour les données d'objet.
   - **Données répliquées** : estimation de la quantité de données d'objet répliqué sur ce nœud, site ou grille.
   - **Données avec code d'effacement** : estimation de la quantité de données d'objet avec code d'effacement sur ce nœud, ce site ou ce grid.
   - **Total** : la quantité totale d'espace utilisable sur ce nœud, site ou grille. La valeur utilisée est la `storagegrid_storage_utilization_data_bytes` métrique.



6. Sélectionnez les commandes de temps au-dessus du graphique pour afficher l'utilisation du stockage sur différentes périodes.

   Pour mieux comprendre la quantité de stockage utilisée auparavant et après le déclenchement de l'alerte, vous pouvez estimer le temps nécessaire pour que l'espace restant du nœud devienne complet.

7. Dès que possible, "ajouter de la capacité de stockage" à votre grille.

   Vous pouvez ajouter des volumes de stockage (LUN) à des nœuds de stockage existants ou ajouter de nouveaux nœuds de stockage.

   Pour plus d'informations, voir "Gérer des nœuds de stockage complets".

Informations associées

"Dépannage de l'alarme d'état du stockage (SSTS) (hérité)"

Dépanner les alertes de remplacement de filigrane en lecture seule faible

Si vous utilisez des valeurs personnalisées pour les filigranes de volume de stockage, vous devrez peut-être résoudre l'alerte **dépassement de filigrane en lecture seule faible**. Si possible, vous devez mettre à jour votre système pour commencer à utiliser les valeurs optimisées.

Dans les versions précédentes, les trois "filigranes de volume de stockage" Étaient des paramètres globaux &#8212 ; les mêmes valeurs s'appliquent à chaque volume de stockage sur chaque nœud de stockage. À partir de StorageGRID 11.6, le logiciel peut optimiser ces filigranes pour chaque volume de stockage, en fonction de la taille du nœud de stockage et de la capacité relative du volume.

Lorsque vous effectuez une mise à niveau vers StorageGRID 11.6 ou une version ultérieure, des filigranes optimisés en lecture seule et en lecture-écriture sont automatiquement appliqués à tous les volumes de stockage, sauf si l'une des conditions suivantes est vraie :

- Votre système est proche de sa capacité et ne pourra pas accepter de nouvelles données si des filigranes optimisés ont été appliqués. Dans ce cas, StorageGRID ne modifie pas les paramètres du filigrane.
- Vous avez précédemment défini n'importe laquelle des filigranes du volume de stockage sur une valeur personnalisée. StorageGRID ne remplacera pas les paramètres de filigrane personnalisés avec des valeurs optimisées. Cependant, StorageGRID peut déclencher l'alerte **valeur de remplacement du filigrane en lecture seule faible** si votre valeur personnalisée pour le filigrane en lecture seule programmable du volume de stockage est trop petite.

Description de l'alerte

Si vous utilisez des valeurs personnalisées pour les filigranes du volume de stockage, l'alerte **valeur de remplacement du filigrane en lecture seule faible** peut être déclenchée pour un ou plusieurs nœuds de stockage.

Chaque instance de l'alerte indique que la valeur personnalisée du filigrane **Volume de stockage en lecture seule** est inférieure à la valeur minimale optimisée pour ce noeud de stockage. Si vous continuez à utiliser le paramètre personnalisé, le nœud de stockage risque d'être extrêmement faible sur l'espace avant qu'il ne puisse passer en mode lecture seule en toute sécurité. Certains volumes de stockage peuvent devenir inaccessibles (lorsqu'ils sont démontés automatiquement) lorsqu'ils atteignent la capacité.

Par exemple, supposons que vous ayez précédemment défini le filigrane **Volume de stockage en lecture seule** sur 5 Go. Supposons maintenant que StorageGRID a calculé les valeurs optimisées suivantes pour les quatre volumes de stockage du nœud A :

Volume 0	12 GO
Volume 1	12 GO
Volume 2	11 GO
Volume 3	15 GO

L'alerte **dépassement de seuil en lecture seule faible** est déclenchée pour le nœud de stockage A car votre filigrane personnalisé (5 Go) est inférieur à la valeur minimale optimisée pour tous les volumes de ce nœud (11 Go). Si vous continuez à utiliser le paramètre personnalisé, le nœud risque d'avoir un espace insuffisant avant

de passer en mode lecture seule en toute sécurité.

Résolution de l'alerte

Suivez ces étapes si une ou plusieurs alertes **prioritaire de filigrane en lecture seule basse** ont été déclenchées. Vous pouvez également utiliser ces instructions si vous utilisez actuellement des paramètres de filigrane personnalisés et souhaitez commencer à utiliser des paramètres optimisés, même si aucune alerte n'a été déclenchée.

Avant de commencer

- Vous avez terminé la mise à niveau vers StorageGRID 11.6 ou une version ultérieure.
- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous disposez de l'autorisation d'accès racine.

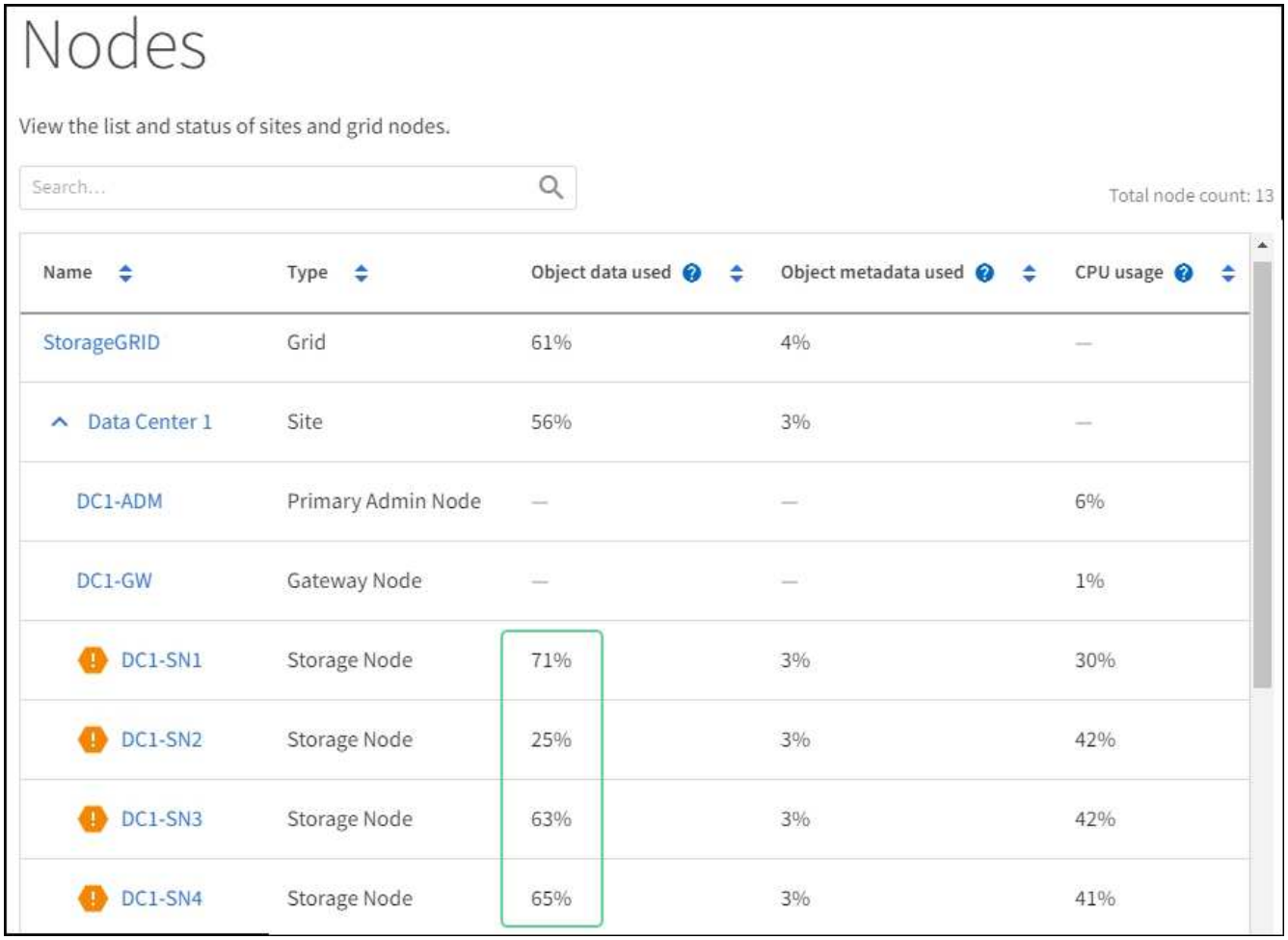
Description de la tâche

Vous pouvez résoudre l'alerte **dépassement de filigrane en lecture seule** en mettant à jour les paramètres de filigrane personnalisés vers les nouveaux remplacements de filigrane. Toutefois, si un ou plusieurs nœuds de stockage sont proches de leur emplacement complet ou si vous avez des exigences ILM spécifiques, vous devez d'abord consulter les filigranes de stockage optimisés et déterminer s'il est sûr de les utiliser.

Évaluer l'utilisation des données d'objet pour l'ensemble de la grille

Étapes

1. Sélectionnez **NOEUDS**.
2. Pour chaque site de la grille, développez la liste des nœuds.
3. Examinez les valeurs de pourcentage affichées dans la colonne **données objet utilisées** pour chaque nœud de stockage de chaque site.



4. Si aucun des nœuds de stockage n'est presque plein (par exemple, toutes les valeurs **données objet utilisées** sont inférieures à 80 %), vous pouvez commencer à utiliser les paramètres de remplacement. Accédez à Utilisez des filigranes optimisés.

> Il y a quelques exceptions à cette règle générale. Par exemple, si les règles ILM utilisent un comportement d'ingestion strict ou si les pools de stockage spécifiques sont proches de la version complète, vous devez d'abord effectuer les étapes de la Afficher des filigranes de stockage optimisés et Déterminez si vous pouvez utiliser des filigranes optimisés.

5. Si un autre nœud de stockage est presque complet, effectuez les étapes de la section Afficher des filigranes de stockage optimisés et Déterminez si vous pouvez utiliser des filigranes optimisés.

Afficher des filigranes de stockage optimisés

StorageGRID utilise deux metrics Prometheus pour afficher les valeurs optimisées qu'il a calculées pour le filigrane **Volume de stockage en lecture seule**. Vous pouvez afficher les valeurs minimale et maximale optimisées pour chaque nœud de stockage de la grille.

Étapes

1. Sélectionnez **SUPPORT** > **Outils** > **métriques**.
2. Dans la section Prometheus, sélectionnez le lien permettant d'accéder à l'interface utilisateur Prometheus.
3. Pour afficher le filigrane minimum en lecture seule programmable recommandé, entrez la mesure Prometheus suivante et sélectionnez **Execute** :

`storagegrid_storage_volume_minimum_optimized_soft_readonly_watermark`

La dernière colonne affiche la valeur minimale optimisée du filigrane en lecture seule pour tous les volumes de stockage de chaque nœud de stockage. Si cette valeur est supérieure au paramètre personnalisé pour le filigrane **Volume de stockage en lecture seule**, l'alerte **dépassement de filigrane en lecture seule faible** est déclenchée pour le nœud de stockage.

4. Pour afficher le filigrane maximal en lecture seule programmable recommandé, entrez la mesure Prometheus suivante et sélectionnez **Execute** :

   `storagegrid_storage_volume_maximum_optimized_soft_readonly_watermark`

   La dernière colonne affiche la valeur maximale optimisée du filigrane en lecture seule pour tous les volumes de stockage de chaque nœud de stockage.

5. Notez la valeur maximale optimisée pour chaque nœud de stockage.

Déterminez si vous pouvez utiliser des filigranes optimisés

Étapes

1. Sélectionnez **NOEUDS**.
2. Répétez la procédure suivante pour chaque nœud de stockage en ligne :
   a. Sélectionnez ***Storage Node*** > **Storage**.
   b. Faites défiler jusqu'au tableau magasins d'objets.
   c. Comparez la valeur **disponible** pour chaque magasin d'objets (volume) au filigrane optimisé maximum que vous avez indiqué pour ce noeud de stockage.
3. Si au moins un volume de chaque nœud de stockage en ligne dispose de plus d'espace disponible que le seuil maximal optimisé pour ce nœud, accédez à Utilisez des filigranes optimisés pour commencer à utiliser les filigranes optimisés.

   Sinon, développez votre grille dès que possible. Soit "ajout de volumes de stockage" à un nœud existant ou "Ajout de nœuds de stockage". Ensuite, passez à Utilisez des filigranes optimisés pour mettre à jour les paramètres du filigrane.

4. Si vous devez continuer à utiliser des valeurs personnalisées pour les filigranes de volume de stockage, "silence" ou "désactiver" L'alerte **dépassement de filigrane en lecture seule** faible.

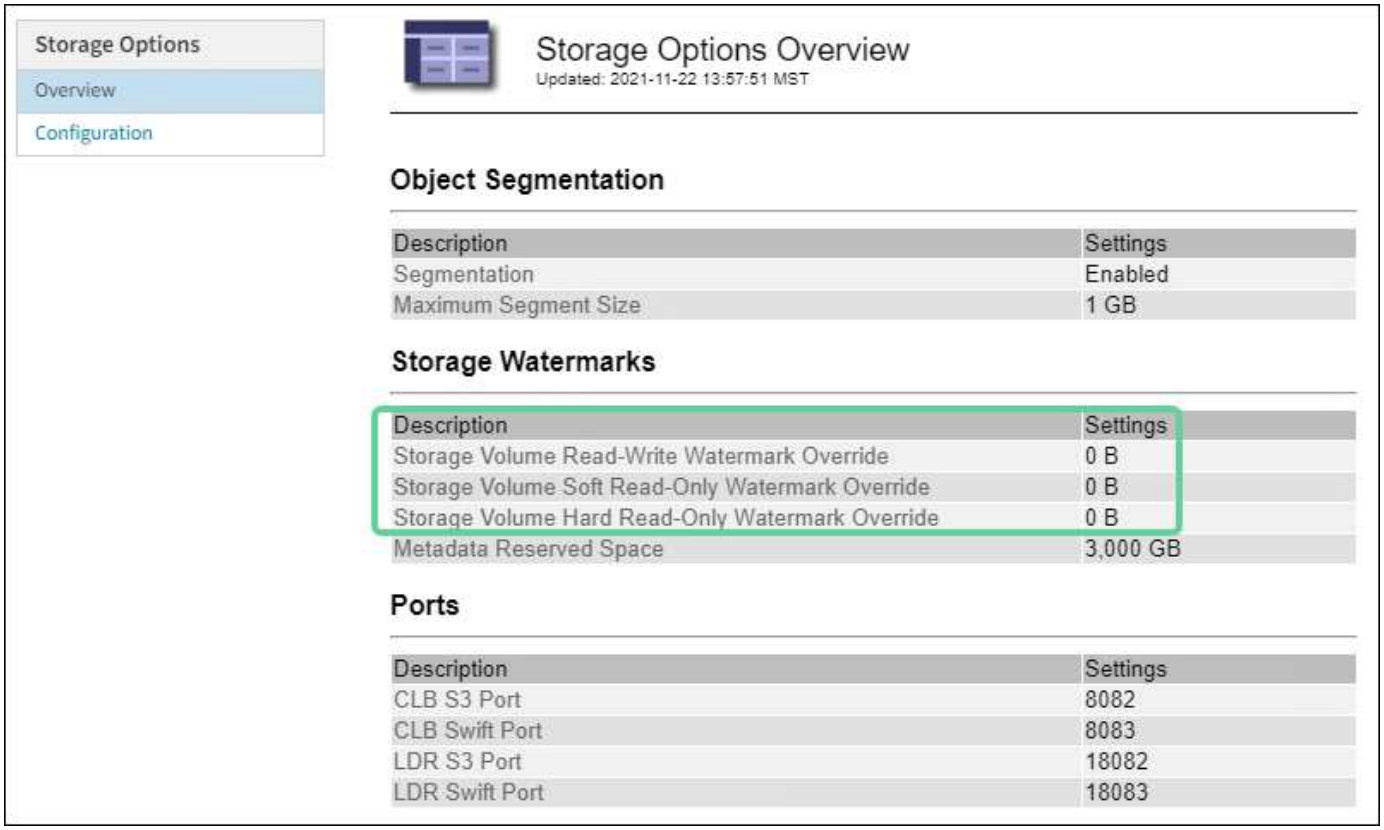
> Les mêmes valeurs de filigrane personnalisées sont appliquées à chaque volume de stockage sur chaque nœud de stockage. L'utilisation de valeurs inférieures aux valeurs recommandées pour les filigranes du volume de stockage peut rendre certains volumes de stockage inaccessibles (démontés automatiquement) lorsque le nœud atteint sa capacité.

Utilisez des filigranes optimisés

Étapes

1. Accédez à **CONFIGURATION** > **système** > **Options de stockage**.
2. Sélectionnez **Configuration** dans le menu Options de stockage.
3. Remplacez les trois remplacements de filigrane par 0.
4. Sélectionnez **appliquer les modifications**.

Les paramètres de filigrane du volume de stockage optimisé sont désormais en vigueur pour chaque volume de stockage, en fonction de la taille du nœud de stockage et de la capacité relative du volume.



Dépanner l'alarme Storage Status (SSTS)

L'alarme Storage Status (SSTS) (État du stockage) est déclenchée si un nœud de stockage ne dispose pas d'espace disponible suffisant pour le stockage d'objets.

Avant de commencer

- Vous devez être connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous devez disposer d'autorisations d'accès spécifiques.

Description de la tâche

L'alarme SSTS (État de stockage) est déclenchée au niveau Avertissement lorsque la quantité d'espace libre sur chaque volume d'un nœud de stockage est inférieure à la valeur du filigrane Storage Volume Soft Read Only (**CONFIGURATION** > **système** > **Options de stockage**).

Storage Options Overview

Updated: 2019-10-09 13:09:30 MDT

Object Segmentation

Description	Settings
Segmentation	Enabled
Maximum Segment Size	1 GB

Storage Watermarks

Description	Settings
Storage Volume Read-Write Watermark	30 GB
Storage Volume Soft Read-Only Watermark	10 GB
Storage Volume Hard Read-Only Watermark	5 GB
Metadata Reserved Space	3,000 GB

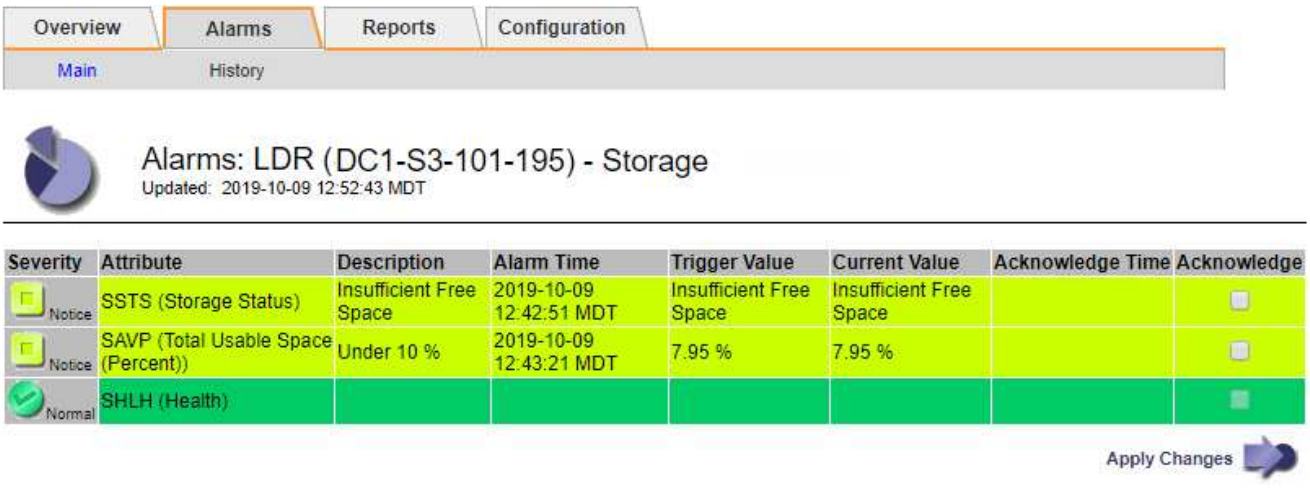
Par exemple, supposons que le filigrane de volume de stockage en lecture seule soit défini sur 10 Go, ce qui est sa valeur par défaut. L'alarme SSTS est déclenchée si moins de 10 Go d'espace utilisable reste sur chaque volume de stockage du nœud de stockage. Si l'un des volumes dispose d'au moins 10 Go d'espace disponible, l'alarme n'est pas déclenchée.

Si une alarme SSTS a été déclenchée, vous pouvez suivre ces étapes pour mieux comprendre le problème.

Étapes

1. Sélectionnez **SUPPORT** > **alarmes (hérité)** > **alarmes actuelles**.
2. Dans la colonne Service, sélectionnez le centre de données, le nœud et le service associés à l'alarme SSTS.

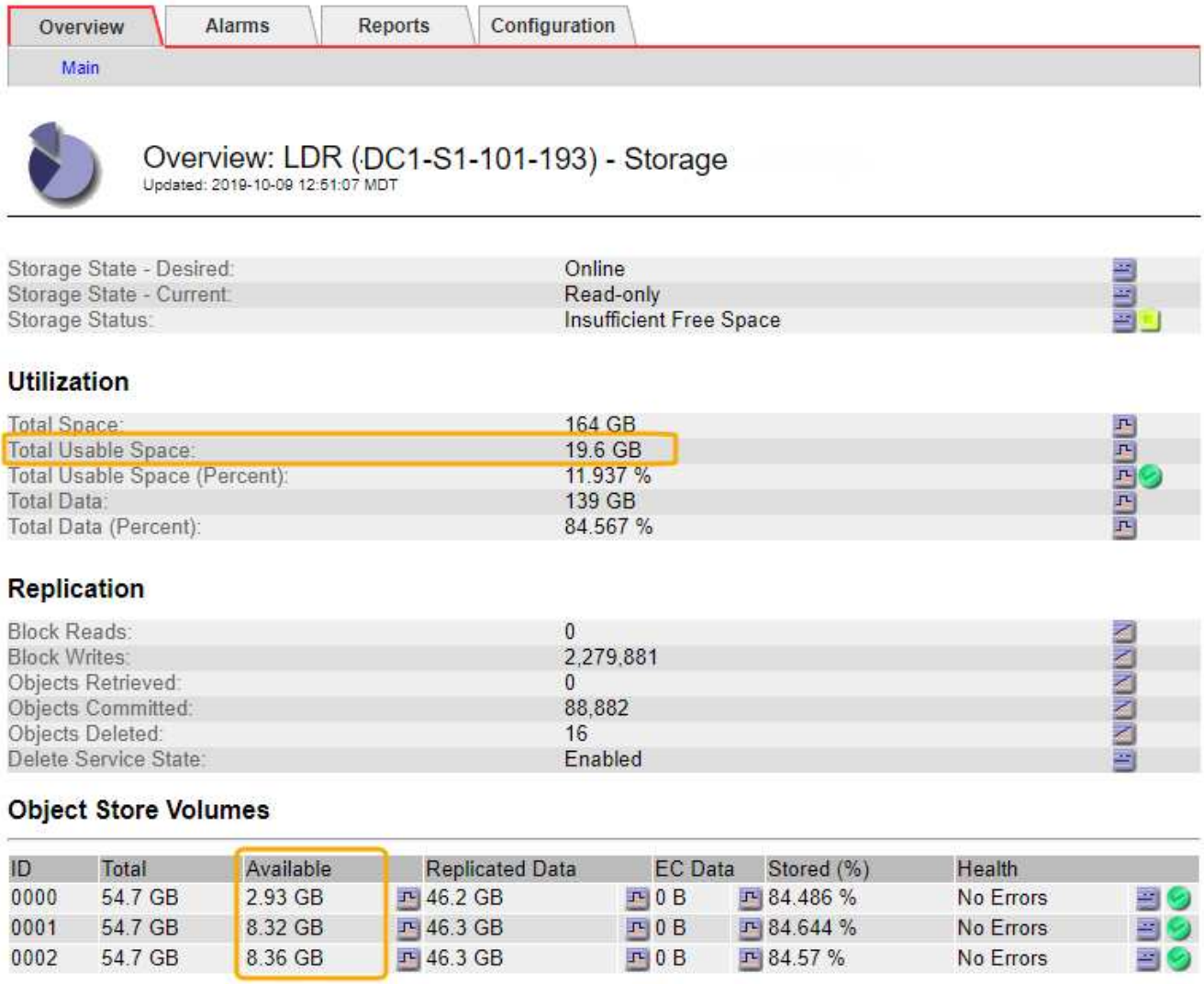
   La page topologie de la grille s'affiche. L'onglet alarmes affiche les alarmes actives pour le nœud et le service que vous avez sélectionnés.



   Dans cet exemple, les alarmes SSTS (Storage Status) et SAVP (Total Usable Space (pourcentage)) ont été déclenchées au niveau Avis.

En général, l'alarme SSTS et l'alarme SAVP sont déclenchées à peu près à la même heure ; cependant, si les deux alarmes sont déclenchées dépend du paramètre de filigrane en GB et du paramètre d'alarme SAVP en pourcentage.

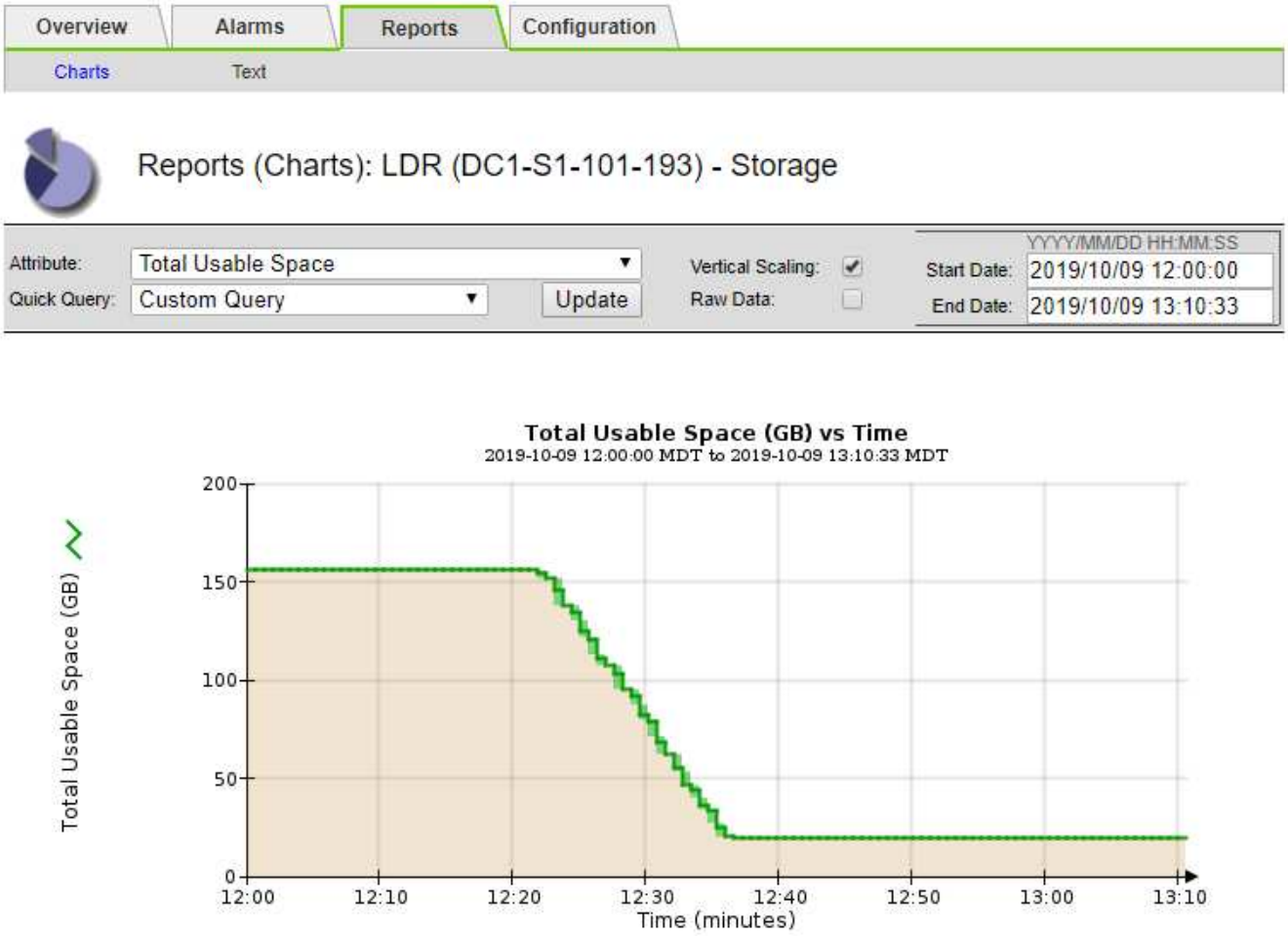
3. Pour déterminer la quantité d'espace utilisable réellement disponible, sélectionnez **LDR** > **Storage** > **Overview** et recherchez l'attribut Total Usable (STAS).



Dans cet exemple, seuls 19.6 Go d'espace de 164 Go sur ce nœud de stockage restent disponibles. Notez que la valeur totale est la somme des valeurs **disponibles** pour les trois volumes du magasin d'objets. L'alarme SSTS a été déclenchée car chacun des trois volumes de stockage avait moins de 10 Go d'espace disponible.

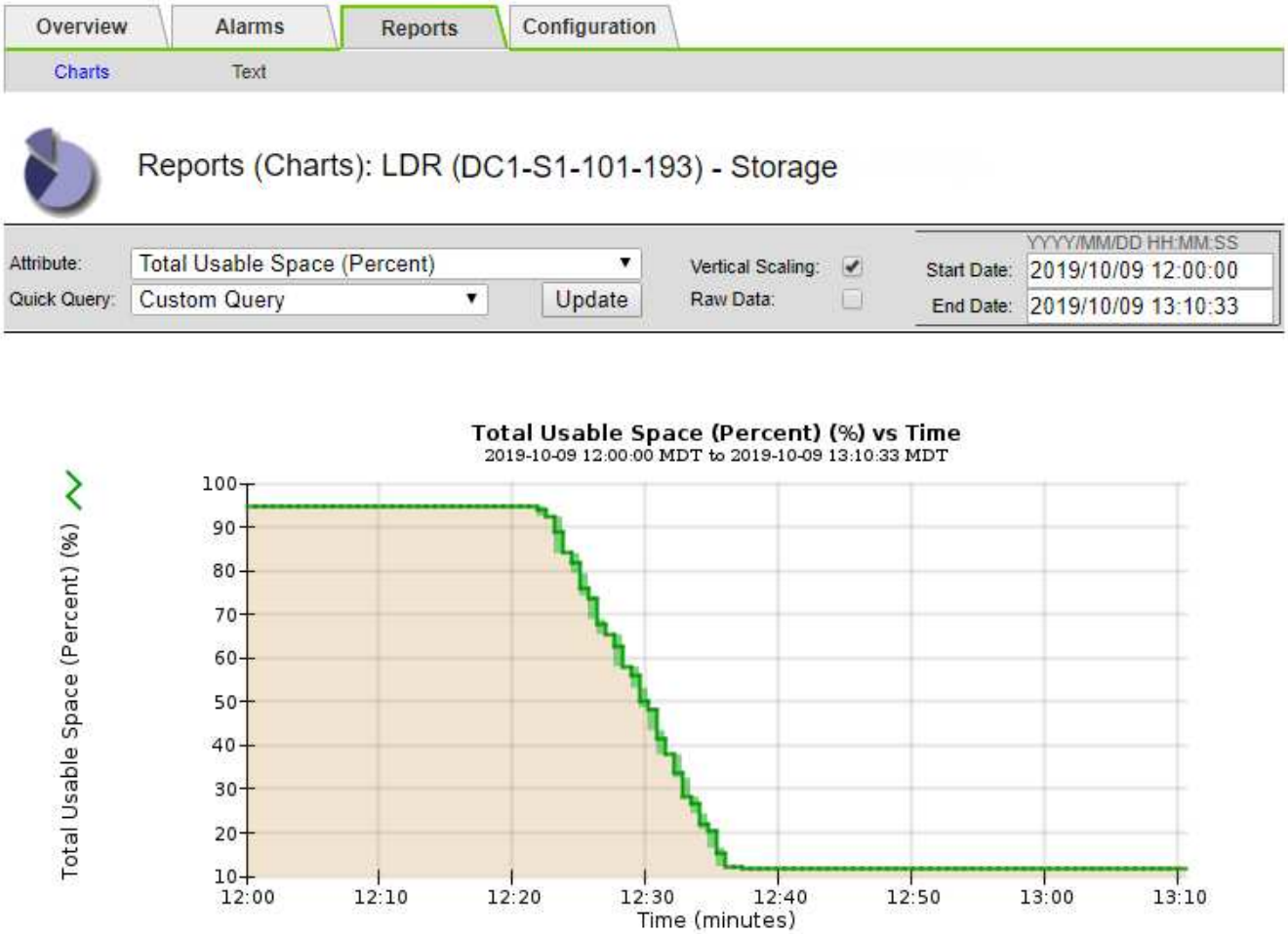
4. Pour comprendre comment le stockage a été utilisé au fil du temps, sélectionnez l'onglet **Rapports** et tracez l'espace utilisable total au cours des dernières heures.

   Dans cet exemple, l'espace utilisable total est passé d'environ 155 Go à 12:00 à 20 Go à 12:35, ce qui correspond à l'heure à laquelle l'alarme SSTS a été déclenchée.



5. Pour comprendre comment le stockage est utilisé en pourcentage du total, tracez l'espace utilisable total (pourcentage) au cours des dernières heures.

   Dans cet exemple, l'espace utilisable total a chuté de 95 % à un peu plus de 10 % environ au même moment.



6. Selon les besoins, "ajouter de la capacité de stockage".

   Voir aussi "Gérer des nœuds de stockage complets".

Résolution des problèmes de transmission des messages des services de plate-forme (alarme SMTT)

L'alarme Total Events (SMTT) est déclenchée dans Grid Manager si un message de service de plate-forme est envoyé à une destination qui ne peut pas accepter les données.

Description de la tâche

Par exemple, un téléchargement partitionné S3 peut réussir même si la réplication ou le message de notification associé ne peut pas être remis au terminal configuré. Ou bien, un message pour la réplication CloudMirror peut ne pas être livré si les métadonnées sont trop longues.

L'alarme SMTT contient un message du dernier événement qui indique : `Failed to publish notifications for bucket-name object key` pour le dernier objet dont la notification a échoué.

Les messages d'événement sont également répertoriés dans le `/var/local/log/bycast-err.log` fichier journal. Voir la "Référence des fichiers journaux".

Pour plus d'informations, reportez-vous au "Résoudre les problèmes liés aux services de plateforme". Vous devrez peut-être le faire "Accédez au locataire à partir du gestionnaire de locataires" pour déboguer une erreur de service de plate-forme.

Étapes

1. Pour afficher l'alarme, sélectionnez **NOEUDS** > ***site*** > ***grid node*** > **Events**.
2. Afficher le dernier événement en haut du tableau.

   Les messages d'événement sont également répertoriés dans le `/var/local/log/bycast-err.log`.

3. Suivez les instructions fournies dans le contenu de l'alarme SMTT pour corriger le problème.
4. Sélectionnez **Réinitialiser le nombre d'événements**.
5. Notifier le locataire des objets dont les messages de services de plate-forme n'ont pas été livrés.
6. Demandez au locataire de déclencher l'échec de la réplication ou de la notification en mettant à jour les métadonnées ou balises de l'objet.

Diagnostiquez les problèmes liés aux métadonnées

Vous pouvez effectuer plusieurs tâches pour déterminer la source des problèmes de métadonnées.

Alerte de stockage des métadonnées faible

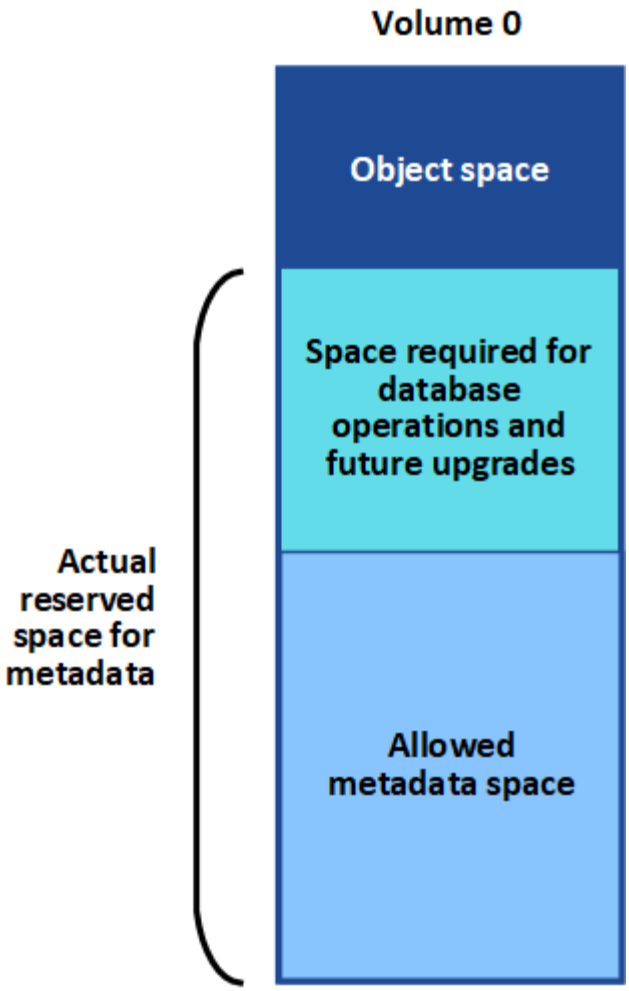
Si l'alerte **stockage de métadonnées faible** est déclenchée, vous devez ajouter de nouveaux nœuds de stockage.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".

Description de la tâche

StorageGRID réserve un certain espace sur le volume 0 de chaque nœud de stockage pour les métadonnées de l'objet. Cet espace est appelé espace réservé réel, et il est divisé en l'espace autorisé pour les métadonnées d'objet (espace de métadonnées autorisé) et l'espace requis pour les opérations essentielles de base de données, telles que la compaction et la réparation. L'espace de métadonnées autorisé régit la capacité globale des objets.



Si les métadonnées d'objet consomment plus de 100 % de l'espace autorisé pour les métadonnées, les opérations de base de données ne peuvent pas s'exécuter efficacement et des erreurs se produisent.

C'est possible "Surveillez la capacité des métadonnées d'objet pour chaque nœud de stockage" pour vous aider à anticiper les erreurs et à les corriger avant qu'elles ne se produisent.

StorageGRID utilise la métrique Prometheus suivante pour mesurer la totalité de l'espace de métadonnées autorisé :

```
storagegrid_storage_utilization_metadata_bytes/storagegrid_storage_utiliza
tion_metadata_allowed_bytes
```

Lorsque cette expression Prometheus atteint certains seuils, l'alerte **stockage de métadonnées faible** est déclenchée.

- **Mineure** : les métadonnées d'objet utilisent au moins 70 % de l'espace autorisé pour les métadonnées. Vous devez ajouter des nœuds de stockage dès que possible.
- **Majeur** : les métadonnées d'objet utilisent au moins 90 % de l'espace autorisé pour les métadonnées. Vous devez immédiatement ajouter de nouveaux nœuds de stockage.

Lorsque les métadonnées d'objet utilisent au moins 90 % de l'espace de métadonnées autorisé, un avertissement s'affiche sur le tableau de bord. Si cet avertissement s'affiche, vous devez immédiatement ajouter de nouveaux nœuds de stockage. Vous ne devez jamais autoriser les métadonnées objet à utiliser plus de 100 % de l'espace autorisé.

- **Critique** : les métadonnées d'objet utilisent au moins 100 % de l'espace de métadonnées autorisé et commencent à consommer l'espace requis pour les opérations essentielles de la base de données. Vous devez arrêter l'ingestion des nouveaux objets et vous devez immédiatement ajouter de nouveaux nœuds de stockage.

Dans l'exemple suivant, les métadonnées d'objet utilisent plus de 100 % de l'espace autorisé pour les métadonnées. Cette situation est critique, ce qui entraîne un fonctionnement inefficace de la base de données et des erreurs.

The following Storage Nodes are using more than 90% of the space allowed for object metadata:

Node	% Used	Used	Allowed
DC1-S2-227	104.51%	6.73 GB	6.44 GB
DC1-S3-228	104.36%	6.72 GB	6.44 GB
DC2-S2-233	104.20%	6.71 GB	6.44 GB
DC1-S1-226	104.20%	6.71 GB	6.44 GB
DC2-S3-234	103.43%	6.66 GB	6.44 GB

Undesirable results can occur if object metadata uses more than 100% of the allowed space. You must add new Storage Nodes immediately or contact support.

Si la taille du volume 0 est inférieure à celle de l'option de stockage de l'espace réservé aux métadonnées (par exemple, dans un environnement non productif), le calcul de l'alerte **stockage de métadonnées faible** peut être inexact.

Étapes

1. Sélectionnez **ALERTES** > **actuel**.
2. Dans le tableau des alertes, développez le groupe d'alertes **stockage de métadonnées faible**, si nécessaire, et sélectionnez l'alerte spécifique que vous souhaitez afficher.
3. Vérifiez les détails dans la boîte de dialogue d'alerte.
4. Si une alerte majeure ou critique **stockage de métadonnées faible** a été déclenchée, effectuez immédiatement une extension pour ajouter des nœuds de stockage.

Dans la mesure où StorageGRID conserve des copies complètes de toutes les métadonnées d'objet sur chaque site, la capacité de métadonnées de l'ensemble de la grille est limitée par la capacité des métadonnées du site le plus petit. Si vous avez besoin d'ajouter de la capacité de métadonnées à un site, vous devriez également "développez n'importe quel autre site" Par le même nombre de nœuds de stockage.

Une fois l'extension effectuée, StorageGRID redistribue les métadonnées de l'objet existantes vers les nouveaux nœuds, qui augmentent la capacité globale des métadonnées de la grille. Aucune action de l'utilisateur n'est requise. L'alerte **stockage de métadonnées faible** est effacée.

Services : état - alarme Cassandra (SVST)

L'alarme Services : Status - Cassandra (SVST) indique que vous devrez peut-être reconstruire la base de données Cassandra pour un nœud de stockage. Cassandra est utilisée comme magasin de métadonnées pour StorageGRID.

Avant de commencer

- Vous devez être connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous devez disposer d'autorisations d'accès spécifiques.
- Vous devez avoir le `Passwords.txt` fichier.

Description de la tâche

Si Cassandra est arrêtée pendant plus de 15 jours (par exemple, le nœud de stockage est mis hors tension), Cassandra ne démarre pas lorsque le nœud est remis en ligne. Vous devez reconstruire la base de données Cassandra pour le service DDS affecté.

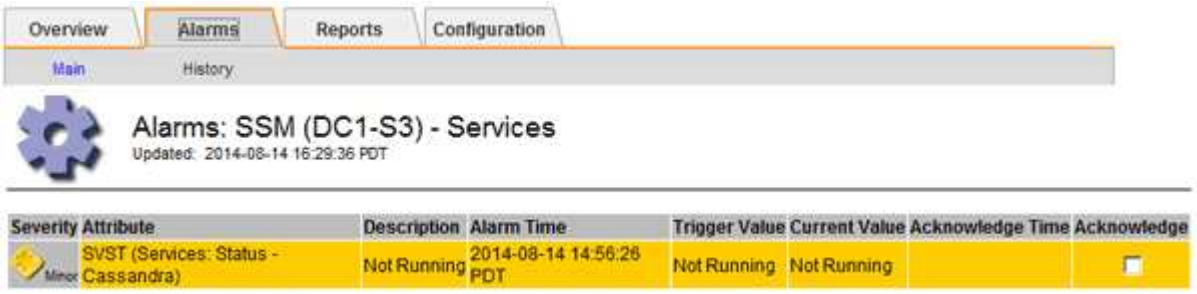
C'est possible "exécuter les diagnostics" pour obtenir des informations supplémentaires sur l'état actuel de votre grille.

> Si deux services de base de données Cassandra ou plus sont en panne pendant plus de 15 jours, contactez le support technique et ne suivez pas les étapes ci-dessous.

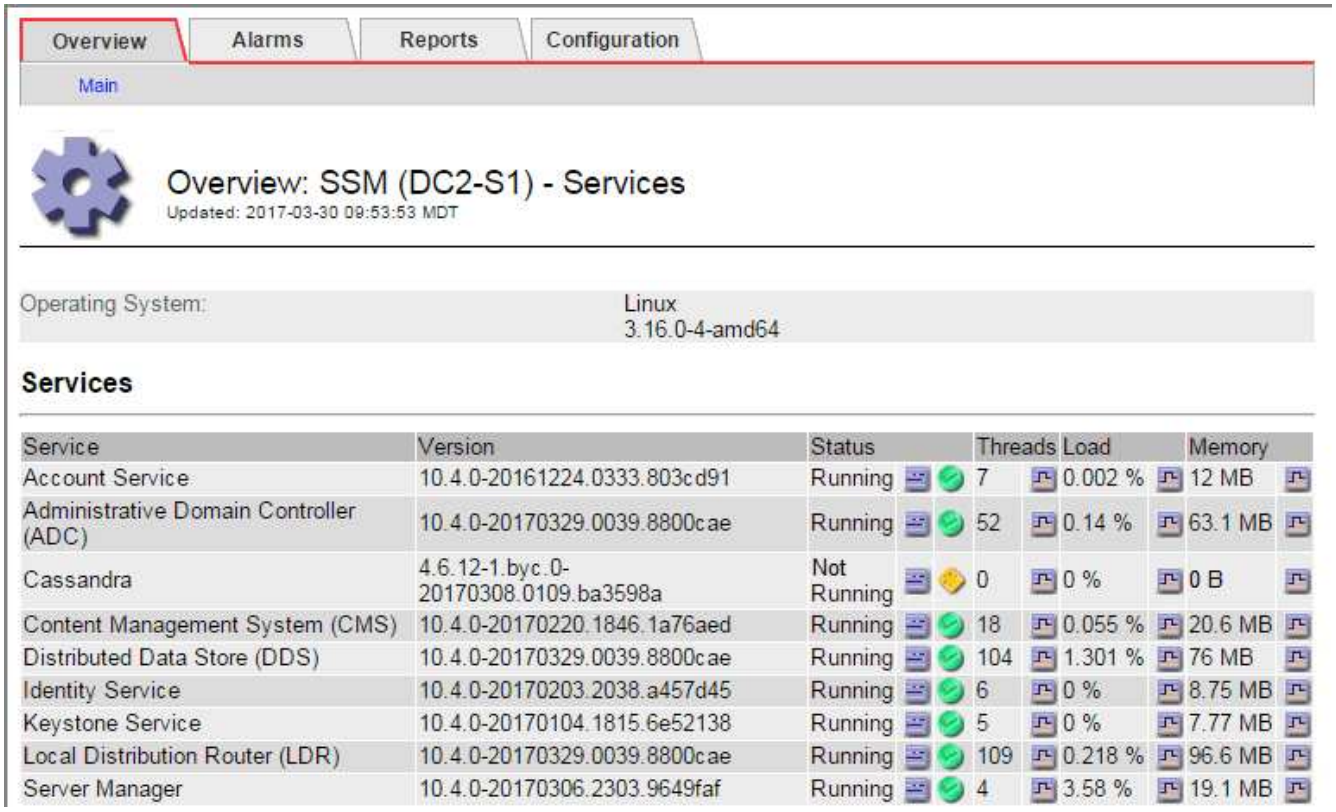
Étapes

1. Sélectionnez **SUPPORT** > **Outils** > **topologie de grille**.
2. Sélectionnez ***site*** > ***Storage Node*** > **SSM** > **Services** > **alarmes** > **main** pour afficher les alarmes.

   Cet exemple montre que l'alarme SVST a été déclenchée.



   La page principale des services SSM indique également que Cassandra n'est pas en cours d'exécution.



3. essayez de redémarrer Cassandra à partir du nœud de stockage :
   a. Connectez-vous au nœud grid :
      i. Saisissez la commande suivante : `ssh admin@grid_node_IP`
      ii. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
      iii. Entrez la commande suivante pour passer à la racine : `su -`
      iv. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier. Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.
   b. Entrez : `/etc/init.d/cassandra status`
   c. Si Cassandra n'est pas en cours d'exécution, redémarrez-le : `/etc/init.d/cassandra restart`
4. Si Cassandra ne redémarre pas, déterminez la durée de sa panne. Si Cassandra a été indisponible pendant plus de 15 jours, il vous faut reconstruire la base de données Cassandra.

   Si deux services de base de données Cassandra ou plus sont en panne, contactez le support technique et ne procédez pas comme suit.

   Vous pouvez déterminer la durée d'interruption de Cassandra en la transcritant ou en consultant le fichier servermanager.log.

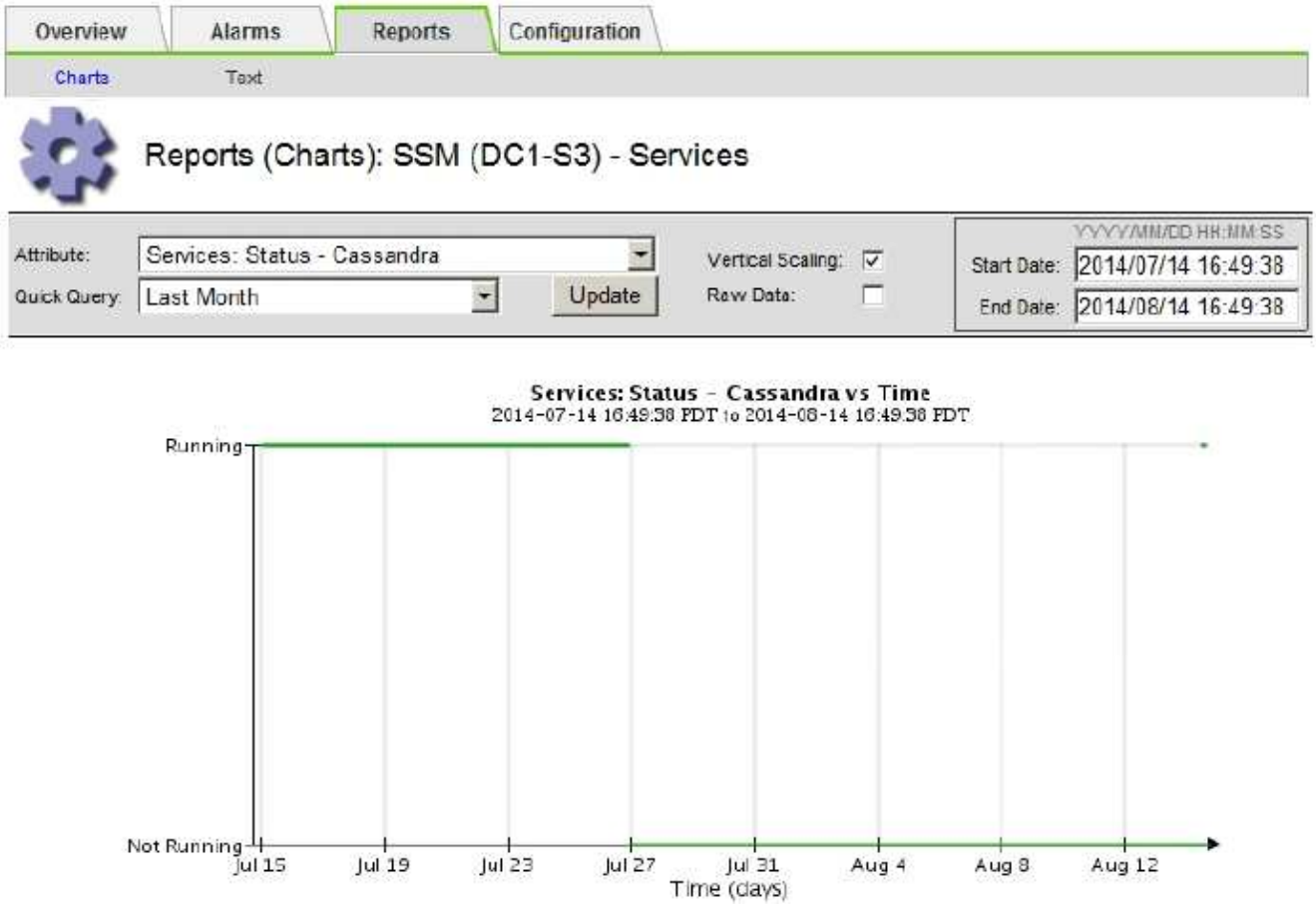
5. Pour le tableau Cassandra :
   a. Sélectionnez **SUPPORT** > **Outils** > **topologie de grille**. Sélectionnez ensuite ***site*** > ***Storage Node*** > **SSM** > **Services** > **Rapports** > **diagrammes**.
   b. Sélectionnez **attribut** > **Service : état - Cassandra**.
   c. Pour **Date de début**, entrez une date qui est au moins 16 jours avant la date du jour. Pour **Date de fin**,

saisissez la date actuelle.

d. Cliquez sur **mettre à jour**.

e. Si Cassandra est indisponible durant plus de 15 jours, reconstruisez la base de données Cassandra.

L'exemple de tableau suivant montre que Cassandra a été indisponible pendant au moins 17 jours.



6. Pour consulter le fichier servermanager.log sur le nœud de stockage :

a. Connectez-vous au nœud grid :

i. Saisissez la commande suivante : `ssh admin@grid_node_IP`

ii. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

iii. Entrez la commande suivante pour passer à la racine : `su -`

iv. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier. Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

b. Entrez : `cat /var/local/log/servermanager.log`

Le contenu du fichier servermanager.log s'affiche.

Si Cassandra a été indisponible pendant plus de 15 jours, le message suivant s'affiche dans le fichier servermanager.log :

```
"2014-08-14 21:01:35 +0000 | cassandra | cassandra not
started because it has been offline for longer than
its 15 day grace period - rebuild cassandra
```

a. Assurez-vous que l'horodatage de ce message correspond à l'heure à laquelle vous avez tenté de redémarrer Cassandra, comme indiqué à l'étape Redémarrez Cassandra à partir du nœud de stockage.

   Il peut y avoir plusieurs entrées pour Cassandra ; vous devez trouver l'entrée la plus récente.

b. Si Cassandra a été indisponible pendant plus de 15 jours, il vous faut reconstruire la base de données Cassandra.

   Pour obtenir des instructions, reportez-vous à la section "Panne d'un nœud de stockage de plus de 15 jours".

c. Contactez le support technique si les alarmes ne s'effacent pas après la reconstruction de Cassandra.

Erreurs Cassandra mémoire insuffisante (alarme SMTT)

Une alarme Total Events (SMTT) est déclenchée lorsque la base de données Cassandra a une erreur de mémoire insuffisante. Si cette erreur se produit, contactez le support technique pour résoudre le problème.

Description de la tâche

Si une erreur de mémoire insuffisante se produit pour la base de données Cassandra, un vidage de mémoire est créé, une alarme Total Events (SMTT) est déclenchée et le nombre d'erreurs de mémoire de Cassandra est incrémenté d'un.

Étapes

1. Pour afficher l'événement, sélectionnez **SUPPORT** > **Outils** > **topologie de grille** > **Configuration**.
2. Vérifiez que le nombre d'erreurs de mémoire du tas Cassandra est égal ou supérieur à 1.

   C'est possible "exécuter les diagnostics" pour obtenir des informations supplémentaires sur l'état actuel de votre grille.

3. Accédez à `/var/local/core/`, comprimer le `Cassandra.hprof` dossier et envoyez-le au support technique.
4. Faire une sauvegarde du `Cassandra.hprof` et supprimez-le de la `/var/local/core/ directory`.

   Ce fichier peut contenir jusqu'à 24 Go. Vous devez donc le supprimer pour libérer de l'espace.

5. Une fois le problème résolu, cochez la case **Réinitialiser** pour le nombre d'erreurs mémoire insuffisante du tas Cassandra. Sélectionnez ensuite **appliquer les modifications**.

   Pour réinitialiser le nombre d'événements, vous devez disposer de l'autorisation de configuration de la page de topologie de la grille.

Résoudre les erreurs de certificat

Si vous constatez un problème de sécurité ou de certificat lorsque vous essayez de vous connecter à StorageGRID à l'aide d'un navigateur Web, d'un client S3 ou Swift ou d'un outil de surveillance externe, vérifiez le certificat.

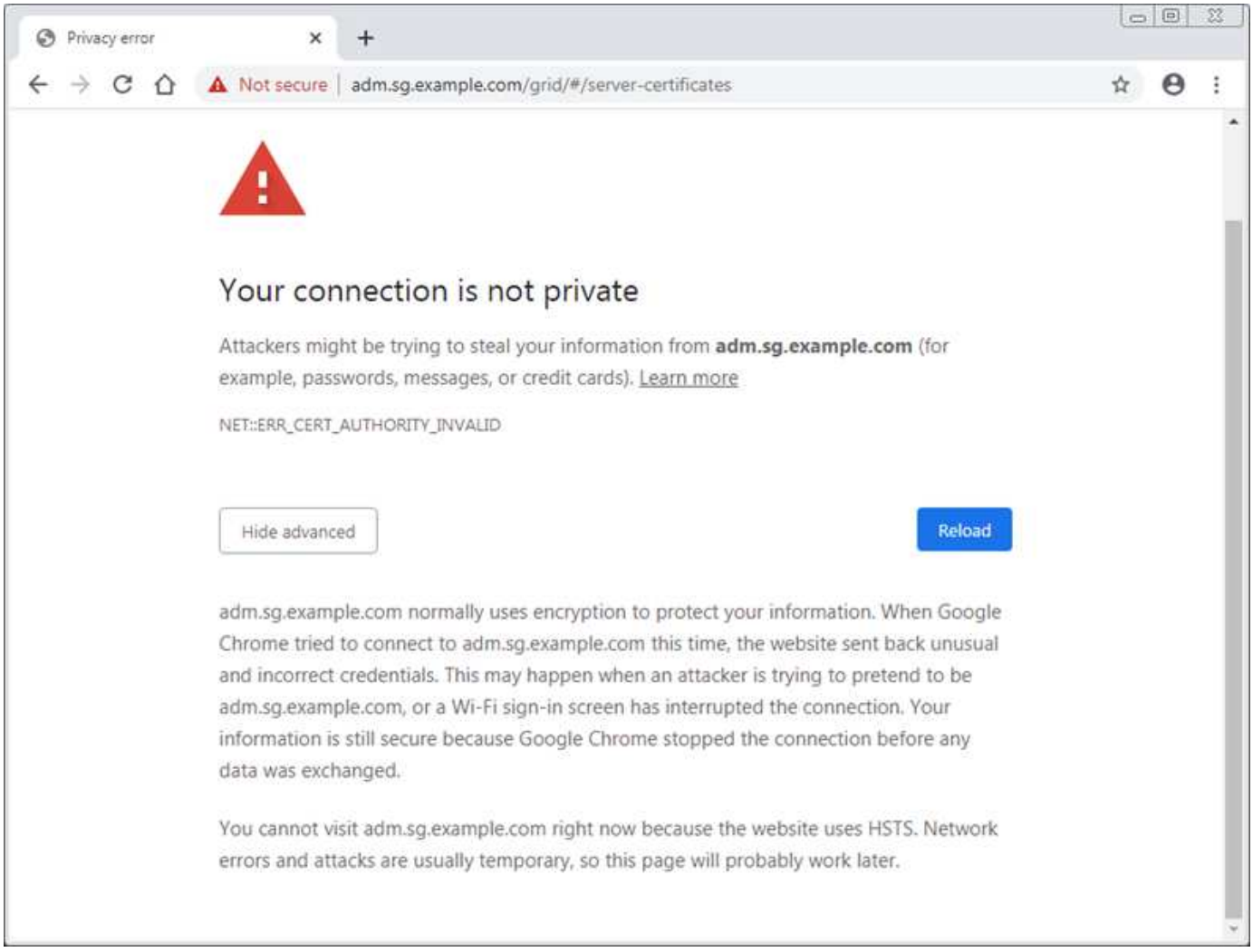
Description de la tâche

Les erreurs de certificat peuvent entraîner des problèmes lors de votre tentative de connexion à StorageGRID à l'aide de Grid Manager, de l'API de gestion du grid, du gestionnaire de locataires ou de l'API de gestion des locataires. Des erreurs liées au certificat peuvent également se produire lorsque vous tentez de vous connecter à un client S3 ou Swift ou à un outil de surveillance externe.

Si vous accédez à Grid Manager ou au Gestionnaire de locataires à l'aide d'un nom de domaine au lieu d'une adresse IP, le navigateur affiche une erreur de certificat sans option de contournement si l'un des cas suivants se produit :

- Votre certificat d'interface de gestion personnalisée expire.
- Vous restaurez un certificat d'interface de gestion personnalisée vers le certificat de serveur par défaut.

L'exemple suivant montre une erreur de certificat lorsque le certificat de l'interface de gestion personnalisée a expiré :



Pour garantir que les opérations ne sont pas interrompues par un certificat de serveur défaillant, l'alerte **expiration du certificat de serveur pour l'interface de gestion** est déclenchée lorsque le certificat de serveur est sur le point d'expirer.

Lorsque vous utilisez des certificats client pour l'intégration avec Prometheus externe, les erreurs de certificat peuvent être dues au certificat de l'interface de gestion StorageGRID ou aux certificats client. L'alerte **expiration des certificats client configurés sur la page certificats** est déclenchée lorsqu'un certificat client arrive à expiration.

Étapes

Si vous avez reçu une notification d'alerte concernant un certificat expiré, accédez aux détails du certificat : . Sélectionnez **CONFIGURATION** > **sécurité** > **certificats**, puis "sélectionnez l'onglet certificat approprié".

1. Vérifiez la période de validité du certificat. + certains navigateurs Web et clients S3 ou Swift n'acceptent pas les certificats dont la période de validité est supérieure à 398 jours.
2. Si le certificat a expiré ou expire bientôt, téléchargez ou générez un nouveau certificat.
   - Pour un certificat de serveur, reportez-vous aux étapes pour "Configuration d'un certificat de serveur personnalisé pour le Grid Manager et le tenant Manager".
   - Pour un certificat client, reportez-vous aux étapes de "configuration d'un certificat client".
3. Pour les erreurs de certificat de serveur, essayez l'une des options suivantes ou les deux :
   - Assurez-vous que le nom d'alternative de l'objet (SAN) du certificat est renseigné et que le SAN correspond à l'adresse IP ou au nom d'hôte du nœud auquel vous vous connectez.
   - Si vous tentez de vous connecter à StorageGRID à l'aide d'un nom de domaine :
     i. Entrez l'adresse IP du noeud d'administration au lieu du nom de domaine pour contourner l'erreur de connexion et accéder à Grid Manager.
     ii. Dans Grid Manager, sélectionnez **CONFIGURATION** > **sécurité** > **certificats**, puis "sélectionnez l'onglet certificat approprié" pour installer un nouveau certificat personnalisé ou continuer avec le certificat par défaut.
     iii. Dans les instructions d'administration de StorageGRID, reportez-vous aux étapes de "Configuration d'un certificat de serveur personnalisé pour le Grid Manager et le tenant Manager".

Résolution des problèmes liés au nœud d'administration et à l'interface utilisateur

Plusieurs tâches sont à effectuer pour déterminer la source des problèmes liés aux nœuds d'administration et à l'interface utilisateur de StorageGRID.

Erreurs de connexion

Si une erreur s'est produite lors de la connexion à un nœud d'administration StorageGRID, votre système peut rencontrer un problème avec "configuration de la fédération des identités", a "la mise en réseau" ou "matériel" problème, un problème avec "Services de nœuds d'administration", ou un "Problème avec la base de données Cassandra" Sur les nœuds de stockage connectés.

Avant de commencer

- Vous avez le `Passwords.txt` fichier.
- Vous avez "autorisations d'accès spécifiques".

Description de la tâche

Suivez ces instructions de dépannage si vous voyez l'un des messages d'erreur suivants lorsque vous tentez

de vous connecter à un noeud d'administration :

- `Your credentials for this account were invalid. Please try again.`
- `Waiting for services to start…`
- `Internal server error. The server encountered an error and could not complete your request. Please try again. If the problem persists, contact Technical Support.`
- `Unable to communicate with server. Reloading page…`

Étapes

1. Attendez 10 minutes et essayez à nouveau de vous connecter.

   Si l'erreur n'est pas résolue automatiquement, passez à l'étape suivante.

2. Si votre système StorageGRID comporte plusieurs nœuds d'administration, essayez de vous connecter à Grid Manager à partir d'un autre nœud d'administration.
   - Si vous pouvez vous connecter, vous pouvez utiliser les options **Dashboard**, **NODES**, **Alerts** et **SUPPORT** pour déterminer la cause de l'erreur.
   - Si vous n'avez qu'un seul nœud d'administration ou si vous ne pouvez toujours pas vous connecter, passez à l'étape suivante.
3. Déterminez si le matériel du nœud est hors ligne.
4. Si l'authentification unique (SSO) est activée pour votre système StorageGRID, reportez-vous aux étapes de "configuration de l'authentification unique".

   Pour résoudre ces problèmes, il peut être nécessaire de désactiver et de réactiver temporairement l'authentification SSO pour un nœud d'administration unique.

   > ⓘ Si SSO est activé, vous ne pouvez pas vous connecter à l'aide d'un port restreint. Vous devez utiliser le port 443.

5. Déterminez si le compte que vous utilisez appartient à un utilisateur fédéré.

   Si le compte d'utilisateur fédéré ne fonctionne pas, essayez de vous connecter à Grid Manager en tant qu'utilisateur local, tel que root.

   - Si l'utilisateur local peut se connecter :
     i. Examinez toutes les alarmes affichées.
     ii. Sélectionnez **CONFIGURATION** > **contrôle d'accès** > **fédération d'identités**.
     iii. Cliquez sur **Tester la connexion** pour valider vos paramètres de connexion pour le serveur LDAP.
     iv. Si le test échoue, corrigez toute erreur de configuration.
   - Si l'utilisateur local ne peut pas se connecter et que vous êtes sûr que les informations d'identification sont correctes, passez à l'étape suivante.
6. Utilisez SSH (Secure Shell) pour vous connecter au nœud d'administration :
   a. Saisissez la commande suivante : `ssh admin@Admin_Node_IP`
   b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
   c. Entrez la commande suivante pour passer à la racine : `su -`

d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

   Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

7. Afficher l'état de tous les services s'exécutant sur le nœud grid : `storagegrid-status`

   Assurez-vous que les services nms, mi, nginx et api de gestion sont tous en cours d'exécution.

   La sortie est immédiatement mise à jour si l'état d'un service change.

```
$ storagegrid-status
Host Name                      99-211
IP Address                     10.96.99.211
Operating System Kernel        4.19.0          Verified
Operating System Environment   Debian 10.1     Verified
StorageGRID Webscale Release   11.4.0          Verified
Networking                                     Verified
Storage Subsystem                              Verified
Database Engine                5.5.9999+default Running
Network Monitoring             11.4.0          Running
Time Synchronization           1:4.2.8p10+dfsg Running
ams                            11.4.0          Running
cmn                            11.4.0          Running
nms                            11.4.0          Running
ssm                            11.4.0          Running
mi                             11.4.0          Running
dynip                          11.4.0          Running
nginx                          1.10.3          Running
tomcat                         9.0.27          Running
grafana                        6.4.3           Running
mgmt api                       11.4.0          Running
prometheus                     11.4.0          Running
persistence                    11.4.0          Running
ade exporter                   11.4.0          Running
alertmanager                   11.4.0          Running
attrDownPurge                  11.4.0          Running
attrDownSamp1                  11.4.0          Running
attrDownSamp2                  11.4.0          Running
node exporter                  0.17.0+ds       Running
sg snmp agent                  11.4.0          Running
```

8. Vérifiez que le service nginx-gw est en cours d'exécution `# service nginx-gw status`
9. utilisez Lumberjack pour collecter les journaux : `# /usr/local/sbin/lumberjack.rb`

   Si l'authentification a échoué par le passé, vous pouvez utiliser les options de script --start et --end Lumberjack pour spécifier la plage horaire appropriée. Utilisez lumberjack -h pour plus de détails sur ces options.

La sortie vers le terminal indique l'emplacement où l'archive de journal a été copiée.

10. consultez les journaux suivants :
    - `/var/local/log/bycast.log`
    - `/var/local/log/bycast-err.log`
    - `/var/local/log/nms.log`
    - `**/*commands.txt`
11. Si vous n'avez pas pu identifier de problèmes avec le nœud d'administration, exécutez l'une ou l'autre des commandes suivantes pour déterminer les adresses IP des trois nœuds de stockage exécutant le service ADC sur votre site. Il s'agit généralement des trois premiers nœuds de stockage installés sur le site.

```
# cat /etc/hosts
```

```
# vi /var/local/gpt-data/specs/grid.xml
```

    Les nœuds Admin utilisent le service ADC pendant le processus d'authentification.

12. À partir du nœud d'administration, connectez-vous à chacun des nœuds de stockage ADC en utilisant les adresses IP que vous avez identifiées.
    a. Saisissez la commande suivante : `ssh admin@grid_node_IP`
    b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
    c. Entrez la commande suivante pour passer à la racine : `su -`
    d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

    Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

13. Afficher l'état de tous les services s'exécutant sur le nœud grid : `storagegrid-status`

    Assurez-vous que tous les services idnt, acct, nginx et cassandra fonctionnent.

14. Répéter les étapes Utilisez Lumberjack pour récupérer les journaux et Journaux de révision Pour consulter les journaux sur les nœuds de stockage.
15. Si vous ne parvenez pas à résoudre le problème, contactez le support technique.

    Fournissez les journaux que vous avez collectés au support technique. Voir aussi "Référence des fichiers journaux".

Problèmes liés à l'interface utilisateur

L'interface utilisateur du Gestionnaire de grille ou du Gestionnaire de locataires peut ne pas répondre comme prévu après la mise à niveau du logiciel StorageGRID.

Étapes

1. Assurez-vous d'utiliser un "navigateur web pris en charge".

La prise en charge du navigateur peut changer à chaque version de StorageGRID. Vérifiez que vous utilisez un navigateur pris en charge par votre version de StorageGRID.

2. Effacez le cache de votre navigateur Web.

   L'effacement du cache supprime les ressources obsolètes utilisées par la version précédente du logiciel StorageGRID et permet à l'interface utilisateur de fonctionner de nouveau correctement. Pour obtenir des instructions, reportez-vous à la documentation de votre navigateur Web.

Nœud d'administration indisponible

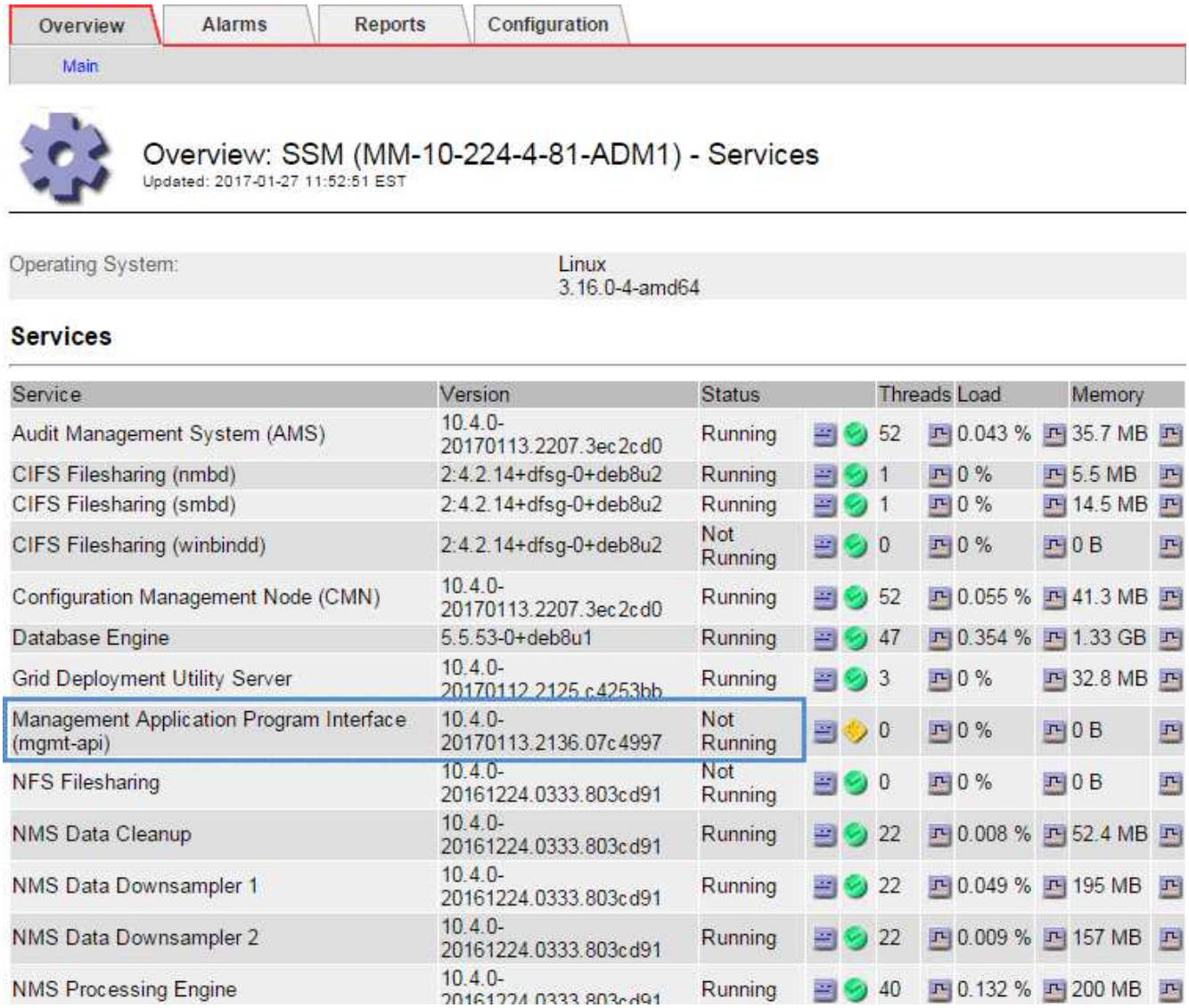
Si le système StorageGRID inclut plusieurs nœuds d'administration, vous pouvez utiliser un autre nœud d'administration pour vérifier l'état d'un nœud d'administration non disponible.

Avant de commencer

Vous devez disposer d'autorisations d'accès spécifiques.

Étapes

1. À partir d'un noeud d'administration disponible, connectez-vous à Grid Manager à l'aide d'un "navigateur web pris en charge".
2. Sélectionnez **SUPPORT** > **Outils** > **topologie de grille**.
3. Sélectionnez ***site*** **> noeud d'administration non disponible** > **SSM** > **Services** > **Présentation** > **main**.
4. Recherchez les services dont l'état n'est pas en cours d'exécution et qui peuvent également s'afficher en bleu.



5. Déterminez si des alarmes ont été déclenchées.
6. Prenez les mesures appropriées pour résoudre le problème.

Résolution des problèmes de réseau, de matériel et de plateforme

Vous pouvez effectuer plusieurs tâches pour déterminer la source des problèmes liés au réseau, au matériel et à la plateforme StorageGRID.

Erreurs "`422: Entité non traitable'"

L'erreur 422 : entité détraitable peut se produire pour différentes raisons. Consultez le message d'erreur pour déterminer la cause de votre problème.

Si l'un des messages d'erreur répertoriés s'affiche, effectuez l'action recommandée.

Message d'erreur	Cause première et action corrective

`422: Unprocessable Entity`
 	
`Validation failed. Please check the values you entered for errors. Test connection failed. Please verify your configuration. Unable to authenticate, please verify your username and password: LDAP Result Code 8 "Strong Auth Required": 00002028: LdapErr: DSID-0C090256, comment: The server requires binds to turn on integrity checking if SSL\TLS are not already active on the connection, data 0, v3839`
	Ce message peut se produire si vous sélectionnez l'option **ne pas utiliser TLS** pour transport Layer Security (TLS) lors de la configuration de la fédération d'identités à l'aide de Windows Active Directory (AD).
	
	L'utilisation de l'option **ne pas utiliser TLS** n'est pas prise en charge pour les serveurs AD qui appliquent la signature LDAP. Vous devez sélectionner l'option **Use STARTTLS** ou l'option **use LDAPS** pour TLS.

`422: Unprocessable Entity`
 	
`Validation failed. Please check the values you entered for errors. Test connection failed. Please verify your configuration.Unable to begin TLS, verify your certificate and TLS configuration: LDAP Result Code 200 "Network Error": TLS handshake failed (EOF)`
	Ce message s'affiche si vous essayez d'utiliser un chiffrement non pris en charge pour établir une connexion TLS (transport Layer Security) entre StorageGRID et un système externe utilisé pour identifier la fédération ou les pools de stockage dans le cloud.
	
	Vérifiez les chiffrements proposés par le système externe. Le système doit utiliser l'un des "Chiffrements pris en charge par StorageGRID" Pour les connexions TLS sortantes, comme indiqué dans les instructions d'administration de StorageGRID.

alerte de non-concordance MTU du réseau de la grille

L'alerte **Grid Network MTU mismatch** est déclenchée lorsque le paramètre MTU (maximum transmission Unit) de l'interface réseau Grid (eth0) diffère considérablement sur les nœuds de la grille.

Description de la tâche

Les différences dans les paramètres MTU peuvent indiquer que certains réseaux eth0, mais pas tous, sont configurés pour les trames jumbo. Une différence de taille de MTU supérieure à 1000 peut entraîner des problèmes de performances du réseau.

Étapes

1. Répertorie les paramètres MTU pour eth0 sur tous les nœuds.
   - Utilisez la requête fournie dans Grid Manager.
   - Accédez à *primary Admin Node IP address*`/metrics/graph` et entrez la requête suivante : `node_network_mtu_bytes{interface='eth0'}`
2. "Modifiez les paramètres MTU" Si nécessaire, pour s'assurer qu'ils sont identiques pour l'interface réseau Grid (eth0) sur tous les nœuds.
   - Pour les nœuds Linux et VMware, utilisez la commande suivante : `/usr/sbin/change-ip.py [-h] [-n node] mtu network [network...]`

     Exemple : `change-ip.py -n node 1500 grid admin`

     Remarque : sur les nœuds basés sur Linux, si la valeur MTU souhaitée pour le réseau dans le conteneur dépasse la valeur déjà configurée sur l'interface hôte, vous devez d'abord configurer l'interface hôte pour qu'elle ait la valeur MTU souhaitée, puis utiliser `change-ip.py` Script pour modifier la valeur MTU du réseau dans le conteneur.

     Utilisez les arguments suivants pour modifier la MTU sur les nœuds Linux ou VMware.

Arguments de position	Description
`mtu`	La MTU à définir. Doit être compris entre 1280 et 9216.
`network`	Réseaux auxquels appliquer la MTU. Incluez un ou plusieurs des types de réseau suivants : • grille • admin • client

+

Arguments facultatifs	Description
`-h, - help`	Afficher le message d'aide et quitter.
`-n node, --node node`	Le nœud. La valeur par défaut est le nœud local.

Alarme d'erreur de réception réseau (NRER)

Les alarmes d'erreur de réception réseau (NRER) peuvent être causées par des problèmes de connectivité entre StorageGRID et votre matériel réseau. Dans certains cas, les erreurs NRER peuvent être résolues sans intervention manuelle. Si les erreurs ne s'effacent pas, prenez les mesures recommandées.

Description de la tâche

Les alarmes NRER peuvent être causées par les problèmes suivants avec le matériel réseau connecté à

StorageGRID :

- La correction d’erreur de marche avant (FEC) est requise et n’est pas utilisée
- Le port du commutateur et la MTU de la carte réseau ne correspondent pas
- Taux d’erreur de liaison élevés
- Dépassement de la mémoire tampon de la sonnerie NIC

Étapes

1. Suivez les étapes de dépannage pour toutes les causes potentielles de l’alarme NRER compte tenu de votre configuration réseau.
2. Effectuez les étapes suivantes en fonction de la cause de l’erreur :

Non-concordance FEC

Ces étapes s'appliquent uniquement aux erreurs NRER causées par une incompatibilité FEC sur les appareils StorageGRID.

a. Vérifiez l'état FEC du port du commutateur connecté à votre appliance StorageGRID.
b. Vérifiez l'intégrité physique des câbles entre l'appareil et le commutateur.
c. Si vous souhaitez modifier les paramètres FEC pour essayer de résoudre l'alarme NRER, assurez-vous d'abord que l'appareil est configuré pour le mode **Auto** sur la page Configuration de la liaison du programme d'installation de l'appareil StorageGRID (reportez-vous aux instructions relatives à votre appareil :
   - "SG6000"
   - "SG5700"
   - "SG100 et SG1000"
d. Modifiez les paramètres FEC sur les ports du commutateur. Si possible, les ports de l'appliance StorageGRID ajustent leurs paramètres FEC.

   Vous ne pouvez pas configurer les paramètres FEC sur les appliances StorageGRID. Au lieu de cela, les appareils tentent de détecter et de mettre en miroir les paramètres FEC sur les ports de commutateur auxquels ils sont connectés. Si les liaisons sont forcées à des vitesses de réseau 25 GbE ou 100 GbE, le commutateur et la carte réseau peuvent ne pas négocier un paramètre FEC commun. Sans paramètre FEC commun, le réseau revient en mode « no-FEC ». Lorsque le mode FEC n'est pas activé, les connexions sont plus susceptibles d'erreurs causées par le bruit électrique.

   Les appareils StorageGRID prennent en charge les FEC Firecode (FC) et Reed Solomon (RS), ainsi qu'aucun FEC.

Le port du commutateur et la MTU de la carte réseau ne correspondent pas

Si l'erreur est causée par une discordance de port de commutateur et de MTU de carte réseau, vérifiez que la taille de MTU configurée sur le nœud est identique au paramètre MTU du port de commutateur.

La taille de MTU configurée sur le nœud peut être inférieure à celle définie sur le port de commutateur auquel le nœud est connecté. Si un nœud StorageGRID reçoit une trame Ethernet supérieure à sa MTU, ce qui est possible avec cette configuration, l'alarme NRER peut être signalée. Si vous pensez que c'est ce qui se passe, modifiez la MTU du port du switch pour qu'il corresponde à la MTU de l'interface réseau StorageGRID, ou modifiez la MTU de l'interface réseau StorageGRID pour qu'elle corresponde au port du switch, en fonction de vos objectifs ou de vos exigences MTU de bout en bout.

Pour des performances réseau optimales, tous les nœuds doivent être configurés avec des valeurs MTU similaires sur leurs interfaces réseau Grid. L'alerte **Grid Network MTU mismatch** est déclenchée en cas de différence importante dans les paramètres MTU pour le réseau Grid sur les nœuds individuels. Les valeurs MTU ne doivent pas nécessairement être identiques pour tous les types de réseau. Voir Dépanner l'alerte de non-concordance de MTU du réseau Grid pour en savoir plus.

Voir aussi "Modifier le paramètre MTU".

Taux d'erreur de liaison élevés

a. Activez FEC, si ce n'est déjà fait.

b. Vérifiez que le câblage réseau est de bonne qualité et qu'il n'est pas endommagé ou mal connecté.

c. Si les câbles ne semblent pas être à l'origine du problème, contactez le support technique.

> Vous remarquerez peut-être des taux d'erreur élevés dans un environnement présentant un bruit électrique élevé.

Dépassement de la mémoire tampon de la sonnerie NIC

Si l'erreur est un dépassement de la mémoire tampon de la sonnerie de la carte réseau, contactez le support technique.

La mémoire tampon annulaire peut être surchargée lorsque le système StorageGRID est surchargé et ne peut pas traiter les événements réseau en temps opportun.

3. Une fois que vous avez résolu le problème sous-jacent, réinitialisez le compteur d'erreurs.
   a. Sélectionnez **SUPPORT** > **Outils** > **topologie de grille**.
   b. Sélectionnez ***site*** > ***grid node*** > **SSM** > **Resources** > **Configuration** > **main**.
   c. Sélectionnez **Réinitialiser le nombre d'erreurs de réception** et cliquez sur **appliquer les modifications**.

Informations associées

"Référence des alarmes (système hérité)"

Erreurs de synchronisation de l'heure

Des problèmes de synchronisation de l'heure peuvent s'afficher dans votre grille.

Si vous rencontrez des problèmes de synchronisation du temps, vérifiez que vous avez spécifié au moins quatre sources NTP externes, chacune fournissant une référence Stratum 3 ou supérieure, et que toutes les sources NTP externes fonctionnent normalement et sont accessibles par vos nœuds StorageGRID.

> Quand "Spécification de la source NTP externe" Pour une installation StorageGRID de niveau production, n'utilisez pas le service Windows Time (W32Time) sur une version de Windows antérieure à Windows Server 2016. Le service de temps des versions antérieures de Windows n'est pas suffisamment précis et n'est pas pris en charge par Microsoft pour une utilisation dans des environnements à haute précision, tels que StorageGRID.

Linux : problèmes de connectivité réseau

Il se peut que des problèmes de connectivité réseau existent pour les nœuds grid StorageGRID hébergés sur des hôtes Linux.

Clonage d'adresses MAC

Dans certains cas, les problèmes de réseau peuvent être résolus en utilisant le clonage d'adresses MAC. Si vous utilisez des hôtes virtuels, définissez la valeur de la clé de clonage d'adresse MAC de chacun de vos réseaux sur « true » dans le fichier de configuration de nœud. Ce paramètre entraîne l'utilisation de l'adresse

MAC du conteneur StorageGRID de l'hôte. Pour créer des fichiers de configuration de nœud, reportez-vous aux instructions de "Red Hat Enterprise Linux ou CentOS" ou "Ubuntu ou Debian".

> Créez des interfaces réseau virtuelles distinctes pour le système d'exploitation hôte Linux. L'utilisation des mêmes interfaces réseau pour le système d'exploitation hôte Linux et le conteneur StorageGRID peut rendre le système d'exploitation hôte inaccessible si le mode promiscuous n'a pas été activé sur l'hyperviseur.

Pour plus d'informations sur l'activation du clonage MAC, reportez-vous aux instructions de "Red Hat Enterprise Linux ou CentOS" ou "Ubuntu ou Debian".

Mode promiscueux

Si vous ne souhaitez pas utiliser le clonage d'adresses MAC et que vous préférez autoriser toutes les interfaces à recevoir et transmettre des données pour les adresses MAC autres que celles attribuées par l'hyperviseur, Assurez-vous que les propriétés de sécurité au niveau du commutateur virtuel et du groupe de ports sont définies sur **Accept** pour le mode promiscuous, les modifications d'adresse MAC et les transmissions forgées. Les valeurs définies sur le commutateur virtuel peuvent être remplacées par les valeurs au niveau du groupe de ports, de sorte que les paramètres soient les mêmes aux deux endroits.

Pour plus d'informations sur l'utilisation du mode promiscuous, reportez-vous aux instructions de "Red Hat Enterprise Linux ou CentOS" ou "Ubuntu ou Debian".

Linux : l'état du nœud est « orphelin »

Un nœud Linux à l'état orphelin indique généralement que le service StorageGRID ou le démon du nœud StorageGRID contrôlant le conteneur du nœud est décédé de façon inattendue.

Description de la tâche

Si un nœud Linux signale qu'il est dans un état orphelin, vous devez :

- Vérifiez les journaux à la recherche d'erreurs et de messages.
- Tentative de démarrage du nœud.
- Si nécessaire, utiliser des commandes moteur de conteneur pour arrêter le conteneur de nœuds existant.
- Redémarrez le nœud.

Étapes

1. Vérifiez les journaux du démon du service et du nœud orphelin pour voir si des erreurs évidentes et des messages relatifs à la fermeture inopinée.
2. Connectez-vous à l'hôte en tant que root ou en utilisant un compte avec l'autorisation sudo.
3. Tentative de démarrage du nœud à nouveau en exécutant la commande suivante : `$ sudo storagegrid node start node-name`

   ```
   $ sudo storagegrid node start DC1-S1-172-16-1-172
   ```

   Si le nœud est orphelin, la réponse est

   ```
   Not starting ORPHANED node DC1-S1-172-16-1-172
   ```

4. Depuis Linux, arrêtez le moteur de conteneur et tous les processus de nœud StorageGRID qui contrôlent. Par exemple :`sudo docker stop --time secondscontainer-name`

   Pour `seconds`, saisissez le nombre de secondes que vous souhaitez attendre l'arrêt du conteneur (généralement 15 minutes ou moins). Par exemple :

   ```
   sudo docker stop --time 900 storagegrid-DC1-S1-172-16-1-172
   ```

5. Redémarrez le nœud : `storagegrid node start node-name`

   ```
   storagegrid node start DC1-S1-172-16-1-172
   ```

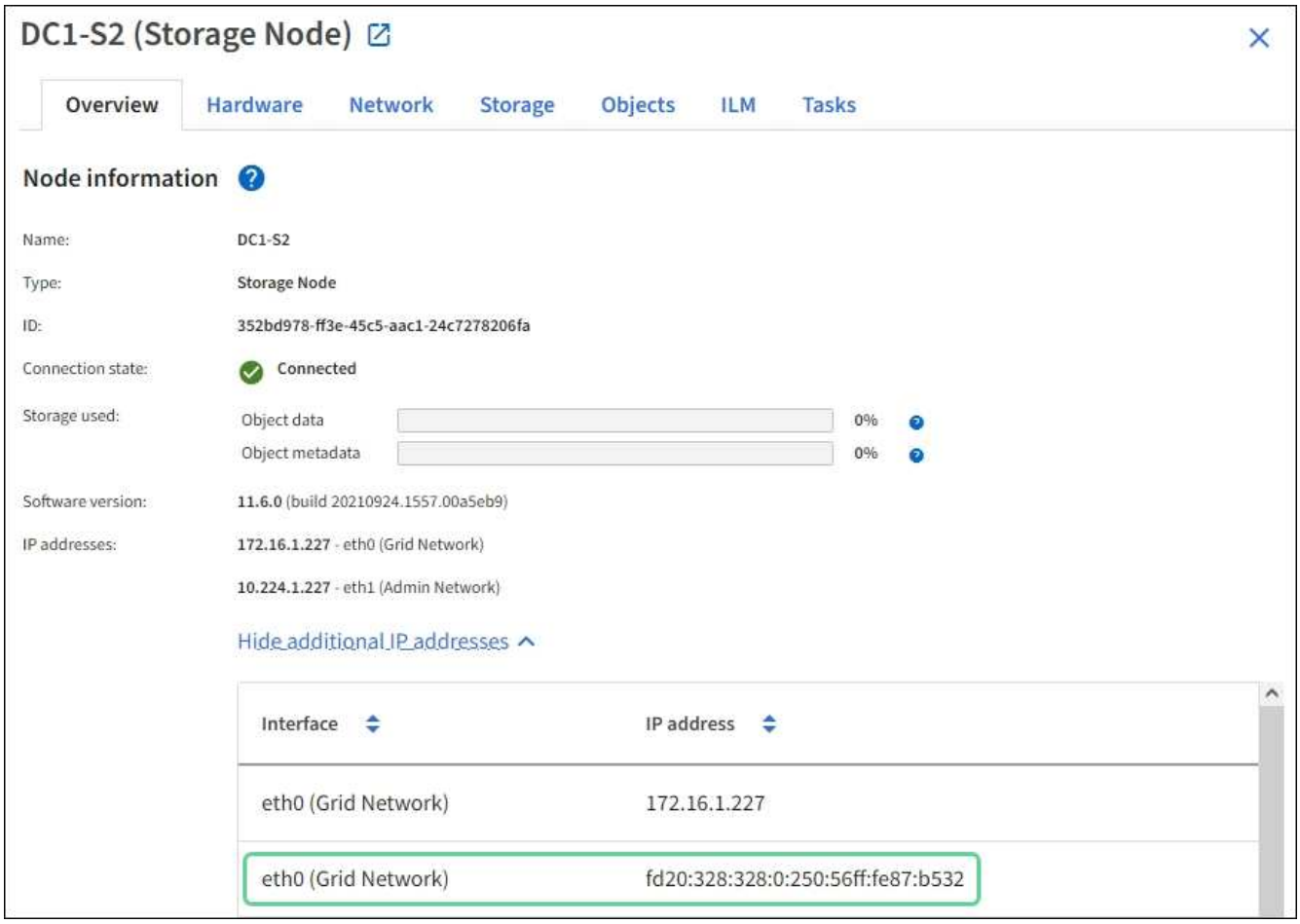
Linux : dépannage de la prise en charge IPv6

Vous devrez peut-être activer la prise en charge IPv6 dans le noyau si vous avez installé des nœuds StorageGRID sur des hôtes Linux et que vous remarquez que les adresses IPv6 n'ont pas été attribuées aux conteneurs de nœuds comme prévu.

Description de la tâche

L'adresse IPv6 attribuée à un nœud de grille s'affiche aux emplacements suivants dans Grid Manager :

- Sélectionnez **NOEUDS** et sélectionnez le noeud. Sélectionnez ensuite **Afficher plus** en regard de **adresses IP** dans l'onglet vue d'ensemble.



- Sélectionnez **SUPPORT** > **Outils** > **topologie de grille**. Sélectionnez ensuite ***node*** > **SSM** > **Ressources**. Si une adresse IPv6 a été attribuée, elle est répertoriée sous l'adresse IPv4 dans la section **adresses réseau**.

Si l'adresse IPv6 n'est pas affichée et que le nœud est installé sur un hôte Linux, procédez comme suit pour activer la prise en charge IPv6 dans le noyau.

Étapes

1. Connectez-vous à l'hôte en tant que root ou en utilisant un compte avec l'autorisation sudo.
2. Exécutez la commande suivante : `sysctl net.ipv6.conf.all.disable_ipv6`

```
root@SG:~ # sysctl net.ipv6.conf.all.disable_ipv6
```

Le résultat doit être 0.

```
net.ipv6.conf.all.disable_ipv6 = 0
```

Si le résultat n'est pas 0, reportez-vous à la documentation de votre système d'exploitation pour la modification `sysctl` paramètres. Ensuite, définissez la valeur sur 0 avant de continuer.

3. Saisissez le conteneur de nœuds StorageGRID : `storagegrid node enter node-name`
4. Exécutez la commande suivante : `sysctl net.ipv6.conf.all.disable_ipv6`

```
root@DC1-S1:~ # sysctl net.ipv6.conf.all.disable_ipv6
```

Le résultat doit être 1.

```
net.ipv6.conf.all.disable_ipv6 = 1
```

> Si le résultat n'est pas 1, cette procédure ne s'applique pas. Contactez l'assistance technique.

5. Quitter le conteneur : `exit`

```
root@DC1-S1:~ # exit
```

6. En tant que racine, modifiez le fichier suivant : `/var/lib/storagegrid/settings/sysctl.d/net.conf`.

```
sudo vi /var/lib/storagegrid/settings/sysctl.d/net.conf
```

7. Localisez les deux lignes suivantes et supprimez les balises de commentaire. Ensuite, enregistrez et fermez le fichier.

```
net.ipv6.conf.all.disable_ipv6 = 0
```

```
net.ipv6.conf.default.disable_ipv6 = 0
```

8. Exécutez ces commandes pour redémarrer le conteneur StorageGRID :

```
storagegrid node stop node-name
```

```
storagegrid node start node-name
```

Dépanner un serveur syslog externe

Le tableau suivant décrit les messages d'erreur du serveur syslog externe et répertorie

les actions correctives.

Message d'erreur	Description et actions recommandées
Impossible de résoudre le nom d'hôte	Le FQDN que vous avez saisi pour le serveur syslog n'a pas pu être résolu en adresse IP. 1. Vérifiez le nom d'hôte que vous avez saisi. Si vous avez saisi une adresse IP, assurez-vous qu'elle est valide en notation W.X.Y.Z (« décimale à points »). 2. Vérifier que les serveurs DNS sont configurés correctement. 3. Vérifiez que chaque nœud peut accéder aux adresses IP du serveur DNS.
Connexion refusée	Une connexion TCP ou TLS au serveur syslog a été refusée. Il se peut qu'il n'y ait pas d'écoute de service sur le port TCP ou TLS de l'hôte, ou qu'un pare-feu bloque l'accès. 1. Vérifiez que vous avez saisi le nom de domaine complet ou l'adresse IP, le port et le protocole corrects pour le serveur syslog. 2. Vérifiez que l'hôte du service syslog exécute un démon syslog écouté sur le port spécifié. 3. Vérifiez qu'un pare-feu ne bloque pas l'accès aux connexions TCP/TLS depuis les nœuds vers l'adresse IP et le port du serveur syslog.
Réseau inaccessible	Le serveur syslog ne se trouve pas sur un sous-réseau directement connecté. Un routeur a renvoyé un message d'échec ICMP pour indiquer qu'il n'a pas pu transférer les messages de test des nœuds répertoriés vers le serveur syslog. 1. Vérifiez que vous avez saisi le nom de domaine complet ou l'adresse IP correct pour le serveur syslog. 2. Pour chaque nœud répertorié, vérifiez la liste de sous-réseaux du réseau Grid, les listes de sous-réseaux des réseaux Admin et les passerelles réseau client. Confirmez que ces éléments sont configurés pour acheminer le trafic vers le serveur syslog via l'interface réseau et la passerelle prévues (grille, Admin ou client).
Hôte inaccessible	Le serveur syslog se trouve sur un sous-réseau directement connecté (sous-réseau utilisé par les nœuds répertoriés pour leurs adresses IP Grid, Admin ou client). Les nœuds ont tenté d'envoyer des messages de test, mais n'ont pas reçu de réponses aux requêtes ARP pour l'adresse MAC du serveur syslog. 1. Vérifiez que vous avez saisi le nom de domaine complet ou l'adresse IP correct pour le serveur syslog. 2. Vérifiez que l'hôte exécutant le service syslog est actif.

Message d’erreur	Description et actions recommandées
La connexion a expiré	Une tentative de connexion TCP/TLS a été effectuée, mais aucune réponse n’a été reçue depuis longtemps du serveur syslog. Il peut y avoir une mauvaise configuration de routage ou un pare-feu peut tomber du trafic sans envoyer de réponse (configuration commune). 1. Vérifiez que vous avez saisi le nom de domaine complet ou l’adresse IP correct pour le serveur syslog. 2. Pour chaque nœud répertorié, vérifiez la liste de sous-réseaux du réseau Grid, les listes de sous-réseaux des réseaux Admin et les passerelles réseau client. Vérifiez qu’ils sont configurés pour acheminer le trafic vers le serveur syslog à l’aide de l’interface réseau et de la passerelle (Grid, Admin ou client) sur lesquelles vous vous attendez à ce que le serveur syslog soit atteint. 3. Vérifiez qu’un pare-feu ne bloque pas l’accès aux connexions TCP/TLS à partir des nœuds répertoriés sur l’IP et le port du serveur syslog.
Connexion fermée par le partenaire	Une connexion TCP au serveur syslog a été établie avec succès, mais elle a été fermée ultérieurement. Plusieurs raisons peuvent expliquer ce phénomène : • Le serveur syslog a peut-être été redémarré ou redémarré. • Le nœud et le serveur syslog peuvent avoir des paramètres TCP/TLS différents. • Un pare-feu intermédiaire pourrait fermer les connexions TCP inactives. • Un serveur non syslog qui écoute sur le port du serveur syslog a peut-être fermé la connexion. a. Vérifiez que vous avez saisi le nom de domaine complet ou l’adresse IP, le port et le protocole corrects pour le serveur syslog. b. Si vous utilisez TLS, confirmez que le serveur syslog utilise également TLS. Si vous utilisez TCP, vérifiez que le serveur syslog utilise également TCP. c. Vérifiez qu’un pare-feu intermédiaire n’est pas configuré pour fermer les connexions TCP inactives.
Erreur de certificat TLS	Le certificat de serveur reçu du serveur syslog n’était pas compatible avec le bundle de certificats CA et le certificat client que vous avez fournis. 1. Vérifiez que le groupe de certificats de l’autorité de certification et le certificat client (le cas échéant) sont compatibles avec le certificat de serveur sur le serveur syslog. 2. Vérifiez que les identités du certificat de serveur du serveur syslog incluent les valeurs IP ou FQDN attendues.

Message d'erreur	Description et actions recommandées
Transfert suspendu	Les enregistrements syslog ne sont plus transférés vers le serveur syslog et StorageGRID ne peut pas détecter la raison. Examinez les journaux de débogage fournis avec cette erreur pour tenter de déterminer la cause principale.
Session TLS interrompue	Le serveur syslog a mis fin à la session TLS et StorageGRID ne parvient pas à détecter la raison. 1. Examinez les journaux de débogage fournis avec cette erreur pour tenter de déterminer la cause principale. 2. Vérifiez que vous avez saisi le nom de domaine complet ou l'adresse IP, le port et le protocole corrects pour le serveur syslog. 3. Si vous utilisez TLS, confirmez que le serveur syslog utilise également TLS. Si vous utilisez TCP, vérifiez que le serveur syslog utilise également TCP. 4. Vérifiez que le groupe de certificats de l'autorité de certification et le certificat client (le cas échéant) sont compatibles avec le certificat de serveur du serveur syslog. 5. Vérifiez que les identités du certificat de serveur du serveur syslog incluent les valeurs IP ou FQDN attendues.
Échec de la requête de résultats	Le nœud d'administration utilisé pour la configuration et le test du serveur syslog ne peut pas demander les résultats de test à partir des nœuds répertoriés. Un ou plusieurs nœuds sont peut-être en panne. 1. Suivez les étapes de dépannage standard pour vous assurer que les nœuds sont en ligne et que tous les services attendus sont en cours d'exécution. 2. Redémarrez le service ETCD sur les nœuds répertoriés.

Examiner les journaux d'audit

Examiner les journaux d'audit : présentation

Ces instructions contiennent des informations sur la structure et le contenu des messages d'audit StorageGRID et des journaux d'audit. Vous pouvez utiliser ces informations pour lire et analyser la piste d'audit de l'activité du système.

Ces instructions s'adresse aux administrateurs responsables de la production de rapports d'activité et d'utilisation du système qui nécessitent une analyse des messages d'audit du système StorageGRID.

Pour utiliser le fichier journal texte, vous devez avoir accès au partage d'audit configuré sur le nœud d'administration.

Pour plus d'informations sur la configuration des niveaux de messages d'audit et l'utilisation d'un serveur syslog externe, reportez-vous à la section "Configurez les messages d'audit et les destinations des journaux".

Flux et conservation des messages d'audit

Tous les services StorageGRID génèrent des messages d'audit pendant le fonctionnement normal du système. Vous devez comprendre comment ces messages d'audit passent du système StorageGRID au système `audit.log` fichier.

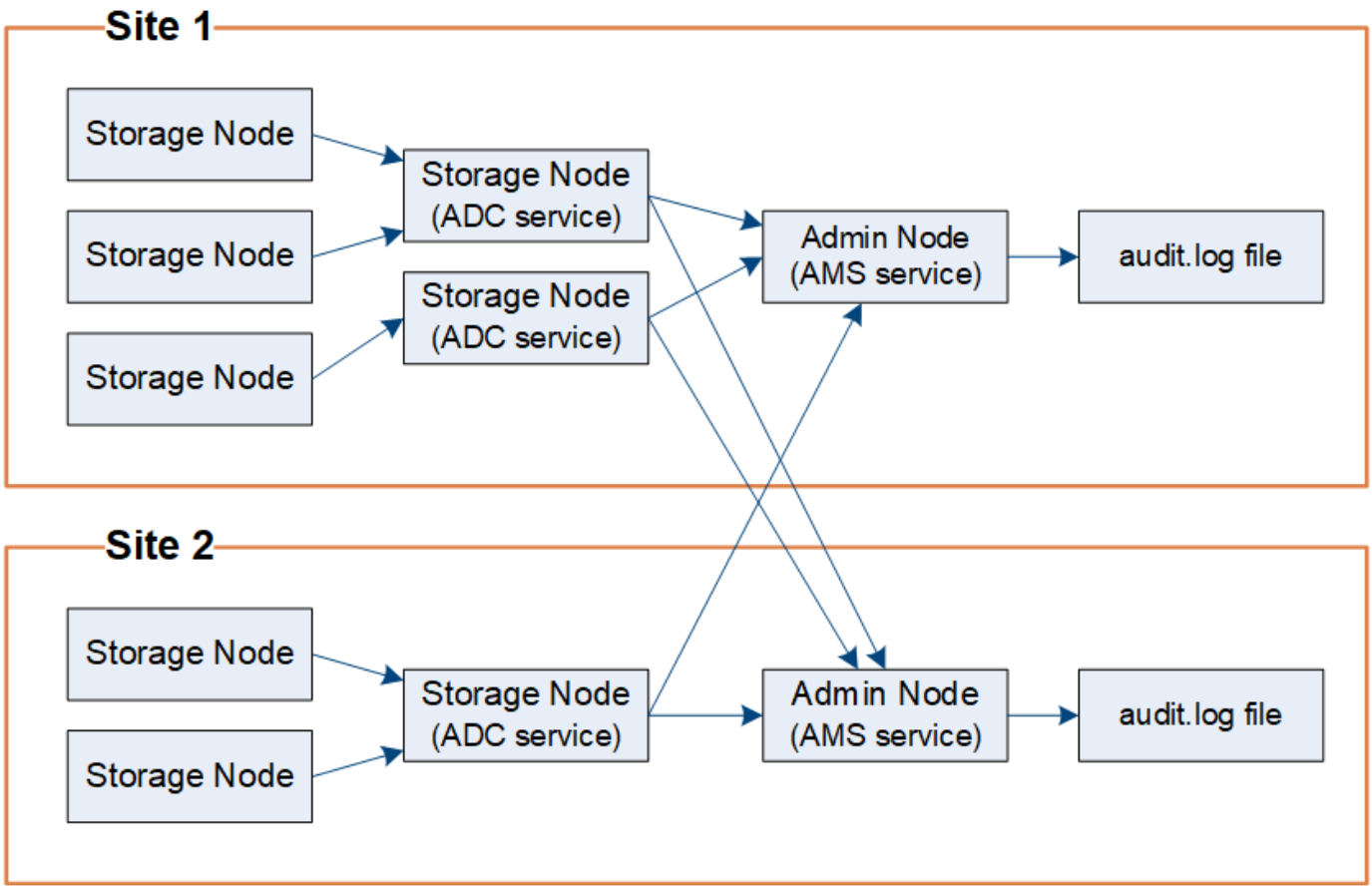
Flux de message d'audit

Les messages d'audit sont traités par des nœuds d'administration et par les nœuds de stockage disposant d'un service ADC (administrative Domain Controller).

Comme indiqué dans le schéma de flux des messages d'audit, chaque nœud StorageGRID envoie ses messages d'audit à l'un des services ADC du site du centre de données. Le service ADC est automatiquement activé pour les trois premiers nœuds de stockage installés sur chaque site.

De son tour, chaque service ADC agit comme un relais et envoie sa collection de messages d'audit à chaque nœud d'administration du système StorageGRID, ce qui donne à chaque nœud d'administration un enregistrement complet de l'activité du système.

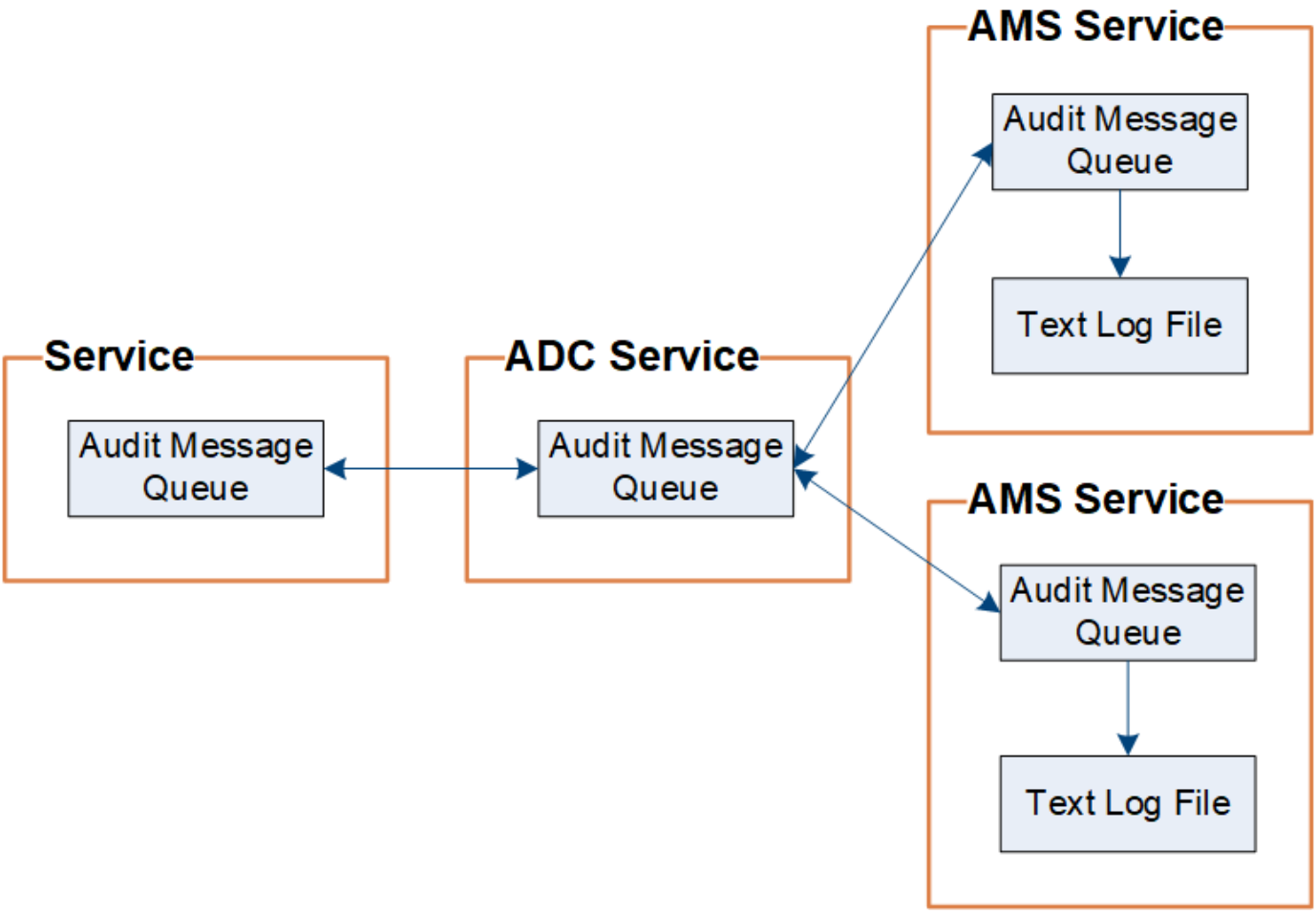
Chaque nœud d'administration stocke les messages d'audit dans des fichiers journaux texte ; le fichier journal actif est nommé `audit.log`.



Conservation des messages d'audit

StorageGRID utilise un processus de copie et de suppression pour garantir qu'aucun message d'audit ne soit perdu avant d'être écrit dans le journal d'audit.

Lorsqu'un nœud génère ou transmet un message d'audit, celui-ci est stocké dans une file d'attente de messages d'audit sur le disque système du nœud de la grille. Une copie du message est toujours conservée dans une file d'attente de messages d'audit jusqu'à ce que le message soit écrit dans le fichier journal d'audit du nœud d'administration `/var/local/audit/export` répertoire. Cela permet d'éviter la perte d'un message d'audit pendant le transport.



La file d'attente des messages d'audit peut augmenter temporairement en raison de problèmes de connectivité réseau ou d'une capacité d'audit insuffisante. Au fur et à mesure que les files d'attente augmentent, elles consomment davantage d'espace disponible dans chaque nœud `/var/local/` répertoire. Si le problème persiste et que le répertoire des messages d'audit d'un nœud devient trop plein, les nœuds individuels priorisent le traitement de leur carnet de commandes et deviennent temporairement indisponibles pour les nouveaux messages.

Plus précisément, vous pouvez voir les comportements suivants :

- Si le `/var/local/audit/export` Le répertoire utilisé par un nœud d'administration devient plein, le nœud d'administration sera signalé comme indisponible pour les nouveaux messages d'audit jusqu'à ce que le répertoire ne soit plus plein. Les demandes des clients S3 et Swift ne sont pas affectées. L'alarme XAMS (Unreable Audit Revers) est déclenchée lorsqu'un référentiel d'audit est inaccessible.
- Si le `/var/local/` Le répertoire utilisé par un nœud de stockage avec le service ADC devient plein à 92 %, le nœud sera signalé comme indisponible pour les messages d'audit jusqu'à ce que le répertoire soit plein à seulement 87 %. Les requêtes des clients S3 et Swift vers d'autres nœuds ne sont pas affectées. L'alarme NRLY (relais d'audit disponibles) est déclenchée lorsque les relais d'audit sont inaccessibles.

Si aucun nœud de stockage n'est disponible avec le service ADC, les nœuds de stockage stockent les messages d'audit localement dans le `/var/local/log/localaudit.log` fichier.

- Si le `/var/local/` Le répertoire utilisé par un nœud de stockage devient plein à 85 %. Le nœud refuse les demandes des clients S3 et Swift avec `503 Service Unavailable`.

Les types de problèmes suivants peuvent entraîner une augmentation très importante des files d'attente de messages d'audit :

- Panne d'un nœud d'administration ou d'un nœud de stockage avec le service ADC. Si l'un des nœuds du système est en panne, les nœuds restants peuvent devenir connectés à un nœud défaillant.
- Un taux d'activité soutenu qui dépasse la capacité d'audit du système.
- Le `/var/local/` L'espace sur un nœud de stockage ADC est saturé pour des raisons sans rapport avec les messages d'audit. Dans ce cas, le nœud n'accepte plus de nouveaux messages d'audit et hiérarchise son carnet de commandes actuel, ce qui peut entraîner des arriérés sur les autres nœuds.

Alerte de file d'attente d'audit et alarme de messages d'audit en file d'attente (AMQS)

Pour vous aider à surveiller la taille des files d'attente de messages d'audit dans le temps, l'alerte **grande file d'attente d'audit** et l'alarme AMQS héritée sont déclenchées lorsque le nombre de messages dans une file d'attente de nœud de stockage ou une file d'attente de nœud d'administration atteint certains seuils.

Si l'alerte **grande file d'attente d'audit** ou l'alarme AMQS héritée est déclenchée, commencez par vérifier la charge sur le système—s'il y a eu un nombre important de transactions récentes, l'alerte et l'alarme doivent être résolus au fil du temps et peuvent être ignorées.

Si l'alerte ou l'alarme persiste et augmente la gravité, affichez un graphique de la taille de la file d'attente. Si ce chiffre augmente régulièrement au fil des heures ou des jours, la charge d'audit a probablement dépassé la capacité d'audit du système. Réduisez le taux de fonctionnement du client ou diminuez le nombre de messages d'audit consignés en modifiant le niveau d'audit pour les écritures du client et les lectures du client sur erreur ou Désactivé. Voir "Configurez les messages d'audit et les destinations des journaux".

Dupliquer les messages

Le système StorageGRID adopte une approche prudente en cas de panne sur un réseau ou un nœud. Pour cette raison, des messages en double peuvent exister dans le journal d'audit.

Accéder au fichier journal d'audit

Le partage d'audit contient le partage actif `audit.log` fichier et tous les fichiers journaux d'audit compressés. Pour accéder facilement aux journaux d'audit, vous pouvez le faire "Configurer l'accès client d'audit pour NFS". Vous pouvez également accéder aux fichiers journaux d'audit directement à partir de la ligne de commande du nœud d'administration.

Avant de commencer

- Vous devez disposer d'autorisations d'accès spécifiques.
- Vous devez avoir le `Passwords.txt` fichier.
- Vous devez connaître l'adresse IP d'un nœud d'administration.

Étapes

1. Connectez-vous à un nœud d'administration :
   a. Saisissez la commande suivante : `ssh admin@primary_Admin_Node_IP`
   b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
   c. Entrez la commande suivante pour passer à la racine : `su -`
   d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

   Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

2. Accédez au répertoire contenant les fichiers journaux d'audit :

```
cd /var/local/audit/export
```

3. Afficher le fichier journal d'audit actuel ou enregistré, selon les besoins.

Rotation du fichier journal d'audit

Les fichiers journaux d'audit sont enregistrés sur un nœud d'administration `/var/local/audit/export` répertoire. Les fichiers journaux d'audit actifs sont nommés `audit.log`.

> Vous pouvez également modifier la destination des journaux d'audit et envoyer des informations d'audit à un serveur syslog externe. Les journaux locaux des enregistrements d'audit continuent à être générés et stockés lorsqu'un serveur syslog externe est configuré. Voir "Configurez les messages d'audit et les destinations des journaux".

Une fois par jour, le actif `audit.log` le fichier est enregistré et un nouveau `audit.log` le fichier est démarré. Le nom du fichier enregistré indique quand il a été enregistré, au format *`yyyy-mm-dd.txt`*. Si plusieurs journaux d'audit sont créés dans un seul jour, les noms de fichiers utilisent la date d'enregistrement du fichier, ajoutée par un nombre, dans le format *`yyyy-mm-dd.txt.n`*. Par exemple : `2018-04-15.txt` et `2018-04-15.txt.1` Sont les premier et deuxième fichiers journaux créés et enregistrés le 15 avril 2018.

Après un jour, le fichier enregistré est compressé et renommé, au format *`yyyy-mm-dd.txt.gz`*, qui conserve la date originale. Avec le temps, cela entraîne la consommation du stockage alloué aux journaux d'audit sur le nœud d'administration. Un script surveille la consommation d'espace du journal d'audit et supprime les fichiers journaux si nécessaire pour libérer de l'espace dans le `/var/local/audit/export` répertoire. Les journaux d'audit sont supprimés en fonction de la date de création, le plus ancien étant supprimé en premier. Vous pouvez contrôler les actions du script dans le fichier suivant : `/var/local/log/manage-audit.log`.

Cet exemple montre l'actif `audit.log` fichier du jour précédent (`2018-04-15.txt`), et le fichier compressé pour la veille (`2018-04-14.txt.gz`).

```
audit.log
2018-04-15.txt
2018-04-14.txt.gz
```

Format du fichier journal d'audit

Format du fichier journal d'audit : présentation

Les fichiers journaux d'audit se trouvent sur chaque nœud d'administration et contiennent un ensemble de messages d'audit individuels.

Chaque message d'audit contient les éléments suivants :

- Temps universel coordonné (UTC) de l'événement qui a déclenché le message d'audit (ATIM) au format ISO 8601, suivi d'un espace :

  YYYY-MM-DDTHH:MM:SS.UUUUUU, où *UUUUUU* sont des microsecondes.

- Le message d'audit lui-même, entre crochets et commençant par `AUDT`.

L'exemple suivant montre trois messages d'audit dans un fichier journal d'audit (sauts de ligne ajoutés pour la lisibilité). Ces messages ont été générés lorsqu'un locataire a créé un compartiment S3 et a ajouté deux objets dans ce compartiment.

```
2019-08-07T18:43:30.247711
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991681][TIME(UI64):73520][SAI
P(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::175300642415970547
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][AVER(UI32):10][ATIM(UI64):1565203410247711]
[ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(FC32):S3RQ][ATID(UI64):7074142
142472611085]]

2019-08-07T18:43:30.783597
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991696][TIME(UI64):120713][SA
IP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::175300642415970547
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][S3KY(CSTR):"fh-small-0"]
[CBID(UI64):0x779557A069B2C037][UUID(CSTR):"94BA6949-38E1-4B0C-BC80-
EB44FB4FCC7F"][CSIZ(UI64):1024][AVER(UI32):10]
[ATIM(UI64):1565203410783597][ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(F
C32):S3RQ][ATID(UI64):8439606722108456022]]

2019-08-07T18:43:30.784558
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991693][TIME(UI64):121666][SA
IP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::175300642415970547
18:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"buc
ket1"][S3KY(CSTR):"fh-small-2000"]
[CBID(UI64):0x180CBD8E678EED17][UUID(CSTR):"19CE06D0-D2CF-4B03-9C38-
E578D66F7ADD"][CSIZ(UI64):1024][AVER(UI32):10]
[ATIM(UI64):1565203410784558][ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(F
C32):S3RQ][ATID(UI64):13489590586043706682]]
```

Dans leur format par défaut, les messages d'audit dans les fichiers journaux d'audit ne sont pas faciles à lire ou à interpréter. Vous pouvez utiliser le "outil d'audit-explication" pour obtenir des résumés simplifiés des messages d'audit dans le journal d'audit. Vous pouvez utiliser le "outil de somme d'audit" récapituler le nombre d'opérations d'écriture, de lecture et de suppression consignées et le temps passé par ces opérations.

Utiliser l'outil d'explication d'audit

Vous pouvez utiliser le `audit-explain` outil permettant de traduire les messages d'audit dans le journal d'audit dans un format facile à lire.

Avant de commencer

- Vous devez disposer d'autorisations d'accès spécifiques.
- Vous devez avoir le `Passwords.txt` fichier.
- Vous devez connaître l'adresse IP du nœud d'administration principal.

Description de la tâche

Le `audit-explain` Disponible sur le nœud d'administration principal, cet outil fournit des résumés simplifiés des messages d'audit dans un journal d'audit.

> Le `audit-explain` l'outil est principalement destiné au support technique lors des opérations de dépannage. En cours de traitement `audit-explain` Les requêtes peuvent consommer une très grande quantité d'énergie dans le processeur, ce qui peut affecter les opérations de StorageGRID.

Cet exemple montre une sortie type de l' `audit-explain` outil. Ces quatre "SPUT" Des messages d'audit ont été générés lorsque le locataire S3 associé à l'ID de compte 92484777680322627870 a utilisé des demandes PUT S3 pour créer un compartiment nommé « bucket1 » et ajouter trois objets à ce compartiment.

```
SPUT S3 PUT bucket bucket1 account:92484777680322627870 usec:124673
SPUT S3 PUT object bucket1/part1.txt tenant:92484777680322627870
cbid:9DCB157394F99FE5 usec:101485
SPUT S3 PUT object bucket1/part2.txt tenant:92484777680322627870
cbid:3CFBB07AB3D32CA9 usec:102804
SPUT S3 PUT object bucket1/part3.txt tenant:92484777680322627870
cbid:5373D73831ECC743 usec:93874
```

Le `audit-explain` l'outil peut effectuer les opérations suivantes :

- Traiter les journaux d'audit bruts ou compressés. Par exemple :

  ```
  audit-explain audit.log

  audit-explain 2019-08-12.txt.gz
  ```

- Traitez plusieurs fichiers simultanément. Par exemple :

  ```
  audit-explain audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz

  audit-explain /var/local/audit/export/*
  ```

- Accepter l'entrée d'un tuyau, ce qui vous permet de filtrer et de prétraiter l'entrée à l'aide du `grep` commande ou autre moyen. Par exemple :

  ```
  grep SPUT audit.log | audit-explain

  grep bucket-name audit.log | audit-explain
  ```

Les journaux d'audit pouvant être très volumineux et lents à analyser, vous gagnez du temps en filtrant les

parties que vous souhaitez examiner et en cours d'exécution `audit-explain` sur les pièces, au lieu du fichier entier.

> Le `audit-explain` l'outil n'accepte pas les fichiers compressés comme entrée de canalisation. Pour traiter des fichiers compressés, indiquez leurs noms de fichier comme arguments de ligne de commande ou utilisez le `zcat` outil de décompression des fichiers en premier. Par exemple :
>
> ```
> zcat audit.log.gz | audit-explain
> ```

Utilisez le `help (-h)` pour voir les options disponibles. Par exemple :

```
$ audit-explain -h
```

Étapes

1. Connectez-vous au nœud d'administration principal :
   a. Saisissez la commande suivante : `ssh admin@primary_Admin_Node_IP`
   b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
   c. Entrez la commande suivante pour passer à la racine : `su -`
   d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

   Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

2. Entrez la commande suivante, où `/var/local/audit/export/audit.log` représente le nom et l'emplacement du ou des fichiers à analyser :

   ```
   $ audit-explain /var/local/audit/export/audit.log
   ```

   Le `audit-explain` l'outil imprime les interprétations lisibles par l'homme de tous les messages du ou des fichiers spécifiés.

   > Pour réduire la longueur des lignes et faciliter la lisibilité, les horodatages ne sont pas affichés par défaut. Si vous voulez voir les horodatages, utilisez l'horodatage (`-t`) option.

Utiliser l'outil audit-sum

Vous pouvez utiliser le `audit-sum` outil permettant de compter les messages d'audit d'écriture, de lecture, d'en-tête et de suppression, ainsi que les temps minimum, maximum et moyen (ou taille) pour chaque type d'opération.

Avant de commencer

- Vous devez disposer d'autorisations d'accès spécifiques.
- Vous devez avoir le `Passwords.txt` fichier.
- Vous devez connaître l'adresse IP du nœud d'administration principal.

Description de la tâche

Le `audit-sum` Disponible sur le nœud d'administration principal, cet outil récapitule le nombre d'opérations

d'écriture, de lecture et de suppression enregistrées et la durée de ces opérations.

> Le `audit-sum` l'outil est principalement destiné au support technique lors des opérations de dépannage. En cours de traitement `audit-sum` Les requêtes peuvent consommer une très grande quantité d'énergie dans le processeur, ce qui peut affecter les opérations de StorageGRID.

Cet exemple montre une sortie type de l' `audit-sum` outil. Cet exemple montre la durée des opérations de protocoles.

```
  message group            count     min(sec)        max(sec)
average(sec)
  =============            =====     ========        ========
============
  IDEL                       274
  SDEL                    213371        0.004          20.934
0.352
  SGET                    201906        0.010        1740.290
1.132
  SHEA                     22716        0.005           2.349
0.272
  SPUT                   1771398        0.011        1770.563
0.487
```

Le `audit-sum` Dans un journal d'audit, l'outil indique le nombre et la durée des messages d'audit S3, Swift et ILM suivants :

Code	Description	Reportez-vous à la section
ARCT	Archivage depuis le Tier cloud	"ARCT : récupération d'archives depuis Cloud-Tier"
ASCT	Tier cloud du magasin d'archivage	"ASCT : magasin d'archives, niveau du cloud"
IDEL	ILM initialisée – journaux lorsque l'ILM démarre le processus de suppression d'un objet.	"IDEL : suppression initiée ILM"
SDEL	SUPPRESSION S3 : journal une transaction réussie pour supprimer un objet ou un compartiment.	"SDEL : SUPPRESSION S3"
SGET	S3 GET : log une transaction réussie pour récupérer un objet ou répertorier les objets dans un compartiment.	"SGET : OBTENEZ S3"

Code	Description	Reportez-vous à la section
SHEA	TÊTE S3 : consigne une transaction réussie pour vérifier l'existence d'un objet ou d'un compartiment.	"SHEA : TÊTE S3"
SPUT	S3 PUT : enregistre la réussite d'une transaction pour créer un nouvel objet ou un compartiment.	"SPUT : PUT S3"
WDEL	SUPPRESSION Swift : enregistre une transaction réussie pour supprimer un objet ou un conteneur.	"WDEL : SUPPRESSION rapide"
C'EST PARTI	SWIFT GET : log une transaction réussie pour récupérer un objet ou répertorier les objets dans un conteneur.	"WGET: SWIFT GET"
WHEA	SWIFT HEAD : consigne une transaction réussie afin de vérifier l'existence d'un objet ou d'un conteneur.	"WHEA: TÊTE SWIFT"
WPUT	SWIFT PUT : consigne une transaction réussie pour créer un nouvel objet ou conteneur.	"WPUT : PUT SWIFT"

Le `audit-sum` l'outil peut effectuer les opérations suivantes :

- Traiter les journaux d'audit bruts ou compressés. Par exemple :

```
audit-sum audit.log

audit-sum 2019-08-12.txt.gz
```

- Traitez plusieurs fichiers simultanément. Par exemple :

```
audit-sum audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz

audit-sum /var/local/audit/export/*
```

- Accepter l'entrée d'un tuyau, ce qui vous permet de filtrer et de prétraiter l'entrée à l'aide du `grep` commande ou autre moyen. Par exemple :

```
grep WGET audit.log | audit-sum

grep bucket1 audit.log | audit-sum

grep SPUT audit.log | grep bucket1 | audit-sum
```

Cet outil n'accepte pas les fichiers compressés comme entrée de pipettes. Pour traiter des fichiers compressés, indiquez leurs noms de fichier comme arguments de ligne de commande ou utilisez le `zcat` outil de décompression des fichiers en premier. Par exemple :

```
audit-sum audit.log.gz

zcat audit.log.gz | audit-sum
```

Vous pouvez utiliser les options de ligne de commande pour résumer les opérations sur des compartiments séparément des opérations sur des objets ou pour regrouper les résumés de messages par nom de compartiment, par période ou par type de cible. Par défaut, les résumés indiquent le temps de fonctionnement minimum, maximum et moyen, mais vous pouvez utiliser le `size (-s)` option pour regarder la taille de l'objet.

Utilisez le `help (-h)` pour voir les options disponibles. Par exemple :

```
$ audit-sum -h
```

Étapes

1. Connectez-vous au nœud d'administration principal :
   a. Saisissez la commande suivante : `ssh admin@`*`primary_Admin_Node_IP`*
   b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
   c. Entrez la commande suivante pour passer à la racine : `su -`
   d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

      Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

2. Pour analyser tous les messages liés aux opérations d'écriture, de lecture, de tête et de suppression, procédez comme suit :
   a. Entrez la commande suivante, où `/var/local/audit/export/audit.log` représente le nom et l'emplacement du ou des fichiers à analyser :

      ```
      $ audit-sum /var/local/audit/export/audit.log
      ```

      Cet exemple montre une sortie type de l' `audit-sum` outil. Cet exemple montre la durée des opérations de protocoles.

```
  message group           count     min(sec)        max(sec)
average(sec)
  =============           =====     ========        ========
============
  IDEL                      274
  SDEL                   213371        0.004          20.934
0.352
  SGET                   201906        0.010        1740.290
1.132
  SHEA                    22716        0.005           2.349
0.272
  SPUT                  1771398        0.011        1770.563
0.487
```

Dans cet exemple, les opérations SGET (S3 GET) sont les opérations les plus lentes en moyenne à 1.13 secondes, mais les opérations SGET et SPUT (S3 PUT) affichent toutes les deux de longues périodes de pire des cas d'environ 1,770 secondes.

b. Pour afficher les opérations de récupération 10 les plus lentes, utilisez la commande grep pour sélectionner uniquement les messages SGET et ajouter l'option de sortie longue (`-l`) pour inclure les chemins d'accès aux objets :

```
grep SGET audit.log | audit-sum -l
```

Les résultats incluent le type (objet ou compartiment) et le chemin, ce qui vous permet d'afficher le journal d'audit pour les autres messages relatifs à ces objets particuliers.

```
Total:          201906 operations
    Slowest:      1740.290 sec
    Average:         1.132 sec
    Fastest:         0.010 sec
    Slowest operations:
        time(usec)       source ip         type      size(B) path
        ========== ============== ============ ============ ====
        1740289662   10.96.101.125       object   5663711385
backup/r9O1OaQ8JB-1566861764-4519.iso
        1624414429   10.96.101.125       object   5375001556
backup/r9O1OaQ8JB-1566861764-6618.iso
        1533143793   10.96.101.125       object   5183661466
backup/r9O1OaQ8JB-1566861764-4518.iso
             70839   10.96.101.125       object        28338
bucket3/dat.1566861764-6619
             68487   10.96.101.125       object        27890
bucket3/dat.1566861764-6615
             67798   10.96.101.125       object        27671
bucket5/dat.1566861764-6617
             67027   10.96.101.125       object        27230
bucket5/dat.1566861764-4517
             60922   10.96.101.125       object        26118
bucket3/dat.1566861764-4520
             35588   10.96.101.125       object        11311
bucket3/dat.1566861764-6616
             23897   10.96.101.125       object        10692
bucket3/dat.1566861764-4516
```

+
Dans cet exemple de sortie, vous pouvez constater que les trois demandes GET S3 les plus lentes étaient celles des objets d'une taille d'environ 5 Go (ce qui est beaucoup plus important que les autres objets). La grande taille tient compte des délais de récupération lents les moins importants.

3. Pour déterminer la taille des objets en cours d'ingestion et d'extraction à partir de votre grille, utilisez l'option size (`-s`) :

   ```
   audit-sum -s audit.log
   ```

```
  message group           count       min(MB)          max(MB)
average(MB)
  =============           =====     ========        ========
============
  IDEL                      274        0.004        5000.000
1654.502
  SDEL                   213371        0.000          10.504
1.695
  SGET                   201906        0.000        5000.000
14.920
  SHEA                    22716        0.001          10.504
2.967
  SPUT                 1771398        0.000        5000.000
2.495
```

Dans cet exemple, la taille moyenne des objets pour SPUT est inférieure à 2.5 Mo, mais la taille moyenne pour SGET est beaucoup plus grande. Le nombre de messages SPUT est beaucoup plus élevé que le nombre de messages SGET, ce qui indique que la plupart des objets ne sont jamais récupérés.

4. Si vous voulez déterminer si les récupérations étaient lentes hier :

   a. Exécutez la commande sur le journal d'audit approprié et utilisez l'option group-by-time (`-gt`), suivi de la période (par exemple, 15M, 1H, 10S) :

      ```
      grep SGET audit.log | audit-sum -gt 1H
      ```

```
  message group           count    min(sec)       max(sec)
average(sec)
  =============           =====     ========        ========
============
  2019-09-05T00            7591        0.010        1481.867
1.254
  2019-09-05T01            4173        0.011        1740.290
1.115
  2019-09-05T02           20142        0.011        1274.961
1.562
  2019-09-05T03           57591        0.010        1383.867
1.254
  2019-09-05T04          124171        0.013        1740.290
1.405
  2019-09-05T05          420182        0.021        1274.511
1.562
  2019-09-05T06         1220371        0.015        6274.961
5.562
  2019-09-05T07          527142        0.011        1974.228
2.002
  2019-09-05T08          384173        0.012        1740.290
1.105
  2019-09-05T09           27591        0.010        1481.867
1.354
```

Ces résultats montrent que S3 GÉNÈRE un trafic entre 06:00 et 07:00. Les temps maximum et moyen sont à la fois considérablement plus élevés à ces moments aussi, et ils n'ont pas augmenté progressivement à mesure que le comptage a augmenté. Cela suggère que la capacité a été dépassée quelque part, peut-être dans le réseau ou que la grille peut traiter les demandes.

b. Pour déterminer la taille des objets récupérés chaque heure hier, ajoutez l'option size (`-s`) à la commande :

```
grep SGET audit.log | audit-sum -gt 1H -s
```

```
  message group           count       min(B)          max(B)
average(B)
  =============           =====     ========        ========
============
  2019-09-05T00            7591        0.040        1481.867
1.976
  2019-09-05T01            4173        0.043        1740.290
2.062
  2019-09-05T02           20142        0.083        1274.961
2.303
  2019-09-05T03           57591        0.912        1383.867
1.182
  2019-09-05T04          124171        0.730        1740.290
1.528
  2019-09-05T05          420182        0.875        4274.511
2.398
  2019-09-05T06         1220371        0.691  5663711385.961
51.328
  2019-09-05T07          527142        0.130        1974.228
2.147
  2019-09-05T08          384173        0.625        1740.290
1.878
  2019-09-05T09           27591        0.689        1481.867
1.354
```

Ces résultats indiquent que des récupérations très importantes se sont produites lorsque le trafic global de récupération était à son maximum.

c. Pour plus de détails, utilisez le "outil d'audit-explication" Pour revoir toutes les opérations de SGET pendant cette heure :

```
grep 2019-09-05T06 audit.log | grep SGET | audit-explain | less
```

Si la sortie de la commande grep est censée être de nombreuses lignes, ajoutez le `less` commande pour afficher le contenu du fichier journal d'audit une page (un écran) à la fois.

5. Si vous souhaitez déterminer si les opérations SPUT sur les godets sont plus lentes que les opérations SPUT pour les objets :

a. Commencez par utiliser le `-go` option, qui regroupe les messages pour les opérations liées aux objets et aux compartiments séparément :

```
grep SPUT sample.log | audit-sum -go
```

```
  message group           count     min(sec)        max(sec)
average(sec)
  =============           =====     ========        ========
============
  SPUT.bucket                 1        0.125           0.125
0.125
  SPUT.object                12        0.025           1.019
0.236
```

Les résultats montrent que les opérations SPUT pour les compartiments ont des caractéristiques de performances différentes de celles des opérations SPUT pour les objets.

b. Pour déterminer les godets dont les opérations SPUT sont les plus lentes, utiliser le `-gb` option, qui regroupe les messages par compartiment :

```
grep SPUT audit.log | audit-sum -gb
```

```
  message group                  count     min(sec)        max(sec)
average(sec)
  =============                  =====     ========        ========
============
  SPUT.cho-non-versioning        71943        0.046        1770.563
1.571
  SPUT.cho-versioning            54277        0.047        1736.633
1.415
  SPUT.cho-west-region           80615        0.040          55.557
1.329
  SPUT.ldt002                  1564563        0.011          51.569
0.361
```

c. Pour déterminer quels compartiments ont la plus grande taille d'objet SPUT, utilisez les deux `-gb` et le `-s` options :

```
grep SPUT audit.log | audit-sum -gb -s
```

```
  message group                  count       min(B)          max(B)
average(B)
  =============                  =====     ========        ========
============
  SPUT.cho-non-versioning        71943        2.097        5000.000
21.672
  SPUT.cho-versioning            54277        2.097        5000.000
21.120
  SPUT.cho-west-region           80615        2.097         800.000
14.433
  SPUT.ldt002                  1564563        0.000         999.972
0.352
```

Format du message d'audit

Format du message d'audit : présentation

Les messages d'audit échangés dans le système StorageGRID incluent des informations standard communes à tous les messages et du contenu spécifique décrivant l'événement ou l'activité signalé.

Si le résumé fourni par le "audit - expliquer" et "somme-audit" les outils sont insuffisants, reportez-vous à cette section pour comprendre le format général de tous les messages de vérification.

Voici un exemple de message d'audit tel qu'il peut apparaître dans le fichier journal d'audit :

```
2014-07-17T03:50:47.484627
[AUDT:[RSLT(FC32):VRGN][AVER(UI32):10][ATIM(UI64):1405569047484627][ATYP(F
C32):SYSU][ANID(UI32):11627225][AMID(FC32):ARNI][ATID(UI64):94457363265006
03516]]
```

Chaque message d'audit contient une chaîne d'éléments d'attribut. L'ensemble de la chaîne est entre crochets (`[ ]`), et chaque élément d'attribut de la chaîne possède les caractéristiques suivantes :

- Entre crochets `[ ]`
- Introduit par la chaîne `AUDT`, qui indique un message d'audit
- Sans délimiteurs (pas de virgules ni d'espaces) avant ou après
- Terminé par un caractère de flux de ligne `\n`

Chaque élément inclut un code d'attribut, un type de données et une valeur qui sont rapportées dans ce format :

```
[ATTR(type):value][ATTR(type):value]...
[ATTR(type):value]\n
```

Le nombre d'éléments d'attribut dans le message dépend du type d'événement du message. Les éléments d'attribut ne sont pas répertoriés dans un ordre particulier.

La liste suivante décrit les éléments d'attribut :

- `ATTR` est un code à quatre caractères pour l'attribut en cours de signalement. Certains attributs sont communs à tous les messages d'audit et à d'autres, qui sont spécifiques à un événement.
- `type` Est un identificateur à quatre caractères du type de données de programmation de la valeur, comme UI64, FC32, etc. Le type est entre parenthèses `( )`.
- `value` est le contenu de l'attribut, généralement une valeur numérique ou de texte. Les valeurs suivent toujours deux-points (`:`). Les valeurs du type de données CSTR sont entourées de guillemets doubles `" "`.

Types de données

Différents types de données sont utilisés pour stocker les informations dans les messages d'audit.

Type	Description
UI32	Entier long non signé (32 bits) ; il peut stocker les nombres 0 à 4,294,967,295.
UI64	Entier double non signé (64 bits) ; il peut stocker les nombres 0 à 18,446,744,073,709,551,615.
FC32	Constante de quatre caractères ; valeur entière non signée de 32 bits représentée par quatre caractères ASCII tels que « ABCD ».
IPAD	Utilisé pour les adresses IP.
REST	Tableau de caractères UTF-8 de longueur variable. Les caractères peuvent être échappé avec les conventions suivantes : • La barre oblique inverse est \\. • Le retour chariot est \r. • Les guillemets sont \". • La ligne d'alimentation (nouvelle ligne) est \n. • Les caractères peuvent être remplacés par leurs équivalents hexadécimaux (au format \XHH, où HH est la valeur hexadécimale représentant le caractère).

Données spécifiques à un événement

Chaque message d'audit du journal d'audit enregistre les données spécifiques à un

événement système.

Après l'ouverture `[AUDT:` conteneur qui identifie le message lui-même, l'ensemble d'attributs suivant fournit des informations sur l'événement ou l'action décrit par le message d'audit. Ces attributs sont mis en évidence dans l'exemple suivant :

2018-12-05T08:24 10.224.0 600256215956112464 99:45.921845 100 6002562159561124649 9 [AUDT:*\[RSLT\(FC32\):SUCS\] **\[TIME\(UI64\):11454\]\[SAIP\(IPAD\)\[S3AI(CSTR\\)(CSTR\\\ 6002562159561124649 9\« STU3S\\ »\« STC\ »\« STC\ »\[STC\ » :\[S6S]\[STC\[STC\[STC**\\« STC\ » :\[STE]\[STC\[STC\[STC\[STE]\[STC*\[STC\[STC\[STC\[STC*\[STC\« S]\ » :\[STC\« STE\ » :\[STC\« STE\ » :\[STE\« S\ » :\[STE\ »\ » :\[STE\[S3S\ » :*\[STC\[STC\[STC\[S37 30720 10 1543998285921845 12281045 15552417629170647261

Le `ATYP` elément (souligné dans l'exemple) identifie l'événement qui a généré le message. Cet exemple de message inclut le "SHEA" Code de message ([ATYP(FC32):SHEA]), indiquant qu'il a été généré par une demande S3 HEAD réussie.

Éléments communs dans les messages d'audit

Tous les messages d'audit contiennent les éléments communs.

Code	Type	Description
AU MILIEU	FC32	ID de module : identificateur à quatre caractères de l'ID de module qui a généré le message. Ceci indique le segment de code dans lequel le message d'audit a été généré.
ANID	UI32	ID de nœud : ID de nœud de la grille attribué au service qui a généré le message. Un identifiant unique est attribué à chaque service au moment de la configuration et de l'installation du système StorageGRID. Cet ID ne peut pas être modifié.
ASE	UI64	Identifiant de session d'audit : dans les versions précédentes, cet élément indique l'heure à laquelle le système d'audit a été initialisé après le démarrage du service. Cette valeur temporelle a été mesurée en microsecondes depuis l'époque du système d'exploitation (00:00:00 UTC le 1er janvier 1970). **Remarque :** cet élément est obsolète et n'apparaît plus dans les messages d'audit.
ASQN	UI64	Nombre de séquences : dans les versions précédentes, ce compteur a été incrémenté pour chaque message d'audit généré sur le nœud de la grille (ANID) et remis à zéro au redémarrage du service. **Remarque :** cet élément est obsolète et n'apparaît plus dans les messages d'audit.
ATID	UI64	Trace ID : identifiant partagé par l'ensemble de messages déclenchés par un seul événement.

Code	Type	Description
ATIM	UI64	Timestamp: Heure à laquelle l'événement a été généré le message d'audit, mesuré en microsecondes depuis l'époque du système d'exploitation (00:00:00 UTC le 1er janvier 1970). Notez que la plupart des outils disponibles pour convertir l'horodatage en date et heure locales sont basés sur des millisecondes. Il peut être nécessaire d'arrondir ou de tronquer l'horodatage enregistré. Temps lisible par l'utilisateur qui apparaît au début du message d'audit dans le `audit.log` Fichier est l'attribut ATIM au format ISO 8601. La date et l'heure sont représentées sous la forme *`YYYY-MMDDTHH:MM:SS.UUUUUU`*, où `T` est un caractère de chaîne littérale indiquant le début du segment de temps de la date. *`UUUUUU`* sont des microsecondes.
ATYP	FC32	Type d'événement : identificateur à quatre caractères de l'événement en cours de consignation. Cela régit le contenu « charge utile » du message : les attributs inclus.
FINISSEUR	UI32	Version : version du message d'audit. À mesure que le logiciel StorageGRID évolue, les nouvelles versions de services peuvent intégrer de nouvelles fonctionnalités dans les rapports d'audit. Ce champ permet une rétrocompatibilité dans le service AMS pour traiter les messages provenant de versions antérieures de services.
RSLT	FC32	Résultat : résultat de l'événement, du processus ou de la transaction. Si n'est pas pertinent pour un message, AUCUN n'est utilisé plutôt que LES CMC pour que le message ne soit pas filtré accidentellement.

Exemples de messages d'audit

Vous trouverez des informations détaillées dans chaque message d'audit. Tous les messages d'audit utilisent le même format.

Voici un exemple de message d'audit tel qu'il peut apparaître dans le `audit.log` fichier :

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small1"][S3K
Y(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):0
][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP(FC32):SPUT
][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):1579224144
102530435]]
```

Le message d'audit contient des informations sur l'événement en cours d'enregistrement, ainsi que des informations sur le message d'audit lui-même.

Pour identifier l'événement enregistré par le message d'audit, recherchez l'attribut ATYP (mis en évidence ci-dessous) :

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small1"][S3K
Y(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):0
][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP(FC32):SP
UT][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):1579224
144102530435]]
```

La valeur de l'attribut ATYP est SPUT. "SPUT" Représente une transaction PUT S3, qui consigne l'ingestion d'un objet dans un compartiment.

Le message d'audit suivant indique également le compartiment à partir duquel l'objet est associé :

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK\(CSTR\):"s3small1"][S3
KY(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):
0][AVER(UI32):10][ATIM(UI64):1405631878959669][ATYP(FC32):SPU
T][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):157922414
4102530435]]
```

Pour savoir quand l'événement PUT s'est produit, notez l'horodatage universel coordonné (UTC) au début du message d'audit. Cette valeur est une version lisible par l'utilisateur de l'attribut ATIM du message d'audit lui-même :

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small1"][S3K
Y(CSTR):"hello1"][CBID(UI64):0x50C4F7AC2BC8EDF7][CSIZ(UI64):0
][AVER(UI32):10][ATIM\(UI64\):1405631878959669][ATYP(FC32):SP
UT][ANID(UI32):12872812][AMID(FC32):S3RQ][ATID(UI64):15792241
44102530435]]
```

ATIM enregistre le temps, en microsecondes, depuis le début de l'époque UNIX. Dans l'exemple, la valeur `1405631878959669` Traduit au jeudi 17 juillet 2014 21:17:59 UTC.

Messages d'audit et cycle de vie de l'objet

Quand un message d'audit est-il généré ?

Des messages d'audit sont générés à chaque ingestion, récupération ou suppression d'un objet. Vous pouvez identifier ces transactions dans le journal des audits en localisant les messages d'audit spécifiques à l'API (S3 ou Swift).

Les messages d'audit sont liés par des identificateurs spécifiques à chaque protocole.

Protocole	Code
Liaison des opérations S3	S3BK (godet), S3KY (clé), ou les deux
Liaison d'opérations Swift	WCON (conteneur), WOBJ (objet) ou les deux
Liaison des opérations internes	CBID (identifiant interne de l'objet)

Calendrier des messages d'audit

En raison de facteurs tels que les différences de synchronisation entre les nœuds de la grille, la taille de l'objet et les retards réseau, l'ordre des messages d'audit générés par les différents services peut varier de celui présenté dans les exemples de cette section.

Nœuds d'archivage

La série de messages d'audit générés lorsqu'un nœud d'archivage envoie des données d'objet à un système de stockage d'archives externe est similaire à celle des nœuds de stockage, à l'exception du message SCMT (Store Object commit), Et les messages ATCE (Archive Object Store Begin) et ASCE (Archive Object Store End) sont générés pour chaque copie archivée de données d'objet.

La série de messages d'audit générés lorsqu'un nœud d'archivage récupère des données d'objet à partir d'un système de stockage d'archives externe est similaire à celle des nœuds de stockage, sauf que les messages ARCB (début de la récupération de l'objet d'archivage) et ARCE (fin de la récupération de l'objet d'archivage) sont générés pour chaque copie récupérée des données d'objet.

La série de messages d'audit générés lorsqu'un nœud d'archivage supprime des données d'objet d'un système de stockage d'archives externe est similaire à celle des nœuds de stockage, sauf qu'il n'y a pas de message SREM (Object Store Remove) et qu'il y a un message AREM (Archive Object Remove) pour chaque demande de suppression.

Transactions d'ingestion d'objets

Vous pouvez identifier les transactions d'entrée de clients dans le journal d'audit en localisant les messages d'audit spécifiques aux API (S3 ou Swift).

Tous les messages d'audit générés lors d'une transaction d'entrée ne sont pas répertoriés dans les tableaux suivants. Seuls les messages nécessaires au suivi de la transaction d'acquisition sont inclus.

Ingestion des messages d'audit S3

Code	Nom	Description	Tracé	Voir
SPUT	Transaction PUT S3	Une transaction d'entrée DE PUT S3 a été effectuée avec succès.	CBID, S3BK, S3KY	"SPUT : PUT S3"
ORLM	Règles d'objet respectées	La politique ILM a été satisfaite pour cet objet.	CBID	"ORLM : règles d'objet respectées"

Ingestion des messages d'audit Swift

Code	Nom	Description	Tracé	Voir
WPUT	EFFECTUER la transaction Swift	Une transaction d'entrée DE PUT Swift a été effectuée avec succès.	CBID, WCON, WOBJ	"WPUT : PUT SWIFT"
ORLM	Règles d'objet respectées	La politique ILM a été satisfaite pour cet objet.	CBID	"ORLM : règles d'objet respectées"

Exemple : ingestion d'objet S3

La série de messages d'audit ci-dessous est un exemple des messages d'audit générés et enregistrés dans le journal d'audit lorsqu'un client S3 ingère un objet à un nœud de stockage (LDR).

Dans cet exemple, la règle ILM active inclut la règle ILM Make 2 copies.

> Tous les messages d'audit générés pendant une transaction ne sont pas répertoriés dans l'exemple ci-dessous. Seules les personnes liées à la transaction de transfert S3 (SPUT) sont répertoriées.

Dans cet exemple, un compartiment S3 a déjà été créé.

SPUT : PUT S3

Le message SPUT est généré pour indiquer qu'une transaction PUT S3 a été émise pour créer un objet dans un compartiment spécifique.

```
2017-07-
17T21:17:58.959669[AUDT:[RSLT(FC32):SUCS][TIME(UI64):25771][SAIP(IPAD):"10
.96.112.29"][S3AI(CSTR):"70899244468554783528"][SACC(CSTR):"test"][S3AK(CS
TR):"SGKHyalRU_5cLflqajtaFmxJn946lAWRJfBF33gAOg=="][SUSR(CSTR):"urn:sgws:i
dentity::70899244468554783528:root"][SBAI(CSTR):"70899244468554783528"][SB
AC(CSTR):"test"][S3BK(CSTR):"example"][S3KY(CSTR):"testobject-0-
3"][CBID\(UI64\):0x8EF52DF8025E63A8][CSIZ(UI64):30720][AVER(UI32):10][ATIM
(UI64):150032627859669][ATYP\(FC32\):SPUT][ANID(UI32):12086324][AMID(FC32)
:S3RQ][ATID(UI64):14399932238768197038]]
```

ORLM : règles d'objet respectées

Le message ORLM indique que la politique ILM a été satisfaite pour cet objet. Le message inclut le CBID de l'objet et le nom de la règle ILM appliquée.

Pour les objets répliqués, le champ EMPLACEMENTS inclut l'ID de nœud LDR et l'ID de volume des emplacements d'objets.

```
2019-07-
17T21:18:31.230669[AUDT:[CBID\(UI64\):0x50C4F7AC2BC8EDF7][RULE(CSTR):"Make
2 Copies"][STAT(FC32):DONE][CSIZ(UI64):0][UUID(CSTR):"0B344E18-98ED-4F22-
A6C8-A93ED68F8D3F"][LOCS(CSTR):"CLDI 12828634 2148730112, CLDI 12745543
2147552014"][RSLT(FC32):SUCS][AVER(UI32):10][ATYP\(FC32\):ORLM][ATIM(UI64)
:1563398230669][ATID(UI64):15494889725796157557][ANID(UI32):13100453][AMID
(FC32):BCMS]]
```

Pour les objets avec code d'effacement, le champ EMPLACEMENTS inclut l'ID de profil de code d'effacement et l'ID de groupe de codes d'effacement

```
2019-02-23T01:52:54.647537
[AUDT:[CBID(UI64):0xFA8ABE5B5001F7E2][RULE(CSTR):"EC_2_plus_1"][STAT(FC32)
:DONE][CSIZ(UI64):10000][UUID(CSTR):"E291E456-D11A-4701-8F51-
D2F7CC9AFECA"][LOCS(CSTR):"CLEC 1 A471E45D-A400-47C7-86AC-
12E77F229831"][RSLT(FC32):SUCS][AVER(UI32):10][ATIM(UI64):1550929974537]\[
ATYP\(FC32\):ORLM\][ANID(UI32):12355278][AMID(FC32):ILMX][ATID(UI64):41685
59046473725560]]
```

Le champ CHEMIN d'ACCÈS inclut des informations clés et un compartiment S3 ou des informations sur le conteneur Swift et l'objet, selon l'API utilisée.

```
2019-09-15.txt:2018-01-24T13:52:54.131559
[AUDT:[CBID(UI64):0x82704DFA4C9674F4][RULE(CSTR):"Make 2
Copies"][STAT(FC32):DONE][CSIZ(UI64):3145729][UUID(CSTR):"8C1C9CAC-22BB-
4880-9115-
CE604F8CE687"][PATH(CSTR):"frisbee_Bucket1/GridDataTests151683676324774_1_
1vf9d"][LOCS(CSTR):"CLDI 12525468, CLDI
12222978"][RSLT(FC32):SUCS][AVER(UI32):10][ATIM(UI64):1568555574559][ATYP(
FC32):ORLM][ANID(UI32):12525468][AMID(FC32):OBDI][ATID(UI64):3448338865383
69336]]
```

Transactions de suppression d'objet

Vous pouvez identifier les transactions de suppression d'objets dans le journal d'audit en localisant les messages d'audit spécifiques aux API (S3 et Swift).

Tous les messages d'audit générés lors d'une opération de suppression ne sont pas répertoriés dans les tableaux suivants. Seuls les messages requis pour suivre la transaction de suppression sont inclus.

S3 supprime les messages d'audit

Code	Nom	Description	Tracé	Voir
SDEL	Suppression S3	Demande de suppression de l'objet d'un compartiment.	CBID, S3KY	"SDEL : SUPPRESSION S3"

Supprimez les messages d'audit Swift

Code	Nom	Description	Tracé	Voir
WDEL	Suppression Swift	Demande de suppression de l'objet d'un conteneur ou du conteneur.	CBID, WOBJ	"WDEL : SUPPRESSION rapide"

Exemple : suppression d'objet S3

Lorsqu'un client S3 supprime un objet d'un nœud de stockage (service LDR), un message d'audit est généré et enregistré dans le journal des audits.

> Tous les messages d'audit générés lors d'une opération de suppression ne sont pas répertoriés dans l'exemple ci-dessous. Seules les personnes liées à la transaction de suppression S3 (SDEL) sont répertoriées.

SDEL : suppression S3

La suppression d'objet commence lorsque le client envoie une requête DE SUPPRESSION d'objet à un service LDR. Le message contient le compartiment à partir duquel vous souhaitez supprimer l'objet ainsi que la clé S3 de l'objet, qui permet d'identifier l'objet.

```
2017-07-
17T21:17:58.959669[AUDT:[RSLT(FC32):SUCS][TIME(UI64):14316][SAIP(IPAD):"10
.96.112.29"][S3AI(CSTR):"70899244468554783528"][SACC(CSTR):"test"][S3AK(CS
TR):"SGKHyalRU_5cLflqajtaFmxJn946lAWRJfBF33gAOg=="][SUSR(CSTR):"urn:sgws:i
dentity::70899244468554783528:root"][SBAI(CSTR):"70899244468554783528"][SB
AC(CSTR):"test"]\[S3BK\(CSTR\):"example"\]\[S3KY\(CSTR\):"testobject-0-
7"\][CBID\(UI64\):0x339F21C5A6964D89][CSIZ(UI64):30720][AVER(UI32):10][ATI
M(UI64):150032627859669][ATYP\(FC32\):SDEL][ANID(UI32):12086324][AMID(FC32
):S3RQ][ATID(UI64):4727861330952970593]]
```

Transactions de récupération d'objet

Vous pouvez identifier les transactions de récupération d'objets dans le journal d'audit en localisant les messages d'audit spécifiques à l'API (S3 et Swift).

Tous les messages d'audit générés lors d'une transaction de récupération ne sont pas répertoriés dans les

tableaux suivants. Seuls les messages requis pour suivre la transaction de récupération sont inclus.

Messages d'audit de récupération S3

Code	Nom	Description	Tracé	Voir
SGET	OBTENTION S3	Demande de récupération d'un objet à partir d'un compartiment.	CBID, S3BK, S3KY	"SGET : OBTENEZ S3"

Messages d'audit de récupération Swift

Code	Nom	Description	Tracé	Voir
C'EST PARTI	PROFITEZ-en rapidement	Demande de récupération d'un objet à partir d'un conteneur.	CBID, WCON, WOBJ	"WGET: SWIFT GET"

Exemple : récupération d'objets S3

Lorsqu'un client S3 récupère un objet à partir d'un nœud de stockage (service LDR), un message d'audit est généré et enregistré dans le journal d'audit.

Notez que tous les messages d'audit générés pendant une transaction ne sont pas répertoriés dans l'exemple ci-dessous. Seules les transactions liées à la transaction de récupération S3 (SGET) sont répertoriées.

SGET : OBTENEZ S3

L'extraction d'objet commence lorsque le client envoie une requête GET Object à un service LDR. Le message contient le compartiment à partir duquel vous pouvez récupérer l'objet ainsi que la clé S3 de l'objet, qui permet d'identifier l'objet.

```
2017-09-20T22:53:08.782605
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):47807][SAIP(IPAD):"10.96.112.26"][S3AI(
CSTR):"43979298178977966408"][SACC(CSTR):"s3-account-
a"][S3AK(CSTR):"SGKHt7GzEcu0yXhFhT_rL5mep4nJt1w75GBh-
O_FEw=="][SUSR(CSTR):"urn:sgws:identity::43979298178977966408:root"][SBAI(
CSTR):"43979298178977966408"][SBAC(CSTR):"s3-account-
a"]\[S3BK\(CSTR\):"bucket-
anonymous"\]\[S3KY\(CSTR\):"Hello.txt"\][CBID(UI64):0x83D70C6F1F662B02][CS
IZ(UI64):12][AVER(UI32):10][ATIM(UI64):1505947988782605]\[ATYP\(FC32\):SGE
T\][ANID(UI32):12272050][AMID(FC32):S3RQ][ATID(UI64):17742374343649889669]
]
```

Si la règle de compartiment le permet, un client peut récupérer des objets de façon anonyme ou récupérer des objets à partir d'un compartiment qui est détenu par un autre compte de locataire. Le message d'audit contient des informations sur le compte du propriétaire du compartiment afin que vous puissiez suivre ces demandes anonymes et inter-comptes.

Dans l'exemple de message suivant, le client envoie une requête GET Object pour un objet stocké dans un compartiment qu'il n'est pas propriétaire. Les valeurs de SBAI et SBAC enregistrent l'ID et le nom de compte du propriétaire du compartiment, qui diffèrent de l'ID et du nom du compte du locataire enregistré dans S3AI et

SACC.

```
2017-09-20T22:53:15.876415
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):53244][SAIP(IPAD):"10.96.112.26"]\[S3AI
\(CSTR\):"17915054115450519830"\]\[SACC\(CSTR\):"s3-account-
b"\][S3AK(CSTR):"SGKHpoblWlP_kBkqSCbTi754Ls8lBUog67I2LlSiUg=="][SUSR(CSTR)
:"urn:sgws:identity::17915054115450519830:root"]\[SBAI\(CSTR\):"4397929817
8977966408"\]\[SBAC\(CSTR\):"s3-account-a"\][S3BK(CSTR):"bucket-
anonymous"][S3KY(CSTR):"Hello.txt"][CBID(UI64):0x83D70C6F1F662B02][CSIZ(UI
64):12][AVER(UI32):10][ATIM(UI64):1505947995876415][ATYP(FC32):SGET][ANID(
UI32):12272050][AMID(FC32):S3RQ][ATID(UI64):6888780247515624902]]
```

Exemple : S3 Select sur un objet

Lorsqu'un client S3 émet une requête S3 Select sur un objet, des messages d'audit sont générés et enregistrés dans le journal d'audit.

Notez que tous les messages d'audit générés pendant une transaction ne sont pas répertoriés dans l'exemple ci-dessous. Seules les transactions liées à la transaction S3 Select (SelectObjectContent) sont répertoriées.

Chaque requête génère deux messages d'audit : un qui effectue l'autorisation de la requête S3 Select (le champ S3SR est défini sur « SELECT ») et une opération GET standard qui récupère les données du stockage pendant le traitement.

```
2021-11-08T15:35:30.750038
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1636385730715700][TIME(UI64):29173][SAI
P(IPAD):"192.168.7.44"][S3AI(CSTR):"63147909414576125820"][SACC(CSTR):"Ten
ant1636027116"][S3AK(CSTR):"AUFD1XNVZ905F3TW7KSU"][SUSR(CSTR):"urn:sgws:id
entity::63147909414576125820:root"][SBAI(CSTR):"63147909414576125820"][SBA
C(CSTR):"Tenant1636027116"][S3BK(CSTR):"619c0755-9e38-42e0-a614-
05064f74126d"][S3KY(CSTR):"SUB-
EST2020_ALL.csv"][CBID(UI64):0x0496F0408A721171][UUID(CSTR):"D64B1A4A-
9F01-4EE7-B133-
08842A099628"][CSIZ(UI64):0][S3SR(CSTR):"select"][AVER(UI32):10][ATIM(UI64
):1636385730750038][ATYP(FC32):SPOS][ANID(UI32):12601166][AMID(FC32):S3RQ]
[ATID(UI64):1363009709396895985]]
```

```
2021-11-08T15:35:32.604886
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1636383069486504][TIME(UI64):430690][SA
IP(IPAD):"192.168.7.44"][HTRH(CSTR):"{\"x-forwarded-
for\":\"unix:\"}"][S3AI(CSTR):"63147909414576125820"][SACC(CSTR):"Tenant16
36027116"][S3AK(CSTR):"AUFD1XNVZ905F3TW7KSU"][SUSR(CSTR):"urn:sgws:identit
y::63147909414576125820:root"][SBAI(CSTR):"63147909414576125820"][SBAC(CST
R):"Tenant1636027116"][S3BK(CSTR):"619c0755-9e38-42e0-a614-
05064f74126d"][S3KY(CSTR):"SUB-
EST2020_ALL.csv"][CBID(UI64):0x0496F0408A721171][UUID(CSTR):"D64B1A4A-
9F01-4EE7-B133-
08842A099628"][CSIZ(UI64):10185581][MTME(UI64):1636380348695262][AVER(UI32
):10][ATIM(UI64):1636385732604886][ATYP(FC32):SGET][ANID(UI32):12733063][A
MID(FC32):S3RQ][ATID(UI64):16562288121152341130]]
```

Messages de mise à jour des métadonnées

Des messages d'audit sont générés lorsqu'un client S3 met à jour les métadonnées d'un objet.

Messages d'audit de la mise à jour des métadonnées S3

Code	Nom	Description	Tracé	Voir
SUPD	Métadonnées S3 mises à jour	Générées lorsqu'un client S3 met à jour les métadonnées d'un objet ingéré.	CBID, S3KY, HTRH	"SUPD : métadonnées S3 mises à jour"

Exemple : mise à jour des métadonnées S3

L'exemple illustre la réussite d'une transaction permettant de mettre à jour les métadonnées d'un objet S3 existant.

SUPD : mise à jour des métadonnées S3

Le client S3 demande (SUPD) de mettre à jour les métadonnées spécifiées (`x-amz-meta-\*`) Pour l'objet S3 (S3KY). Dans cet exemple, les en-têtes de requête sont inclus dans le champ HTRH car ils ont été configurés comme en-tête de protocole d'audit (**CONFIGURATION** > **surveillance** > **Audit et serveur syslog**). Voir "Configurez les messages d'audit et les destinations des journaux".

```
2017-07-11T21:54:03.157462
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):17631][SAIP(IPAD):"10.96.100.254"]
[HTRH(CSTR):"{\"accept-encoding\":\"identity\",\"authorization\":\"AWS
LIUF17FGJARQHPY2E761:jul/hnZs/uNY+aVvV0lTSYhEGts=\",
\"content-length\":\"0\",\"date\":\"Tue, 11 Jul 2017 21:54:03
GMT\",\"host\":\"10.96.99.163:18082\",
\"user-agent\":\"aws-cli/1.9.20 Python/2.7.6 Linux/3.13.0-119-generic
botocore/1.3.20\",
\"x-amz-copy-source\":\"/testbkt1/testobj1\",\"x-amz-metadata-
directive\":\"REPLACE\",\"x-amz-meta-city\":\"Vancouver\"}"]
[S3AI(CSTR):"20956855414285633225"][SACC(CSTR):"acct1"][S3AK(CSTR):"SGKHyy
v9ZQqWRbJSQc5vI7mgioJwrdplShE02AUaww=="]
[SUSR(CSTR):"urn:sgws:identity::20956855414285633225:root"]
[SBAI(CSTR):"20956855414285633225"][SBAC(CSTR):"acct1"][S3BK(CSTR):"testbk
t1"]
[S3KY(CSTR):"testobj1"][CBID(UI64):0xCB1D5C213434DD48][CSIZ(UI64):10][AVER
(UI32):10]
[ATIM(UI64):1499810043157462][ATYP(FC32):SUPD][ANID(UI32):12258396][AMID(F
C32):S3RQ]
[ATID(UI64):8987436599021955788]]
```

Messages d’audit

Messages d’audit : présentation

Les descriptions détaillées des messages d’audit renvoyés par le système sont répertoriées dans les sections suivantes. Chaque message d’audit est d’abord répertorié dans un tableau qui regroupe les messages associés en fonction de la classe d’activité que le message représente. Ces regroupements sont utiles à la fois pour comprendre les types d’activités auditées et pour sélectionner le type souhaité de filtrage des messages d’audit.

Les messages d’audit sont également répertoriés par ordre alphabétique par leur code à quatre caractères. Cette liste alphabétique vous permet de trouver des informations sur des messages spécifiques.

Les codes à quatre caractères utilisés dans ce chapitre sont les valeurs ATYP trouvées dans les messages d’audit comme indiqué dans l’exemple de message suivant :

```
2014-07-17T03:50:47.484627
\[AUDT:[RSLT(FC32):VRGN][AVER(UI32):10][ATIM(UI64):1405569047484627][ATYP\
(FC32\):SYSU][ANID(UI32):11627225][AMID(FC32):ARNI][ATID(UI64):94457363265
00603516]]
```

Pour plus d’informations sur la définition des niveaux de messages d’audit, la modification des destinations des journaux et l’utilisation d’un serveur syslog externe pour vos informations d’audit, reportez-vous à la

section "Configurez les messages d'audit et les destinations des journaux"

Catégories de messages d'audit

Messages d'audit système

Les messages d'audit appartenant à la catégorie d'audit du système sont utilisés pour les événements liés au système d'audit lui-même, aux États des nœuds de la grille, à l'activité des tâches à l'échelle du système (tâches de la grille) et aux opérations de sauvegarde des services.

Code	Titre et description du message	Voir
ECMC	Fragment de données avec code d'effacement manquant : indique qu'un fragment de données avec code d'effacement manquant a été détecté.	"ECMC : fragment de données codé d'effacement manquant"
ECOC	Fragment de données codé d'effacement corrompu : indique qu'un fragment de données codé d'effacement corrompu a été détecté.	"ECOC : fragment de données codé d'effacement corrompu"
EN	Échec de l'authentification de sécurité : une tentative de connexion à l'aide du protocole TLS (transport Layer Security) a échoué.	"ETAF : échec de l'authentification de sécurité"
GNRG	Enregistrement GNDS : service mis à jour ou enregistré des informations sur lui-même dans le système StorageGRID.	"GNRG : enregistrement GNDS"
GNUR	Annulation de l'enregistrement du GNDS : un service s'est désinscrit du système StorageGRID.	"GNUR : non-inscription du GNDS"
GTED	Tâche de grille terminée : le service CMN a terminé le traitement de la tâche de grille.	"GTED : tâche de grille terminée"
GTST	Tâche de grille démarrée : le service CMN a commencé à traiter la tâche de grille.	"GTST : tâche de grille démarrée"
GTSU	Tâche de grille soumise : une tâche de grille a été envoyée au service CMN.	"GTSU : tâche de grille soumise"
LLST	Emplacement perdu : ce message d'audit est généré en cas de perte d'un emplacement.	"LLST : emplacement perdu"
OLST	Objet perdu : un objet demandé ne peut pas se trouver dans le système StorageGRID.	"OLST : le système a détecté un objet perdu"
AJOUTER	Désactivation de l'audit de sécurité : l'enregistrement des messages d'audit a été désactivé.	"SADD : désactivation de l'audit de sécurité"

Code	Titre et description du message	Voir
SADE	Activation de l'audit de sécurité : la journalisation des messages d'audit a été restaurée.	"SADE : activation de l'audit de sécurité"
SVRF	Échec de la vérification du magasin d'objets : échec de la vérification d'un bloc de contenu.	"SVRF : échec de la vérification du magasin d'objets"
SVRU	Vérification du magasin d'objets Inconnu : données d'objet inattendues détectées dans le magasin d'objets.	"SVRU : Vérification du magasin d'objets inconnue"
SYSD	Arrêt du nœud : un arrêt a été demandé.	"SYSD : arrêt du nœud"
SYST	Arrêt du nœud : un service a démarré un arrêt normal.	"SYST : arrêt du nœud"
SYSU	Node Start : service démarré, la nature de l'arrêt précédent est indiquée dans le message.	"SYSU : démarrage du nœud"

Messages d'audit du stockage objet

Les messages d'audit appartenant à la catégorie d'audit du stockage objet sont utilisés pour les événements liés au stockage et à la gestion d'objets au sein du système StorageGRID. Il s'agit notamment du stockage objet et des récupérations, des transferts entre nœuds grid et nœuds.

Code	Description	Voir
APCT	Suppression d'archivage à partir du Tier cloud : les données d'objet archivé sont supprimées d'un système de stockage d'archivage externe qui se connecte au StorageGRID via l'API S3.	"APCT : archive Purge à partir du Tier cloud"
ARCB	Début de la récupération de l'objet d'archive : le service ARC lance la récupération des données d'objet à partir du système de stockage d'archives externe.	"ARCB : début de la récupération de l'objet d'archive"
ARCE	Fin de la récupération de l'objet d'archive : les données de l'objet ont été extraites d'un système de stockage d'archives externe et le service ARC signale l'état de l'opération de récupération.	"ARCE : fin de la récupération de l'objet d'archive"

Code	Description	Voir
ARCT	Archivage à partir du Tier cloud : les données d'objet archivé sont récupérées depuis un système de stockage d'archivage externe qui se connecte à StorageGRID via l'API S3.	"ARCT : récupération d'archives depuis Cloud-Tier"
AREM	Suppression de l'objet d'archive : un bloc de contenu a été supprimé avec succès ou sans succès du système de stockage d'archives externe.	"AREM : suppression de l'objet d'archive"
ASCE	Fin du magasin d'objets d'archivage : un bloc de contenu a été écrit dans le système de stockage d'archives externe et le service ARC signale l'état de l'opération d'écriture.	"ASCE : fin du magasin d'objets d'archivage"
ASCT	Tier dans le stockage d'archives : les données d'objet sont stockées dans un système de stockage d'archives externe qui se connecte à StorageGRID via l'API S3.	"ASCT : magasin d'archives, niveau du cloud"
ATCE	Début de l'archive du magasin d'objets : l'écriture d'un bloc de contenu sur un stockage d'archivage externe a commencé.	"ATCE : début du magasin d'objets d'archivage"
AVCC	Archive Valider la configuration du Tier cloud : les paramètres du compte et des compartiments fournis ont été validés avec succès ou non.	"AVCC : validation de la configuration du Tier cloud"
BROR	Demande de lecture seule du compartiment : un compartiment est entré ou a quitté le mode lecture seule.	"BROR : demande en lecture seule du compartiment"
CBSE	Objet Envoyer fin : l'entité source a terminé une opération de transfert des données nœud-grille vers nœud-grille.	"CBSE : fin de l'envoi de l'objet"
CBRE	Fin de réception de l'objet : l'entité de destination a terminé une opération de transfert des données nœud-grille vers nœud-grille.	"CBRE : fin de la réception de l'objet"
CGRR	Demande de réplication multigrille : StorageGRID a tenté une opération de réplication multigrille pour répliquer des objets entre des compartiments dans une connexion de fédération de grille.	"CGRR : demande de réplication croisée"
EBDL	Suppression d'un compartiment vide : l'analyse ILM a supprimé un objet d'un compartiment qui supprime tous les objets (opération de compartiment vide).	"EBDL : suppression du compartiment vide"

Code	Description	Voir
EBKR	Demande de compartiment vide : un utilisateur a envoyé une demande d'activation ou de désactivation de compartiment vide (c'est-à-dire de supprimer des objets de compartiment ou d'arrêter la suppression d'objets).	"EBKR : demande de godet vide"
BALAYAGE	Validation d'un magasin d'objets : un bloc de contenu a été entièrement stocké et vérifié, et peut désormais être demandé.	"SCMT : demande de validation de magasin d'objets"
SREM	Suppression du magasin d'objets : un bloc de contenu a été supprimé d'un nœud de grille et ne peut plus être demandé directement.	"SREM : Suppression du magasin d'objets"

Messages d'audit de lecture du client

Les messages d'audit de lecture des clients sont consignés lorsqu'une application client S3 ou Swift demande de récupérer un objet.

Code	Description	Utilisé par	Voir
S3SL	Demande S3 Select : enregistre une fin d'étude après le renvoi d'une demande S3 Select au client. Le message S3SL peut inclure des détails de message d'erreur et de code d'erreur. La demande n'a peut-être pas abouti.	Client S3	"S3SL: Demande S3 Select"
SGET	S3 GET : log une transaction réussie pour récupérer un objet ou répertorier les objets dans un compartiment. **Remarque :** si la transaction fonctionne sur une sous-ressource, le message d'audit inclura le champ S3SR.	Client S3	"SGET : OBTENEZ S3"
SHEA	TÊTE S3 : consigne une transaction réussie pour vérifier l'existence d'un objet ou d'un compartiment.	Client S3	"SHEA : TÊTE S3"
C'EST PARTI	SWIFT GET : log une transaction réussie pour récupérer un objet ou répertorier les objets dans un conteneur.	Client Swift	"WGET: SWIFT GET"
WHEA	SWIFT HEAD : consigne une transaction réussie afin de vérifier l'existence d'un objet ou d'un conteneur.	Client Swift	"WHEA: TÊTE SWIFT"

Écrire des messages d'audit client

Les messages d'audit d'écriture client sont consignés lorsqu'une application client S3 ou Swift demande de créer ou de modifier un objet.

Code	Description	Utilisé par	Voir
OVWR	Remplacement d'objet : consigne une transaction afin de remplacer un objet par un autre.	Clients S3 et Swift	"OVWR : remplacement d'objet"
SDEL	SUPPRESSION S3 : journal une transaction réussie pour supprimer un objet ou un compartiment. **Remarque :** si la transaction fonctionne sur une sous-ressource, le message d'audit inclura le champ S3SR.	Client S3	"SDEL : SUPPRESSION S3"
SPR	POST S3 : consigne une transaction réussie pour restaurer un objet à partir du stockage AWS Glacier vers un pool de stockage cloud.	Client S3	"SPO : BORNE S3"
SPUT	S3 PUT : enregistre la réussite d'une transaction pour créer un nouvel objet ou un compartiment. **Remarque :** si la transaction fonctionne sur une sous-ressource, le message d'audit inclura le champ S3SR.	Client S3	"SPUT : PUT S3"
SUPD	Métadonnées S3 mises à jour : enregistre une transaction réussie pour mettre à jour les métadonnées d'un objet ou d'un compartiment.	Client S3	"SUPD : métadonnées S3 mises à jour"
WDEL	SUPPRESSION Swift : enregistre une transaction réussie pour supprimer un objet ou un conteneur.	Client Swift	"WDEL : SUPPRESSION rapide"
WPUT	SWIFT PUT : consigne une transaction réussie pour créer un nouvel objet ou conteneur.	Client Swift	"WPUT : PUT SWIFT"

Message d'audit de gestion

La catégorie gestion consigne les requêtes utilisateur dans l'API de gestion.

Code	Titre et description du message	Voir
MGAU	Message d'audit de l'API de gestion : journal des demandes utilisateur.	"MGAU : message d'audit de gestion"

Messages d'audit des opérations ILM

Les messages d'audit appartenant à la catégorie d'audit ILM sont utilisés pour les événements liés aux opérations de gestion du cycle de vie des informations (ILM).

Code	Titre et description du message	Voir
IDEL	Suppression initiée de l'ILM : ce message d'audit est généré lorsque l'ILM démarre le processus de suppression d'un objet.	"IDEL : suppression initiée ILM"
LKCU	Nettoyage d'objet écrasé. Ce message d'audit est généré lorsqu'un objet écrasé est automatiquement supprimé pour libérer de l'espace de stockage.	"LKCU : nettoyage d'objet écrasé"
ORLM	Règles objet respectées : ce message d'audit est généré lorsque les données objet sont stockées comme spécifié par les règles ILM.	"ORLM : règles d'objet respectées"

Référence du message d'audit

APCT : archive Purge à partir du Tier cloud

Ce message est généré lorsque les données d'objet archivé sont supprimées d'un système de stockage d'archives externe qui se connecte à StorageGRID via l'API S3.

Code	Champ	Description
CBID	ID du bloc de contenu	Identifiant unique du bloc de contenu supprimé.
CSIZ	Taille du contenu	Taille de l'objet en octets. Renvoie toujours 0.
RSLT	Code de résultat	Renvoie réussi (CS) ou l'erreur signalée par le back-end.
SUID	Identifiant unique du stockage	Identifiant unique (UUID) du Tier cloud à partir duquel l'objet a été supprimé.

ARCB : début de la récupération de l'objet d'archive

Ce message est généré lorsqu'une demande est faite pour récupérer les données d'objet archivées et que le processus de récupération commence. Les demandes de récupération sont traitées immédiatement, mais peuvent être réorganisées pour améliorer l'efficacité de la récupération à partir de supports linéaires tels que des bandes.

Code	Champ	Description
CBID	ID du bloc de contenu	Identifiant unique du bloc de contenu à extraire du système de stockage d'archives externe.

Code	Champ	Description
RSLT	Résultat	Indique le résultat du démarrage du processus de récupération des archives. La valeur actuellement définie est :SUCS : la demande de contenu a été reçue et mise en file d'attente pour récupération.

Ce message d'audit indique l'heure de récupération d'une archive. Il vous permet de faire correspondre le message avec un message de fin D'ARCE correspondant pour déterminer la durée de récupération de l'archive et si l'opération a réussi.

ARCE : fin de la récupération de l'objet d'archive

Ce message est généré lorsqu'une tentative du nœud d'archivage de récupérer des données d'objet à partir d'un système de stockage d'archives externe est terminée. En cas de réussite, le message indique que les données de l'objet demandé ont été entièrement lues à partir de l'emplacement d'archivage et qu'elles ont été vérifiées avec succès. Une fois que les données de l'objet ont été récupérées et vérifiées, elles sont envoyées au service requérant.

Code	Champ	Description
CBID	ID du bloc de contenu	Identifiant unique du bloc de contenu à extraire du système de stockage d'archives externe.
VLID	Identifiant du volume	Identifiant du volume sur lequel les données ont été archivées. Si aucun emplacement d'archive n'est trouvé pour le contenu, un ID de volume de 0 est renvoyé.
RSLT	Résultat de la récupération	L'état d'achèvement du processus de récupération des archives : • CMC : réussi • VRFL : échec (échec de la vérification de l'objet) • ARUN : échec (système de stockage d'archivage externe indisponible) • ANNUL : échec (opération de récupération annulée) • GERR : échec (erreur générale)

Le fait de faire correspondre ce message au message ARCB correspondant peut indiquer le temps nécessaire à la récupération de l'archive. Ce message indique si la récupération a réussi et, en cas d'échec, la cause de l'échec de récupération du bloc de contenu.

ARCT : récupération d'archives depuis Cloud-Tier

Ce message est généré lorsque les données d'objet archivé sont récupérées depuis un système de stockage d'archives externe qui se connecte à StorageGRID via l'API S3.

Code	Champ	Description
CBID	ID du bloc de contenu	Identifiant unique du bloc de contenu qui a été récupéré.
CSIZ	Taille du contenu	Taille de l'objet en octets. La valeur est précise uniquement pour les résultats des récupération.
RSLT	Code de résultat	Renvoie réussi (CS) ou l'erreur signalée par le back-end.
SUID	Identifiant unique du stockage	Identificateur unique (UUID) du système de stockage d'archives externe.
TEMPS	Temps	Temps de traitement total de la demande en microsecondes.

AREM : suppression de l'objet d'archive

Le message d'audit de suppression d'objet d'archive indique qu'un bloc de contenu a été supprimé avec succès ou sans succès d'un nœud d'archive. Si le résultat est réussi, le nœud d'archivage a bien informé le système de stockage d'archives externe qu'StorageGRID a libéré un emplacement d'objet. La suppression de l'objet du système de stockage d'archives externe dépend du type de système et de sa configuration.

Code	Champ	Description
CBID	ID du bloc de contenu	Identifiant unique du bloc de contenu à extraire du système de supports d'archivage externe.
VLID	Identifiant du volume	Identificateur du volume sur lequel les données de l'objet ont été archivées.
RSLT	Résultat	L'état d'achèvement du processus de suppression d'archive : • CMC : réussi • ARUN : échec (système de stockage d'archivage externe indisponible) • GERR : échec (erreur générale)

ASCE : fin du magasin d'objets d'archivage

Ce message indique que l'écriture d'un bloc de contenu sur un système de stockage d'archives externe est terminée.

Code	Champ	Description
CBID	Identificateur du bloc de contenu	Identifiant du bloc de contenu stocké sur le système de stockage d'archives externe.

Code	Champ	Description
VLID	Identifiant du volume	Identifiant unique du volume d'archivage sur lequel les données de l'objet sont écrites.
VREN	Vérification activée	Indique si la vérification est effectuée pour les blocs de contenu. Les valeurs actuellement définies sont : • VENA : la vérification est activée • VDSA : la vérification est désactivée
CLM	Classe de gestion	Chaîne identifiant la classe de gestion TSM à laquelle le bloc de contenu est affecté, le cas échéant.
RSLT	Résultat	Indique le résultat du processus d'archivage. Les valeurs actuellement définies sont : • SUCS : succès (processus d'archivage réussi) • OFFL : échec (archivage hors ligne) • VRFL : échec (échec de la vérification de l'objet) • ARUN : échec (système de stockage d'archivage externe indisponible) • GERR : échec (erreur générale)

Ce message d'audit signifie que le bloc de contenu spécifié a été écrit sur le système de stockage d'archivage externe. Si l'écriture échoue, le résultat fournit des informations de dépannage de base sur l'emplacement de la défaillance. Pour obtenir des informations plus détaillées sur les échecs d'archivage, consultez les attributs du nœud d'archivage dans le système StorageGRID.

ASCT : magasin d'archives, niveau du cloud

Ce message est généré lorsque les données d'objet archivé sont stockées sur un système de stockage d'archives externe qui se connecte à StorageGRID via l'API S3.

Code	Champ	Description
CBID	ID du bloc de contenu	Identifiant unique du bloc de contenu qui a été récupéré.
CSIZ	Taille du contenu	Taille de l'objet en octets.
RSLT	Code de résultat	Renvoie réussi (CS) ou l'erreur signalée par le back-end.
SUID	Identifiant unique du stockage	Identifiant unique (UUID) du Tier cloud sur lequel le contenu a été stocké.
TEMPS	Temps	Temps de traitement total de la demande en microsecondes.

ATCE : début du magasin d'objets d'archivage

Ce message indique que l'écriture d'un bloc de contenu sur un système de stockage d'archivage externe a démarré.

Code	Champ	Description
CBID	ID du bloc de contenu	Identifiant unique du bloc de contenu à archiver.
VLID	Identifiant du volume	L'identifiant unique du volume sur lequel le bloc de contenu est écrit. Si l'opération échoue, un ID de volume 0 est renvoyé.
RSLT	Résultat	Indique le résultat du transfert du bloc de contenu. Les valeurs actuellement définies sont : • SUC : succès (le bloc de contenu a été enregistré avec succès) • EXIS : ignoré (le bloc de contenu était déjà stocké) • ISFD : échec (espace disque insuffisant) • STER : échec (erreur lors du stockage du CBID) • OFFL : échec (archivage hors ligne) • GERR : échec (erreur générale)

AVCC : validation de la configuration du Tier cloud

Ce message est généré lorsque les paramètres de configuration sont validés pour un type de cible Cloud Tiering - simple Storage Service (S3).

Code	Champ	Description
RSLT	Code de résultat	Renvoie réussi (CS) ou l'erreur signalée par le back-end.
SUID	Identifiant unique du stockage	UUID associé au système de stockage d'archivage externe validé.

BROR : demande en lecture seule du compartiment

Le service LDR génère ce message d'audit lorsqu'un compartiment passe en mode lecture seule ou quitte ce mode. Par exemple, un compartiment passe en mode lecture seule tandis que tous les objets sont en cours de suppression.

Code	Champ	Description
BKHD	UUID de compartiment	ID du compartiment.

Code	Champ	Description
BROV	Valeur de demande de lecture seule du compartiment	Que le compartiment soit en lecture seule ou qu'il quitte l'état en lecture seule (1 = lecture seule, 0 = non-lecture seule).
BROS	Motif de compartiment en lecture seule	Raison pour laquelle le compartiment est en lecture seule ou quitte l'état en lecture seule. Par exemple, emptyBucket.
S3AI	ID de compte locataire S3	ID du compte de locataire qui a envoyé la demande. Une valeur vide indique un accès anonyme.
S3BK	Compartiment S3	Nom du compartiment S3.

CBRB : début de la réception de l'objet

Dans le cadre d'opérations normales, les blocs de contenu sont transférés en continu entre différents nœuds lorsque des données sont accessibles, répliquées et conservées. Lorsque le transfert d'un bloc de contenu d'un nœud à un autre est lancé, ce message est émis par l'entité de destination.

Code	Champ	Description
CNID	Identificateur de connexion	Identifiant unique de la session/connexion nœud à nœud.
CBID	Identificateur du bloc de contenu	Identifiant unique du bloc de contenu en cours de transfert.
CTDR	Direction de transfert	Indique si le transfert CBID a été initié par Push ou par Pull : PUSH : l'opération de transfert a été demandée par l'entité émettrice. EXTRACTION : l'opération de transfert a été demandée par l'entité destinataire.
CTSR	Entité source	ID de nœud de la source (expéditeur) du transfert CBID.
CTD	Entité de destination	ID de nœud de la destination (récepteur) du transfert CBID.
CTSS	Nombre de séquences de début	Indique le premier nombre de séquences demandé. En cas de réussite, le transfert commence à partir de ce nombre de séquences.

Code	Champ	Description
CTE	Nombre de séquences de fin prévu	Indique le dernier nombre de séquences demandé. En cas de réussite, le transfert est considéré comme terminé lorsque ce nombre de séquences a été reçu.
RSLT	Statut de début du transfert	État au moment du démarrage du transfert : CMC : le transfert a démarré avec succès.

Ce message d'audit signifie qu'une opération de transfert de données nœud à nœud a été lancée sur un seul élément de contenu, tel qu'identifié par son identificateur de bloc de contenu. L'opération demande des données de « nombre de séquences de début » à « nombre de séquences de fin attendu ». Les nœuds d'envoi et de réception sont identifiés par leurs ID de nœud. Ces informations peuvent être utilisées pour suivre le flux de données du système et lorsqu'elles sont associées à des messages d'audit de stockage, pour vérifier le nombre de répliques.

CBRE : fin de la réception de l'objet

Lorsque le transfert d'un bloc de contenu d'un nœud à un autre est terminé, ce message est émis par l'entité de destination.

Code	Champ	Description
CNID	Identificateur de connexion	Identifiant unique de la session/connexion nœud à nœud.
CBID	Identificateur du bloc de contenu	Identifiant unique du bloc de contenu en cours de transfert.
CTDR	Direction de transfert	Indique si le transfert CBID a été initié par Push ou par Pull : PUSH : l'opération de transfert a été demandée par l'entité émettrice. EXTRACTION : l'opération de transfert a été demandée par l'entité destinataire.
CTSR	Entité source	ID de nœud de la source (expéditeur) du transfert CBID.
CTD	Entité de destination	ID de nœud de la destination (récepteur) du transfert CBID.
CTSS	Nombre de séquences de début	Indique le nombre de séquences sur lesquelles le transfert a démarré.
CTAS	Nombre de séquences de fin réelles	Indique que le dernier nombre de séquences a été transféré avec succès. Si le nombre de séquences de fin réelles est le même que le nombre de séquences de début et que le résultat du transfert n'a pas réussi, aucune donnée n'a été échangée.

Code	Champ	Description
RSLT	Résultat du transfert	Résultat de l'opération de transfert (du point de vue de l'entité émettrice) : SUC : transfert terminé avec succès ; tous les comptes de séquence demandés ont été envoyés. CONL : connexion perdue pendant le transfert CTMO : expiration de la connexion pendant l'établissement ou le transfert UNRE : ID de nœud de destination inaccessible CRPT : transfert terminé en raison de la réception de données corrompues ou non valides

Ce message d'audit signifie qu'une opération de transfert des données nœud à nœud est terminée. Si le résultat du transfert a réussi, l'opération a transféré les données de « nombre de séquences de début » à « nombre de séquences de fin réelles ». Les nœuds d'envoi et de réception sont identifiés par leurs ID de nœud. Ces informations peuvent être utilisées pour suivre le flux de données système et pour localiser, tabuler et analyser les erreurs. Lorsqu'il est associé à des messages d'audit du stockage, il peut également être utilisé pour vérifier le nombre de répliques.

CBSB : début de l'envoi de l'objet

Dans le cadre d'opérations normales, les blocs de contenu sont transférés en continu entre différents nœuds lorsque des données sont accessibles, répliquées et conservées. Lorsque le transfert d'un bloc de contenu d'un nœud à un autre est lancé, ce message est émis par l'entité source.

Code	Champ	Description
CNID	Identificateur de connexion	Identifiant unique de la session/connexion nœud à nœud.
CBID	Identificateur du bloc de contenu	Identifiant unique du bloc de contenu en cours de transfert.
CTDR	Direction de transfert	Indique si le transfert CBID a été initié par Push ou par Pull : PUSH : l'opération de transfert a été demandée par l'entité émettrice. EXTRACTION : l'opération de transfert a été demandée par l'entité destinataire.
CTSR	Entité source	ID de nœud de la source (expéditeur) du transfert CBID.
CTD	Entité de destination	ID de nœud de la destination (récepteur) du transfert CBID.

Code	Champ	Description
CTSS	Nombre de séquences de début	Indique le premier nombre de séquences demandé. En cas de réussite, le transfert commence à partir de ce nombre de séquences.
CTE	Nombre de séquences de fin prévu	Indique le dernier nombre de séquences demandé. En cas de réussite, le transfert est considéré comme terminé lorsque ce nombre de séquences a été reçu.
RSLT	Statut de début du transfert	État au moment du démarrage du transfert : CMC : le transfert a démarré avec succès.

Ce message d'audit signifie qu'une opération de transfert de données nœud à nœud a été lancée sur un seul élément de contenu, tel qu'identifié par son identificateur de bloc de contenu. L'opération demande des données de « nombre de séquences de début » à « nombre de séquences de fin attendu ». Les nœuds d'envoi et de réception sont identifiés par leurs ID de nœud. Ces informations peuvent être utilisées pour suivre le flux de données du système et lorsqu'elles sont associées à des messages d'audit de stockage, pour vérifier le nombre de répliques.

CBSE : fin de l'envoi de l'objet

Lorsque le transfert d'un bloc de contenu d'un nœud à un autre est terminé, ce message est émis par l'entité source.

Code	Champ	Description
CNID	Identificateur de connexion	Identifiant unique de la session/connexion nœud à nœud.
CBID	Identificateur du bloc de contenu	Identifiant unique du bloc de contenu en cours de transfert.
CTDR	Direction de transfert	Indique si le transfert CBID a été initié par Push ou par Pull : PUSH : l'opération de transfert a été demandée par l'entité émettrice. EXTRACTION : l'opération de transfert a été demandée par l'entité destinataire.
CTSR	Entité source	ID de nœud de la source (expéditeur) du transfert CBID.
CTD	Entité de destination	ID de nœud de la destination (récepteur) du transfert CBID.
CTSS	Nombre de séquences de début	Indique le nombre de séquences sur lesquelles le transfert a démarré.

Code	Champ	Description
CTAS	Nombre de séquences de fin réelles	Indique que le dernier nombre de séquences a été transféré avec succès. Si le nombre de séquences de fin réelles est le même que le nombre de séquences de début et que le résultat du transfert n'a pas réussi, aucune donnée n'a été échangée.
RSLT	Résultat du transfert	Résultat de l'opération de transfert (du point de vue de l'entité émettrice) : SUC : transfert terminé avec succès ; tous les comptes de séquence demandés ont été envoyés. CONL : connexion perdue pendant le transfert CTMO : expiration de la connexion pendant l'établissement ou le transfert UNRE : ID de nœud de destination inaccessible CRPT : transfert terminé en raison de la réception de données corrompues ou non valides

Ce message d'audit signifie qu'une opération de transfert des données nœud à nœud est terminée. Si le résultat du transfert a réussi, l'opération a transféré les données de « nombre de séquences de début » à « nombre de séquences de fin réelles ». Les nœuds d'envoi et de réception sont identifiés par leurs ID de nœud. Ces informations peuvent être utilisées pour suivre le flux de données système et pour localiser, tabuler et analyser les erreurs. Lorsqu'il est associé à des messages d'audit du stockage, il peut également être utilisé pour vérifier le nombre de répliques.

CGRR : demande de réplication croisée

Ce message est généré lorsque StorageGRID tente une opération de réplication multigrille pour répliquer des objets entre des compartiments dans une connexion de fédération de grille. Un message d'audit est envoyé uniquement si la demande a échoué de façon permanente (RÉSULTAT GIR).

Code	Champ	Description
S3AI	ID de compte locataire S3	ID du compte de locataire qui détient le compartiment à partir duquel l'objet est répliqué.
GFID	ID de connexion de fédération de grille	ID de la connexion de fédération de grille utilisée pour la réplication inter-grille.

Code	Champ	Description
OPER	Opération CGR	Type d'opération de réplication inter-grille qui a été tentée : • 0 = objet répliqué • 1 = objet multipièce répliqué • 2 = marqueur de suppression répliqué
S3BK	Compartiment S3	Nom du compartiment S3.
S3KY	Clé S3	Le nom de la clé S3 n'inclut pas le nom du compartiment.
VSID	ID de version	ID de version de la version spécifique d'un objet en cours de réplication.
RSLT	Code de résultat	Renvoie réussi (SUCS) ou erreur générale (GERR).

EBDL : suppression du compartiment vide

Le scanner ILM a supprimé un objet d'un compartiment qui supprime tous les objets (en cours d'exécution d'une opération de compartiment vide).

Code	Champ	Description
CSIZ	Taille de l'objet	Taille de l'objet en octets.
CHEMIN	Compartiment/clé S3	Nom du compartiment S3 et nom de la clé S3.
SEGC	UUID de conteneur	UUID du conteneur pour l'objet segmenté. Cette valeur n'est disponible que si l'objet est segmenté.
UUID	Identifiant unique universel	Identifiant de l'objet dans le système StorageGRID.
RSLT	Résultat de l'opération de suppression	Résultat de l'événement, du processus ou de la transaction. Si n'est pas pertinent pour un message, AUCUN n'est utilisé plutôt que LES CMC pour que le message ne soit pas filtré accidentellement.

EBKR : demande de godet vide

Ce message indique qu'un utilisateur a envoyé une demande d'activation ou de désactivation de compartiment vide (c'est-à-dire de supprimer des objets de compartiment ou d'arrêter de supprimer des objets).

Code	Champ	Description
BUID	UUID de compartiment	ID du compartiment.
EBJS	Configuration JSON de compartiment vide	Contient le fichier JSON représentant la configuration de compartiment vide actuelle.
S3AI	ID de compte locataire S3	ID de compte de locataire de l'utilisateur qui a envoyé la demande. Une valeur vide indique un accès anonyme.
S3BK	Compartiment S3	Nom du compartiment S3.

ECMC : fragment de données codé d'effacement manquant

Ce message d'audit indique que le système a détecté un fragment de données avec code d'effacement manquant.

Code	Champ	Description
VCMC	ID VCS	Nom du VCS contenant le bloc manquant.
CODE DE DIAGNOSTIC	ID de bloc	Identifiant du fragment avec code d'effacement manquant.
RSLT	Résultat	Ce champ a la valeur 'NONE'. RSLT est un champ de message obligatoire, mais n'est pas pertinent pour ce message particulier. 'AUCUN' est utilisé plutôt que 'UCS' pour que ce message ne soit pas filtré.

ECOC : fragment de données codé d'effacement corrompu

Ce message d'audit indique que le système a détecté un fragment de données codé par effacement corrompu.

Code	Champ	Description
VCCO	ID VCS	Nom du VCS contenant le bloc corrompu.
VLID	ID du volume	Volume RangeDB contenant le fragment codé d'effacement corrompu.
CCID	ID de bloc	Identificateur du fragment codé d'effacement corrompu.

Code	Champ	Description
RSLT	Résultat	Ce champ a la valeur 'NONE'. RSLT est un champ de message obligatoire, mais n'est pas pertinent pour ce message particulier. 'AUCUN' est utilisé plutôt que 'UCS' pour que ce message ne soit pas filtré.

ETAF : échec de l'authentification de sécurité

Ce message est généré lorsqu'une tentative de connexion avec TLS (transport Layer Security) a échoué.

Code	Champ	Description
CNID	Identificateur de connexion	Identifiant système unique pour la connexion TCP/IP sur laquelle l'authentification a échoué.
RUID	Identité de l'utilisateur	Identifiant dépendant du service représentant l'identité de l'utilisateur distant.
RSLT	Code de motif	La raison de l'échec : SCNI : échec de l'établissement de connexion sécurisée. CERM : certificat manquant. CERT : le certificat n'était pas valide. CERE: Le certificat a expiré. CERR : le certificat a été révoqué. CSGN : la signature du certificat n'est pas valide. CSGU : le signataire de certificat était inconnu. UCRM : les informations d'identification de l'utilisateur étaient manquantes. UCRI : les informations d'identification de l'utilisateur étaient incorrectes. UCRU : les informations d'identification de l'utilisateur ont été interdites. TOUT : expiration du délai d'authentification.

Lorsqu'une connexion est établie à un service sécurisé qui utilise TLS, les informations d'identification de l'entité distante sont vérifiées à l'aide du profil TLS et de la logique supplémentaire intégrée au service. Si cette authentification échoue en raison de certificats ou d'informations d'identification non valides, inattendus ou interdits, un message d'audit est consigné. Cela permet de rechercher des tentatives d'accès non autorisées et d'autres problèmes de connexion liés à la sécurité.

Le message peut être dû à une entité distante ayant une configuration incorrecte ou à des tentatives de

présentation d'informations d'identification non valides ou interdites au système. Ce message d'audit doit être surveillé pour détecter les tentatives d'accès non autorisé au système.

GNRG : enregistrement GNDS

Le service CMN génère ce message d'audit lorsqu'un service a mis à jour ou enregistré des informations sur lui-même dans le système StorageGRID.

Code	Champ	Description
RSLT	Résultat	Résultat de la demande de mise à jour : • CMC : réussi • SUNV : service non disponible • GERR : autre panne
GNID	ID de nœud	ID de nœud du service qui a lancé la demande de mise à jour.
GNTP	Type de périphérique	Type de périphérique du nœud de grid (par exemple BLDR pour un service LDR).
GNDV	Version du modèle de périphérique	Chaîne identifiant la version du modèle de terminal du nœud de grille dans le bundle DMDL.
GNP	Groupe	Groupe auquel appartient le nœud de la grille (dans le contexte des coûts de lien et du classement des requêtes de service).
GNIA	Adresse IP	Adresse IP du nœud de la grille.

Ce message est généré chaque fois qu'un nœud de la grille met à jour son entrée dans le pack Grid Nodes.

GNUR : non-inscription du GNDS

Le service CMN génère ce message d'audit lorsqu'un service a des informations non enregistrées sur lui-même à partir du système StorageGRID.

Code	Champ	Description
RSLT	Résultat	Résultat de la demande de mise à jour : • CMC : réussi • SUNV : service non disponible • GERR : autre panne
GNID	ID de nœud	ID de nœud du service qui a lancé la demande de mise à jour.

GTED : tâche de grille terminée

Ce message d'audit indique que le service CMN a terminé le traitement de la tâche de grille spécifiée et a déplacé la tâche vers la table Historique. Si le résultat est SUC, ABRT ou ROLF, un message d'audit correspondant à la tâche de grille démarrée sera affiché. Les autres résultats indiquent que le traitement de cette tâche de grille n'a jamais démarré.

Code	Champ	Description
2	ID de tâche	Ce champ identifie de manière unique une tâche de grille générée et permet de gérer la tâche de grille tout au long de son cycle de vie. **Remarque :** l'ID de tâche est attribué au moment où une tâche de grille est générée, et non au moment où elle est soumise. Une tâche de grille donnée peut être soumise plusieurs fois. Dans ce cas, le champ ID tâche n'est pas suffisant pour lier de manière unique les messages d'audit soumis, lancés et terminés.
RSLT	Résultat	Résultat de l'état final de la tâche de grille : • SUC : la tâche de grille s'est terminée avec succès. • ABRT : la tâche de grille a été interrompue sans erreur de retour arrière. • ROLF : la tâche de grille a été interrompue et n'a pas pu terminer le processus de restauration. • ANNUL : la tâche de grille a été annulée par l'utilisateur avant son démarrage. • EXPR : la tâche de grille a expiré avant son démarrage. • IVLD : la tâche de grille n'était pas valide. • AUTH : la tâche de grille n'était pas autorisée. • DUPL : la tâche de grille a été rejetée en double.

GTST : tâche de grille démarrée

Ce message d'audit indique que le service CMN a commencé à traiter la tâche de grille spécifiée. Le message d'audit suit immédiatement le message de la tâche de grille soumise pour les tâches de grille initiées par le service interne Grid Task Submission et sélectionnées pour l'activation automatique. Pour les tâches de grille soumises dans la table en attente, ce message est généré lorsque l'utilisateur démarre la tâche de grille.

Code	Champ	Description
2	ID de tâche	Ce champ identifie de manière unique une tâche de grille générée et permet de gérer la tâche tout au long de son cycle de vie. **Remarque :** l'ID de tâche est attribué au moment où une tâche de grille est générée, et non au moment où elle est soumise. Une tâche de grille donnée peut être soumise plusieurs fois. Dans ce cas, le champ ID tâche n'est pas suffisant pour lier de manière unique les messages d'audit soumis, lancés et terminés.
RSLT	Résultat	Résultat. Ce champ n'a qu'une seule valeur : • SUC : la tâche de grille a été démarrée avec succès.

GTSU : tâche de grille soumise

Ce message d'audit indique qu'une tâche de grille a été envoyée au service CMN.

Code	Champ	Description
2	ID de tâche	Identifie de manière unique une tâche de grille générée et permet de gérer la tâche tout au long de son cycle de vie. **Remarque :** l'ID de tâche est attribué au moment où une tâche de grille est générée, et non au moment où elle est soumise. Une tâche de grille donnée peut être soumise plusieurs fois. Dans ce cas, le champ ID tâche n'est pas suffisant pour lier de manière unique les messages d'audit soumis, lancés et terminés.
TTYP	Type de tâche	Type de tâche de grille.
VER	Version de la tâche	Numéro indiquant la version de la tâche de grille.
TDSC	Description de la tâche	Description lisible par l'homme de la tâche de grille.
CUVES	Valide après horodatage	La première fois (UINT64 microsecondes à partir du 1er janvier 1970 - heure UNIX) à laquelle la tâche de grille est valide.
VBTS	Valide avant horodatage	Dernière heure (UINT64 microsecondes à partir du 1er janvier 1970 - heure UNIX) à laquelle la tâche de grille est valide.

Code	Champ	Description
TSRC	Source	Source de la tâche : • TXTB : la tâche de grille a été soumise via le système StorageGRID sous forme de bloc de texte signé. • GRILLE : la tâche de grille a été soumise via le service de soumission de tâches Grid interne.
ACTV	Type d'activation	Type d'activation : • AUTO : la tâche de grille a été soumise pour l'activation automatique. • PEND : la tâche de grille a été envoyée dans la table en attente. C'est la seule possibilité pour la source TXTB.
RSLT	Résultat	Résultat de la soumission : • SUC : la tâche de grille a été envoyée avec succès. • ECHEC : la tâche a été déplacée directement vers la table historique.

IDEL : suppression initiée ILM

Ce message est généré lorsque ILM démarre le processus de suppression d'un objet.

Le message IDEL est généré dans l'une ou l'autre des situations suivantes :

- **Pour les objets dans des compartiments S3 conformes** : ce message est généré lorsque ILM démarre le processus de suppression automatique d'un objet parce que sa période de conservation a expiré (en supposant que le paramètre de suppression automatique est activé et que la conservation légale est désactivée).
- **Pour les objets dans des compartiments S3 non conformes ou des conteneurs Swift**. Ce message est généré lorsque ILM démarre le processus de suppression d'un objet, car aucune instruction de placement dans la politique ILM active ne s'applique actuellement à cet objet.

Code	Champ	Description
CBID	Identificateur du bloc de contenu	CBID de l'objet.
CMPA	Conformité : suppression automatique	Pour les objets des compartiments S3 uniquement. 0 (false) ou 1 (true), indiquant si un objet conforme doit être supprimé automatiquement à la fin de sa période de conservation, à moins que le compartiment ne soit soumis à une conservation légale.
CMPL	Conformité : obligation légale	Pour les objets des compartiments S3 uniquement. 0 (faux) ou 1 (vrai), indiquant si le godet est actuellement en attente légale.

Code	Champ	Description
CMPR	Conformité : période de conservation	Pour les objets des compartiments S3 uniquement. Durée de conservation de l'objet en minutes.
CTME	Conformité : temps d'entrée	Pour les objets des compartiments S3 uniquement. Temps d'ingestion de l'objet. Vous pouvez ajouter la période de conservation en minutes à cette valeur pour déterminer quand l'objet peut être supprimé du compartiment.
DMRM	Supprimer l'ID de version de marqueur	ID de version du marqueur de suppression créé lors de la suppression d'un objet d'un compartiment multiversion. Les opérations sur les compartiments n'incluent pas ce champ.
CSIZ	Taille du contenu	Taille de l'objet en octets.
EMPLACEMENTS	Emplacements	L'emplacement de stockage des données d'objet dans le système StorageGRID. La valeur des EMPLACEMENTS est "" si l'objet n'a pas d'emplacement (par exemple, il a été supprimé). CLEC : pour les objets avec code d'effacement, l'ID du profil de code d'effacement et l'ID du groupe de code d'effacement appliqué aux données de l'objet. CLDI : pour les objets répliqués, l'ID de nœud LDR et l'ID de volume de l'emplacement de l'objet. CLNL : ID de nœud D'ARC de l'emplacement de l'objet si les données de l'objet sont archivées.
CHEMIN	Compartiment/clé S3 ou ID de conteneur/objet Swift	Le nom du compartiment S3 et la clé S3 ou le nom du conteneur Swift et l'identifiant de l'objet Swift.
RSLT	Résultat	Résultat de l'opération ILM. SUC : l'opération ILM a réussi.
RÈGLE	Libellé de règles	• Si un objet d'un compartiment S3 conforme est supprimé automatiquement car sa période de conservation a expiré, ce champ est vide. • Si l'objet est supprimé car il n'y a plus d'instructions de placement qui s'appliquent actuellement à l'objet, ce champ affiche l'étiquette lisible par l'homme de la dernière règle ILM appliquée à l'objet.
SGRP	Site (groupe)	S'il est présent, l'objet a été supprimé sur le site spécifié, ce qui n'est pas le site où l'objet a été ingéré.

Code	Champ	Description
UUID	Identifiant unique universel	Identifiant de l'objet dans le système StorageGRID.
VSID	ID de version	ID de version de la version spécifique d'un objet qui a été supprimé. Les opérations sur les compartiments et les objets dans les compartiments non versionnés n'incluent pas ce champ.

LKCU : nettoyage d'objet écrasé

Ce message est généré lorsque StorageGRID supprime un objet écrasé qui auparavant requiert un nettoyage pour libérer de l'espace de stockage. Un objet est écrasé lorsqu'un client S3 ou Swift écrit un objet sur un chemin déjà contenant un objet. Le processus de suppression se produit automatiquement et en arrière-plan.

Code	Champ	Description
CSIZ	Taille du contenu	Taille de l'objet en octets.
LTYP	Type de nettoyage	*Usage interne uniquement.*
LUID	UUID d'objet supprimé	Identifiant de l'objet qui a été supprimé.
CHEMIN	Compartiment/clé S3 ou ID de conteneur/objet Swift	Le nom du compartiment S3 et la clé S3 ou le nom du conteneur Swift et l'identifiant de l'objet Swift.
SEGC	UUID de conteneur	UUID du conteneur pour l'objet segmenté. Cette valeur n'est disponible que si l'objet est segmenté.
UUID	Identifiant unique universel	Identifiant de l'objet qui existe toujours. Cette valeur est disponible uniquement si l'objet n'a pas été supprimé.

LLST : emplacement perdu

Ce message est généré chaque fois qu'un emplacement pour une copie d'objet (répliquée ou codée d'effacement) est introuvable.

Code	Champ	Description
BIL	CBID	CBID affecté.
ECPR	Profil de codage d'effacement	Pour les données d'objet avec code d'effacement. ID du profil de code d'effacement utilisé.

Code	Champ	Description
LTYP	Type d'emplacement	CLDI (Online) : pour les données d'objet répliquées CLEC (en ligne) : pour les données d'objet avec code d'effacement CLNL (Nearline) : pour les données d'objets répliqués archivés
NON	ID de nœud source	ID de nœud sur lequel les emplacements ont été perdus.
PCLD	Chemin d'accès à l'objet répliqué	Chemin complet vers l'emplacement du disque des données de l'objet perdu. Renvoyé uniquement lorsque LTYP a une valeur CLDI (c'est-à-dire pour les objets répliqués). Prend la forme `/var/local/rangedb/2/p/13/13/00oJs6X%{h{U)SeUFxE@`
RSLT	Résultat	Toujours AUCUNE. RSLT est un champ de message obligatoire, mais n'est pas pertinent pour ce message. AUCUN n'est utilisé plutôt que LES CMC pour que ce message ne soit pas filtré.
TSRC	Déclenchement de la source	UTILISATEUR : utilisateur déclenché SYST : déclenchement du système
UUID	ID universel unique	Identifiant de l'objet affecté dans le système StorageGRID.

MGAU : message d'audit de gestion

La catégorie gestion consigne les requêtes utilisateur dans l'API de gestion. Chaque requête qui n'est pas une requête GET ou HEAD à l'API consigne une réponse avec le nom d'utilisateur, l'IP et le type de requête à l'API.

Code	Champ	Description
MDIP	Adresse IP de destination	Adresse IP du serveur (destination).
ADNM	Nom de domaine	Nom du domaine hôte.
MPAT	CHEMIN de la demande	Le chemin de la demande.
MPQP	Paramètres de requête	Paramètres de requête pour la demande.

Code	Champ	Description
MBD	Corps de la demande	Le contenu de l'organisme de demande. Lorsque le corps de réponse est enregistré par défaut, le corps de la demande est enregistré dans certains cas lorsque le corps de réponse est vide. Comme les informations suivantes ne sont pas disponibles dans le corps de réponse, elles sont extraites du corps de la demande pour les méthodes SUIVANTES : • Nom d'utilisateur et ID de compte dans **POST Authorise** • Nouvelle configuration de sous-réseaux dans **POST /grid/grid-Networks/update** • Nouveaux serveurs NTP dans **POST /grid/ntp-servers/update** • ID de serveur déclassés dans **POST /grid/serveurs/désaffecter** **Remarque :** les informations sensibles sont soit supprimées (par exemple, une clé d'accès S3), soit masquées par des astérisques (par exemple, un mot de passe).
MMD	Méthode de demande	La méthode de requête HTTP : • POST • EN • SUPPRIMER • CORRECTIF
MRSC	Code de réponse	Le code de réponse.
MRSP	Corps de réponse	Le contenu de la réponse (le corps de réponse) est consigné par défaut. **Remarque :** les informations sensibles sont soit supprimées (par exemple, une clé d'accès S3), soit masquées par des astérisques (par exemple, un mot de passe).
MSIP	Adresse IP source	Adresse IP du client (source).
UUUN	URN de l'utilisateur	URN (nom de ressource uniforme) de l'utilisateur qui a envoyé la demande.
RSLT	Résultat	Renvoie réussi (CS) ou l'erreur signalée par le back-end.

OLST : le système a détecté un objet perdu

Ce message est généré lorsque le service DDS ne trouve aucune copie d'un objet dans le système StorageGRID.

Code	Champ	Description
CBID	Identificateur du bloc de contenu	CBID de l'objet perdu.
NON	ID de nœud	S'il est disponible, dernier emplacement direct ou proche de la ligne connue de l'objet perdu. Il est possible d'avoir uniquement l'ID de nœud sans ID de volume si les informations sur le volume ne sont pas disponibles.
CHEMIN	Compartiment/clé S3 ou ID de conteneur/objet Swift	Si disponible, le nom du compartiment S3 et la clé S3 ou le nom du conteneur Swift et l'identifiant d'objet Swift.
RSLT	Résultat	Ce champ a la valeur AUCUNE. RSLT est un champ de message obligatoire, mais n'est pas pertinent pour ce message. AUCUN n'est utilisé plutôt que LES CMC pour que ce message ne soit pas filtré.
UUID	ID universel unique	Identificateur de l'objet perdu dans le système StorageGRID.
VOLI	ID du volume	Le cas échéant, l'ID de volume du nœud de stockage ou du nœud d'archivage pour le dernier emplacement connu de l'objet perdu.

ORLM : règles d'objet respectées

Ce message est généré lorsque l'objet est stocké et copié comme spécifié par les règles ILM.

> Le message ORLM n'est pas généré lorsqu'un objet est stocké avec succès par la règle de création de 2 copies par défaut si une autre règle de la stratégie utilise le filtre avancé taille d'objet.

Code	Champ	Description
BUID	Cueilleur de godet	Champ ID de compartiment. Utilisé pour les opérations internes. S'affiche uniquement si STAT est PRGD.
CBID	Identificateur du bloc de contenu	CBID de l'objet.
CSIZ	Taille du contenu	Taille de l'objet en octets.

Code	Champ	Description
EMPLACEMENTS	Emplacements	L'emplacement de stockage des données d'objet dans le système StorageGRID. La valeur des EMPLACEMENTS est "" si l'objet n'a pas d'emplacement (par exemple, il a été supprimé). CLEC : pour les objets avec code d'effacement, l'ID du profil de code d'effacement et l'ID du groupe de code d'effacement appliqué aux données de l'objet. CLDI : pour les objets répliqués, l'ID de nœud LDR et l'ID de volume de l'emplacement de l'objet. CLNL : ID de nœud D'ARC de l'emplacement de l'objet si les données de l'objet sont archivées.
CHEMIN	Compartiment/clé S3 ou ID de conteneur/objet Swift	Le nom du compartiment S3 et la clé S3 ou le nom du conteneur Swift et l'identifiant de l'objet Swift.
RSLT	Résultat	Résultat de l'opération ILM. SUC : l'opération ILM a réussi.
RÈGLE	Libellé de règles	Étiquette lisible par l'homme donnée à la règle ILM appliquée à cet objet.
SEGC	UUID de conteneur	UUID du conteneur pour l'objet segmenté. Cette valeur n'est disponible que si l'objet est segmenté.
SGCB	CBID conteneur	CBID du conteneur pour l'objet segmenté. Cette valeur n'est disponible que pour les objets segmentés et partitionnés.
URGENCE	État	État de l'opération ILM. L'OPÉRATION ILM est terminée pour l'objet. DFER: L'objet a été marqué pour une future réévaluation ILM. PRGD : l'objet a été supprimé du système StorageGRID. NLOC : les données d'objet ne sont plus disponibles dans le système StorageGRID. Cet état peut indiquer que toutes les copies des données d'objet sont manquantes ou endommagées.
UUID	Identifiant unique universel	Identifiant de l'objet dans le système StorageGRID.

Code	Champ	Description
VSID	ID de version	L'ID de version d'un nouvel objet créé dans un compartiment multiversion. Les opérations sur les compartiments et les objets dans les compartiments non versionnés n'incluent pas ce champ.

Le message d'audit ORLM peut être émis plusieurs fois pour un seul objet. Par exemple, il est émis chaque fois que l'un des événements suivants se produit :

- Les règles ILM de l'objet sont satisfaites à jamais.
- Les règles ILM de l'objet sont satisfaites pour cette époque.
- Les règles ILM ont supprimé l'objet.
- Le processus de vérification en arrière-plan détecte qu'une copie des données d'objet répliqué est corrompue. Le système StorageGRID effectue une évaluation ILM pour remplacer l'objet corrompu.

Informations associées

- "Transactions d'ingestion d'objets"
- "Transactions de suppression d'objet"

OVWR : remplacement d'objet

Ce message est généré lorsqu'une opération externe (client-demandé) provoque le remplacement d'un objet par un autre objet.

Code	Champ	Description
CBID	Identifiant de bloc de contenu (nouveau)	CBID du nouvel objet.
CSIZ	Taille d'objet précédente	Taille, en octets, de l'objet à remplacer.
OCBD	Identifiant de bloc de contenu (précédent)	CBID de l'objet précédent.
UUID	ID universel unique (nouveau)	Identifiant du nouvel objet dans le système StorageGRID.
OUID	ID universel unique (précédent)	Identifiant de l'objet précédent dans le système StorageGRID.
CHEMIN	Chemin d'accès à l'objet S3 ou Swift	Chemin d'accès à l'objet S3 ou Swift utilisé pour le nouvel objet ou le précédent

Code	Champ	Description
RSLT	Code de résultat	Résultat de la transaction de remplacement d'objet. Le résultat est toujours : CMC : réussi
SGRP	Site (groupe)	S'il est présent, l'objet écrasé a été supprimé sur le site spécifié, ce qui n'est pas le site où l'objet écrasé a été ingéré.

S3SL: Demande S3 Select

Ce message consigne une fin d'étude après le renvoi d'une demande S3 Select au client. Le message S3SL peut inclure des détails de message d'erreur et de code d'erreur. La demande n'a peut-être pas abouti.

Code	Champ	Description
BYSC	Octets analysés	Nombre d'octets analysés (reçus) à partir des nœuds de stockage. BYSC et BYPR sont susceptibles d'être différents si l'objet est compressé. Si l'objet est compressé, BYSC aura le nombre d'octets compressés et BYPR les octets après décompression.
MODÈLE BYPR	Octets traités	Nombre d'octets traités. Indique le nombre d'octets analysés ou traités par un travail S3 Select.
MODÈLE BYRT	Octets renvoyés	Nombre d'octets renvoyés par une tâche S3 Select au client.
RÉFÉRENTIEL	Enregistrements traités	Nombre d'enregistrements ou de lignes qu'un travail S3 Select a reçus des nœuds de stockage.
REIU	Documents renvoyés	Nombre d'enregistrements ou de lignes qu'un travail S3 Select a renvoyé au client.
JOFI	Travail terminé	Indique si le traitement du travail S3 Select est terminé ou non. Si cette valeur est faux, le travail n'a pas pu se terminer et les champs d'erreur contiennent probablement des données. Le client a peut-être reçu des résultats partiels ou aucun résultat.
REID	ID de la demande	Identifiant de la demande S3 Select.
EXTM	Heure d'exécution	Temps, en secondes, nécessaire à la réalisation de S3 Select Job.
GROUPE DE GESTION	Message d'erreur	Message d'erreur généré par le travail S3 Select.

Code	Champ	Description
QTÉ	Type d'erreur	Type d'erreur généré par le travail S3 Select.
ERST	Erreur Stacktrace	Erreur Stacktrace générée par le travail S3 Select.
S3BK	Compartiment S3	Nom du compartiment S3.
S3AK	ID de clé d'accès S3 (expéditeur de la demande)	ID de clé d'accès S3 pour l'utilisateur qui a envoyé la demande.
S3AI	ID de compte de locataire S3 (expéditeur de la demande)	ID de compte de locataire de l'utilisateur qui a envoyé la demande.
S3KY	Clé S3	Le nom de la clé S3 n'inclut pas le nom du compartiment.

SADD : désactivation de l'audit de sécurité

Ce message indique que le service d'origine (ID de nœud) a désactivé la journalisation des messages d'audit ; les messages d'audit ne sont plus collectés ou livrés.

Code	Champ	Description
AETM	Activer la méthode	Méthode utilisée pour désactiver l'audit.
AEUN	Nom d'utilisateur	Nom d'utilisateur qui a exécuté la commande pour désactiver la journalisation d'audit.
RSLT	Résultat	Ce champ a la valeur AUCUNE. RSLT est un champ de message obligatoire, mais n'est pas pertinent pour ce message. AUCUN n'est utilisé plutôt que LES CMC pour que ce message ne soit pas filtré.

Ce message implique que la journalisation était déjà activée, mais qu'elle a été désactivée. Ces éléments sont généralement utilisés uniquement lors de l'ingestion en bloc afin d'améliorer les performances du système. Suite à l'activité groupée, l'audit est restauré (SADE) et la capacité de désactivation de l'audit est ensuite bloquée de manière permanente.

SADE : activation de l'audit de sécurité

Ce message indique que le service d'origine (ID de nœud) a restauré la journalisation des messages d'audit ; les messages d'audit sont de nouveau collectés et livrés.

Code	Champ	Description
AETM	Activer la méthode	Méthode utilisée pour activer l'audit.
AEUN	Nom d'utilisateur	Nom d'utilisateur qui a exécuté la commande pour activer la journalisation d'audit.
RSLT	Résultat	Ce champ a la valeur AUCUNE. RSLT est un champ de message obligatoire, mais n'est pas pertinent pour ce message. AUCUN n'est utilisé plutôt que LES CMC pour que ce message ne soit pas filtré.

Ce message implique que la consignation a été précédemment désactivée (SADD), mais qu'elle a maintenant été restaurée. Ces éléments sont généralement utilisés uniquement lors de l'ingestion en bloc afin d'améliorer les performances du système. Suite à l'activité groupée, l'audit est restauré et la fonctionnalité de désactivation de l'audit est bloquée définitivement.

SCMT : validation du magasin d'objets

Le contenu de la grille n'est pas disponible ou reconnu comme stocké tant qu'il n'a pas été engagé (c'est-à-dire qu'il a été stocké de manière persistante). Le contenu stocké de manière persistante a été entièrement écrit sur le disque et a transmis des contrôles d'intégrité liés. Ce message est émis lorsqu'un bloc de contenu est attribué au stockage.

Code	Champ	Description
CBID	Identificateur du bloc de contenu	Identifiant unique du bloc de contenu engagé dans le stockage permanent.
RSLT	Code de résultat	Statut au moment où l'objet était stocké sur le disque : SUCS : objet enregistré avec succès.

Ce message signifie qu'un bloc de contenu donné a été complètement stocké et vérifié, et qu'il peut maintenant être demandé. Il peut être utilisé pour suivre le flux de données dans le système.

SDEL : SUPPRESSION S3

Lorsqu'un client S3 émet une transaction DE SUPPRESSION, une demande de suppression de l'objet ou du compartiment spécifié ou de suppression d'une sous-ressource de compartiment/objet est formulée. Ce message est émis par le serveur si la transaction a réussi.

Code	Champ	Description
CBID	Identificateur du bloc de contenu	Identifiant unique du bloc de contenu demandé. Si le CBID est inconnu, ce champ est défini sur 0. Les opérations sur les compartiments n'incluent pas ce champ.

Code	Champ	Description
CNCH	En-tête de contrôle de cohérence	Valeur de l'en-tête de la requête HTTP de contrôle de cohérence, s'il est présent dans la demande.
CNID	Identificateur de connexion	Identifiant système unique pour la connexion TCP/IP.
CSIZ	Taille du contenu	Taille de l'objet supprimé en octets. Les opérations sur les compartiments n'incluent pas ce champ.
DMRM	Supprimer l'ID de version de marqueur	ID de version du marqueur de suppression créé lors de la suppression d'un objet d'un compartiment multiversion. Les opérations sur les compartiments n'incluent pas ce champ.
GFID	ID de connexion de fédération de grille	ID de connexion de la connexion de fédération de grille associée à une demande de suppression de réplication de grille croisée. Inclus uniquement dans les journaux d'audit sur la grille de destination.
GFSA	ID de compte source de fédération de grille	ID de compte du locataire sur la grille source pour une demande de suppression de réplication multigrille. Inclus uniquement dans les journaux d'audit sur la grille de destination.
HTRH	En-tête de requête HTTP	Liste des noms et valeurs d'en-tête de requête HTTP consignés sélectionnés lors de la configuration. `` `X-Forwarded-For` est automatiquement inclus si elle est présente dans la demande et si `X-Forwarded-For` La valeur est différente de l'adresse IP de l'expéditeur de la demande (champ d'audit SAIP). `` `x-amz-bypass-governance-retention` est automatiquement inclus s'il est présent dans la demande.
MTME	Heure de la dernière modification	Horodatage Unix, en microsecondes, indiquant quand l'objet a été modifié pour la dernière fois.
RSLT	Code de résultat	Résultat de la transaction DE SUPPRESSION. Le résultat est toujours : CMC : réussi

Code	Champ	Description
S3AI	ID de compte de locataire S3 (expéditeur de la demande)	ID de compte de locataire de l'utilisateur qui a envoyé la demande. Une valeur vide indique un accès anonyme.
S3AK	ID de clé d'accès S3 (expéditeur de la demande)	ID de clé d'accès S3 écrasé pour l'utilisateur qui a envoyé la demande. Une valeur vide indique un accès anonyme.
S3BK	Compartiment S3	Nom du compartiment S3.
S3KY	Clé S3	Le nom de la clé S3 n'inclut pas le nom du compartiment. Les opérations sur les compartiments n'incluent pas ce champ.
S3SR	Sous-ressource S3	Le godet ou la sous-ressource d'objet utilisé, le cas échéant.
CCUA	Nom du compte de locataire S3 (expéditeur de la demande)	Nom du compte de tenant pour l'utilisateur qui a envoyé la demande. Vide pour les demandes anonymes.
SAIP	Adresse IP (expéditeur de la demande)	Adresse IP de l'application client qui a fait la demande.
SBAC	Nom de compte de locataire S3 (propriétaire du compartiment)	Nom du compte du locataire pour le propriétaire du compartiment. Permet d'identifier les accès inter-comptes ou anonymes.
SBAI	ID de compte de locataire S3 (propriétaire du compartiment)	ID du compte du locataire du propriétaire du compartiment cible. Permet d'identifier les accès inter-comptes ou anonymes.
SGRP	Site (groupe)	S'il est présent, l'objet a été supprimé sur le site spécifié, ce qui n'est pas le site où l'objet a été ingéré.
SUSR	URN de l'utilisateur S3 (expéditeur de la demande)	L'ID du compte de locataire et le nom d'utilisateur de l'utilisateur qui fait la demande. L'utilisateur peut être un utilisateur local ou LDAP. Par exemple : `urn:sgws:identity::03393893651506583485:root` Vide pour les demandes anonymes.
TEMPS	Temps	Temps de traitement total de la demande en microsecondes.

Code	Champ	Description
TIP	Adresse IP de l'équilibreur de charge approuvée	Si la demande a été routée par un équilibreur de charge de couche 7 approuvé, l'adresse IP de l'équilibreur de charge.
UUID	Identifiant unique universel	Identifiant de l'objet dans le système StorageGRID.
VSID	ID de version	ID de version de la version spécifique d'un objet qui a été supprimé. Les opérations sur les compartiments et les objets dans les compartiments non versionnés n'incluent pas ce champ.

SGET : OBTENEZ S3

Lorsqu'un client S3 émet une transaction GET, une demande est formulée pour extraire un objet ou répertorier les objets dans un compartiment, ou pour supprimer une sous-ressource de compartiment/objet. Ce message est émis par le serveur si la transaction a réussi.

Code	Champ	Description
CBID	Identificateur du bloc de contenu	Identifiant unique du bloc de contenu demandé. Si le CBID est inconnu, ce champ est défini sur 0. Les opérations sur les compartiments n'incluent pas ce champ.
CNCH	En-tête de contrôle de cohérence	Valeur de l'en-tête de la requête HTTP de contrôle de cohérence, s'il est présent dans la demande.
CNID	Identificateur de connexion	Identifiant système unique pour la connexion TCP/IP.
CSIZ	Taille du contenu	Taille de l'objet récupéré en octets. Les opérations sur les compartiments n'incluent pas ce champ.
HTRH	En-tête de requête HTTP	Liste des noms et valeurs d'en-tête de requête HTTP consignés sélectionnés lors de la configuration. `` `X-Forwarded-For` est automatiquement inclus si elle est présente dans la demande et si `X-Forwarded-For` La valeur est différente de l'adresse IP de l'expéditeur de la demande (champ d'audit SAIP). ``

Code	Champ	Description
AU RANG	Plage lue	Pour les opérations de lecture de plage uniquement. Indique la plage d'octets lus par cette demande. La valeur après la barre oblique (/) indique la taille de l'objet entier.
RSLT	Code de résultat	Résultat de la transaction GET. Le résultat est toujours : CMC : réussi
S3AI	ID de compte de locataire S3 (expéditeur de la demande)	ID de compte de locataire de l'utilisateur qui a envoyé la demande. Une valeur vide indique un accès anonyme.
S3AK	ID de clé d'accès S3 (expéditeur de la demande)	ID de clé d'accès S3 écrasé pour l'utilisateur qui a envoyé la demande. Une valeur vide indique un accès anonyme.
S3BK	Compartiment S3	Nom du compartiment S3.
S3KY	Clé S3	Le nom de la clé S3 n'inclut pas le nom du compartiment. Les opérations sur les compartiments n'incluent pas ce champ.
S3SR	Sous-ressource S3	Le godet ou la sous-ressource d'objet utilisé, le cas échéant.
CCUA	Nom du compte de locataire S3 (expéditeur de la demande)	Nom du compte de tenant pour l'utilisateur qui a envoyé la demande. Vide pour les demandes anonymes.
SAIP	Adresse IP (expéditeur de la demande)	Adresse IP de l'application client qui a fait la demande.
SBAC	Nom de compte de locataire S3 (propriétaire du compartiment)	Nom du compte du locataire pour le propriétaire du compartiment. Permet d'identifier les accès inter-comptes ou anonymes.
SBAI	ID de compte de locataire S3 (propriétaire du compartiment)	ID du compte du locataire du propriétaire du compartiment cible. Permet d'identifier les accès inter-comptes ou anonymes.

Code	Champ	Description
SUSR	URN de l'utilisateur S3 (expéditeur de la demande)	L'ID du compte de locataire et le nom d'utilisateur de l'utilisateur qui fait la demande. L'utilisateur peut être un utilisateur local ou LDAP. Par exemple : `urn:sgws:identity::03393893651506583485:root` Vide pour les demandes anonymes.
TEMPS	Temps	Temps de traitement total de la demande en microsecondes.
TIP	Adresse IP de l'équilibreur de charge approuvée	Si la demande a été routée par un équilibreur de charge de couche 7 approuvé, l'adresse IP de l'équilibreur de charge.
UUID	Identifiant unique universel	Identifiant de l'objet dans le système StorageGRID.
VSID	ID de version	ID de version de la version spécifique d'un objet demandé. Les opérations sur les compartiments et les objets dans les compartiments non versionnés n'incluent pas ce champ.

SHEA : TÊTE S3

Lorsqu'un client S3 émet une transaction DE TÊTE, une requête est effectuée afin de vérifier l'existence d'un objet ou d'un compartiment et de récupérer les métadonnées relatives à un objet. Ce message est émis par le serveur si la transaction a réussi.

Code	Champ	Description
CBID	Identificateur du bloc de contenu	Identifiant unique du bloc de contenu demandé. Si le CBID est inconnu, ce champ est défini sur 0. Les opérations sur les compartiments n'incluent pas ce champ.
CNID	Identificateur de connexion	Identifiant système unique pour la connexion TCP/IP.
CSIZ	Taille du contenu	Taille de l'objet vérifié en octets. Les opérations sur les compartiments n'incluent pas ce champ.

Code	Champ	Description
HTRH	En-tête de requête HTTP	Liste des noms et valeurs d'en-tête de requête HTTP consignés sélectionnés lors de la configuration. `X-Forwarded-For` est automatiquement inclus si elle est présente dans la demande et si `X-Forwarded-For` La valeur est différente de l'adresse IP de l'expéditeur de la demande (champ d'audit SAIP).
RSLT	Code de résultat	Résultat de la transaction GET. Le résultat est toujours : CMC : réussi
S3AI	ID de compte de locataire S3 (expéditeur de la demande)	ID de compte de locataire de l'utilisateur qui a envoyé la demande. Une valeur vide indique un accès anonyme.
S3AK	ID de clé d'accès S3 (expéditeur de la demande)	ID de clé d'accès S3 écrasé pour l'utilisateur qui a envoyé la demande. Une valeur vide indique un accès anonyme.
S3BK	Compartiment S3	Nom du compartiment S3.
S3KY	Clé S3	Le nom de la clé S3 n'inclut pas le nom du compartiment. Les opérations sur les compartiments n'incluent pas ce champ.
CCUA	Nom du compte de locataire S3 (expéditeur de la demande)	Nom du compte de tenant pour l'utilisateur qui a envoyé la demande. Vide pour les demandes anonymes.
SAIP	Adresse IP (expéditeur de la demande)	Adresse IP de l'application client qui a fait la demande.
SBAC	Nom de compte de locataire S3 (propriétaire du compartiment)	Nom du compte du locataire pour le propriétaire du compartiment. Permet d'identifier les accès inter-comptes ou anonymes.

Code	Champ	Description
SBAI	ID de compte de locataire S3 (propriétaire du compartiment)	ID du compte du locataire du propriétaire du compartiment cible. Permet d'identifier les accès inter-comptes ou anonymes.
SUSR	URN de l'utilisateur S3 (expéditeur de la demande)	L'ID du compte de locataire et le nom d'utilisateur de l'utilisateur qui fait la demande. L'utilisateur peut être un utilisateur local ou LDAP. Par exemple : `urn:sgws:identity::03393893651506583485:root` Vide pour les demandes anonymes.
TEMPS	Temps	Temps de traitement total de la demande en microsecondes.
TIP	Adresse IP de l'équilibreur de charge approuvée	Si la demande a été routée par un équilibreur de charge de couche 7 approuvé, l'adresse IP de l'équilibreur de charge.
UUID	Identifiant unique universel	Identifiant de l'objet dans le système StorageGRID.
VSID	ID de version	ID de version de la version spécifique d'un objet demandé. Les opérations sur les compartiments et les objets dans les compartiments non versionnés n'incluent pas ce champ.

SPO : BORNE S3

Lorsqu'un client S3 émet une requête POST-objet, ce message est émis par le serveur si la transaction a réussi.

Code	Champ	Description
CBID	Identificateur du bloc de contenu	Identifiant unique du bloc de contenu demandé. Si le CBID est inconnu, ce champ est défini sur 0.
CNCH	En-tête de contrôle de cohérence	Valeur de l'en-tête de la requête HTTP de contrôle de cohérence, s'il est présent dans la demande.
CNID	Identificateur de connexion	Identifiant système unique pour la connexion TCP/IP.
CSIZ	Taille du contenu	Taille de l'objet récupéré en octets.

Code	Champ	Description
HTRH	En-tête de requête HTTP	Liste des noms et valeurs d'en-tête de requête HTTP consignés sélectionnés lors de la configuration. `X-Forwarded-For` est automatiquement inclus si elle est présente dans la demande et si `X-Forwarded-For` La valeur est différente de l'adresse IP de l'expéditeur de la demande (champ d'audit SAIP). (Non prévu pour SPOS).
RSLT	Code de résultat	Résultat de la demande DE restauration POST Object. Le résultat est toujours : CMC : réussi
S3AI	ID de compte de locataire S3 (expéditeur de la demande)	ID de compte de locataire de l'utilisateur qui a envoyé la demande. Une valeur vide indique un accès anonyme.
S3AK	ID de clé d'accès S3 (expéditeur de la demande)	ID de clé d'accès S3 écrasé pour l'utilisateur qui a envoyé la demande. Une valeur vide indique un accès anonyme.
S3BK	Compartiment S3	Nom du compartiment S3.
S3KY	Clé S3	Le nom de la clé S3 n'inclut pas le nom du compartiment. Les opérations sur les compartiments n'incluent pas ce champ.
S3SR	Sous-ressource S3	Le godet ou la sous-ressource d'objet utilisé, le cas échéant. Défini sur `sélectionner` pour une opération S3 Select.
CCUA	Nom du compte de locataire S3 (expéditeur de la demande)	Nom du compte de tenant pour l'utilisateur qui a envoyé la demande. Vide pour les demandes anonymes.
SAIP	Adresse IP (expéditeur de la demande)	Adresse IP de l'application client qui a fait la demande.

Code	Champ	Description
SBAC	Nom de compte de locataire S3 (propriétaire du compartiment)	Nom du compte du locataire pour le propriétaire du compartiment. Permet d'identifier les accès inter-comptes ou anonymes.
SBAI	ID de compte de locataire S3 (propriétaire du compartiment)	ID du compte du locataire du propriétaire du compartiment cible. Permet d'identifier les accès inter-comptes ou anonymes.
SFCF	Configuration des sous-ressources	Informations sur la restauration.
SUSR	URN de l'utilisateur S3 (expéditeur de la demande)	L'ID du compte de locataire et le nom d'utilisateur de l'utilisateur qui fait la demande. L'utilisateur peut être un utilisateur local ou LDAP. Par exemple : `urn:sgws:identity::03393893651506583485:root` Vide pour les demandes anonymes.
TEMPS	Temps	Temps de traitement total de la demande en microsecondes.
TIP	Adresse IP de l'équilibreur de charge approuvée	Si la demande a été routée par un équilibreur de charge de couche 7 approuvé, l'adresse IP de l'équilibreur de charge.
UUID	Identifiant unique universel	Identifiant de l'objet dans le système StorageGRID.
VSID	ID de version	ID de version de la version spécifique d'un objet demandé. Les opérations sur les compartiments et les objets dans les compartiments non versionnés n'incluent pas ce champ.

SPUT : PUT S3

Lorsqu'un client S3 émet une transaction PUT, une demande est formulée pour créer un nouvel objet ou un nouveau compartiment, ou pour supprimer une sous-ressource bucket/objet. Ce message est émis par le serveur si la transaction a réussi.

Code	Champ	Description
CBID	Identificateur du bloc de contenu	Identifiant unique du bloc de contenu demandé. Si le CBID est inconnu, ce champ est défini sur 0. Les opérations sur les compartiments n'incluent pas ce champ.

Code	Champ	Description
CMPS	Paramètres de conformité	Les paramètres de conformité utilisés lors de la création du compartiment, s'ils sont présents dans la requête PUT Bucket (tronqué aux 1024 premiers caractères).
CNCH	En-tête de contrôle de cohérence	Valeur de l'en-tête de la requête HTTP de contrôle de cohérence, s'il est présent dans la demande.
CNID	Identificateur de connexion	Identifiant système unique pour la connexion TCP/IP.
CSIZ	Taille du contenu	Taille de l'objet récupéré en octets. Les opérations sur les compartiments n'incluent pas ce champ.
GFID	ID de connexion de fédération de grille	ID de connexion de la connexion de fédération de grille associée à une demande PUT de réplication de grille croisée. Inclus uniquement dans les journaux d'audit sur la grille de destination.
GFSA	ID de compte source de fédération de grille	ID de compte du locataire sur la grille source pour une demande PUT de réplication multigrille. Inclus uniquement dans les journaux d'audit sur la grille de destination.
HTRH	En-tête de requête HTTP	Liste des noms et valeurs d'en-tête de requête HTTP consignés sélectionnés lors de la configuration. `` `X-Forwarded-For` est automatiquement inclus si elle est présente dans la demande et si `X-Forwarded-For` La valeur est différente de l'adresse IP de l'expéditeur de la demande (champ d'audit SAIP). `` `x-amz-bypass-governance-retention` est automatiquement inclus s'il est présent dans la demande.
LKEN	Verrouillage d'objet activé	Valeur de l'en-tête de demande `x-amz-bucket-object-lock-enabled`, Si présent dans la demande de godet PUT.
LKLH	Verrouillage de l'objet en attente légale	Valeur de l'en-tête de demande `x-amz-object-lock-legal-hold`, S'il est présent dans la demande D'objet PUT.

Code	Champ	Description
LKMD	Mode de conservation du verrouillage d'objet	Valeur de l'en-tête de demande `x-amz-object-lock-mode`, S'il est présent dans la demande D'objet PUT.
LKRU	Conservation de l'objet jusqu'à la date	Valeur de l'en-tête de demande `x-amz-object-lock-retain-until-date`, S'il est présent dans la demande D'objet PUT.
MTME	Heure de la dernière modification	Horodatage Unix, en microsecondes, indiquant quand l'objet a été modifié pour la dernière fois.
RSLT	Code de résultat	Résultat de la transaction PUT. Le résultat est toujours : CMC : réussi
S3AI	ID de compte de locataire S3 (expéditeur de la demande)	ID de compte de locataire de l'utilisateur qui a envoyé la demande. Une valeur vide indique un accès anonyme.
S3AK	ID de clé d'accès S3 (expéditeur de la demande)	ID de clé d'accès S3 écrasé pour l'utilisateur qui a envoyé la demande. Une valeur vide indique un accès anonyme.
S3BK	Compartiment S3	Nom du compartiment S3.
S3KY	Clé S3	Le nom de la clé S3 n'inclut pas le nom du compartiment. Les opérations sur les compartiments n'incluent pas ce champ.
S3SR	Sous-ressource S3	Le godet ou la sous-ressource d'objet utilisé, le cas échéant.
CCUA	Nom du compte de locataire S3 (expéditeur de la demande)	Nom du compte de tenant pour l'utilisateur qui a envoyé la demande. Vide pour les demandes anonymes.
SAIP	Adresse IP (expéditeur de la demande)	Adresse IP de l'application client qui a fait la demande.

Code	Champ	Description
SBAC	Nom de compte de locataire S3 (propriétaire du compartiment)	Nom du compte du locataire pour le propriétaire du compartiment. Permet d'identifier les accès inter-comptes ou anonymes.
SBAI	ID de compte de locataire S3 (propriétaire du compartiment)	ID du compte du locataire du propriétaire du compartiment cible. Permet d'identifier les accès inter-comptes ou anonymes.
SFCF	Configuration des sous-ressources	La nouvelle configuration de sous-ressource (tronquée aux 1024 premiers caractères).
SUSR	URN de l'utilisateur S3 (expéditeur de la demande)	L'ID du compte de locataire et le nom d'utilisateur de l'utilisateur qui fait la demande. L'utilisateur peut être un utilisateur local ou LDAP. Par exemple : `urn:sgws:identity::03393893651506583485:root` Vide pour les demandes anonymes.
TEMPS	Temps	Temps de traitement total de la demande en microsecondes.
TIP	Adresse IP de l'équilibreur de charge approuvée	Si la demande a été routée par un équilibreur de charge de couche 7 approuvé, l'adresse IP de l'équilibreur de charge.
ID ULID	ID de téléchargement	Inclus uniquement dans les messages SPUT pour les opérations de téléchargement multipièces complètes. Indique que toutes les pièces ont été téléchargées et assemblées.
UUID	Identifiant unique universel	Identifiant de l'objet dans le système StorageGRID.
VSID	ID de version	L'ID de version d'un nouvel objet créé dans un compartiment multiversion. Les opérations sur les compartiments et les objets dans les compartiments non versionnés n'incluent pas ce champ.
VSST	Etat de gestion des versions	Nouvel état de gestion des versions d'un compartiment. Deux États sont utilisés : « activé » ou « suspendu ». Les opérations sur les objets n'incluent pas ce champ.

SREM : Suppression du magasin d'objets

Ce message est émis lorsque le contenu est supprimé du stockage persistant et n'est plus accessible via des API régulières.

Code	Champ	Description
CBID	Identificateur du bloc de contenu	Identifiant unique du bloc de contenu supprimé du stockage permanent.
RSLT	Code de résultat	Indique le résultat des opérations de suppression de contenu. La seule valeur définie est : SUCS : contenu supprimé du stockage persistant

Ce message d'audit signifie qu'un bloc de contenu donné a été supprimé d'un nœud et ne peut plus être demandé directement. Le message peut être utilisé pour suivre le flux de contenu supprimé dans le système.

SUPD : métadonnées S3 mises à jour

Ce message est généré par l'API S3 lorsqu'un client S3 met à jour les métadonnées pour un objet ingéré. Le message est émis par le serveur si la mise à jour des métadonnées a réussi.

Code	Champ	Description
CBID	Identificateur du bloc de contenu	Identifiant unique du bloc de contenu demandé. Si le CBID est inconnu, ce champ est défini sur 0. Les opérations sur les compartiments n'incluent pas ce champ.
CNCH	En-tête de contrôle de cohérence	Valeur de l'en-tête de requête HTTP de contrôle de cohérence, s'il est présent dans la demande, lors de la mise à jour des paramètres de conformité d'un compartiment.
CNID	Identificateur de connexion	Identifiant système unique pour la connexion TCP/IP.
CSIZ	Taille du contenu	Taille de l'objet récupéré en octets. Les opérations sur les compartiments n'incluent pas ce champ.
HTRH	En-tête de requête HTTP	Liste des noms et valeurs d'en-tête de requête HTTP consignés sélectionnés lors de la configuration. `X-Forwarded-For` est automatiquement inclus si elle est présente dans la demande et si `X-Forwarded-For` La valeur est différente de l'adresse IP de l'expéditeur de la demande (champ d'audit SAIP).
RSLT	Code de résultat	Résultat de la transaction GET. Le résultat est toujours : CMC : réussi

Code	Champ	Description
S3AI	ID de compte de locataire S3 (expéditeur de la demande)	ID de compte de locataire de l'utilisateur qui a envoyé la demande. Une valeur vide indique un accès anonyme.
S3AK	ID de clé d'accès S3 (expéditeur de la demande)	ID de clé d'accès S3 écrasé pour l'utilisateur qui a envoyé la demande. Une valeur vide indique un accès anonyme.
S3BK	Compartiment S3	Nom du compartiment S3.
S3KY	Clé S3	Le nom de la clé S3 n'inclut pas le nom du compartiment. Les opérations sur les compartiments n'incluent pas ce champ.
CCUA	Nom du compte de locataire S3 (expéditeur de la demande)	Nom du compte de tenant pour l'utilisateur qui a envoyé la demande. Vide pour les demandes anonymes.
SAIP	Adresse IP (expéditeur de la demande)	Adresse IP de l'application client qui a fait la demande.
SBAC	Nom de compte de locataire S3 (propriétaire du compartiment)	Nom du compte du locataire pour le propriétaire du compartiment. Permet d'identifier les accès inter-comptes ou anonymes.
SBAI	ID de compte de locataire S3 (propriétaire du compartiment)	ID du compte du locataire du propriétaire du compartiment cible. Permet d'identifier les accès inter-comptes ou anonymes.
SUSR	URN de l'utilisateur S3 (expéditeur de la demande)	L'ID du compte de locataire et le nom d'utilisateur de l'utilisateur qui fait la demande. L'utilisateur peut être un utilisateur local ou LDAP. Par exemple : `urn:sgws:identity::03393893651506583485:root` Vide pour les demandes anonymes.
TEMPS	Temps	Temps de traitement total de la demande en microsecondes.
TIP	Adresse IP de l'équilibreur de charge approuvée	Si la demande a été routée par un équilibreur de charge de couche 7 approuvé, l'adresse IP de l'équilibreur de charge.

Code	Champ	Description
UUID	Identifiant unique universel	Identifiant de l'objet dans le système StorageGRID.
VSID	ID de version	ID de version de la version spécifique d'un objet dont les métadonnées ont été mises à jour. Les opérations sur les compartiments et les objets dans les compartiments non versionnés n'incluent pas ce champ.

SVRF : échec de la vérification du magasin d'objets

Ce message est émis chaque fois qu'un bloc de contenu échoue au processus de vérification. Chaque fois que les données d'objet répliqué sont lues ou écrites sur le disque, plusieurs vérifications et vérifications d'intégrité sont effectuées pour s'assurer que les données envoyées à l'utilisateur requérant sont identiques aux données initialement ingérées sur le système. Si l'une de ces vérifications échoue, le système met automatiquement en quarantaine les données d'objet répliqué corrompues pour les empêcher d'être récupérées à nouveau.

Code	Champ	Description
CBID	Identificateur du bloc de contenu	Identifiant unique du bloc de contenu qui a échoué à la vérification.
RSLT	Code de résultat	Type d'échec de vérification : CRCF : échec du contrôle de redondance cyclique (CRC). HMAC : échec de la vérification du code d'authentification du message basé sur le hachage (HMAC). EHSH : hachage de contenu crypté inattendu. PHSH : hachage de contenu original inattendu. SEQC : séquence de données incorrecte sur le disque. PERR : structure non valide du fichier de disque. DERR : erreur disque. FNAM : nom de fichier incorrect.

Ce message doit être surveillé de près. Les défaillances de vérification de contenu peuvent indiquer des pannes matérielles imminentes.

Pour déterminer quelle opération a déclenché le message, reportez-vous à la valeur du champ ID du module. Par exemple, une valeur SVFY indique que le message a été généré par le module Storage Verifier, c'est-à-dire la vérification en arrière-plan et STOR indique que le message a été déclenché par la récupération du contenu.

SVRU : Vérification du magasin d'objets inconnue

Le composant de stockage du service LDR analyse en continu toutes les copies des données objet répliquées dans le magasin d'objets. Ce message est émis lorsqu'une copie inconnue ou inattendue des données d'objet répliqué est détectée dans le magasin d'objets et déplacée vers le répertoire de quarantaine.

Code	Champ	Description
FPTH	Chemin du fichier	Chemin du fichier de la copie d'objet inattendue.
RSLT	Résultat	Ce champ a la valeur 'NONE'. RSLT est un champ de message obligatoire, mais n'est pas pertinent pour ce message. 'AUCUN' est utilisé plutôt que 'UCS' pour que ce message ne soit pas filtré.

Le message d'audit SVRU: Object Store Verify Unknown doit être suivi de près. Cela signifie que des copies inattendues de données objet ont été détectées dans le magasin d'objets. Cette situation doit être examinée immédiatement pour déterminer comment ces copies ont été créées, car elle peut indiquer des défaillances matérielles imminentes.

SYSD : arrêt du nœud

Lorsqu'un service est arrêté avec élégance, ce message est généré pour indiquer que l'arrêt a été demandé. Généralement, ce message est envoyé uniquement après un redémarrage ultérieur, car la file d'attente des messages d'audit n'est pas effacée avant l'arrêt. Recherchez le message SYST, envoyé au début de la séquence d'arrêt, si le service n'a pas redémarré.

Code	Champ	Description
RSLT	Nettoyer l'arrêt	La nature de l'arrêt : SUCS : le système s'est arrêté correctement.

Le message n'indique pas si le serveur hôte est arrêté, seul le service de génération de rapports. Le RSLT d'un SYSD ne peut pas indiquer un arrêt « non planifié », car le message est généré uniquement par des arrêts « corrects ».

SYST : arrêt du nœud

Lorsqu'un service est correctement arrêté, ce message est généré pour indiquer que l'arrêt a été demandé et que le service a lancé sa séquence d'arrêt. SYST peut être utilisé pour déterminer si l'arrêt a été demandé, avant le redémarrage du service (contrairement à SYSD, qui est généralement envoyé après le redémarrage du service).

Code	Champ	Description
RSLT	Nettoyer l'arrêt	La nature de l'arrêt : SUCS : le système s'est arrêté correctement.

Le message n'indique pas si le serveur hôte est arrêté, seul le service de génération de rapports. Le code RSLT d'un message SYST ne peut pas indiquer un arrêt « non planifié », car le message est généré uniquement par des arrêts « corrects ».

SYSU : démarrage du nœud

Lors du redémarrage d'un service, ce message est généré pour indiquer si l'arrêt précédent était propre (commandé) ou désordonné (inattendu).

Code	Champ	Description
RSLT	Nettoyer l'arrêt	La nature de l'arrêt : SUCS : le système a été arrêté proprement. DSDN : le système n'a pas été arrêté complètement. VRGN : le système a été démarré pour la première fois après l'installation du serveur (ou la réinstallation).

Le message n'indique pas si le serveur hôte a été démarré, seul le service de génération de rapports. Ce message peut être utilisé pour :

- Détecter la discontinuité dans la piste d'audit.
- Déterminez si un service échoue pendant le fonctionnement (étant donné que la nature distribuée du système StorageGRID peut masquer ces défaillances). Server Manager redémarre automatiquement un service en panne.

WDEL : SUPPRESSION rapide

Lorsqu'un client Swift émet une transaction DE SUPPRESSION, une demande est faite pour supprimer l'objet ou le conteneur spécifié. Ce message est émis par le serveur si la transaction a réussi.

Code	Champ	Description
CBID	Identificateur du bloc de contenu	Identifiant unique du bloc de contenu demandé. Si le CBID est inconnu, ce champ est défini sur 0. Les opérations sur les conteneurs n'incluent pas ce champ.
CSIZ	Taille du contenu	Taille de l'objet supprimé en octets. Les opérations sur les conteneurs n'incluent pas ce champ.

Code	Champ	Description
HTRH	En-tête de requête HTTP	Liste des noms et valeurs d'en-tête de requête HTTP consignés sélectionnés lors de la configuration. `X-Forwarded-For` est automatiquement inclus si elle est présente dans la demande et si `X-Forwarded-For` La valeur est différente de l'adresse IP de l'expéditeur de la demande (champ d'audit SAIP).
MTME	Heure de la dernière modification	Horodatage Unix, en microsecondes, indiquant quand l'objet a été modifié pour la dernière fois.
RSLT	Code de résultat	Résultat de la transaction DE SUPPRESSION. Le résultat est toujours : CMC : réussi
SAIP	Adresse IP du client requérant	Adresse IP de l'application client qui a fait la demande.
SGRP	Site (groupe)	S'il est présent, l'objet a été supprimé sur le site spécifié, ce qui n'est pas le site où l'objet a été ingéré.
TEMPS	Temps	Temps de traitement total de la demande en microsecondes.
TIP	Adresse IP de l'équilibreur de charge approuvée	Si la demande a été routée par un équilibreur de charge de couche 7 approuvé, l'adresse IP de l'équilibreur de charge.
UUID	Identifiant unique universel	Identifiant de l'objet dans le système StorageGRID.
WACC	ID de compte Swift	ID de compte unique tel que spécifié par le système StorageGRID.
CONEM	Conteneur Swift	Nom du conteneur Swift.
WOBJ	Objet Swift	Identifiant de l'objet Swift. Les opérations sur les conteneurs n'incluent pas ce champ.
WUSR	Utilisateur du compte Swift	Nom d'utilisateur du compte Swift qui identifie de manière unique le client effectuant la transaction.

WGET: SWIFT GET

Lorsqu'un client Swift émet une transaction GET, une demande est faite pour récupérer un objet, répertorier les objets dans un conteneur ou répertorier les conteneurs dans un compte. Ce message est émis par le serveur si la transaction a réussi.

Code	Champ	Description
CBID	Identificateur du bloc de contenu	Identifiant unique du bloc de contenu demandé. Si le CBID est inconnu, ce champ est défini sur 0. Les opérations sur les comptes et les conteneurs n'incluent pas ce champ.
CSIZ	Taille du contenu	Taille de l'objet récupéré en octets. Les opérations sur les comptes et les conteneurs n'incluent pas ce champ.
HTRH	En-tête de requête HTTP	Liste des noms et valeurs d'en-tête de requête HTTP consignés sélectionnés lors de la configuration. `X-Forwarded-For` est automatiquement inclus si elle est présente dans la demande et si `X-Forwarded-For` La valeur est différente de l'adresse IP de l'expéditeur de la demande (champ d'audit SAIP).
RSLT	Code de résultat	Résultat de la transaction GET. Le résultat est toujours CMC : réussi
SAIP	Adresse IP du client requérant	Adresse IP de l'application client qui a fait la demande.
TEMPS	Temps	Temps de traitement total de la demande en microsecondes.
TIP	Adresse IP de l'équilibreur de charge approuvée	Si la demande a été routée par un équilibreur de charge de couche 7 approuvé, l'adresse IP de l'équilibreur de charge.
UUID	Identifiant unique universel	Identifiant de l'objet dans le système StorageGRID.
WACC	ID de compte Swift	ID de compte unique tel que spécifié par le système StorageGRID.
CONEM	Conteneur Swift	Nom du conteneur Swift. Les opérations sur les comptes n'incluent pas ce champ.

Code	Champ	Description
WOBJ	Objet Swift	Identifiant de l'objet Swift. Les opérations sur les comptes et les conteneurs n'incluent pas ce champ.
WUSR	Utilisateur du compte Swift	Nom d'utilisateur du compte Swift qui identifie de manière unique le client effectuant la transaction.

WHEA: TÊTE SWIFT

Lorsqu'un client Swift émet une transaction DE TÊTE, une demande est faite pour vérifier l'existence d'un compte, d'un conteneur ou d'un objet, et pour récupérer toutes les métadonnées pertinentes. Ce message est émis par le serveur si la transaction a réussi.

Code	Champ	Description
CBID	Identificateur du bloc de contenu	Identifiant unique du bloc de contenu demandé. Si le CBID est inconnu, ce champ est défini sur 0. Les opérations sur les comptes et les conteneurs n'incluent pas ce champ.
CSIZ	Taille du contenu	Taille de l'objet récupéré en octets. Les opérations sur les comptes et les conteneurs n'incluent pas ce champ.
HTRH	En-tête de requête HTTP	Liste des noms et valeurs d'en-tête de requête HTTP consignés sélectionnés lors de la configuration. `X-Forwarded-For` est automatiquement inclus si elle est présente dans la demande et si `X-Forwarded-For` La valeur est différente de l'adresse IP de l'expéditeur de la demande (champ d'audit SAIP).
RSLT	Code de résultat	Résultat de la transaction DE TÊTE. Le résultat est toujours : CMC : réussi
SAIP	Adresse IP du client requérant	Adresse IP de l'application client qui a fait la demande.
TEMPS	Temps	Temps de traitement total de la demande en microsecondes.
TIP	Adresse IP de l'équilibreur de charge approuvée	Si la demande a été routée par un équilibreur de charge de couche 7 approuvé, l'adresse IP de l'équilibreur de charge.

Code	Champ	Description
UUID	Identifiant unique universel	Identifiant de l'objet dans le système StorageGRID.
WACC	ID de compte Swift	ID de compte unique tel que spécifié par le système StorageGRID.
CONEM	Conteneur Swift	Nom du conteneur Swift. Les opérations sur les comptes n'incluent pas ce champ.
WOBJ	Objet Swift	Identifiant de l'objet Swift. Les opérations sur les comptes et les conteneurs n'incluent pas ce champ.
WUSR	Utilisateur du compte Swift	Nom d'utilisateur du compte Swift qui identifie de manière unique le client effectuant la transaction.

WPUT : PUT SWIFT

Lorsqu'un client Swift émet une transaction PUT, une demande est faite pour créer un objet ou un conteneur. Ce message est émis par le serveur si la transaction a réussi.

Code	Champ	Description
CBID	Identificateur du bloc de contenu	Identifiant unique du bloc de contenu demandé. Si le CBID est inconnu, ce champ est défini sur 0. Les opérations sur les conteneurs n'incluent pas ce champ.
CSIZ	Taille du contenu	Taille de l'objet récupéré en octets. Les opérations sur les conteneurs n'incluent pas ce champ.
HTRH	En-tête de requête HTTP	Liste des noms et valeurs d'en-tête de requête HTTP consignés sélectionnés lors de la configuration. `X-Forwarded-For` est automatiquement inclus si elle est présente dans la demande et si `X-Forwarded-For` La valeur est différente de l'adresse IP de l'expéditeur de la demande (champ d'audit SAIP).
MTME	Heure de la dernière modification	Horodatage Unix, en microsecondes, indiquant quand l'objet a été modifié pour la dernière fois.

Code	Champ	Description
RSLT	Code de résultat	Résultat de la transaction PUT. Le résultat est toujours : CMC : réussi
SAIP	Adresse IP du client requérant	Adresse IP de l'application client qui a fait la demande.
TEMPS	Temps	Temps de traitement total de la demande en microsecondes.
TIP	Adresse IP de l'équilibreur de charge approuvée	Si la demande a été routée par un équilibreur de charge de couche 7 approuvé, l'adresse IP de l'équilibreur de charge.
UUID	Identifiant unique universel	Identifiant de l'objet dans le système StorageGRID.
WACC	ID de compte Swift	ID de compte unique tel que spécifié par le système StorageGRID.
CONEM	Conteneur Swift	Nom du conteneur Swift.
WOBJ	Objet Swift	Identifiant de l'objet Swift. Les opérations sur les conteneurs n'incluent pas ce champ.
WUSR	Utilisateur du compte Swift	Nom d'utilisateur du compte Swift qui identifie de manière unique le client effectuant la transaction.

Maintenance

Développez votre grille

Développez votre grille : présentation

Utilisez ces instructions pour étendre la capacité ou les capacités de votre système StorageGRID sans interrompre les opérations système.

À propos de ces instructions

Procédez à une extension StorageGRID pour ajouter des volumes de stockage aux nœuds de stockage, aux nouveaux nœuds grid à un site existant ou à un nouveau site.

Ces instructions s'adresse aux équipes techniques responsables de la configuration et de la prise en charge du système StorageGRID après son installation.

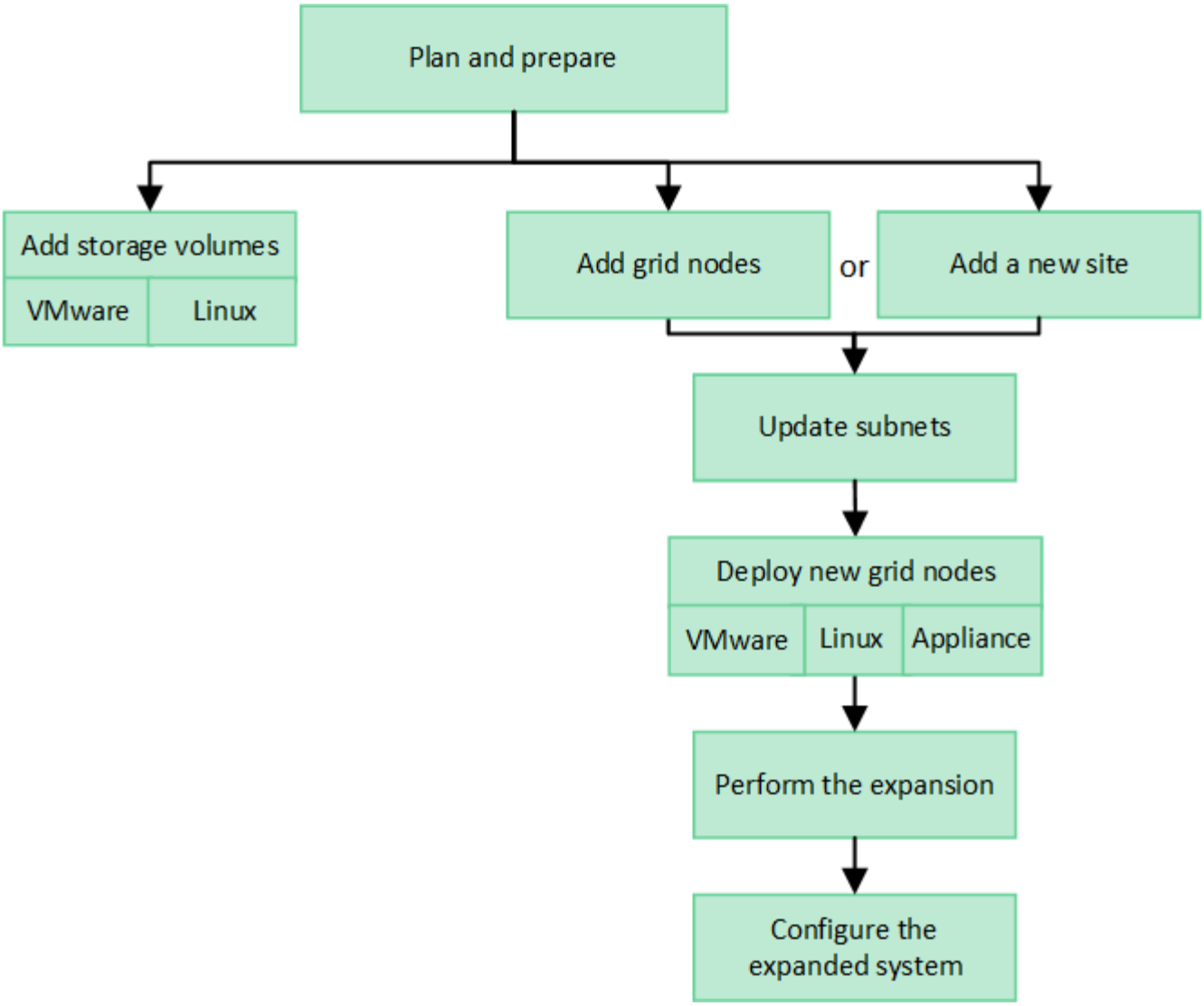
Flux de travail d'extension

La raison pour laquelle vous exécutez l'extension détermine le nombre de nouveaux nœuds de chaque type que vous devez ajouter et l'emplacement de ces nouveaux nœuds. Par exemple, les exigences en matière de nœuds sont différentes si vous effectuez une extension pour augmenter la capacité de stockage, ajouter de la capacité des métadonnées ou ajouter de la redondance ou de nouvelles fonctionnalités.

Comme indiqué dans le workflow, les étapes d'extension dépendent de l'ajout ou non de volumes de stockage à un nœud de stockage, de l'ajout de nœuds à un site existant ou de l'ajout d'un nouveau site. Dans tous les cas, vous pouvez effectuer l'extension sans interrompre le fonctionnement de votre système actuel.

Les étapes d'ajout de nœuds dépendent également de l'ajout d'appliances StorageGRID ou d'hôtes exécutant VMware ou Linux.

> « Linux » désigne un déploiement Red Hat® Enterprise Linux®, Ubuntu®, CentOS ou Debian®. Utilisez le "Matrice d'interopérabilité NetApp (IMT)" pour obtenir une liste des versions prises en charge.



Planifiez l'extension de StorageGRID

Ajoutez de la capacité de stockage

Instructions d'ajout de capacité d'objet

Pour étendre la capacité de stockage objet de votre système StorageGRID, ajoutez des volumes de stockage aux nœuds de stockage existants ou ajoutez de nouveaux nœuds de stockage aux sites existants. Vous devez ajouter de la capacité de stockage qui répond aux besoins de votre stratégie de gestion du cycle de vie des informations (ILM).

Instructions d'ajout de volumes de stockage

Avant d'ajouter des volumes de stockage à des nœuds de stockage existants, consultez les consignes et limites suivantes :

- Vous devez examiner vos règles ILM actuelles pour déterminer où et quand vous en avez besoin "ajout de volumes de stockage" pour augmenter le stockage disponible pour "objets répliqués" ou "objets avec code d'effacement".

- L'ajout de volumes de stockage ne permet pas d'augmenter la capacité de métadonnées du système, car les métadonnées d'objet sont stockées uniquement sur le volume 0.
- Chaque nœud de stockage logiciel peut prendre en charge un maximum de 16 volumes de stockage. Si vous avez besoin d'ajouter de la capacité, vous devez ajouter des nœuds de stockage.
- Vous pouvez ajouter un ou deux tiroirs d'extension à chaque appliance SG6060. Chaque tiroir d'extension ajoute 16 volumes de stockage. Avec les deux tiroirs d'extension installés, le SG6060 peut prendre en charge un total de 48 volumes de stockage.
- Vous ne pouvez pas ajouter de volumes de stockage à une autre appliance de stockage.
- Vous ne pouvez pas augmenter la taille d'un volume de stockage existant.
- Vous ne pouvez pas ajouter de volumes de stockage à un nœud de stockage en même temps que vous effectuez une mise à niveau du système, une opération de restauration ou une autre extension.

Une fois que vous avez décidé d'ajouter des volumes de stockage et que vous avez déterminé les nœuds de stockage à étendre pour répondre à la règle ILM, suivez les instructions relatives à votre type de nœud de stockage :

- Pour ajouter une ou deux tiroirs d'extension à une appliance de stockage SG6060, accédez à "Ajoutez un tiroir d'extension à SG6060 déployé".
- Pour un nœud logiciel, suivez les instructions de la section"Ajout de volumes de stockage aux nœuds de stockage".

Instructions sur l'ajout de nœuds de stockage

Avant d'ajouter des nœuds de stockage à des sites existants, consultez les consignes et limites suivantes :

- Vous devez examiner vos règles ILM actuelles pour déterminer où et quand ajouter des nœuds de stockage afin d'augmenter le stockage disponible pour "objets répliqués" ou "objets avec code d'effacement".
- Vous ne devez pas ajouter plus de 10 nœuds de stockage en une seule procédure d'extension.
- Vous pouvez ajouter des nœuds de stockage à plusieurs sites en une seule procédure d'extension.
- Vous pouvez ajouter des nœuds de stockage et d'autres types de nœuds en une seule procédure d'extension.
- Avant de démarrer la procédure d'extension, vous devez vérifier que toutes les opérations de réparation des données effectuées dans le cadre d'une restauration sont terminées. Voir "Vérifier les travaux de réparation des données".
- Si vous devez supprimer des nœuds de stockage avant ou après une extension, vous ne devez pas désaffecter plus de 10 nœuds de stockage dans une procédure de nœud de mise hors service unique.

Instructions relatives au service ADC sur les nœuds de stockage

Lors de la configuration de l'extension, vous devez choisir d'inclure le service contrôleur de domaine d'administration (ADC) sur chaque nouveau nœud de stockage. Le service ADC conserve le suivi de l'emplacement et de la disponibilité des services de réseau.

- Le système StorageGRID nécessite un "Quorum des services ADC" d'être disponible sur chaque site et en tout temps.
- Au moins trois nœuds de stockage de chaque site doivent inclure le service ADC.
- Il est déconseillé d'ajouter le service ADC à chaque nœud de stockage. L'inclusion d'un trop grand nombre de services ADC peut provoquer des ralentissements en raison de l'augmentation de la quantité de

communication entre les nœuds.

- Une seule grille ne doit pas comporter plus de 48 nœuds de stockage avec le service ADC. Cela équivaut à 16 sites avec trois services ADC sur chaque site.
- En général, lorsque vous sélectionnez le paramètre **Service ADC** pour un nouveau nœud, vous devez sélectionner **automatique**. Sélectionnez **Oui** uniquement si le nouveau nœud remplace un autre nœud de stockage qui inclut le service ADC. Comme vous ne pouvez pas désaffecter un nœud de stockage si trop peu de services ADC sont conservés, cela garantit qu'un nouveau service ADC est disponible avant la suppression de l'ancien service.
- Vous ne pouvez pas ajouter le service ADC à un nœud après son déploiement.

Ajoutez de la capacité de stockage pour les objets répliqués

Si la règle de gestion du cycle de vie des informations (ILM) de votre déploiement inclut une règle qui crée des copies répliquées des objets, vous devez tenir compte de la quantité de stockage à ajouter et de l'emplacement où ajouter les nouveaux volumes ou nœuds de stockage.

Pour savoir où ajouter du stockage, consultez les règles ILM qui créent des copies répliquées. Si les règles ILM créent au moins deux copies d'objet, prévoyez d'ajouter du stockage à chaque emplacement où les copies d'objet sont créées. À titre d'exemple simple, si vous disposez d'une grille à deux sites et d'une règle ILM pour créer une copie d'objet sur chaque site, vous devez "ajouter du stockage" pour chaque site afin d'augmenter la capacité d'objet globale de la grille. Pour plus d'informations sur la réplication d'objet, reportez-vous à la section "Qu'est-ce que la réplication ?".

Pour des raisons de performance, essayez de préserver l'équilibre entre la capacité de stockage et la puissance de calcul entre les sites. Pour cet exemple, vous devez ajouter le même nombre de nœuds de stockage à chaque site ou des volumes de stockage supplémentaires sur chaque site.

Si vous disposez d'une règle ILM plus complexe qui comprend des règles permettant de placer les objets à différents emplacements en fonction de critères tels que le nom de compartiment ou des règles qui modifient les emplacements des objets au fil du temps, votre analyse des emplacements de stockage requis pour l'extension sera similaire, mais plus complexe.

La vitesse à laquelle la capacité de stockage globale est consommée peut vous aider à déterminer la quantité de stockage à ajouter lors de l'extension et les moments où il faut ajouter de l'espace de stockage. Vous pouvez utiliser le Gestionnaire de grille pour "surveillez et tracez la capacité de stockage".

Lorsque vous planifiez une extension, pensez au délai d'acquisition et d'installation d'un stockage supplémentaire.

Ajoutez de la capacité de stockage pour les objets avec code d'effacement

Si votre règle ILM comprend une règle qui effectue des copies avec code d'effacement, vous devez prévoir où ajouter du stockage, et quand ajouter de la capacité de stockage. La quantité de stockage que vous ajoutez, et la durée de l'ajout peut affecter la capacité de stockage utilisable de la grille.

La première étape de la planification d'une extension de stockage consiste à examiner les règles de la règle ILM qui créent des objets avec code d'effacement. Étant donné que StorageGRID crée des fragments *k+m* pour chaque objet avec code d'effacement et stocke chaque fragment sur un nœud de stockage différent, vous devez vous assurer qu'au moins *k+m* les nœuds de stockage disposent d'espace pour les nouvelles données avec code d'effacement après l'extension. Si le profil de code d'effacement assure la protection contre les

pertes de site, vous devez ajouter du stockage à chaque site. Voir "Que sont les schémas de code d'effacement ?" pour plus d'informations sur les profils de code d'effacement.

Le nombre de nœuds à ajouter dépend également de la totalité des nœuds existants lors de l'extension.

Recommandations générales pour l'ajout de capacité de stockage pour les objets avec code d'effacement

Pour éviter les calculs détaillés, vous pouvez ajouter deux nœuds de stockage par site lorsque les nœuds de stockage existants atteignent 70 % de capacité.

Cette recommandation générale donne des résultats raisonnables dans le cadre d'un large éventail de schémas de codage d'effacement pour les grilles à site unique et pour les grilles où le codage d'effacement assure la protection de la perte au niveau du site.

Pour mieux comprendre les facteurs qui ont conduit à cette recommandation ou pour développer un plan plus précis pour votre site, voir "Considérations relatives au rééquilibrage des données avec code d'effacement". Pour obtenir des recommandations personnalisées et optimisées selon votre situation, contactez votre consultant en services professionnels NetApp.

Considérations relatives au rééquilibrage des données avec code d'effacement

Si vous effectuez une extension pour ajouter des nœuds de stockage et que vous utilisez des règles ILM pour effacer les données de code, vous devrez peut-être effectuer la procédure de rééquilibrage EC si vous ne pouvez pas ajouter suffisamment de nœuds de stockage pour le modèle de code d'effacement que vous utilisez.

Après avoir passé en revue ces considérations, procédez à l'extension, puis allez à "Rééquilibrent les données codées après l'ajout de nœuds de stockage" pour exécuter la procédure.

Qu'est-ce que le rééquilibrage EC ?

Le rééquilibrage EC est une procédure StorageGRID qui peut être requise après l'extension d'un nœud de stockage. La procédure est exécutée en tant que script de ligne de commande à partir du nœud d'administration principal. Lorsque vous exécutez la procédure de rééquilibrage EC, StorageGRID redistribue des fragments avec code d'effacement entre les nœuds de stockage existants et nouvellement ajoutés sur un site.

La procédure de rééquilibrage de la ce :

- Seul le déplacement des données d'objet avec code d'effacement Il ne déplace pas les données d'objet répliqué.
- Redistribue les données au sein d'un site. Il ne déplace pas les données entre les sites.
- Redistribue les données entre tous les nœuds de stockage du site. Elle ne rerépartit pas les données au sein des volumes de stockage.
- Ne prend pas en compte l'utilisation des données répliquées sur chaque nœud de stockage lors de la détermination de l'emplacement de déplacement des données avec code d'effacement.
- Redistribue uniformément les données avec code d'effacement entre les nœuds de stockage sans tenir compte des capacités relatives de chaque nœud.
- Ne distribuera pas les données avec code d'effacement aux nœuds de stockage pleins à plus de 70 %.
- Risque de diminuer les performances des opérations ILM et des opérations client S3 et Swift lorsqu'elles

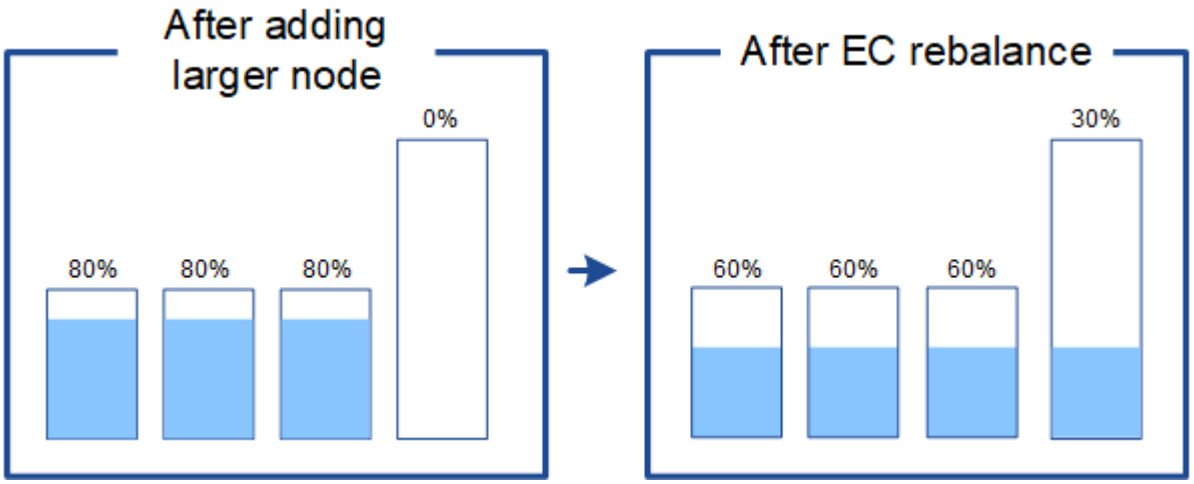
s’exécutent—des ressources supplémentaires sont nécessaires pour redistribuer les fragments de code d’effacement.

- Peut avoir besoin d’être exécuté plusieurs fois pour les systèmes comportant un très grand nombre d’objets avec code d’effacement. Pour limiter l’utilisation des ressources, le nombre maximal de déplacements est plafonné pour chaque travail.

Lorsque la procédure de rééquilibrage EC est terminée :

- Les données avec code d’effacement auront été transférées des nœuds de stockage disposant de moins d’espace disponible vers des nœuds de stockage disposant de plus d’espace disponible.
- Les données protégées des objets avec code d’effacement restent les mêmes.
- Les valeurs utilisées (%) peuvent différer d’un nœud de stockage à un autre, et ce pour deux raisons :
  - Les copies d’objet répliquées continueront à consommer de l’espace sur les nœuds existants—la procédure de rééquilibrage EC ne déplace pas les données répliquées.
  - Les nœuds de plus grande capacité seront relativement moins remplis que les nœuds de plus petite capacité, même si tous les nœuds finissent par représenter environ le même volume de données avec code d’effacement.

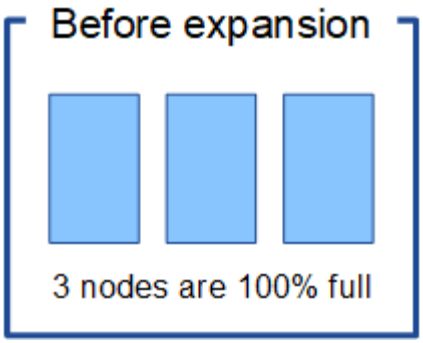
    Par exemple, supposons que trois nœuds de 200 To soient remplis à 80 % (200 et#215 ; 0.8 = 160 To sur chaque nœud, ou 480 To pour le site). Si vous ajoutez un nœud de 400 To et exécutez la procédure de rééquilibrage, tous les nœuds auront à peu près le même volume de données de code d’effacement (480/4 = 120 To). Cependant, le pourcentage utilisé pour le nœud le plus grand sera inférieur au pourcentage utilisé pour les nœuds plus petits.



Quand rééquilibrer les données avec code d’effacement

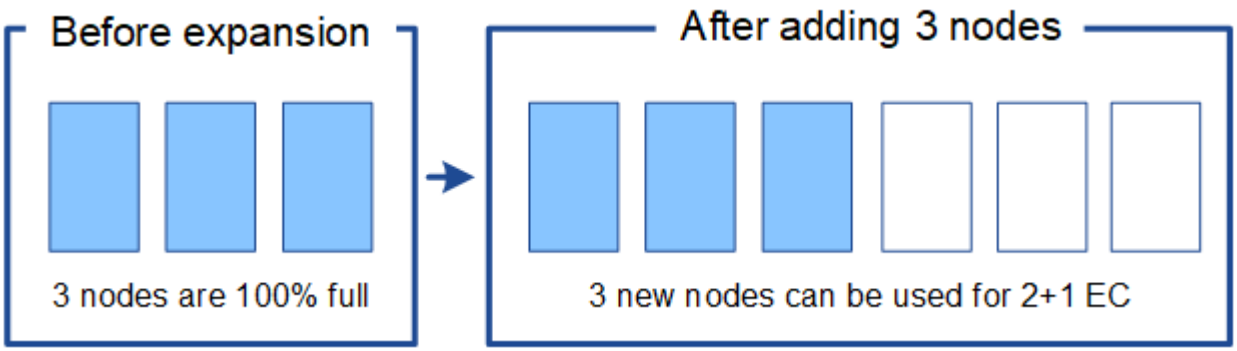
Prenons le scénario suivant :

- StorageGRID s’exécute sur un seul site, qui contient trois nœuds de stockage.
- La règle ILM utilise une règle de code d’effacement 2+1 pour tous les objets de plus de 1.0 Mo et une règle de réplication à 2 copies pour les objets plus petits.
- Tous les nœuds de stockage sont devenus complètement pleins. L’alerte **Low Object Storage** a été déclenchée au niveau de gravité principal.



Le rééquilibrage n'est pas requis si vous ajoutez suffisamment de nœuds

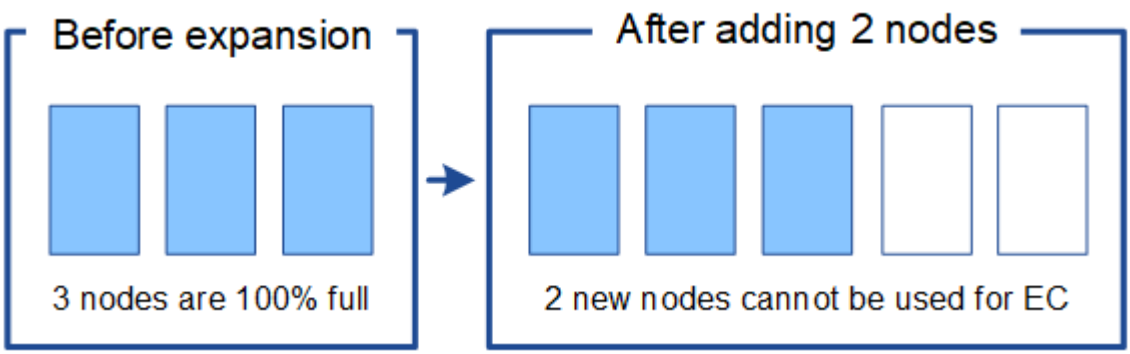
Pour savoir quand le rééquilibrage EC n'est pas nécessaire, supposons que vous ayez ajouté trois (ou plus) nouveaux nœuds de stockage. Dans ce cas, vous n'avez pas besoin d'effectuer le rééquilibrage EC. Les nœuds de stockage d'origine resteront pleins, mais les nouveaux objets utiliseront désormais les trois nouveaux nœuds pour le code d'effacement 2+1—les deux fragments de données et le fragment de parité peuvent chacun être stockés sur un nœud différent.



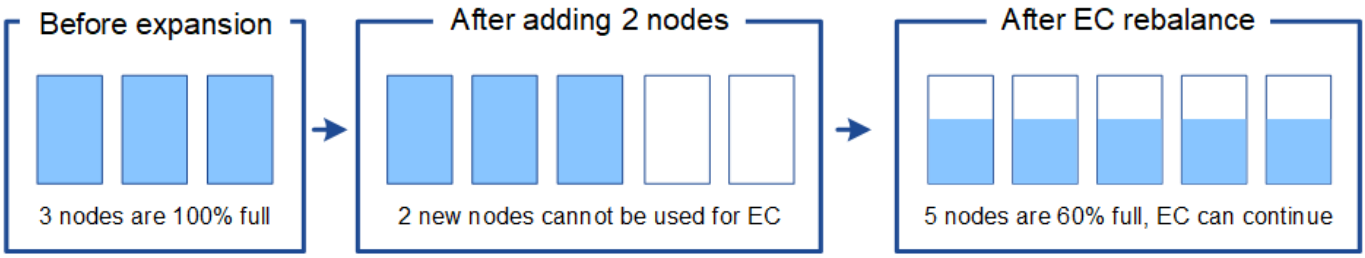
Dans ce cas, vous pouvez exécuter la procédure de rééquilibrage de l'effacement, mais le déplacement des données existantes avec code d'effacement réduit temporairement les performances de la grille, ce qui peut avoir un impact sur les opérations client.

Vous devez rééquilibrer la capacité si vous ne pouvez pas ajouter suffisamment de nœuds

Pour savoir quand un rééquilibrage EC est nécessaire, supposons que vous ne pouvez ajouter que deux nœuds de stockage au lieu de trois. Étant donné que le modèle 2+1 requiert au moins trois nœuds de stockage pour disposer d'espace disponible, les nœuds vides ne peuvent pas être utilisés pour les nouvelles données avec code d'effacement.



Pour utiliser les nouveaux nœuds de stockage, vous devez exécuter la procédure de rééquilibrage EC. À l'exécution de cette procédure, StorageGRID redistribue les données avec code d'effacement et les fragments de parité existants entre tous les nœuds de stockage sur le site. Dans cet exemple, lorsque la procédure de rééquilibrage EC est terminée, les cinq nœuds sont maintenant pleins à 60 % et les objets peuvent continuer à être ingérées sur le schéma de codage d'effacement 2+1 sur tous les nœuds de stockage.



Recommandations pour le rééquilibrage de la ce

NetApp exige un rééquilibrage de l'EC si *l'ensemble* des affirmations suivantes est vrai :

- Vous utilisez le code d'effacement pour vos données d'objet.
- L'alerte **Low Object Storage** a été déclenchée pour un ou plusieurs nœuds de stockage d'un site, ce qui indique que les nœuds sont pleins à 80 % ou plus.
- Vous ne pouvez pas ajouter suffisamment de nœuds de stockage pour le schéma de code d'effacement utilisé. Voir "Ajoutez de la capacité de stockage pour les objets avec code d'effacement".
- Vos clients S3 et Swift peuvent tolérer des performances plus faibles pour leurs opérations d'écriture et de lecture pendant l'exécution de la procédure de rééquilibrage EC.

Vous pouvez éventuellement exécuter la procédure de rééquilibrage EC si vous préférez que les nœuds de stockage soient remplis à des niveaux similaires et que vos clients S3 et Swift puissent tolérer des performances moins élevées pour leurs opérations d'écriture et de lecture pendant que la procédure de rééquilibrage EC est en cours d'exécution.

Interaction entre la procédure de rééquilibrage EC et d'autres tâches de maintenance

Vous ne pouvez pas effectuer certaines procédures de maintenance en même temps que vous exécutez la procédure de rééquilibrage EC.

Procédure	Autorisé pendant la procédure de rééquilibrage EC ?
Procédures EC de rééquilibrage supplémentaires	Non Vous ne pouvez exécuter qu'une seule procédure de rééquilibrage EC à la fois.
Procédure de mise hors service Tâche de réparation des données EC	Non • Vous ne pouvez pas démarrer une procédure de déclassement ou de réparation de données EC pendant que la procédure de rééquilibrage EC est en cours d'exécution. • Vous ne pouvez pas démarrer la procédure de rééquilibrage EC lorsque la procédure de déclassement du nœud de stockage ou de réparation de données EC est en cours d'exécution.

Procédure	Autorisé pendant la procédure de rééquilibrage EC ?
Procédure d'expansion	Non Si vous devez ajouter de nouveaux nœuds de stockage dans une extension, exécutez la procédure de rééquilibrage de l'EC après avoir ajouté tous les nouveaux nœuds.
Procédure de mise à jour	Non Si vous devez mettre à niveau le logiciel StorageGRID, effectuez la procédure de mise à niveau avant ou après l'exécution de la procédure de rééquilibrage EC. Si nécessaire, vous pouvez mettre fin à la procédure EC Rebalance pour effectuer une mise à niveau logicielle.
Procédure de clonage des nœuds d'appliance	Non Si vous devez cloner un nœud de stockage de l'appliance, exécutez la procédure de rééquilibrage EC après avoir ajouté le nouveau nœud.
Procédure de correctif	Oui. Vous pouvez appliquer un correctif StorageGRID pendant l'exécution de la procédure EC Rerééquilibrage.
Autres procédures de maintenance	Non Vous devez arrêter la procédure de rééquilibrage EC avant d'exécuter d'autres procédures de maintenance.

La façon dont ce rééquilibrage interagit avec ILM

Pendant l'exécution de la procédure de rééquilibrage EC, évitez d'apporter des modifications au ILM susceptibles de modifier l'emplacement des objets avec code d'effacement existants. Par exemple, ne commencez pas à utiliser une règle ILM dont le profil de code d'effacement est différent. Si vous devez effectuer de telles modifications ILM, vous devez mettre fin à la procédure de rééquilibrage EC.

Ajoutez de la capacité des métadonnées

Pour assurer la disponibilité de l'espace adéquat pour les métadonnées des objets, vous devez effectuer une procédure d'extension afin d'ajouter de nouveaux nœuds de stockage sur chaque site.

StorageGRID réserve de l'espace pour les métadonnées d'objet sur le volume 0 de chaque nœud de stockage. Trois copies de toutes les métadonnées d'objet sont conservées sur chaque site, réparties de manière homogène entre tous les nœuds de stockage.

Vous pouvez utiliser Grid Manager pour surveiller la capacité des métadonnées des nœuds de stockage et estimer la vitesse de consommation de la capacité des métadonnées. En outre, l'alerte **stockage de métadonnées faible** est déclenchée pour un nœud de stockage lorsque l'espace de métadonnées utilisé atteint certains seuils.

La capacité des métadonnées d'objet d'une grille peut être consommée plus rapidement que la capacité de stockage objet, selon l'utilisation de la grille. Par exemple, si vous ingérer d'importants volumes d'objets de petite taille ou si vous ajoutez de grandes quantités de métadonnées ou de balises utilisateur aux objets, vous devrez ajouter des nœuds de stockage pour augmenter la capacité des métadonnées, même si la capacité de stockage objet reste suffisante.

Pour plus d'informations, reportez-vous aux sections suivantes :

- "Gérer le stockage des métadonnées d'objet"
- "Surveillez la capacité des métadonnées d'objet pour chaque nœud de stockage"

Instructions d'augmentation de la capacité des métadonnées

Avant d'ajouter des nœuds de stockage pour augmenter la capacité des métadonnées, consultez les directives et les limites suivantes :

- En supposant une capacité de stockage objet suffisante, l'augmentation de l'espace disponible pour les métadonnées d'objet augmente le nombre d'objets que vous pouvez stocker dans votre système StorageGRID.
- Vous pouvez augmenter la capacité des métadonnées d'une grille en ajoutant un ou plusieurs nœuds de stockage à chaque site.
- L'espace réel réservé pour les métadonnées d'objet sur un nœud de stockage donné dépend de l'option de stockage de l'espace réservé aux métadonnées (paramètre pour tout le système), de la quantité de RAM allouée au nœud et de la taille du volume 0 du nœud.
- Il est impossible d'augmenter la capacité des métadonnées en ajoutant des volumes de stockage aux nœuds de stockage existants, car les métadonnées ne sont stockées que sur le volume 0.
- L'ajout d'un nouveau site ne permet pas d'augmenter la capacité des métadonnées.
- StorageGRID conserve trois copies de toutes les métadonnées d'objets sur chaque site. C'est pourquoi la capacité de métadonnées de votre système est limitée par la capacité de métadonnées de votre plus petit site.
- Lorsque vous ajoutez de la capacité des métadonnées, vous devez ajouter le même nombre de nœuds de stockage à chaque site.

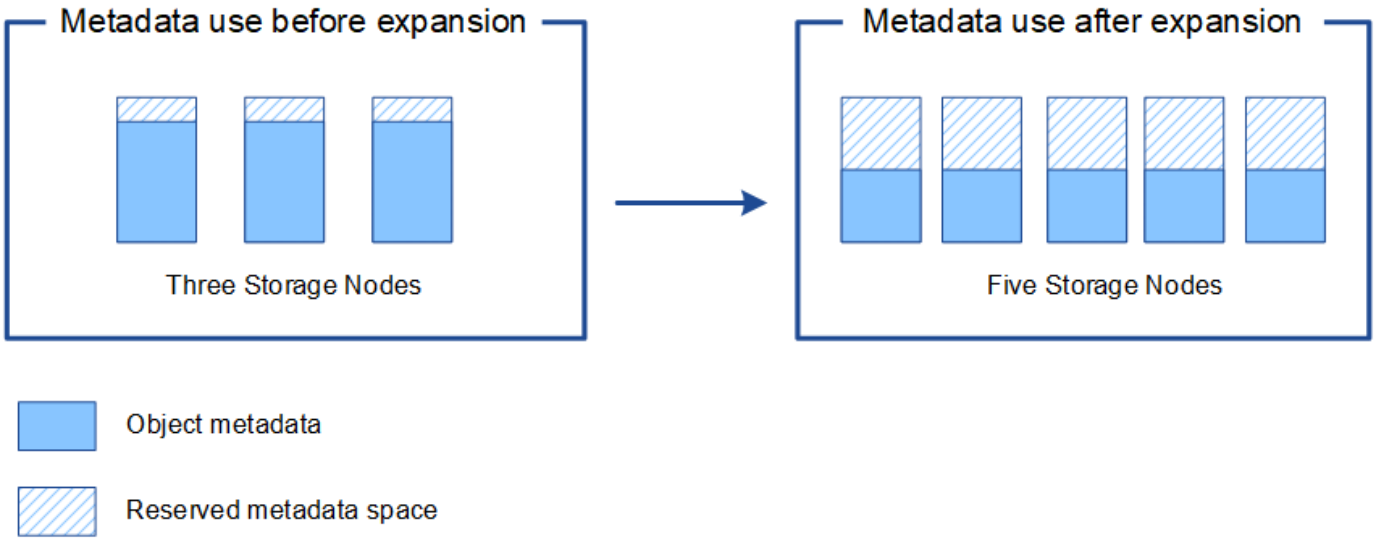
Voir la "Description de l'espace réservé aux métadonnées".

Comment les métadonnées sont redistribuées lorsque vous ajoutez des nœuds de stockage

Lorsque vous ajoutez des nœuds de stockage dans une extension, StorageGRID redistribue les métadonnées de l'objet vers les nouveaux nœuds de chaque site, ce qui augmente la capacité globale des métadonnées de la grille. Aucune action de l'utilisateur n'est requise.

La figure suivante montre comment StorageGRID redistribue les métadonnées d'objet lorsque vous ajoutez des nœuds de stockage dans une extension. La partie gauche de la figure représente le volume 0 de trois nœuds de stockage avant toute extension. Les métadonnées consomment une portion relativement importante de l'espace disponible de métadonnées de chaque nœud et l'alerte **stockage de métadonnées faible** a été déclenchée.

La partie droite de la figure montre comment les métadonnées existantes sont redistribuées après deux nœuds de stockage ajoutés au site. La quantité de métadonnées sur chaque nœud a diminué, l'alerte **stockage de métadonnées faible** n'est plus déclenchée et l'espace disponible pour les métadonnées a augmenté.



Ajoutez des nœuds grid pour ajouter des fonctionnalités à votre système

Vous pouvez ajouter de la redondance ou des fonctionnalités supplémentaires à un système StorageGRID en ajoutant de nouveaux nœuds grid à des sites existants.

Par exemple, vous pouvez choisir d'ajouter des nœuds de passerelle à utiliser dans un groupe haute disponibilité (HA) ou d'ajouter un nœud d'administration sur un site distant pour permettre la surveillance à l'aide d'un nœud local.

Vous pouvez ajouter un ou plusieurs des types de nœuds suivants à un ou plusieurs sites existants au cours d'une seule opération d'extension :

- Nœuds d'administration non primaires
- Nœuds de stockage
- Nœuds de passerelle

Lorsque vous préparez l'ajout de nœuds grid, tenez compte des limites suivantes :

- Le nœud d'administration principal est déployé lors de l'installation initiale. Vous ne pouvez pas ajouter de nœud d'administration principal pendant une extension.
- Vous pouvez ajouter des nœuds de stockage et d'autres types de nœuds dans la même extension.
- Lorsque vous ajoutez des nœuds de stockage, vous devez planifier soigneusement le nombre et l'emplacement des nouveaux nœuds. Voir "Instructions d'ajout de capacité d'objet".
- Si l'option **définir nouveau noeud par défaut** est **non fiable** sur l'onglet réseaux clients non approuvés de la page de contrôle du pare-feu, les applications clientes qui se connectent aux nœuds d'extension à l'aide du réseau client doivent se connecter à l'aide d'un port de noeud final d'équilibrage de charge (**CONFIGURATION** > **sécurité** > **contrôle du pare-feu**). Voir les instructions à "modifiez le paramètre de sécurité du nouveau nœud" et à "configurez les terminaux d'équilibrage de charge".

Ajouter un site

Vous pouvez étendre votre système StorageGRID en ajoutant un nouveau site.

Instructions pour l'ajout d'un site

Avant d'ajouter un site, vérifiez les exigences et limites suivantes :

- Vous ne pouvez ajouter qu'un site par opération d'extension.
- Vous ne pouvez pas ajouter de nœuds grid à un site existant dans le cadre d'une même extension.
- Tous les sites doivent inclure au moins trois nœuds de stockage.
- L'ajout d'un nouveau site n'augmente pas automatiquement le nombre d'objets que vous pouvez stocker. La capacité totale d'objet d'un grid dépend de la quantité de stockage disponible, de la règle ILM et de la capacité des métadonnées sur chaque site.
- Lors du dimensionnement d'un nouveau site, vous devez vous assurer qu'il inclut suffisamment de capacité de métadonnées.

  StorageGRID conserve une copie de toutes les métadonnées d'objet sur chaque site. Lorsque vous ajoutez un nouveau site, vous devez vous assurer qu'il inclut une capacité de métadonnées suffisante pour les métadonnées d'objet existantes et une capacité de métadonnées suffisante pour croître.

  Pour plus d'informations, reportez-vous aux sections suivantes :

  - "Gérer le stockage des métadonnées d'objet"
  - "Surveillez la capacité des métadonnées d'objet pour chaque nœud de stockage"
- Vous devez tenir compte de la bande passante réseau disponible entre les sites et du niveau de latence du réseau. Les mises à jour des métadonnées sont continuellement répliquées entre les sites, même si tous les objets sont stockés uniquement sur le site où ils sont ingéré.
- Votre système StorageGRID reste opérationnel pendant son développement. Vous devez donc revoir les règles ILM avant de démarrer la procédure d'extension. Vous devez vous assurer que les copies d'objet ne sont pas stockées sur le nouveau site tant que la procédure d'extension n'est pas terminée.

  Par exemple, avant de commencer l'extension, déterminez si des règles utilisent le pool de stockage par défaut (tous les nœuds de stockage). Le cas échéant, vous devez créer un nouveau pool de stockage contenant les nœuds de stockage existants et mettre à jour les règles ILM pour utiliser le nouveau pool de stockage. Sinon, les objets seront copiés sur le nouveau site dès que le premier nœud de ce site devient actif.

  Pour plus d'informations sur la modification d'ILM lors de l'ajout d'un nouveau site, consultez le "Exemple de modification d'une règle ILM".

Rassembler les matériaux nécessaires

Avant d'effectuer une opération d'extension, rassemblez les matériaux et installez et configurez tout nouveau matériel et tout nouveau réseau.

Élément	Remarques
Archive de l'installation de StorageGRID	Si vous ajoutez de nouveaux nœuds de grille ou un nouveau site, vous devez télécharger et extraire l'archive d'installation de StorageGRID. Vous devez utiliser la même version que celle actuellement en cours d'exécution sur la grille. Pour plus de détails, reportez-vous aux instructions de Téléchargement et extraction des fichiers d'installation de StorageGRID. **Remarque :** vous n'avez pas besoin de télécharger des fichiers si vous ajoutez de nouveaux volumes de stockage aux nœuds de stockage existants ou si vous installez une nouvelle appliance StorageGRID.
L'ordinateur portable de service	L'ordinateur portable de service présente les caractéristiques suivantes : • Port réseau • Client SSH (par exemple, PuTTY) • "Navigateur Web pris en charge"
`Passwords.txt` fichier	Contient les mots de passe requis pour accéder aux nœuds de la grille sur la ligne de commande. Inclus dans le package de restauration.
Phrase secrète pour le provisionnement	La phrase de passe est créée et documentée lors de l'installation initiale du système StorageGRID. La phrase de passe de provisionnement n'est pas dans le `Passwords.txt` fichier.
Documentation StorageGRID	• "Administrer StorageGRID" • "Notes de mise à jour" • Instructions d'installation pour votre plate-forme ◦ "Installez Red Hat Enterprise Linux ou CentOS" ◦ "Installez Ubuntu ou Debian" ◦ "Installez VMware"
Documentation actuelle pour votre plate-forme	Pour les versions prises en charge, reportez-vous à la section "Matrice d'interopérabilité (IMT)".

Téléchargez et extrayez les fichiers d'installation de StorageGRID

Avant de pouvoir ajouter de nouveaux nœuds de grille ou un nouveau site, vous devez télécharger l'archive d'installation StorageGRID appropriée et extraire les fichiers.

Description de la tâche

Vous devez effectuer des opérations d'extension à l'aide de la version de StorageGRID actuellement exécutée sur la grille.

Étapes

1. Accédez à "Téléchargement NetApp : StorageGRID".
2. Sélectionnez la version de StorageGRID en cours d'exécution sur la grille.
3. Connectez-vous avec le nom d'utilisateur et le mot de passe de votre compte NetApp.
4. Lisez le contrat de licence de l'utilisateur final, cochez la case, puis sélectionnez **accepter et continuer**.
5. Dans la colonne **installer StorageGRID** de la page de téléchargement, sélectionnez `.tgz` ou `.zip` fichier pour votre plate-forme.

   La version affichée dans le fichier d'archive d'installation doit correspondre à la version du logiciel actuellement installé.

   Utilisez le `.zip` Fichier si vous exécutez Windows sur l'ordinateur portable de service.

Plateforme	Archive d'installation

Red Hat Enterprise Linux ou CentOS	`StorageGRID-Webscale-`*`version`*`-RPM-`*`uniqueID`*`.zip`
	
	`StorageGRID-Webscale-`*`version`*`-RPM-`*`uniqueID`*`.tgz`

Ubuntu ou Debian ou Appliances	`StorageGRID-Webscale-`*`version`*`-DEB-`*`uniqueID`*`.zip`
	
	`StorageGRID-Webscale-`*`version`*`-DEB-`*`uniqueID`*`.tgz`

VMware	`StorageGRID-Webscale-`*`version`*`-VMware-`*`uniqueID`*`.zip`
	
	`StorageGRID-Webscale-`*`version`*`-VMware-`*`uniqueID`*`.tgz`

OpenStack/autre hyperviseur	Pour étendre un déploiement existant sur OpenStack, vous devez déployer une machine virtuelle exécutant l'une des distributions Linux prises en charge répertoriées ci-dessus et suivre les instructions appropriées pour Linux.

6. Téléchargez et extrayez le fichier d'archive.
7. Suivez les étapes appropriées pour votre plate-forme afin de choisir les fichiers dont vous avez besoin, en fonction de votre plate-forme, de la topologie de grille planifiée et de la manière dont vous allez étendre votre système StorageGRID.

   Les chemins répertoriés dans l'étape pour chaque plate-forme sont relatifs au répertoire de niveau supérieur installé par le fichier d'archive.

8. Si vous étendez un système Red Hat Enterprise Linux ou CentOS, sélectionnez les fichiers appropriés.

Chemin d'accès et nom de fichier	Description
	Fichier texte qui décrit tous les fichiers contenus dans le fichier de téléchargement StorageGRID.
	Licence gratuite qui ne fournit aucun droit d'assistance pour le produit.

Chemin d'accès et nom de fichier	Description
	Package RPM pour l'installation des images des nœuds StorageGRID sur vos hôtes RHEL ou CentOS.
	Package RPM pour l'installation du service hôte StorageGRID sur vos hôtes RHEL ou CentOS.
Outil de script de déploiement	Description
	Script Python utilisé pour automatiser la configuration d'un système StorageGRID.
	Script Python utilisé pour automatiser la configuration des appliances StorageGRID.
	Exemple de fichier de configuration à utiliser avec `configure-storagegrid.py` script.
	Exemple de script Python que vous pouvez utiliser pour vous connecter à l'API Grid Management lorsque l'authentification unique est activée. Vous pouvez également utiliser ce script pour le Federate Ping.
	Un fichier de configuration vierge à utiliser avec le `configure-storagegrid.py` script.
	Exemple de rôle et de manuel de vente Ansible pour la configuration des hôtes RHEL ou CentOS pour le déploiement de conteneurs StorageGRID. Vous pouvez personnaliser le rôle ou le PlayBook selon vos besoins.
	Exemple de script Python que vous pouvez utiliser pour vous connecter à l'API de gestion de grille lorsque l'authentification unique (SSO) est activée à l'aide d'Active Directory ou de Ping Federate.
	Script d'aide appelé par le compagnon `storagegrid-ssoauth-azure.py` Script Python pour effectuer des interactions SSO avec Azure.

Chemin d'accès et nom de fichier	Description
	Schémas API pour StorageGRID. **Remarque** : avant d'effectuer une mise à niveau, vous pouvez utiliser ces schémas pour confirmer que tout code que vous avez écrit pour utiliser les API de gestion StorageGRID sera compatible avec la nouvelle version de StorageGRID si vous ne disposez pas d'un environnement StorageGRID non productif pour le test de compatibilité de mise à niveau.

1. Si vous étendez un système Ubuntu ou Debian, sélectionnez les fichiers appropriés.

Chemin d'accès et nom de fichier	Description
	Fichier texte qui décrit tous les fichiers contenus dans le fichier de téléchargement StorageGRID.
	Un fichier de licence NetApp hors production que vous pouvez utiliser pour tester et réaliser des démonstrations de faisabilité.
	DEB paquet pour installer les images de noeud StorageGRID sur des hôtes Ubuntu ou Debian.
	Somme de contrôle MD5 pour le fichier `/debs/storagegrid-webscale-images-version-SHA.deb`.
	Paquet DEB pour l'installation du service hôte StorageGRID sur des hôtes Ubuntu ou Debian.
Outil de script de déploiement	Description
	Script Python utilisé pour automatiser la configuration d'un système StorageGRID.
	Script Python utilisé pour automatiser la configuration des appliances StorageGRID.
	Exemple de script Python que vous pouvez utiliser pour vous connecter à l'API Grid Management lorsque l'authentification unique est activée. Vous pouvez également utiliser ce script pour le Federate Ping.
	Exemple de fichier de configuration à utiliser avec `configure-storagegrid.py` script.

Chemin d'accès et nom de fichier	Description
	Un fichier de configuration vierge à utiliser avec le `configure-storagegrid.py` script.
	Exemple de rôle et de manuel de vente Ansible pour la configuration des hôtes Ubuntu ou Debian pour le déploiement de conteneurs StorageGRID. Vous pouvez personnaliser le rôle ou le PlayBook selon vos besoins.
	Exemple de script Python que vous pouvez utiliser pour vous connecter à l'API de gestion de grille lorsque l'authentification unique (SSO) est activée à l'aide d'Active Directory ou de Ping Federate.
	Script d'aide appelé par le compagnon `storagegrid-ssoauth-azure.py` Script Python pour effectuer des interactions SSO avec Azure.
	Schémas API pour StorageGRID. **Remarque** : avant d'effectuer une mise à niveau, vous pouvez utiliser ces schémas pour confirmer que tout code que vous avez écrit pour utiliser les API de gestion StorageGRID sera compatible avec la nouvelle version de StorageGRID si vous ne disposez pas d'un environnement StorageGRID non productif pour le test de compatibilité de mise à niveau.

1. Si vous étendez un système VMware, sélectionnez les fichiers appropriés.

Chemin d'accès et nom de fichier	Description
	Fichier texte qui décrit tous les fichiers contenus dans le fichier de téléchargement StorageGRID.
	Licence gratuite qui ne fournit aucun droit d'assistance pour le produit.
	Fichier de disque de machine virtuelle utilisé comme modèle pour créer des machines virtuelles de nœud de grille.
	Fichier modèle du format Open Virtualization (`.ovf`) et fichier manifeste (`.mf`) Pour le déploiement du nœud d'administration principal.

Chemin d'accès et nom de fichier	Description
	Le fichier de modèle (`.ovf`) et fichier manifeste (`.mf`) Pour le déploiement de nœuds d'administration non primaires.
	Le fichier de modèle (`.ovf`) et fichier manifeste (`.mf`) Pour le déploiement des nœuds d'archivage.
	Le fichier de modèle (`.ovf`) et fichier manifeste (`.mf`) Pour le déploiement des nœuds de passerelle.
	Le fichier de modèle (`.ovf`) et fichier manifeste (`.mf`) Pour le déploiement de nœuds de stockage basés sur des machines virtuelles.
Outil de script de déploiement	Description
	Script de shell de Bash utilisé pour automatiser le déploiement de nœuds de grille virtuels.
	Exemple de fichier de configuration à utiliser avec `deploy-vsphere-ovftool.sh` script.
	Script Python utilisé pour automatiser la configuration d'un système StorageGRID.
	Script Python utilisé pour automatiser la configuration des appliances StorageGRID.
	Exemple de script Python que vous pouvez utiliser pour vous connecter à l'API de gestion de grille lorsque l'authentification unique (SSO) est activée. Vous pouvez également utiliser ce script pour le Federate Ping.
	Exemple de fichier de configuration à utiliser avec `configure-storagegrid.py` script.
	Un fichier de configuration vierge à utiliser avec le `configure-storagegrid.py` script.
	Exemple de script Python que vous pouvez utiliser pour vous connecter à l'API de gestion de grille lorsque l'authentification unique (SSO) est activée à l'aide d'Active Directory ou de Ping Federate.

Chemin d'accès et nom de fichier	Description
	Script d'aide appelé par le compagnon `storagegrid-ssoauth-azure.py` Script Python pour effectuer des interactions SSO avec Azure.
	Schémas API pour StorageGRID. **Remarque** : avant d'effectuer une mise à niveau, vous pouvez utiliser ces schémas pour confirmer que tout code que vous avez écrit pour utiliser les API de gestion StorageGRID sera compatible avec la nouvelle version de StorageGRID si vous ne disposez pas d'un environnement StorageGRID non productif pour le test de compatibilité de mise à niveau.

1. Si vous étendez un système basé sur l'appliance StorageGRID, sélectionnez les fichiers appropriés.

Chemin d'accès et nom de fichier	Description
	DEB package pour l'installation des images de noeud StorageGRID sur vos appareils.
	Somme de contrôle MD5 pour le fichier `/debs/storagegridwebscale-images-version-SHA.deb`.

> Pour l'installation de l'appliance, ces fichiers ne sont nécessaires que si vous devez éviter le trafic réseau. L'appliance peut télécharger les fichiers requis à partir du nœud d'administration principal.

Vérification du matériel et de la mise en réseau

Avant de commencer l'extension de votre système StorageGRID, vérifiez les points suivants :

- Le matériel nécessaire pour prendre en charge les nouveaux nœuds grid ou le nouveau site a été installé et configuré.
- Tous les nouveaux nœuds disposent de chemins de communication bidirectionnels vers tous les nœuds existants et nouveaux (exigence pour le réseau Grid). Vérifiez en particulier que les ports TCP suivants sont ouverts entre les nouveaux nœuds que vous ajoutez dans l'extension et le nœud d'administration principal :
  - 1055
  - 7443
  - 8011
  - 10342

  Voir "Communications internes sur les nœuds de la grille".
- Le nœud d'administration principal peut communiquer avec tous les serveurs d'extension destinés à

héberger le système StorageGRID.

- Si l'un des nouveaux nœuds possède une adresse IP de réseau Grid sur un sous-réseau non utilisé précédemment, vous l'avez déjà "ajout du nouveau sous-réseau" À la liste des sous-réseaux du réseau de la grille. Sinon, vous devrez annuler l'extension, ajouter le nouveau sous-réseau et recommencer la procédure.
- Vous n'utilisez pas la traduction d'adresses réseau (NAT) sur le réseau de grille entre les nœuds de grille ou entre les sites StorageGRID. Lorsque vous utilisez des adresses IPv4 privées pour le réseau Grid, ces adresses doivent être directement routables à partir de chaque nœud de la grille sur chaque site. L'utilisation de la fonction NAT pour relier le réseau Grid sur un segment de réseau public n'est prise en charge que si vous utilisez une application de tunneling transparente pour tous les nœuds de la grille, ce qui signifie que les nœuds de la grille ne nécessitent aucune connaissance des adresses IP publiques.

  Cette restriction NAT est spécifique aux nœuds de la grille et au réseau Grid. Si nécessaire, vous pouvez utiliser NAT entre des clients externes et des nœuds de grille, par exemple pour fournir une adresse IP publique pour un nœud de passerelle.

Ajout de volumes de stockage

Ajout de volumes de stockage aux nœuds de stockage

Vous pouvez étendre la capacité de stockage des nœuds de stockage disposant d'au moins 16 volumes de stockage en ajoutant des volumes de stockage supplémentaires. Vous pouvez avoir besoin d'ajouter des volumes de stockage à plusieurs nœuds de stockage pour répondre aux exigences ILM des copies répliquées ou avec code d'effacement.

Avant de commencer

Avant d'ajouter des volumes de stockage, vérifiez la "instructions d'ajout de capacité d'objet" Vous devez ainsi savoir où ajouter des volumes afin de répondre aux exigences de la règle ILM.

> Ces instructions s'appliquent uniquement aux nœuds de stockage basés sur logiciel. Voir "Ajoutez un tiroir d'extension à SG6060 déployé" Apprenez à ajouter des volumes de stockage à SG6060 en installant des tiroirs d'extension. Les autres nœuds de stockage de l'appliance ne peuvent pas être étendus.

Description de la tâche

Le stockage sous-jacent d'un nœud de stockage est divisé en volumes de stockage. Les volumes de stockage sont des périphériques de stockage basés sur des blocs formatés par le système StorageGRID et montés pour stocker des objets. Chaque nœud de stockage peut prendre en charge jusqu'à 16 volumes de stockage, appelés *object stores* dans Grid Manager.

> Les métadonnées d'objet sont toujours stockées dans le magasin d'objets 0.

Chaque magasin d'objets est monté sur un volume qui correspond à son ID. Par exemple, le magasin d'objets avec un ID de 0000 correspond à l' `/var/local/rangedb/0` point de montage.

Avant d'ajouter de nouveaux volumes de stockage, utilisez la grille Manager pour afficher les magasins d'objets actuels pour chaque nœud de stockage ainsi que les points de montage correspondants. Vous pouvez utiliser ces informations lors de l'ajout de volumes de stockage.

Étapes

1. Sélectionnez **NODES** > ***site*** > ***Storage Node*** > **Storage**.
2. Faites défiler vers le bas pour afficher les quantités de stockage disponibles pour chaque volume et magasin d'objets.

   Pour les nœuds de stockage de l'appliance, le nom mondial de chaque disque correspond à l'identifiant WWID (WWID) du volume qui s'affiche lorsque vous affichez les propriétés standard du volume dans SANtricity OS (le logiciel de gestion connecté au contrôleur de stockage de l'appliance).

   Pour vous aider à interpréter les statistiques de lecture et d'écriture du disque relatives aux points de montage du volume, la première partie du nom affichée dans la colonne **Name** de la table Disk Devices (c'est-à-dire *sdc*, *sdd*, *sde*, etc.) correspond à la valeur indiquée dans la colonne **Device** de la table volumes.

Disk devices

Name	World Wide Name	I/O load	Read rate	Write rate
sdc(8:16,sdb)	N/A	0.05%	0 bytes/s	4 KB/s
sde(8:48,sdd)	N/A	0.00%	0 bytes/s	82 bytes/s
sdf(8:64,sde)	N/A	0.00%	0 bytes/s	82 bytes/s
sdg(8:80,sdf)	N/A	0.00%	0 bytes/s	82 bytes/s
sdd(8:32,sdc)	N/A	0.00%	0 bytes/s	82 bytes/s
croot(8:1,sda1)	N/A	0.04%	0 bytes/s	4 KB/s
cvloc(8:2,sda2)	N/A	0.95%	0 bytes/s	52 KB/s

Volumes

Mount point	Device	Status	Size	Available	Write cache status
/	croot	Online	21.00 GB	14.73 GB	Unknown
/var/local	cvloc	Online	85.86 GB	80.94 GB	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.17 GB	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/2	sde	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/3	sdf	Online	107.32 GB	107.18 GB	Enabled
/var/local/rangedb/4	sdg	Online	107.32 GB	107.18 GB	Enabled

Object stores

ID	Size	Available	Replicated data	EC data	Object data (%)	Health
0000	107.32 GB	96.44 GB	1.55 MB	0 bytes	0.00%	No Errors
0001	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0002	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0003	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors
0004	107.32 GB	107.18 GB	0 bytes	0 bytes	0.00%	No Errors

3. Suivez les instructions fournies par votre plateforme pour ajouter de nouveaux volumes de stockage au nœud de stockage.
   - "VMware : ajoutez des volumes de stockage au nœud de stockage"
   - "Linux : ajoutez des volumes SAN ou DAS au nœud de stockage"

VMware : ajoutez des volumes de stockage au nœud de stockage

Si un nœud de stockage comprend moins de 16 volumes de stockage, vous pouvez augmenter sa capacité en utilisant VMware vSphere pour ajouter des volumes.

Avant de commencer

- Vous avez accès aux instructions d'installation de StorageGRID pour les déploiements.
  - "Installez VMware"
- Vous avez le `Passwords.txt` fichier.
- Vous disposez d'autorisations d'accès spécifiques.

> N'essayez pas d'ajouter des volumes de stockage à un nœud de stockage pendant qu'une mise à niveau logicielle, une procédure de restauration ou une autre procédure d'extension est active.

Description de la tâche

Le nœud de stockage n'est pas disponible brièvement lorsque vous ajoutez des volumes de stockage. Cette procédure doit être effectuée sur un seul nœud de stockage à la fois pour éviter d'affecter les services de grid côté client.

Étapes

1. Si nécessaire, installez un nouveau matériel de stockage et créez de nouveaux datastores VMware.
2. Ajoutez un ou plusieurs disques durs à la machine virtuelle pour l'utiliser comme stockage (magasins d'objets).

   a. Ouvrez le client VMware vSphere.

   b. Modifiez les paramètres de la machine virtuelle pour ajouter un ou plusieurs disques durs supplémentaires.

   Les disques durs sont généralement configurés en tant que disques d'ordinateurs virtuels (VMDK, Virtual machine Disks). Les VMDK sont plus fréquemment utilisés et plus faciles à gérer, tandis que les RDM peuvent fournir de meilleures performances pour les charges de travail utilisant des objets de plus grande taille (par exemple, plus de 100 Mo). Pour plus d'informations sur l'ajout de disques durs aux machines virtuelles, consultez la documentation de VMware vSphere.

3. Redémarrez la machine virtuelle à l'aide de l'option **Restart Guest OS** du client VMware vSphere ou en entrant la commande suivante dans une session ssh à la machine virtuelle :`sudo reboot`

   > N'utilisez pas **Power Off** ou **Reset** pour redémarrer la machine virtuelle.

4. Configurez le nouveau stockage pour qu'il soit utilisé par le nœud de stockage :

   a. Connectez-vous au nœud grid :

      i. Saisissez la commande suivante : `ssh admin@grid_node_IP`

ii. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

iii. Entrez la commande suivante pour passer à la racine : `su -`

iv. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier. Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

b. Configurer les nouveaux volumes de stockage :

```
sudo add_rangedbs.rb
```

Ce script trouve tous les nouveaux volumes de stockage et vous invite à les formater.

c. Saisissez **y** pour accepter le formatage.

d. Si l'un des volumes a déjà été formaté, décidez si vous souhaitez les reformater.

- Entrez **y** pour reformater.
- Saisissez **n** pour ignorer le reformatage.

Le `setup_rangedbs.sh` le script s'exécute automatiquement.

5. Vérifier que les services démarrent correctement :

a. Afficher une liste de l'état de tous les services sur le serveur :

```
sudo storagegrid-status
```

L'état est mis à jour automatiquement.

a. Attendez que tous les services soient en cours d'exécution ou vérifiés.

b. Quitter l'écran d'état :

```
Ctrl+C
```

6. Vérifiez que le nœud de stockage est en ligne :

a. Connectez-vous au Grid Manager à l'aide d'un "navigateur web pris en charge".

b. Sélectionnez **SUPPORT** > **Outils** > **topologie de grille**.

c. Sélectionnez ***site*** > ***Storage Node*** > **LDR** > **Storage**.

d. Sélectionnez l'onglet **Configuration**, puis l'onglet **main**.

e. Si la liste déroulante État de stockage - souhaité* est définie sur lecture seule ou hors ligne, sélectionnez **en ligne**.

f. Sélectionnez **appliquer les modifications**.

7. Pour afficher les nouveaux magasins d'objets :

a. Sélectionnez **NODES** > ***site*** > ***Storage Node*** > **Storage**.

b. Affichez les détails dans le tableau **magasins d'objets**.

Résultat

Vous pouvez utiliser la capacité étendue des nœuds de stockage pour sauvegarder les données d'objet.

Linux : ajoutez des volumes SAN ou DAS au nœud de stockage

Si un nœud de stockage contient moins de 16 volumes de stockage, vous pouvez augmenter sa capacité en ajoutant de nouveaux périphériques de stockage en mode bloc, en les rendant visibles pour les hôtes Linux et en ajoutant les nouveaux mappages de périphériques de bloc au fichier de configuration StorageGRID utilisé pour le nœud de stockage.

Avant de commencer

- Vous avez accès aux instructions d'installation de StorageGRID pour votre plate-forme Linux.
  - "Installez Red Hat Enterprise Linux ou CentOS"
  - "Installez Ubuntu ou Debian"
- Vous avez le `Passwords.txt` fichier.
- Vous disposez d'autorisations d'accès spécifiques.

> N'essayez pas d'ajouter des volumes de stockage à un nœud de stockage pendant qu'une mise à niveau logicielle, une procédure de restauration ou une autre procédure d'extension est active.

Description de la tâche

Le nœud de stockage n'est pas disponible brièvement lorsque vous ajoutez des volumes de stockage. Cette procédure doit être effectuée sur un seul nœud de stockage à la fois pour éviter d'affecter les services de grid côté client.

Étapes

1. Installez le nouveau matériel de stockage.

   Pour plus d'informations, consultez la documentation fournie par votre fournisseur de matériel.

2. Créer de nouveaux volumes de stockage en mode bloc de la taille souhaitée.
   - Connectez les nouveaux disques et mettez à jour la configuration du contrôleur RAID si nécessaire, ou allouez les nouvelles LUN SAN sur les baies de stockage partagées et autorisez l'hôte Linux à y accéder.
   - Utilisez le même schéma de nommage persistant que celui utilisé pour les volumes de stockage sur le nœud de stockage existant.
   - Si vous utilisez la fonctionnalité de migration de nœud StorageGRID, rendez les nouveaux volumes visibles pour les autres hôtes Linux qui sont des cibles de migration pour ce nœud de stockage. Pour plus d'informations, reportez-vous aux instructions d'installation de StorageGRID pour votre plate-forme Linux.
3. Connectez-vous à l'hôte Linux prenant en charge le nœud de stockage en tant qu'utilisateur root ou à l'aide d'un compte disposant de l'autorisation sudo.
4. Vérifiez que les nouveaux volumes de stockage sont visibles sur l'hôte Linux.

   Il se peut que vous deviez effectuer une nouvelle analyse pour les périphériques.

5. Exécutez la commande suivante pour désactiver temporairement le nœud de stockage :

   ```
   sudo storagegrid node stop <node-name>
   ```

6. À l'aide d'un éditeur de texte tel que vim ou pico, modifiez le fichier de configuration de nœud pour le nœud de stockage, qui se trouve à l'adresse `/etc/storagegrid/nodes/<node-name>.conf`.
7. Recherchez la section du fichier de configuration de nœud contenant les mappages de périphériques de bloc de stockage objet existants.

   Dans l'exemple : `BLOCK_DEVICE_RANGEDB_00` à `BLOCK_DEVICE_RANGEDB_03` les mappages de périphériques de blocs de stockage objet sont-ils existants ?

   ```
   NODE_TYPE = VM_Storage_Node
   ADMIN_IP = 10.1.0.2
   BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-sn1-var-local
   BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/sgws-sn1-rangedb-0
   BLOCK_DEVICE_RANGEDB_01 = /dev/mapper/sgws-sn1-rangedb-1
   BLOCK_DEVICE_RANGEDB_02 = /dev/mapper/sgws-sn1-rangedb-2
   BLOCK_DEVICE_RANGEDB_03 = /dev/mapper/sgws-sn1-rangedb-3
   GRID_NETWORK_TARGET = bond0.1001
   ADMIN_NETWORK_TARGET = bond0.1002
   CLIENT_NETWORK_TARGET = bond0.1003
   GRID_NETWORK_IP = 10.1.0.3
   GRID_NETWORK_MASK = 255.255.255.0
   GRID_NETWORK_GATEWAY = 10.1.0.1
   ```

8. Ajoutez de nouveaux mappages de périphériques de blocs de stockage objet correspondant aux volumes de stockage bloc que vous avez ajoutés pour ce nœud de stockage.

   N'oubliez pas de commencer à la suivante `BLOCK_DEVICE_RANGEDB_nn`. Ne laissez pas de place.

   - En fonction de l'exemple ci-dessus, commencez à `BLOCK_DEVICE_RANGEDB_04`.
   - Dans l'exemple ci-dessous, quatre nouveaux volumes de stockage en mode bloc ont été ajoutés au nœud : `BLOCK_DEVICE_RANGEDB_04` à `BLOCK_DEVICE_RANGEDB_07`.

```
NODE_TYPE = VM_Storage_Node
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-sn1-var-local
BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/sgws-sn1-rangedb-0
BLOCK_DEVICE_RANGEDB_01 = /dev/mapper/sgws-sn1-rangedb-1
BLOCK_DEVICE_RANGEDB_02 = /dev/mapper/sgws-sn1-rangedb-2
BLOCK_DEVICE_RANGEDB_03 = /dev/mapper/sgws-sn1-rangedb-3
BLOCK_DEVICE_RANGEDB_04 = /dev/mapper/sgws-sn1-rangedb-4
BLOCK_DEVICE_RANGEDB_05 = /dev/mapper/sgws-sn1-rangedb-5
BLOCK_DEVICE_RANGEDB_06 = /dev/mapper/sgws-sn1-rangedb-6
BLOCK_DEVICE_RANGEDB_07 = /dev/mapper/sgws-sn1-rangedb-7
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003
GRID_NETWORK_IP = 10.1.0.3
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

9. Exécutez la commande suivante pour valider les modifications apportées au fichier de configuration de nœud pour le nœud de stockage :

   `sudo storagegrid node validate <node-name>`

   Traitez les erreurs ou les avertissements avant de passer à l'étape suivante.

   Si vous observez une erreur similaire à celle qui suit, cela signifie que le fichier de configuration du nœud tente de mapper le périphérique de bloc utilisé par `<node-name>` pour `<PURPOSE>` à la donnée `<path-name>` Dans le système de fichiers Linux, mais il n'existe pas de fichier spécial de périphérique de bloc valide (ou de lien logiciel vers un fichier spécial de périphérique de bloc) à cet emplacement.

   ```
   Checking configuration file for node <node-name>…
   ERROR: BLOCK_DEVICE_<PURPOSE> = <path-name>
   <path-name> is not a valid block device
   ```

   Vérifiez que vous avez saisi le bon `<path-name>`.

10. Exécutez la commande suivante pour redémarrer le nœud avec les nouveaux mappages de périphériques de bloc en place :

    `sudo storagegrid node start <node-name>`

11. Connectez-vous au nœud de stockage en tant qu'administrateur à l'aide du mot de passe indiqué dans le `Passwords.txt` fichier.
12. Vérifier que les services démarrent correctement :
    a. Afficher une liste de l'état de tous les services sur le serveur :

```
sudo storagegrid-status
```

L'état est mis à jour automatiquement.

b. Attendez que tous les services soient en cours d'exécution ou vérifiés.

c. Quitter l'écran d'état :

```
Ctrl+C
```

13. Configurez le nouveau stockage pour qu'il soit utilisé par le nœud de stockage :

a. Configurer les nouveaux volumes de stockage :

```
sudo add_rangedbs.rb
```

Ce script trouve tous les nouveaux volumes de stockage et vous invite à les formater.

b. Entrez **y** pour formater les volumes de stockage.

c. Si l'un des volumes a déjà été formaté, décidez si vous souhaitez les reformater.

- Entrez **y** pour reformater.
- Saisissez **n** pour ignorer le reformatage.

Le `setup_rangedbs.sh` le script s'exécute automatiquement.

14. Vérifiez que le nœud de stockage est en ligne :

a. Connectez-vous au Grid Manager à l'aide d'un "navigateur web pris en charge".

b. Sélectionnez **SUPPORT** > **Outils** > **topologie de grille**.

c. Sélectionnez ***site*** > ***Storage Node*** > **LDR** > **Storage**.

d. Sélectionnez l'onglet **Configuration**, puis l'onglet **main**.

e. Si la liste déroulante État de stockage - souhaité* est définie sur lecture seule ou hors ligne, sélectionnez **en ligne**.

f. Cliquez sur **appliquer les modifications**.

15. Pour afficher les nouveaux magasins d'objets :

a. Sélectionnez **NODES** > ***site*** > ***Storage Node*** > **Storage**.

b. Affichez les détails dans le tableau **magasins d'objets**.

Résultat

Vous pouvez maintenant utiliser la capacité étendue des nœuds de stockage pour sauvegarder les données d'objet.

Ajout de nœuds grid ou d'un site

Ajout de nœuds grid à un site existant ou ajout d'un site

Vous pouvez suivre cette procédure pour ajouter des nœuds de grille à des sites existants ou pour ajouter un nouveau site, mais vous ne pouvez pas effectuer les deux types d'extension en même temps.

Avant de commencer

- Vous disposez de l'autorisation accès racine ou Maintenance.
- Tous les nœuds existants de la grille sont opérationnels sur tous les sites.
- Toute procédure d'extension, de mise à niveau, de déclassement ou de restauration est terminée.

> Vous ne pouvez pas démarrer une extension pendant qu'une autre procédure d'extension, de mise à niveau, de récupération ou de mise hors service active est en cours. Toutefois, si nécessaire, vous pouvez interrompre une procédure de mise hors service pour démarrer une extension.

Étapes

1. "Mise à jour des sous-réseaux pour le réseau Grid".
2. "Déploiement de nouveaux nœuds grid".
3. "Réaliser une extension".

Mise à jour des sous-réseaux pour le réseau Grid

Lorsque vous ajoutez des nœuds de grille ou un nouveau site dans une extension, vous devrez peut-être mettre à jour ou ajouter des sous-réseaux au réseau Grid.

StorageGRID conserve une liste des sous-réseaux réseau utilisés pour communiquer entre les nœuds de la grille sur le réseau Grid (eth0). Ces entrées incluent les sous-réseaux utilisés pour le réseau Grid par chaque site du système StorageGRID, ainsi que tous les sous-réseaux utilisés pour les serveurs NTP, DNS, LDAP ou autres serveurs externes accessibles via la passerelle réseau Grid.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous avez le "Maintenance ou autorisation d'accès racine".
- Vous avez la phrase secrète pour le provisionnement.
- Les adresses réseau des sous-réseaux que vous souhaitez configurer sont définies, en notation CIDR.

Description de la tâche

Si l'un des nouveaux nœuds possède une adresse IP de réseau Grid sur un sous-réseau non utilisé auparavant, vous devez ajouter le nouveau sous-réseau à la liste de sous-réseaux du réseau Grid avant de démarrer l'extension. Sinon, vous devrez annuler l'extension, ajouter le nouveau sous-réseau et recommencer la procédure.

Étapes

1. Sélectionnez **MAINTENANCE** > **réseau** > **réseau Grid**.
2. Sélectionnez **Ajouter un autre sous-réseau** pour ajouter un nouveau sous-réseau en notation CIDR.

   Par exemple, entrez `10.96.104.0/22`.

3. Saisissez le mot de passe de provisionnement et sélectionnez **Enregistrer**.
4. Attendez que les modifications soient appliquées, puis téléchargez un nouveau progiciel de récupération.
   a. Sélectionnez **MAINTENANCE** > **système** > **progiciel de récupération**.
   b. Saisissez la phrase de passe de provisionnement *.

Le fichier du progiciel de récupération doit être sécurisé car il contient des clés de cryptage et des mots de passe qui peuvent être utilisés pour obtenir des données du système StorageGRID. Elle permet également de restaurer le nœud d'administration principal.

Les sous-réseaux que vous avez spécifiés sont automatiquement configurés pour votre système StorageGRID.

Déploiement de nouveaux nœuds grid

Les étapes du déploiement de nouveaux nœuds de grille dans une extension sont les mêmes que celles utilisées lors de l'installation initiale de la grille. Vous devez déployer tous les nouveaux nœuds de la grille avant de pouvoir réaliser l'extension.

Lorsque vous développez la grille, les nœuds que vous ajoutez n'ont pas à correspondre aux types de nœuds existants. Vous pouvez ajouter des nœuds VMware, des nœuds basés sur des conteneurs Linux ou des nœuds d'appliance.

VMware : déployez les nœuds grid

Vous devez déployer une machine virtuelle dans VMware vSphere pour chaque nœud VMware que vous souhaitez ajouter à l'extension.

Étapes

1. "Déployez le nouveau nœud en tant que machine virtuelle" Et connectez-le à un ou plusieurs réseaux StorageGRID.

   Lorsque vous déployez le nœud, vous pouvez remappage les ports de nœud ou augmenter les paramètres de processeur ou de mémoire.

2. Une fois que vous avez déployé tous les nouveaux nœuds VMware, "effectuer la procédure d'extension".

Linux : déployez des nœuds grid

Vous pouvez déployer des nœuds grid sur de nouveaux hôtes Linux ou sur des hôtes Linux existants. Si vous avez besoin d'hôtes Linux supplémentaires pour prendre en charge les exigences en matière de processeur, de RAM et de stockage des nœuds StorageGRID que vous souhaitez ajouter à votre grille, vous devez les préparer de la même manière que lorsque vous les avez installés pour la première fois. Vous déployez ensuite les nœuds d'extension de la même manière que vous avez déployé des nœuds grid lors de l'installation.

Avant de commencer

- Vous disposez des instructions d'installation de StorageGRID pour votre version de Linux, et vous avez examiné la configuration matérielle et la configuration de stockage requise.
  - "Installez Red Hat Enterprise Linux ou CentOS"
  - "Installez Ubuntu ou Debian"
- Si vous prévoyez de déployer de nouveaux nœuds grid sur des hôtes existants, vous avez confirmé que les hôtes existants disposent de suffisamment de processeur, de mémoire RAM et de capacité de stockage pour les nœuds supplémentaires.
- Vous disposez d'un plan pour réduire les domaines d'échec. Par exemple, vous ne devez pas déployer tous les nœuds de passerelle sur un hôte physique unique.

Dans un déploiement de production, n'exécutez pas plus d'un nœud de stockage sur un seul hôte physique ou virtuel. L'utilisation d'un hôte dédié pour chaque nœud de stockage fournit un domaine de défaillance isolé.

- Si le nœud StorageGRID utilise le stockage affecté à un système NetApp ONTAP, vérifiez que cette FabricPool règle n'est pas activée pour le volume. La désactivation du Tiering FabricPool pour les volumes utilisés avec des nœuds StorageGRID simplifie la résolution des problèmes et les opérations de stockage.

Étapes

1. Si vous ajoutez de nouveaux hôtes, accédez aux instructions d'installation pour le déploiement des nœuds StorageGRID.
2. Pour déployer les nouveaux hôtes, suivez les instructions de préparation des hôtes.
3. Pour créer des fichiers de configuration de nœuds et valider la configuration StorageGRID, suivez les instructions de déploiement des nœuds grid.
4. Si vous ajoutez des nœuds à un nouvel hôte Linux, démarrez le service d'hôte StorageGRID.
5. Si vous ajoutez des nœuds à un hôte Linux existant, démarrez les nouveaux nœuds à l'aide de l'interface de ligne de commande du service hôte StorageGRID :`sudo storagegrid node start [<node name\>]`

Une fois que vous avez terminé

Après le déploiement de tous les nouveaux nœuds de la grille, c'est possible "réalisation de l'extension".

Appliances : déploiement de nœuds de stockage, de passerelle ou d'administration non primaires

Pour installer le logiciel StorageGRID sur un nœud d'appliance, utilisez le programme d'installation de l'appliance StorageGRID, qui est inclus sur l'appliance. Dans une extension, chaque appliance de stockage fonctionne comme un seul nœud de stockage, et chaque appliance de services fonctionne comme un seul nœud de passerelle ou un nœud d'administration non primaire. Tout appareil peut se connecter au réseau Grid, au réseau Admin et au réseau client.

Avant de commencer

- L'appliance a été installée dans un rack ou une armoire, connectée à vos réseaux et sous tension.
- Vous avez terminé "Configurer le matériel" étapes.

  La configuration du matériel de l'appliance comprend les étapes requises pour configurer les connexions StorageGRID (liaisons réseau et adresses IP), ainsi que les étapes facultatives pour activer le chiffrement de nœud, modifier le mode RAID et remaper les ports réseau.

- Tous les sous-réseaux de réseau Grid répertoriés sur la page de configuration IP du programme d'installation de l'appliance StorageGRID ont été définis dans la liste de sous-réseaux de réseau de grille sur le nœud d'administration principal.
- Le firmware du programme d'installation de l'appliance StorageGRID sur l'appliance de remplacement est compatible avec la version du logiciel StorageGRID actuellement exécutée sur votre grid. Si les versions ne sont pas compatibles, vous devez mettre à niveau le micrologiciel du programme d'installation de l'appliance StorageGRID.
- Vous avez un ordinateur portable de service avec un "navigateur web pris en charge".
- Vous connaissez l'une des adresses IP attribuées au contrôleur de calcul de l'appliance. Vous pouvez utiliser l'adresse IP de n'importe quel réseau StorageGRID connecté.

Description de la tâche

Le processus d'installation de StorageGRID sur un nœud d'appliance comprend les phases suivantes :

- Vous spécifiez ou confirmez l'adresse IP du nœud d'administration principal et le nom du nœud d'appliance.
- Vous démarrez l'installation et attendez que les volumes soient configurés et que le logiciel soit installé.

  Pendant les tâches d'installation de l'appliance, l'installation s'interrompt. Pour reprendre l'installation, connectez-vous au Grid Manager, approuvez tous les nœuds de la grille et terminez le processus d'installation de StorageGRID.

> Si vous devez déployer plusieurs nœuds d'appliance à la fois, vous pouvez automatiser le processus d'installation à l'aide du `configure-sga.py` Script d'installation de l'appliance.

Étapes

1. Ouvrez un navigateur et entrez l'une des adresses IP du contrôleur de calcul de l'appliance.

   `https://Controller_IP:8443`

   La page d'accueil du programme d'installation de l'appliance StorageGRID s'affiche.

2. Dans la section connexion **Primary Admin Node**, déterminez si vous devez spécifier l'adresse IP du noeud d'administration principal.

   Si vous avez déjà installé d'autres nœuds dans ce centre de données, le programme d'installation de l'appliance StorageGRID peut détecter automatiquement cette adresse IP, en supposant que le nœud d'administration principal, ou au moins un autre nœud de grille avec ADMIN_IP configuré, soit présent sur le même sous-réseau.

3. Si cette adresse IP n'apparaît pas ou si vous devez la modifier, spécifiez l'adresse :

Option	Description
Entrée IP manuelle	a. Décochez la case **Activer la découverte du noeud d'administration**. b. Saisissez l'adresse IP manuellement. c. Cliquez sur **Enregistrer**. d. Attendez que l'état de connexion de la nouvelle adresse IP soit prêt.
Détection automatique de tous les nœuds d'administration principaux connectés	a. Cochez la case **Activer la découverte du noeud d'administration**. b. Attendez que la liste des adresses IP découvertes s'affiche. c. Sélectionnez le nœud d'administration principal de la grille dans laquelle ce nœud de stockage de l'appliance sera déployé. d. Cliquez sur **Enregistrer**. e. Attendez que l'état de connexion de la nouvelle adresse IP soit prêt.

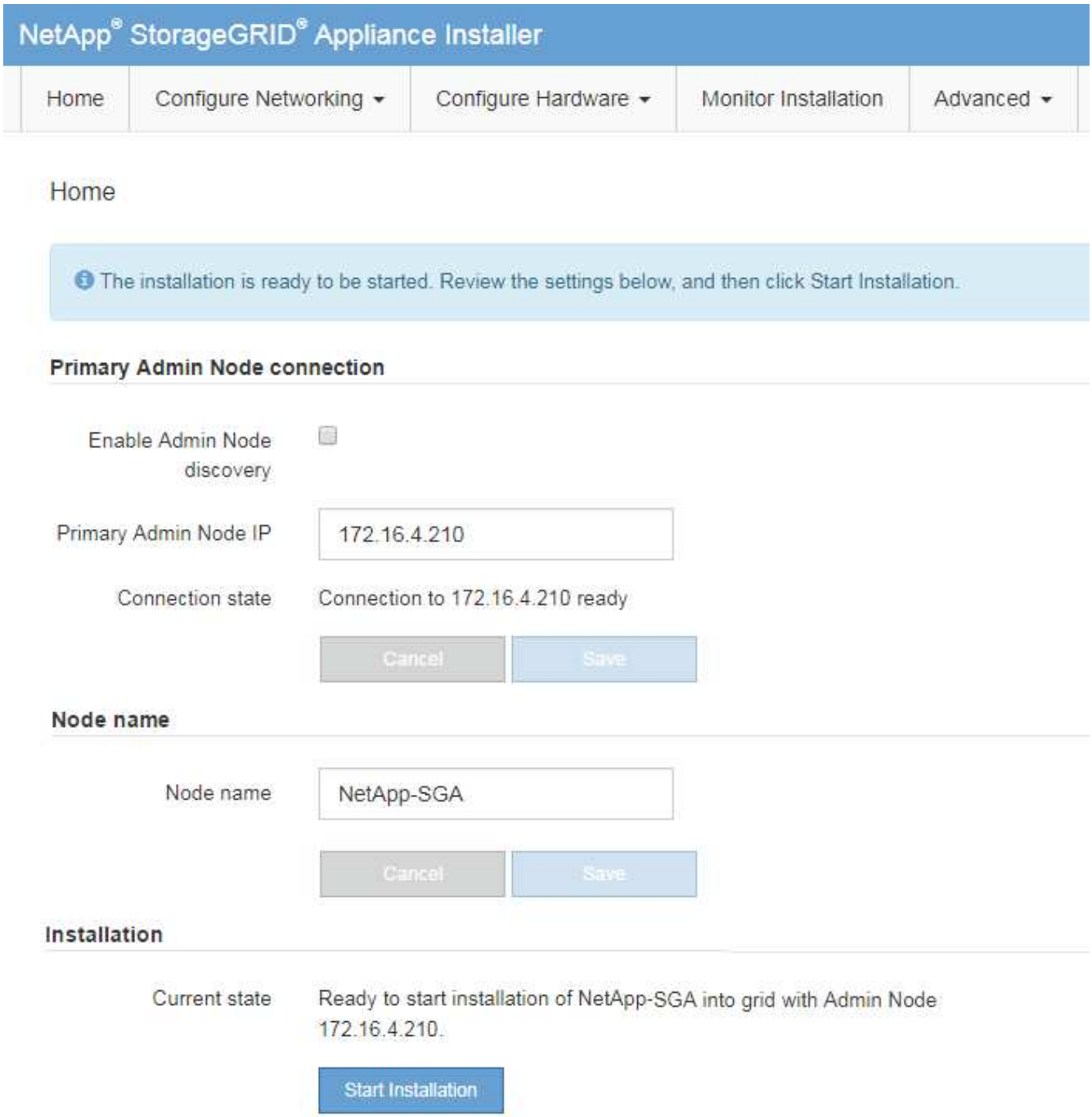
4. Dans le champ **Nom du noeud**, entrez le nom que vous souhaitez utiliser pour ce noeud de l'appliance, puis sélectionnez **Enregistrer**.

   Le nom de nœud est attribué à ce nœud d'appliance dans le système StorageGRID. Elle s'affiche sur la page nœuds (onglet Présentation) dans Grid Manager. Si nécessaire, vous pouvez modifier le nom du nœud lors de l'approbation.

5. Dans la section **installation**, confirmez que l'état actuel est « prêt à démarrer l'installation de *node* dans la grille avec le noeud d'administration principal *admin_ip*» et que le bouton **Démarrer l'installation** est activé.

   Si le bouton **Start installation** n'est pas activé, vous devrez peut-être modifier la configuration réseau ou les paramètres de port. Pour obtenir des instructions, reportez-vous aux instructions d'entretien de votre appareil.

6. Dans la page d'accueil du programme d'installation de l'appliance StorageGRID, sélectionnez **Démarrer l'installation**.



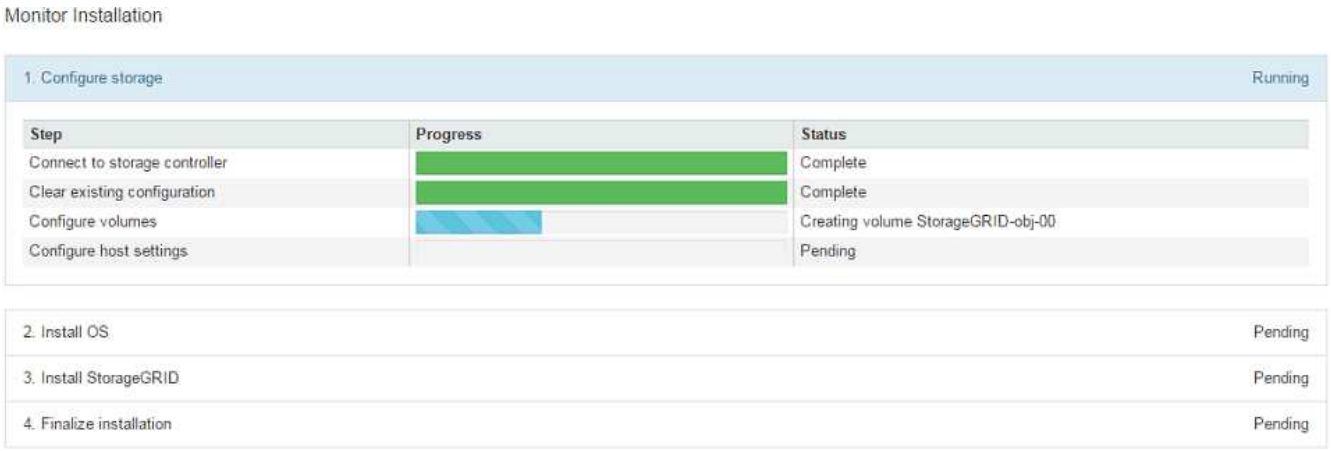
L'état actuel passe à « installation en cours » et la page installation du moniteur s'affiche.

7. Si votre extension inclut plusieurs nœuds d'appliance, répétez les étapes précédentes pour chaque appliance.

> Si vous devez déployer plusieurs nœuds de stockage d'appliance à la fois, vous pouvez automatiser le processus d'installation à l'aide du script d'installation de l'appliance configure-sga.py.

8. Si vous devez accéder manuellement à la page installation du moniteur, sélectionnez **installation du moniteur** dans la barre de menus.

   La page installation du moniteur affiche la progression de l'installation.



La barre d'état bleue indique la tâche en cours. Les barres d'état vertes indiquent que les tâches ont été effectuées avec succès.

> Le programme d'installation s'assure que les tâches terminées lors d'une installation précédente ne sont pas réexécutées. Si vous exécutez à nouveau une installation, toutes les tâches qui n'ont pas besoin d'être réexécutées s'affichent avec une barre d'état verte et un état de « `barrét' ».

9. Passez en revue l'état d'avancement des deux premières étapes d'installation.

   1. Configurer l'appliance

   Au cours de cette étape, l'un des processus suivants se produit :

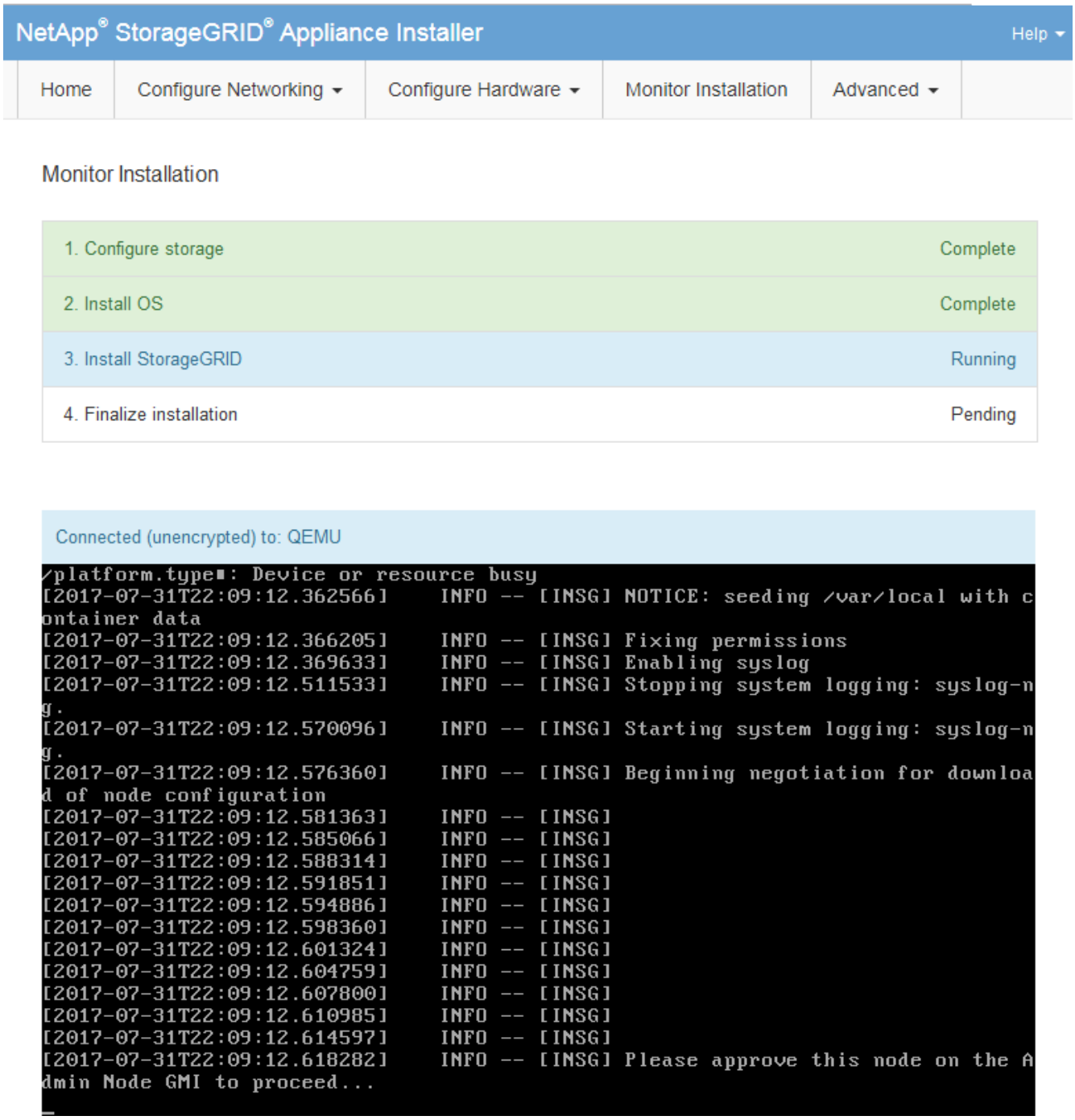
   - Pour une appliance de stockage, le programme d'installation se connecte au contrôleur de stockage, efface toute configuration existante, communique avec SANtricity OS pour configurer les volumes et configure les paramètres de l'hôte.
   - Pour une appliance de services, le programme d'installation efface toute configuration existante des disques du contrôleur de calcul et configure les paramètres de l'hôte.

   2. Installez OS

   Au cours de cette étape, le programme d'installation copie l'image du système d'exploitation de base pour StorageGRID sur l'appliance.

10. Continuez à surveiller la progression de l'installation jusqu'à ce qu'un message s'affiche dans la fenêtre de la console, vous invitant à utiliser le gestionnaire de grille pour approuver le nœud.

> Attendez que tous les nœuds ajoutés à cette extension soient prêts pour approbation avant de passer à Grid Manager pour approuver les nœuds.



Réaliser une extension

Lorsque vous effectuez l'extension, des nœuds grid sont ajoutés à votre déploiement StorageGRID existant.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous avez la phrase secrète pour le provisionnement.
- Vous avez déployé tous les nœuds grid qui sont ajoutés dans cette extension.
- Vous disposez de l'autorisation Maintenance ou accès racine.

- Si vous ajoutez des nœuds de stockage, vous avez confirmé que toutes les opérations de réparation de données réalisées dans le cadre d'une restauration sont terminées. Voir "Vérifier les travaux de réparation des données".
- Si vous ajoutez des nœuds de stockage et que vous souhaitez attribuer une note de stockage personnalisée à ces nœuds, vous l'avez déjà fait "création du niveau de stockage personnalisé". Vous disposez également de l'autorisation d'accès racine ou des autorisations Maintenance et ILM.
- Si vous ajoutez un nouveau site, vous avez examiné et mis à jour les règles ILM. Vous devez vous assurer que les copies d'objet ne sont pas stockées sur le nouveau site tant que l'extension n'est pas terminée. Par exemple, si une règle utilise le pool de stockage par défaut (**tous les nœuds de stockage**), vous devez le faire "créez un nouveau pool de stockage" Qui contient uniquement les nœuds de stockage existants et "Mise à jour des règles ILM" Et la règle ILM pour utiliser ce nouveau pool de stockage. Sinon, les objets seront copiés sur le nouveau site dès que le premier nœud de ce site devient actif.

Description de la tâche

L'exécution de l'extension inclut les tâches utilisateur principales suivantes :

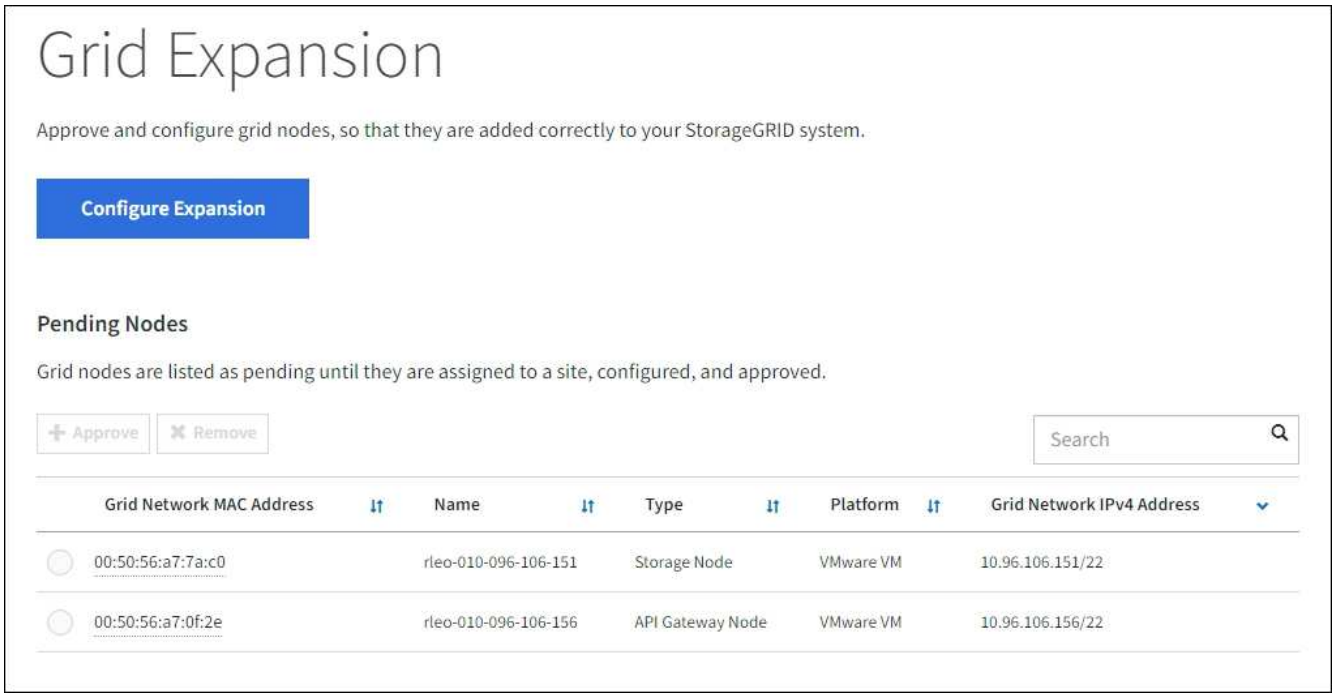
1. Configurer l'extension.
2. Démarrez l'extension.
3. Téléchargez un nouveau fichier de package de récupération.
4. Surveillez les étapes et étapes d'extension jusqu'à ce que tous les nouveaux nœuds soient installés et configurés et que tous les services aient démarré.

> L'exécution de certaines étapes et étapes d'extension sur un grand grid peut prendre beaucoup de temps. Par exemple, si la base de données Cassandra est vide, vous pouvez streaming Cassandra vers un nouveau nœud de stockage. Cependant, si la base de données Cassandra inclut un volume important de métadonnées d'objet, cette étape peut prendre plusieurs heures, voire plus. Ne redémarrez aucun nœud de stockage pendant les étapes « extension du cluster Cassandra » ou « démarrage de Cassandra et des données de streaming ».

Étapes

1. Sélectionnez **MAINTENANCE** > **tâches** > **expansion**.

   La page d'extension de la grille s'affiche. La section nœuds en attente répertorie les nœuds prêts à être ajoutés.

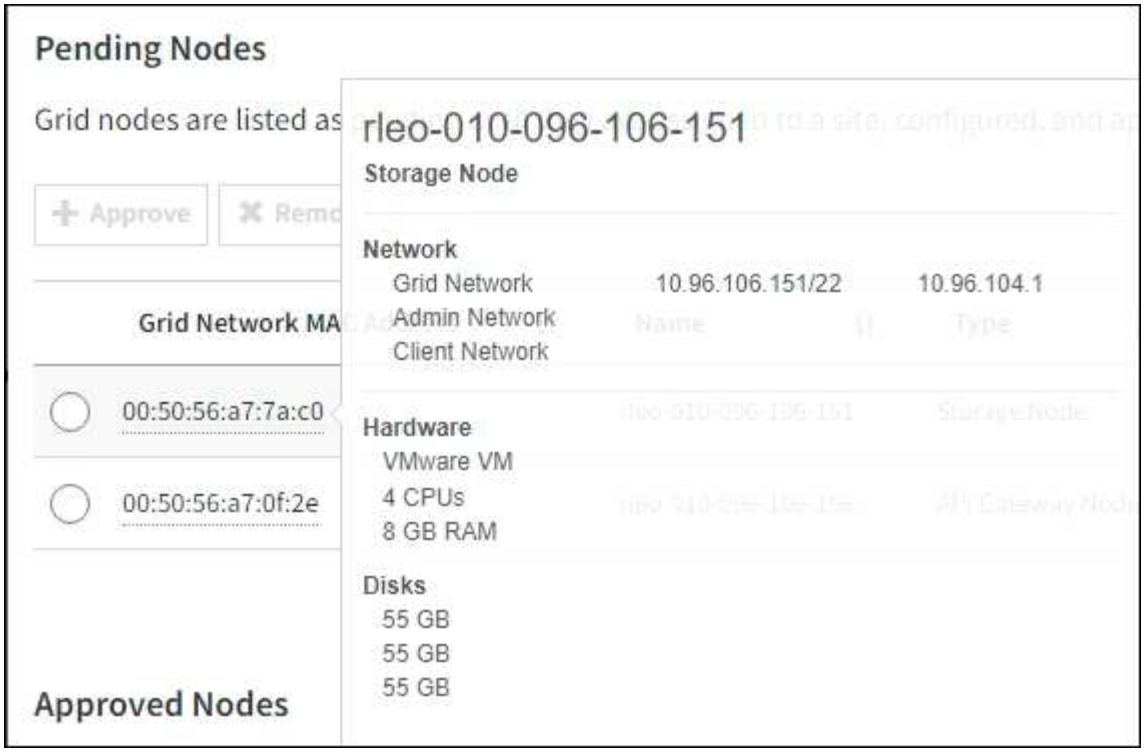


2. Sélectionnez **configurer l'extension**.

   La boîte de dialogue sélection du site s'affiche.

3. Sélectionnez le type d'expansion que vous commencez :
   - Si vous ajoutez un nouveau site, sélectionnez **Nouveau** et entrez le nom du nouveau site.
   - Si vous ajoutez un ou plusieurs nœuds à un site existant, sélectionnez **existant**.
4. Sélectionnez **Enregistrer**.
5. Consultez la liste **nœuds en attente** et vérifiez qu'elle affiche tous les nœuds de la grille que vous avez déployés.

   Si nécessaire, vous pouvez placer votre curseur sur l'adresse **Grid Network MAC Address** d'un nœud pour afficher les détails sur ce nœud.



Si un nœud est manquant, vérifiez qu'il a été déployé avec succès.

6. Dans la liste des nœuds en attente, approuvez les nœuds que vous souhaitez ajouter à cette extension.
   a. Sélectionnez le bouton radio à côté du premier nœud de grille en attente que vous souhaitez approuver.
   b. Sélectionnez **approuver**.

      Le formulaire de configuration des nœuds de la grille s'affiche.

   c. Si nécessaire, modifiez les paramètres généraux :

Champ	Description
Le site	Nom du site auquel le nœud de grille sera associé. Si vous ajoutez plusieurs nœuds, veillez à sélectionner le site approprié pour chaque nœud. Si vous ajoutez un site, tous les nœuds sont ajoutés au nouveau site.
Nom	Nom du système du nœud. Les noms de système sont requis pour les opérations StorageGRID internes et ne peuvent pas être modifiés.

Champ	Description
Rôle NTP	Le rôle NTP (Network Time Protocol) du nœud de grille : • Sélectionnez **automatique** (par défaut) pour attribuer automatiquement le rôle NTP au nœud. Le rôle principal sera attribué aux nœuds d'administration, aux nœuds de stockage avec services ADC, aux nœuds de passerelle et à tous les nœuds de grille ayant des adresses IP non statiques. Le rôle client sera attribué à tous les autres nœuds de la grille. • Sélectionnez **principal** pour attribuer manuellement le rôle NTP principal au nœud. Au moins deux nœuds sur chaque site doivent avoir le rôle principal pour fournir un accès système redondant aux sources de synchronisation externes. • Sélectionnez **client** pour attribuer manuellement le rôle NTP du client au nœud.
Service ADC (nœuds de stockage uniquement)	Si ce nœud de stockage exécute le service contrôleur de domaine administratif (ADC). Le service ADC conserve le suivi de l'emplacement et de la disponibilité des services de réseau. Au moins trois nœuds de stockage de chaque site doivent inclure le service ADC. Vous ne pouvez pas ajouter le service ADC à un nœud après son déploiement. • Sélectionnez **Oui** si le nœud de stockage que vous remplacez inclut le service ADC. Comme vous ne pouvez pas désaffecter un nœud de stockage si trop peu de services ADC sont conservés, cela garantit qu'un nouveau service ADC est disponible avant la suppression de l'ancien service. • Sélectionnez **automatique** pour permettre au système de déterminer si ce nœud nécessite le service ADC. Découvrez le "Quorum ADC".
Qualité de stockage (nœuds de stockage uniquement)	Utilisez le niveau de stockage **par défaut** ou sélectionnez le niveau de stockage personnalisé que vous souhaitez affecter à ce nouveau nœud. Les niveaux de stockage sont utilisés par les pools de stockage ILM. Ainsi, votre sélection peut affecter les objets qui seront placés sur le nœud de stockage.

d. Si nécessaire, modifiez les paramètres du réseau Grid, du réseau Admin et du réseau client.

- **Adresse IPv4 (CIDR)** : adresse réseau CIDR pour l'interface réseau. Par exemple : 172.16.10.100/24

> Si vous découvrez que les nœuds ont des adresses IP dupliquées sur le réseau Grid alors que vous approuvez des nœuds, vous devez annuler l'extension, redéployer les machines virtuelles ou les appliances avec une adresse IP non dupliquée, puis redémarrer l'extension.

- **Gateway** : passerelle par défaut du noeud de la grille. Par exemple : 172.16.10.1
- **Sous-réseaux (CIDR)** : un ou plusieurs sous-réseaux pour le réseau Admin.

e. Sélectionnez **Enregistrer**.

Le nœud de grille approuvé passe à la liste nœuds approuvés.

- Pour modifier les propriétés d'un nœud de grille approuvé, sélectionnez son bouton radio et sélectionnez **Modifier**.
- Pour déplacer un nœud de grille approuvé vers la liste nœuds en attente, sélectionnez son bouton d'option et sélectionnez **Réinitialiser**.
- Pour supprimer définitivement un nœud de grille approuvé, mettez le nœud hors tension. Ensuite, sélectionnez son bouton radio et sélectionnez **Supprimer**.

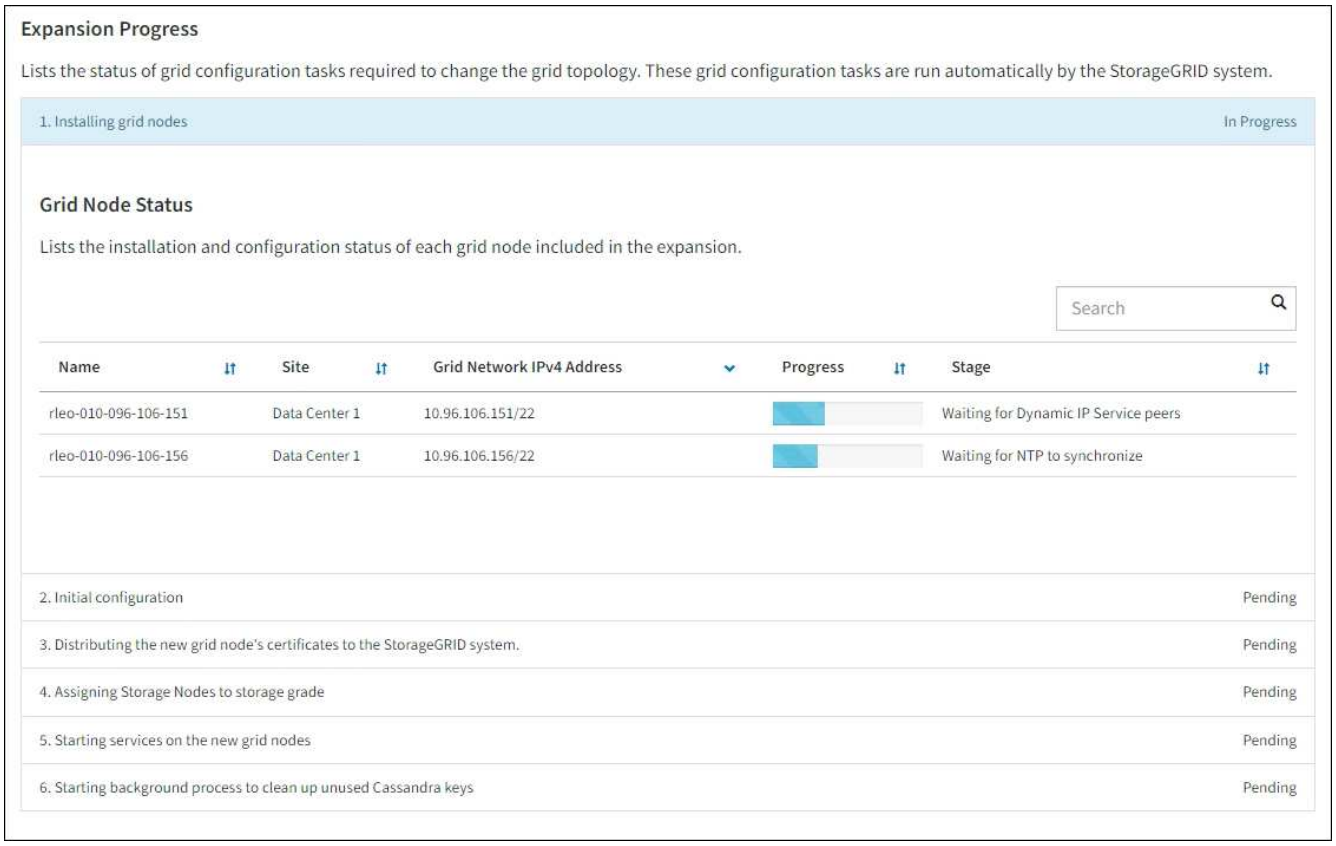
f. Répétez ces étapes pour chaque nœud de grille en attente à approuver.

> Si possible, vous devez approuver toutes les notes de grille en attente et effectuer une extension unique. Plus de temps sera nécessaire si vous réalisez plusieurs petits expansions.

7. Lorsque vous avez approuvé tous les nœuds de la grille, saisissez la phrase de passe de mise en service **, puis sélectionnez *développer**.

Au bout de quelques minutes, cette page se met à jour pour afficher l'état de la procédure d'extension. Lorsque des tâches qui affectent des nœuds de grille individuels sont en cours, la section Etat du nœud de grille répertorie l'état actuel de chaque nœud de grille.

> Lors de l'étape « installation des nœuds grid » pour une nouvelle appliance, le programme d'installation de l'appliance StorageGRID indique que l'installation passe de l'étape 3 à l'étape 4, finalisation de l'installation. Une fois l'étape 4 terminée, le contrôleur est redémarré.



L'extension de site inclut une tâche supplémentaire pour configurer Cassandra pour le nouveau site.

8. Dès que le lien **Download Recovery Package** apparaît, téléchargez le fichier Recovery Package.

   Vous devez télécharger une copie mise à jour du fichier du pack de récupération dès que possible après avoir apporté des modifications de topologie de grille au système StorageGRID. Le fichier du progiciel de récupération vous permet de restaurer le système en cas de défaillance.

   a. Sélectionnez le lien de téléchargement.
   b. Saisissez le mot de passe de provisionnement et sélectionnez **Démarrer le téléchargement**.
   c. Une fois le téléchargement terminé, ouvrez le `.zip` et confirmez que vous pouvez accéder au contenu, y compris au `Passwords.txt` fichier.
   d. Copiez le fichier du progiciel de restauration téléchargé (`.zip`) à deux emplacements sûrs, sécurisés et séparés.

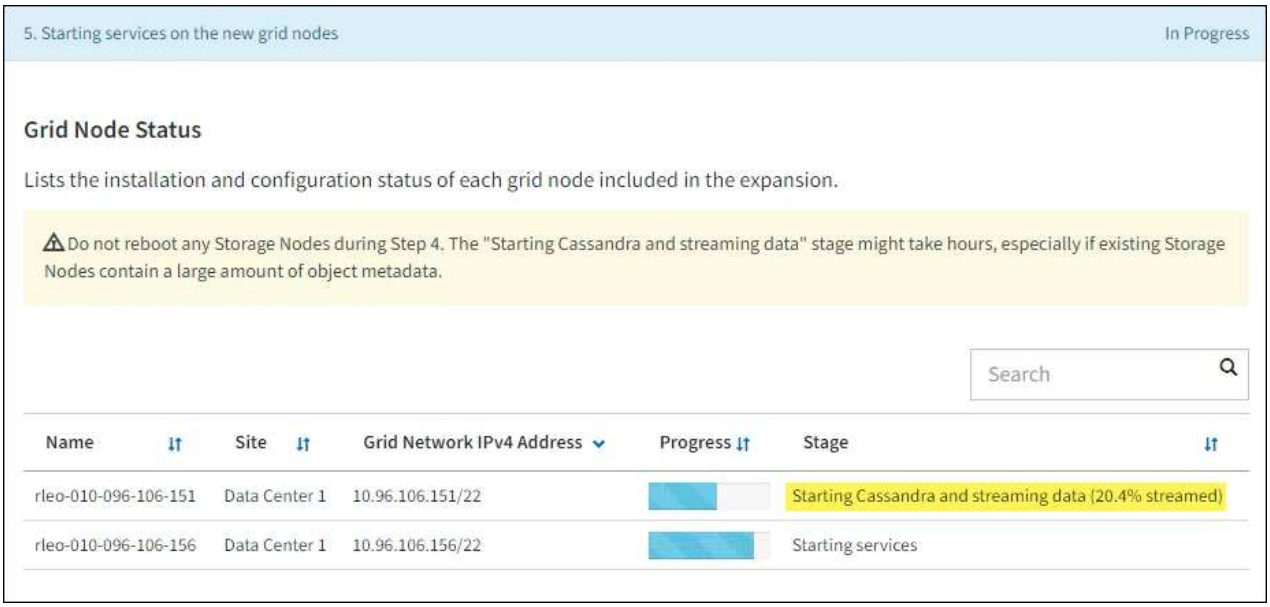
   Le fichier du progiciel de récupération doit être sécurisé car il contient des clés de cryptage et des mots de passe qui peuvent être utilisés pour obtenir des données du système StorageGRID.

9. Si vous ajoutez des nœuds de stockage à un site existant ou que vous ajoutez un site, surveillez les étapes Cassandra qui se produisent lorsque les services sont démarrés sur les nouveaux nœuds de grille.

Ne redémarrez aucun nœud de stockage pendant les étapes « extension du cluster Cassandra » ou « démarrage de Cassandra et des données de streaming ». Ces étapes peuvent prendre plusieurs heures pour chaque nouveau nœud de stockage, en particulier si les nœuds de stockage existants contiennent une quantité importante de métadonnées d'objet.

Ajout de nœuds de stockage

Si vous ajoutez des nœuds de stockage à un site existant, consultez le pourcentage affiché dans le message d'état « Cassandra et données en streaming ».



Ce pourcentage estime que le streaming Cassandra est complet, en fonction du volume total de données Cassandra disponibles et du volume qui a déjà été écrit sur le nouveau nœud.

Ajout d'un site

Si vous ajoutez un nouveau site, utilisez `nodetool status` Pour suivre la progression du streaming Cassandra et connaître le volume de métadonnées copiées vers le nouveau site lors de l'étape « étendre le cluster Cassandra ». La charge totale des données sur le nouveau site devrait se situer à environ 20 % du total d'un site actuel.

10. Continuez à surveiller l'extension jusqu'à ce que toutes les tâches soient terminées et que le bouton **Configure expansion** réapparaît.

Une fois que vous avez terminé

En fonction des types de nœuds de grille que vous avez ajoutés, effectuez des étapes supplémentaires d'intégration et de configuration. Voir "Étapes de configuration après l'extension".

Configuration du système faisant l'objet de l'extension

Étapes de configuration après l'extension

Une fois l'extension terminée, vous devez effectuer d'autres étapes d'intégration et de configuration.

Description de la tâche

Vous devez effectuer les tâches de configuration répertoriées ci-dessous pour les nœuds grid ou les sites que vous ajoutez à votre extension. Certaines tâches peuvent être facultatives, selon les options sélectionnées lors de l'installation et de l'administration du système, et selon la façon dont vous souhaitez configurer les nœuds et les sites ajoutés au cours de l'extension.

Étapes

1. Si vous avez ajouté un site :
   - "Créer un pool de stockage" Pour le site et chaque niveau de stockage que vous avez sélectionnés pour les nouveaux nœuds de stockage.
   - Vérification de la conformité de la politique ILM aux nouvelles exigences Si des modifications de règle sont requises, "créer de nouvelles règles" et "Mise à jour de la règle ILM". Si les règles sont déjà correctes, "activer une nouvelle stratégie" Aucune modification de règle n'est nécessaire pour garantir que StorageGRID utilise les nouveaux nœuds.
   - Vérifiez que les serveurs NTP (Network Time Protocol) sont accessibles depuis ce site. Voir "Gérer les serveurs NTP".

   > Assurez-vous qu'au moins deux nœuds de chaque site peuvent accéder à au moins quatre sources NTP externes. Si un seul nœud d'un site peut atteindre les sources NTP, des problèmes de synchronisation surviennent en cas de panne de ce nœud. En outre, la désignation de deux nœuds par site en tant que sources NTP principales assure une synchronisation précise si un site est isolé du reste de la grille.

2. Si vous avez ajouté un ou plusieurs nœuds de stockage à un site existant :
   - "Afficher les détails du pool de stockage" Vous pouvez vérifier que chaque nœud ajouté est inclus dans les pools de stockage attendus et utilisé dans les règles ILM attendues.
   - Vérification de la conformité de la politique ILM aux nouvelles exigences Si des modifications de règle sont requises, "créer de nouvelles règles" et "Mise à jour de la règle ILM". Si les règles sont déjà correctes, "activer une nouvelle stratégie" Aucune modification de règle n'est nécessaire pour garantir que StorageGRID utilise les nouveaux nœuds.
   - "Vérifiez que le nœud de stockage est actif" et capable d'ingérer des objets.
   - Si vous n'avez pas pu ajouter le nombre recommandé de nœuds de stockage, rééquilibrez les données avec code d'effacement. Voir"Rééquilibrent les données codées après l'ajout de nœuds de stockage".
3. Si vous avez ajouté un nœud de passerelle :
   - Si des groupes haute disponibilité sont utilisés pour les connexions client, ajoutez le nœud de passerelle à un groupe haute disponibilité (HA). Sélectionnez **CONFIGURATION** > **réseau** > **groupes haute disponibilité** pour consulter la liste des groupes haute disponibilité existants et ajouter le nouveau nœud. Voir "Configurez les groupes haute disponibilité".
4. Si vous avez ajouté un nœud d'administration :
   a. Si l'authentification unique est activée pour votre système StorageGRID, créez une confiance en tiers pour le nouveau nœud d'administration. Vous ne pouvez pas vous connecter au nœud tant que vous n'avez pas créé cette confiance de partie utilisatrice. Voir"Configurer l'authentification unique".
   b. Si vous prévoyez d'utiliser le service Load Balancer sur les nœuds d'administration, ajoutez éventuellement le nouveau nœud d'administration à un groupe haute disponibilité. Sélectionnez **CONFIGURATION** > **réseau** > **groupes haute disponibilité** pour consulter la liste des groupes haute disponibilité existants et ajouter le nouveau nœud. Voir "Configurez les groupes haute disponibilité".

c. Vous pouvez également copier la base de données du nœud d'administration principal vers le nœud d'administration d'extension si vous souhaitez préserver la cohérence des informations d'audit et d'attribut sur chaque nœud d'administration. Voir "Copiez la base de données du nœud d'administration".

d. Si vous souhaitez conserver la cohérence des metrics historiques sur chaque nœud d'administration, vous pouvez également copier la base de données Prometheus du nœud d'administration principal vers le nœud d'administration d'extension. Voir "Copie des metrics Prometheus".

e. Si vous souhaitez conserver la cohérence des informations du journal historique sur chaque nœud d'administration, copiez les journaux d'audit existants du nœud d'administration principal vers le nœud d'administration d'extension. Voir "Copie des journaux d'audit".

f. Vous pouvez également configurer l'accès au système à des fins d'audit via un partage de fichiers NFS. Voir "Configurer l'accès client d'audit pour NFS".

5. Pour vérifier si des nœuds d'extension ont été ajoutés avec un réseau client non fiable ou pour modifier si le réseau client d'un nœud n'est pas fiable ou approuvé, accédez à **CONFIGURATION** > **sécurité** > **contrôle pare-feu**.

   Si le réseau client sur le nœud d'extension n'est pas fiable, les connexions au nœud sur le réseau client doivent être effectuées à l'aide d'un noeud final d'équilibreur de charge. Voir "Gérer les contrôles de pare-feu".

6. Configurez le DNS.

   Si vous avez spécifié des paramètres DNS séparément pour chaque nœud de grid, vous devez ajouter des paramètres DNS personnalisés par nœud pour les nouveaux nœuds. Voir "Modifiez la configuration DNS pour un nœud de grid unique".

Pour garantir un fonctionnement correct, spécifiez deux ou trois serveurs DNS. Si vous spécifiez plus de trois, il est possible que seulement trois soient utilisés en raison des limitations connues du système d'exploitation sur certaines plates-formes. Si vous avez des restrictions de routage dans votre environnement, vous pouvez le faire "Personnaliser la liste des serveurs DNS" Pour les nœuds individuels (généralement tous les nœuds d'un site) d'utiliser un ensemble différent de trois serveurs DNS.

Si possible, utilisez des serveurs DNS auxquels chaque site peut accéder localement pour vous assurer qu'un site isdébarqué peut résoudre les FQDN pour les destinations externes.

Vérifiez que le nœud de stockage est actif

Une fois une opération d'extension qui ajoute de nouveaux nœuds de stockage terminée, le système StorageGRID doit démarrer automatiquement à l'aide des nouveaux nœuds de stockage. Vous devez utiliser le système StorageGRID pour vérifier que le nouveau nœud de stockage est actif.

Étapes

1. Connectez-vous au Grid Manager à l'aide d'un "navigateur web pris en charge".
2. Sélectionnez **NODES** > ***expansion Storage Node*** > **Storage**.
3. Placez votre curseur sur le graphique **stockage utilisé - données d'objet** pour afficher la valeur de **utilisé**, qui est la quantité d'espace utilisable total utilisée pour les données d'objet.
4. Vérifiez que la valeur de **utilisé** augmente au fur et à mesure que vous déplacez le curseur vers la droite du graphique.

Copiez la base de données du nœud d'administration

Lorsque vous ajoutez des nœuds d'administration via une procédure d'extension, vous pouvez éventuellement copier la base de données du nœud d'administration principal vers le nouveau nœud d'administration. La copie de la base de données vous permet de conserver des informations historiques sur les attributs, les alertes et les alertes.

Avant de commencer

- Vous avez terminé les étapes d'extension requises pour ajouter un nœud d'administration.
- Vous avez le `Passwords.txt` fichier.
- Vous avez la phrase secrète pour le provisionnement.

Description de la tâche

Le processus d'activation du logiciel StorageGRID crée une base de données vide pour le service NMS sur le nœud d'administration d'extension. Lorsque le service NMS démarre sur le nœud d'administration d'extension, il enregistre les informations concernant les serveurs et services qui font actuellement partie du système ou qui sont ajoutés ultérieurement. Cette base de données de nœud d'administration contient les informations suivantes :

- Historique des alertes
- Historique des alarmes
- Les données d'attributs historiques, qui sont utilisées dans les graphiques et les rapports texte disponibles à partir de la page **SUPPORT** > **Outils** > **topologie de grille**

Pour vous assurer que la base de données du nœud d'administration est cohérente entre les nœuds, vous pouvez copier la base de données du nœud d'administration principal vers le nœud d'administration d'extension.

> La copie de la base de données du noeud d'administration principal (le noeud d'administration__source_) vers un noeud d'administration d'extension peut prendre plusieurs heures. Pendant cette période, le gestionnaire de grille est inaccessible.

Procédez comme suit pour arrêter le service MI et le service API de gestion sur le nœud d'administration principal et le nœud d'administration d'extension avant de copier la base de données.

Étapes

1. Effectuez les étapes suivantes sur le nœud d'administration principal :
   a. Connectez-vous au nœud d'administration :
      i. Saisissez la commande suivante : `ssh admin@grid_node_IP`
      ii. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
      iii. Entrez la commande suivante pour passer à la racine : `su -`
      iv. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
   b. Exécutez la commande suivante : `recover-access-points`
   c. Saisissez la phrase secrète pour le provisionnement.
   d. Arrêtez le service MI : `service mi stop`

e. Arrêtez le service Management application Program interface (Management-api) : `service mgmt-api stop`

2. Procédez comme suit sur le nœud d'administration d'extension :
   a. Connectez-vous au nœud d'administration d'extension :
      i. Saisissez la commande suivante : `ssh admin@grid_node_IP`
      ii. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
      iii. Entrez la commande suivante pour passer à la racine : `su -`
      iv. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
   b. Arrêtez le service MI : `service mi stop`
   c. Arrêt du service mgmt-api : `service mgmt-api stop`
   d. Ajoutez la clé privée SSH à l'agent SSH. Entrez :`ssh-add`
   e. Entrez le mot de passe d'accès SSH répertorié dans le `Passwords.txt` fichier.
   f. Copiez la base de données du nœud d'administration source vers le nœud d'administration d'extension : `/usr/local/mi/bin/mi-clone-db.sh Source_Admin_Node_IP`
   g. Lorsque vous y êtes invité, confirmez que vous souhaitez remplacer la base DE données MI sur le nœud d'administration d'extension.

      La base de données et ses données historiques sont copiées dans le nœud d'administration d'extension. Lorsque la copie est terminée, le script démarre le nœud d'administration d'extension.

   h. Lorsque vous n'avez plus besoin d'un accès sans mot de passe à d'autres serveurs, supprimez la clé privée de l'agent SSH. Entrez :`ssh-add -D`
3. Redémarrez les services sur le nœud d'administration principal : `service servermanager start`

Copie des metrics Prometheus

Après avoir ajouté un nouveau nœud d'administration, vous pouvez éventuellement copier les metrics historiques gérés par Prometheus du nœud d'administration principal vers le nouveau nœud d'administration. La copie des metrics garantit la cohérence des mesures historiques entre les nœuds d'administration.

Avant de commencer

- Le nouveau nœud d'administration est installé et en cours d'exécution.
- Vous avez le `Passwords.txt` fichier.
- Vous avez la phrase secrète pour le provisionnement.

Description de la tâche

Lorsque vous ajoutez un nœud d'administration, le processus d'installation logicielle crée une nouvelle base de données Prometheus. Vous pouvez conserver la cohérence des metrics historiques entre les nœuds en copiant la base de données Prometheus du nœud d'administration principal (*source Admin Node*) vers le nouveau nœud d'administration.

La copie de la base de données Prometheus peut prendre une heure ou plus. Certaines fonctionnalités de Grid Manager ne seront pas disponibles lorsque les services sont arrêtés sur le nœud d'administration source.

Étapes

1. Connectez-vous au nœud d'administration source :
   a. Saisissez la commande suivante : `ssh admin@grid_node_IP`
   b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
   c. Entrez la commande suivante pour passer à la racine : `su -`
   d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
2. Depuis le nœud d'administration source, arrêter le service Prometheus : `service prometheus stop`
3. Suivez les étapes suivantes sur le nouveau nœud d'administration :
   a. Connectez-vous au nouveau nœud d'administration :
      i. Saisissez la commande suivante : `ssh admin@grid_node_IP`
      ii. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
      iii. Entrez la commande suivante pour passer à la racine : `su -`
      iv. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
   b. Arrêtez le service Prometheus : `service prometheus stop`
   c. Ajoutez la clé privée SSH à l'agent SSH. Entrez :`ssh-add`
   d. Entrez le mot de passe d'accès SSH répertorié dans le `Passwords.txt` fichier.
   e. Copiez la base de données Prometheus du nœud d'administration source vers le nouveau nœud d'administration : `/usr/local/prometheus/bin/prometheus-clone-db.sh Source_Admin_Node_IP`
   f. Lorsque vous y êtes invité, appuyez sur **Enter** pour confirmer que vous souhaitez détruire la nouvelle base de données Prometheus sur le nouveau noeud d'administration.

      La base de données Prometheus d'origine et ses données historiques sont copiées sur le nouveau nœud d'administration. Une fois l'opération de copie terminée, le script démarre le nouveau nœud d'administration. L'état suivant apparaît :

```
Database cloned, starting services
```

   a. Lorsque vous n'avez plus besoin d'un accès sans mot de passe à d'autres serveurs, supprimez la clé privée de l'agent SSH. Entrez :

```
ssh-add -D
```

4. Redémarrez le service Prometheus sur le nœud d'administration source.

```
service prometheus start
```

Copie des journaux d'audit

Lorsque vous ajoutez un nouveau nœud d'administration par le biais d'une procédure d'extension, son service AMS consigne uniquement les événements et actions qui se produisent une fois qu'il rejoint le système. Si nécessaire, vous pouvez copier les journaux d'audit à partir d'un nœud d'administration déjà installé vers le nouveau nœud d'administration d'extension afin qu'il soit synchronisé avec le reste du système StorageGRID.

Avant de commencer

- Vous avez terminé les étapes d'extension requises pour ajouter un nœud d'administration.
- Vous avez le `Passwords.txt` fichier.

Description de la tâche

Pour rendre disponibles les messages d'audit historiques sur un nouveau nœud d'administration, vous devez copier manuellement les fichiers journaux d'audit d'un nœud d'administration existant vers le nœud d'administration d'extension.

> Par défaut, les informations d'audit sont envoyées au journal d'audit des nœuds d'administration. Vous pouvez ignorer ces étapes si l'une des conditions suivantes s'applique :
>
> - Un serveur syslog externe et des journaux d'audit sont maintenant envoyés au serveur syslog au lieu de vers les nœuds d'administration.
> - Vous avez explicitement indiqué que les messages d'audit doivent être enregistrés uniquement sur les nœuds locaux qui les ont générés.
>
> Voir "Configurez les messages d'audit et les destinations des journaux" pour plus d'informations.

Étapes

1. Connectez-vous au nœud d'administration principal :
   a. Saisissez la commande suivante : `ssh admin@_primary_Admin_Node_IP`
   b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
   c. Entrez la commande suivante pour passer à la racine : `su -`
   d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

   Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.
2. Arrêtez le service AMS pour l'empêcher de créer un nouveau fichier : `service ams stop`
3. Renommez le `audit.log` Fichier pour s'assurer qu'il n'écrase pas le fichier sur le noeud d'administration d'extension dans lequel vous le copiez :

   ```
   cd /var/local/audit/export
   ls -l
   mv audit.log new_name.txt
   ```

4. Copiez tous les fichiers journaux d'audit sur le nœud d'administration d'extension :

   ```
   scp -p * IP_address:/var/local/audit/export
   ```

5. Si vous êtes invité à saisir la phrase de passe pour `/root/.ssh/id_rsa`, Entrez le mot de passe d'accès SSH du nœud d'administration principal répertorié dans `Passwords.txt` fichier.
6. Restaurez l'original `audit.log` fichier :

   ```
   mv new_name.txt audit.log
   ```

7. Démarrez le service AMS :

   ```
   service ams start
   ```

8. Déconnexion du serveur :

   ```
   exit
   ```

9. Connectez-vous au nœud d'administration d'extension :
   a. Saisissez la commande suivante : `ssh admin@expansion_Admin_Node_IP`
   b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
   c. Entrez la commande suivante pour passer à la racine : `su -`
   d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

      Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

10. Mettez à jour les paramètres utilisateur et groupe des fichiers journaux d'audit :

    ```
    cd /var/local/audit/export
    chown ams-user:bycast *
    ```

11. Déconnexion du serveur :

    ```
    exit
    ```

Rééquilibrent les données codées après l'ajout de nœuds de stockage

Après avoir ajouté des nœuds de stockage, vous pouvez utiliser la procédure de rééquilibrage EC pour redistribuer les fragments avec code d'effacement entre les nœuds de stockage existants et nouveaux.

Avant de commencer

- Vous avez terminé les étapes d'extension pour ajouter les nouveaux nœuds de stockage.
- Vous avez passé en revue le "considérations relatives au rééquilibrage des données avec code d'effacement".
- Vous comprenez que les données d'objet répliqué ne seront pas déplacées par cette procédure et que la procédure de rééquilibrage EC ne tient pas compte de l'utilisation des données répliquées sur chaque nœud de stockage lors de la détermination de l'emplacement du déplacement des données codées par l'effacement.
- Vous avez le `Passwords.txt` fichier.

Que se passe-t-il lorsque cette procédure est exécutée

Avant de commencer la procédure, noter les points suivants :

- La procédure de rééquilibrage EC ne démarre pas si un ou plusieurs volumes sont hors ligne (démontés) ou s'ils sont en ligne (montés) mais en état d'erreur.
- La procédure de rééquilibrage EC réserve temporairement une grande quantité de stockage. Les alertes de stockage peuvent être déclenchées, mais elles seront résolus une fois le rééquilibrage terminé. S'il n'y a pas assez de stockage pour la réservation, la procédure de rééquilibrage EC échoue. Les réservations de stockage sont libérées lorsque la procédure de rééquilibrage EC est terminée, que la procédure ait échoué ou a réussi.
- Si un volume passe hors ligne ou rencontre une erreur pendant le rééquilibrage du code d'effacement, le processus de rééquilibrage se termine partiellement, sans perte de données. La procédure de rééquilibrage EC peut être reprise au point où elle s'est arrêtée lorsque tous les volumes sont en ligne sans erreur.
- L'exécution de la procédure de rééquilibrage EC peut avoir un impact sur les performances des opérations ILM et des opérations clients S3 et Swift.

> Si le processus de rééquilibrage EC prend plus de 24 heures, les opérations des API S3 et Swift pour charger des objets (ou des pièces d'objet) peuvent échouer. Les opérations PUT de longue durée échouent si la règle ILM applicable utilise un placement équilibré ou strict à l'entrée. L'erreur suivante sera signalée : `500 Internal Server Error`.

Étapes

1. consultez les détails actuels du stockage objet pour le site que vous prévoyez de rééquilibrer.
   a. Sélectionnez **NOEUDS**.
   b. Sélectionnez le premier nœud de stockage du site.
   c. Sélectionnez l'onglet **stockage**.
   d. Positionnez le curseur de votre souris sur le graphique stockage utilisé - données d'objet pour afficher la quantité actuelle de données répliquées et de données avec code d'effacement sur le nœud de stockage.
   e. Répétez cette procédure pour afficher les autres nœuds de stockage du site.
2. Connectez-vous au nœud d'administration principal :
   a. Saisissez la commande suivante : `ssh admin@primary_Admin_Node_IP`
   b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
   c. Entrez la commande suivante pour passer à la racine : `su -`
   d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

      Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.
3. Démarrer la procédure :

   `rebalance-data start --site "site-name"`

   Pour "*site-name*", Spécifiez le premier site sur lequel vous avez ajouté un ou plusieurs nœuds de stockage. Entourez-la `site-name` entre guillemets.

   La procédure de rééquilibrage EC démarre et un ID de tâche est renvoyé.

4. Copier l'ID du travail.
5. Surveiller le statut de la procédure de rééquilibrage EC.
   - Pour afficher le statut d'une procédure de rééquilibrage EC unique :

     `rebalance-data status --job-id job-id`

     Pour *job-id*, Spécifiez l'ID renvoyé au début de la procédure.
   - Pour afficher le statut de la procédure de rééquilibrage EC actuelle et toutes les procédures précédemment effectuées :

     `rebalance-data status`

     Pour obtenir de l'aide sur la commande rééquilibrer-données :

     `rebalance-data --help`
6. Effectuer des étapes supplémentaires en fonction de l'état renvoyé :
   - Si l'état est `In progress`, L'opération EC de rééquilibrage est toujours en cours. Vous devez régulièrement surveiller la procédure jusqu'à ce qu'elle soit terminée.

     Pour afficher le temps d'achèvement estimé et le pourcentage d'achèvement de la tâche en cours :

     i. Sélectionnez **SUPPORT** > **Outils** > **métriques**.
     ii. Sélectionnez **EC Overview** dans la section Grafana.
     iii. Examinez les tableaux de bord **Grid EC Job estimé Time to Completion** et **Grid EC Job Percentage Finted**.
   - Si l'état est `Success`, facultatif examinez le stockage objet pour afficher les détails mis à jour pour le site.

     Les données avec code d'effacement doivent désormais être plus équilibrées entre les nœuds de stockage du site.

     Si le message suivant s'affiche, exécutez à nouveau la procédure de rééquilibrage de l'EC jusqu'à ce que toutes les données avec code d'effacement aient été rééquilibrées :

     `The moves in this rebalance job have been limited. To rebalance additional data, start EC rebalance again for the same site.`
   - Si l'état est `Failure`:
     i. Vérifiez que tous les nœuds de stockage du site sont connectés à la grille.
     ii. Recherchez et résolvez les alertes susceptibles d'affecter ces nœuds de stockage.
     iii. Relancez la procédure de rééquilibrage EC :

     `rebalance-data start --job-id job-id`

     iv. Si le statut de la procédure de rééquilibrage de la ce est toujours `Failure`, contactez le support technique.

7. Si la procédure de rééquilibrage EC génère une charge trop importante (par exemple, les opérations d'ingestion sont affectées), mettez la procédure en pause.

   `rebalance-data pause --job-id job-id`

8. Si vous devez terminer la procédure de rééquilibrage EC (par exemple, pour une mise à niveau logicielle StorageGRID), entrez ce qui suit :

   `rebalance-data terminate --job-id job-id`

   > Lorsque vous terminez une procédure de rééquilibrage EC, tout fragment de données qui a déjà été déplacé reste au nouvel emplacement. Les données ne sont pas retransférées à leur emplacement d'origine.

9. Si vous utilisez le code d'effacement sur plusieurs sites, exécutez cette procédure pour tous les autres sites concernés.

Contactez l'assistance technique

Si vous rencontrez des erreurs lors du processus d'extension de la grille que vous ne parvenez pas à résoudre ou si une tâche de grille échoue, contactez le support technique.

Description de la tâche

Lorsque vous contactez le support technique, vous devez fournir les fichiers journaux requis pour vous aider à résoudre les erreurs que vous rencontrez.

Étapes

1. Se connecter au nœud d'extension qui a rencontré des défaillances :

   a. Saisissez la commande suivante :`ssh -p 8022 admin@grid_node_IP`

      > Le port 8022 est le port SSH du système d'exploitation de base, tandis que le port 22 est le port SSH du moteur de mise en conteneurs exécutant StorageGRID.

   b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

   c. Entrez la commande suivante pour passer à la racine : `su -`

   d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

   Une fois que vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

2. En fonction de la phase d'installation atteinte, récupérez l'un des journaux suivants disponibles sur le nœud de la grille :

Plateforme	Journaux
VMware	• `/var/log/daemon.log` • `/var/log/storagegrid/daemon.log` • `/var/log/storagegrid/nodes/<node-name>.log`

Plateforme	Journaux
Linux	• `/var/log/storagegrid/daemon.log` • `/etc/storagegrid/nodes/<node-name>.conf` (pour chaque nœud défaillant) • `/var/log/storagegrid/nodes/<node-name>.log` (pour chaque nœud en panne ; il se peut qu'il n'existe pas)

Restaurez les nœuds et gérez votre grid

Restauration et maintenance : vue d'ensemble

Suivez ces instructions pour entretenir votre système StorageGRID et effectuer une reprise après incident.

À propos de ces instructions

Ces instructions expliquent comment appliquer un correctif logiciel, récupérer des nœuds de la grille, récupérer un site défaillant, désaffecter des nœuds de la grille ou un site entier, effectuer la maintenance du réseau, exécuter des procédures de maintenance au niveau de l'hôte et du middleware et exécuter des procédures de nœud de la grille.

Dans ces instructions, « Linux » fait référence à un déploiement Red Hat® Enterprise Linux®, Ubuntu®, CentOS ou Debian®. Utilisez le "Matrice d'interopérabilité NetApp" pour obtenir une liste des versions prises en charge.

Avant de commencer

- Vous avez une bonne compréhension du système StorageGRID.
- Vous avez examiné la topologie de votre système StorageGRID et compris la configuration de la grille.
- Vous comprenez que vous devez suivre toutes les instructions exactement et tenir compte de tous les avertissements.
- Vous comprenez que les procédures de maintenance non décrites ne sont pas prises en charge ou requièrent une mission de service.

Procédures de maintenance des appareils

Pour connaître les procédures matérielles, reportez-vous aux instructions de maintenance de votre appliance StorageGRID.

- "Maintenance de l'appliance SGF6112"
- "Maintenance des appliances SG100 et SG1000"
- "Entretenir l'appareil SG6000"
- "Conservez l'appliance SG5700"

Téléchargez le progiciel de restauration

Le fichier progiciel de récupération vous permet de restaurer le système StorageGRID en cas de défaillance.

Avant de commencer

- Depuis le nœud d'administration principal, vous êtes connecté au gestionnaire de grille à l'aide d'un "navigateur web pris en charge".
- Vous avez la phrase secrète pour le provisionnement.
- Vous avez "autorisations d'accès spécifiques".

Téléchargez le fichier du pack de récupération actuel avant de modifier la topologie du grid sur le système StorageGRID ou avant de mettre à niveau le logiciel. Téléchargez ensuite une nouvelle copie du progiciel de récupération après avoir modifié la topologie de la grille ou après la mise à niveau du logiciel.

Étapes

1. Sélectionnez **MAINTENANCE** > **système** > **progiciel de récupération**.
2. Saisissez le mot de passe de provisionnement et sélectionnez **Démarrer le téléchargement**.

   Le téléchargement commence immédiatement.

3. Une fois le téléchargement terminé, ouvrez le `.zip` et confirmez que vous pouvez accéder au contenu, y compris au `Passwords.txt` fichier.
4. Copiez le fichier du progiciel de restauration téléchargé (`.zip`) à deux emplacements sûrs, sécurisés et séparés.

> Le fichier du progiciel de récupération doit être sécurisé car il contient des clés de cryptage et des mots de passe qui peuvent être utilisés pour obtenir des données du système StorageGRID.

Procédure de correctif StorageGRID

Procédure de correctif StorageGRID : présentation

Vous devrez peut-être appliquer un correctif à votre système StorageGRID si des problèmes liés au logiciel sont détectés et résolus entre les versions de fonctionnalités.

Les correctifs StorageGRID contiennent des modifications logicielles qui sont disponibles en dehors d'une version de fonctionnalité ou de correctif. Les mêmes modifications seront incluses dans une prochaine version. En outre, chaque version de correctif contient une synthèse de tous les correctifs précédents au sein de la fonction ou de la version de correctif.

Considérations relatives à l'application d'un correctif

Vous ne pouvez pas appliquer un correctif StorageGRID lorsqu'une autre procédure de maintenance est en cours d'exécution. Par exemple, vous ne pouvez pas appliquer un correctif lorsqu'une procédure de mise hors service, d'extension ou de récupération est en cours d'exécution.

Si une procédure de mise hors service d'un nœud ou d'un site est interrompue, vous pouvez appliquer un correctif en toute sécurité. De plus, vous pouvez appliquer un correctif lors des dernières étapes d'une procédure de mise à niveau StorageGRID. Pour plus de détails, reportez-vous aux instructions de mise à niveau du logiciel StorageGRID.

Une fois le correctif téléchargé dans Grid Manager, le correctif est automatiquement appliqué au nœud d'administration principal. Vous pouvez ensuite approuver l'application du correctif sur les autres nœuds de votre système StorageGRID.

Si un correctif ne s'applique pas à un ou plusieurs nœuds, la raison de l'échec s'affiche dans la colonne Détails de la table de progression du correctif. Vous devez résoudre les problèmes qui ont causé les échecs, puis recommencer le processus tout entier. Les nœuds avec une application précédemment réussie du correctif seront ignorés dans les applications suivantes. Vous pouvez réessayer en toute sécurité le processus de correctif autant de fois que nécessaire jusqu'à ce que tous les nœuds aient été mis à jour. Le correctif doit être installé avec succès sur tous les nœuds de la grille pour que l'application soit terminée.

Lorsque les nœuds de grille sont mis à jour avec la nouvelle version de correctif, les modifications réelles d'un correctif peuvent uniquement affecter des services spécifiques sur des types spécifiques de nœuds. Par exemple, un correctif peut uniquement affecter le service LDR sur les nœuds de stockage.

Application des correctifs pour la restauration et l'extension

Une fois qu'un correctif a été appliqué à votre grille, le nœud d'administration principal installe automatiquement la même version de correctif sur tous les nœuds restaurés par les opérations de reprise ou ajoutés dans une extension.

Cependant, si vous devez restaurer le noeud d'administration principal, vous devez installer manuellement la version correcte de StorageGRID, puis appliquer le correctif. La version StorageGRID finale du nœud d'administration principal doit correspondre à la version des autres nœuds de la grille.

L'exemple suivant illustre comment appliquer un correctif lors de la restauration du noeud d'administration principal :

1. Supposons que la grille exécute une version StorageGRID 11.*A.B* avec le dernier correctif. La « version grille » est 11.*A.B.y*.
2. Le nœud d'administration principal tombe en panne.
3. Vous redéployez le nœud d'administration principal à l'aide de StorageGRID 11.*A.B* et exécutez la procédure de restauration.

   Si nécessaire pour correspondre à la version de grille, vous pouvez utiliser une version mineure lors du déploiement du nœud ; vous n'avez pas besoin de déployer la version majeure en premier.

4. Vous appliquez ensuite le correctif 11.*A.B.y* au nœud d'administration principal.

Pour plus d'informations, voir "Configurez le nœud d'administration principal de remplacement".

Quel est l'impact de votre système lorsque vous appliquez un correctif

Vous devez comprendre comment votre système StorageGRID sera affecté lorsque vous appliquez un correctif.

Les applications client peuvent subir des interruptions à court terme

Le système StorageGRID peut ingérer et récupérer les données des applications client tout au long du processus de correctif. Toutefois, les connexions client aux nœuds de passerelle ou de stockage individuels peuvent être interrompues temporairement si le correctif doit redémarrer les services sur ces nœuds. La connectivité sera restaurée une fois le processus de correctif terminé et les services reprendront sur les nœuds individuels.

Vous devrez peut-être planifier des temps d'arrêt pour appliquer un correctif si la perte de connectivité pendant une courte période n'est pas acceptable. Vous pouvez utiliser l'approbation sélective pour planifier la mise à jour de certains nœuds.

> Vous pouvez utiliser plusieurs passerelles et groupes haute disponibilité (HA) pour assurer un basculement automatique pendant le processus de correctif. Reportez-vous aux instructions pour "configuration des groupes haute disponibilité".

Des alertes et des notifications SNMP peuvent être déclenchées

Des alertes et des notifications SNMP peuvent être déclenchées lorsque les services sont redémarrés et lorsque le système StorageGRID fonctionne comme un environnement de version mixte (certains nœuds grid exécutant une version antérieure, alors que d'autres ont été mis à niveau vers une version ultérieure). En général, ces alertes et notifications seront claires lorsque le correctif sera terminé.

Les modifications de configuration sont restreintes

Lors de l'application d'un correctif à StorageGRID :

- N'apportez aucune modification à la configuration de la grille (par exemple, spécification de sous-réseaux Grid Network ou approbation de nœuds grid en attente) tant que le correctif n'a pas été appliqué à tous les nœuds.
- Ne mettez pas à jour la configuration ILM tant que le correctif n'a pas été appliqué à tous les nœuds.

Procurez-vous le matériel requis pour le correctif

Avant d'appliquer un correctif, vous devez obtenir tous les matériaux requis.

Élément	Remarques
Fichier de correctif StorageGRID	Vous devez télécharger le fichier de correctif StorageGRID.
• Port réseau • "Navigateur Web pris en charge" • Client SSH (par exemple, PuTTY)	

Élément	Remarques
Package de restauration (`.zip`) fichier	Avant d'appliquer un correctif, "Téléchargez le dernier fichier de progiciel de récupération" En cas de problème pendant le correctif.puis, après l'application du correctif, téléchargez une nouvelle copie du fichier du progiciel de récupération et enregistrez-la dans un emplacement sûr. Le fichier du progiciel de récupération mis à jour vous permet de restaurer le système en cas de défaillance.
Fichier Passwords.txt	Facultatif et utilisé uniquement si vous appliquez un correctif manuellement à l'aide du client SSH. Le `Passwords.txt` Le fichier fait partie du progiciel de récupération `.zip` fichier.
Phrase secrète pour le provisionnement	La phrase de passe est créée et documentée lors de l'installation initiale du système StorageGRID. La phrase de passe de provisionnement n'est pas répertoriée dans le `Passwords.txt` fichier.
Documentation associée	`readme.txt` fichier du correctif. Ce fichier est inclus sur la page de téléchargement du correctif. N'oubliez pas de passer en revue le `readme` lifile soigneusement avant d'appliquer le correctif.

Téléchargez le fichier de correctif

Vous devez télécharger le fichier de correctif avant de pouvoir appliquer le correctif.

Étapes

1. Accédez à "Téléchargement NetApp : StorageGRID".
2. Sélectionnez la flèche vers le bas sous **logiciel disponible** pour afficher la liste des correctifs disponibles au téléchargement.

   Les versions de fichier correctif ont le format suivant : 11.4.*x.y*.

3. Vérifiez les modifications qui sont incluses dans la mise à jour.

   Si vous avez juste "Restauration du nœud d'administration principal - effectué" et vous devez appliquer un correctif, sélectionnez la même version de correctif installée sur les autres nœuds de la grille.

   a. Sélectionnez la version du correctif que vous souhaitez télécharger et sélectionnez **Go**.

   b. Connectez-vous en utilisant le nom d'utilisateur et le mot de passe de votre compte NetApp.

   c. Lisez et acceptez le contrat de licence de l'utilisateur final.

      La page de téléchargement de la version sélectionnée s'affiche.

   d. Téléchargez le correctif `readme.txt` fichier pour afficher un résumé des modifications incluses dans le correctif.

4. Sélectionnez le bouton de téléchargement du correctif et enregistrez le fichier.

Ne modifiez pas le nom de ce fichier.

Si vous utilisez un périphérique MacOS, le fichier de correctif peut être enregistré automatiquement en tant que `.txt` fichier. Si c'est le cas, vous devez renommer le fichier sans le `.txt` extension.

5. Sélectionnez un emplacement pour le téléchargement et sélectionnez **Enregistrer**.

Vérifiez l'état du système avant d'appliquer le correctif

Vous devez vérifier que le système est prêt à prendre en charge le correctif.

1. Connectez-vous au Grid Manager à l'aide d'un "navigateur web pris en charge".
2. Si possible, assurez-vous que le système fonctionne normalement et que tous les nœuds de la grille sont connectés à la grille.

   Les nœuds connectés ont des coches vertes Sur la page nœuds.

3. Recherchez et résolvez les alertes en cours, si possible.
4. Assurez-vous qu'aucune autre procédure de maintenance n'est en cours, telle qu'une procédure de mise à niveau, de récupération, d'extension ou de mise hors service.

   Vous devez attendre que toutes les procédures de maintenance actives soient terminées avant d'appliquer un correctif.

   Vous ne pouvez pas appliquer un correctif StorageGRID lorsqu'une autre procédure de maintenance est en cours d'exécution. Par exemple, vous ne pouvez pas appliquer un correctif lorsqu'une procédure de mise hors service, d'extension ou de récupération est en cours d'exécution.

   S'il s'agit d'un nœud ou d'un site "la procédure de mise hors service est suspendue", vous pouvez appliquer un correctif en toute sécurité. De plus, vous pouvez appliquer un correctif lors des dernières étapes d'une procédure de mise à niveau StorageGRID. Reportez-vous aux instructions pour "Mise à niveau du logiciel StorageGRID".

Appliquez un correctif

Le correctif est d'abord appliqué automatiquement au nœud d'administration principal. Vous devez ensuite approuver l'application du correctif sur d'autres nœuds de la grille jusqu'à ce que tous les nœuds exécutent la même version logicielle. Vous pouvez personnaliser la séquence d'approbation en sélectionnant pour approuver des nœuds de grille individuels, des groupes de nœuds de grille ou tous les nœuds de la grille.

Avant de commencer

- Vous avez passé en revue le "considérations relatives à l'application d'un correctif".
- Vous avez la phrase secrète pour le provisionnement.
- Vous disposez de l'accès racine ou de l'autorisation Maintenance.

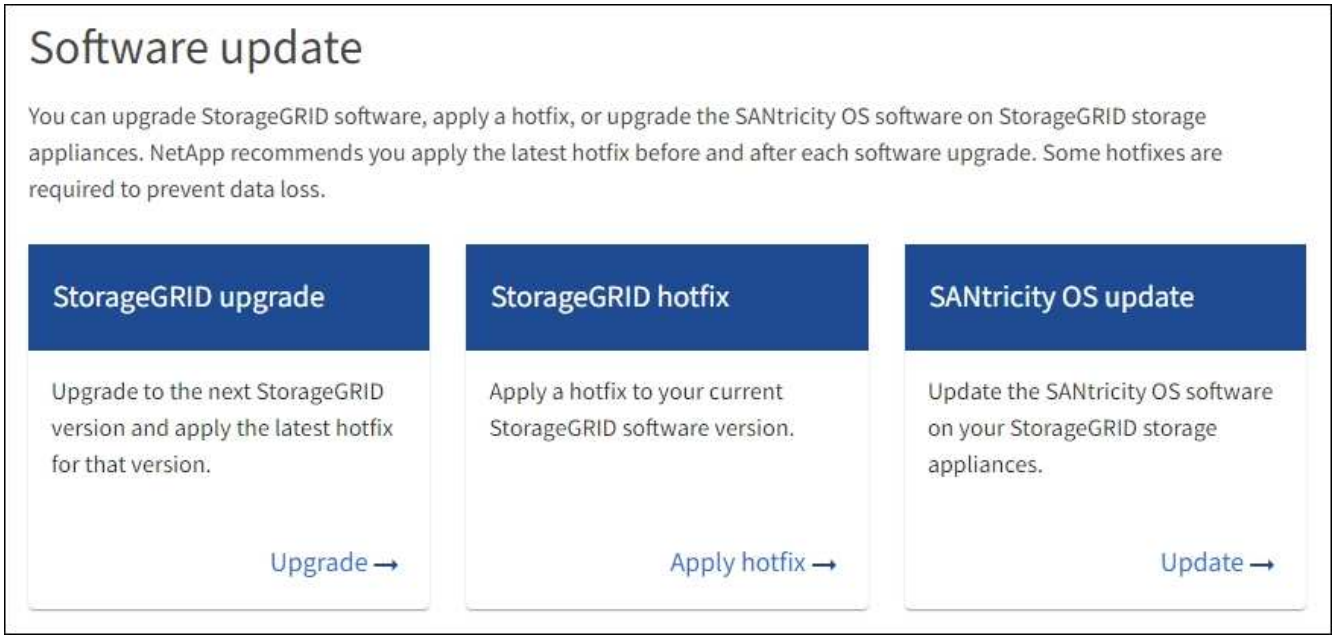
Description de la tâche

- Vous pouvez retarder l'application d'un correctif à un nœud, mais le processus de correctif n'est pas terminé tant que vous n'avez pas appliqué le correctif à tous les nœuds.
- Vous ne pouvez pas effectuer de mise à niveau du logiciel StorageGRID ou de mise à jour du système d'exploitation SANtricity tant que vous n'avez pas terminé le processus de correctif.

Étapes

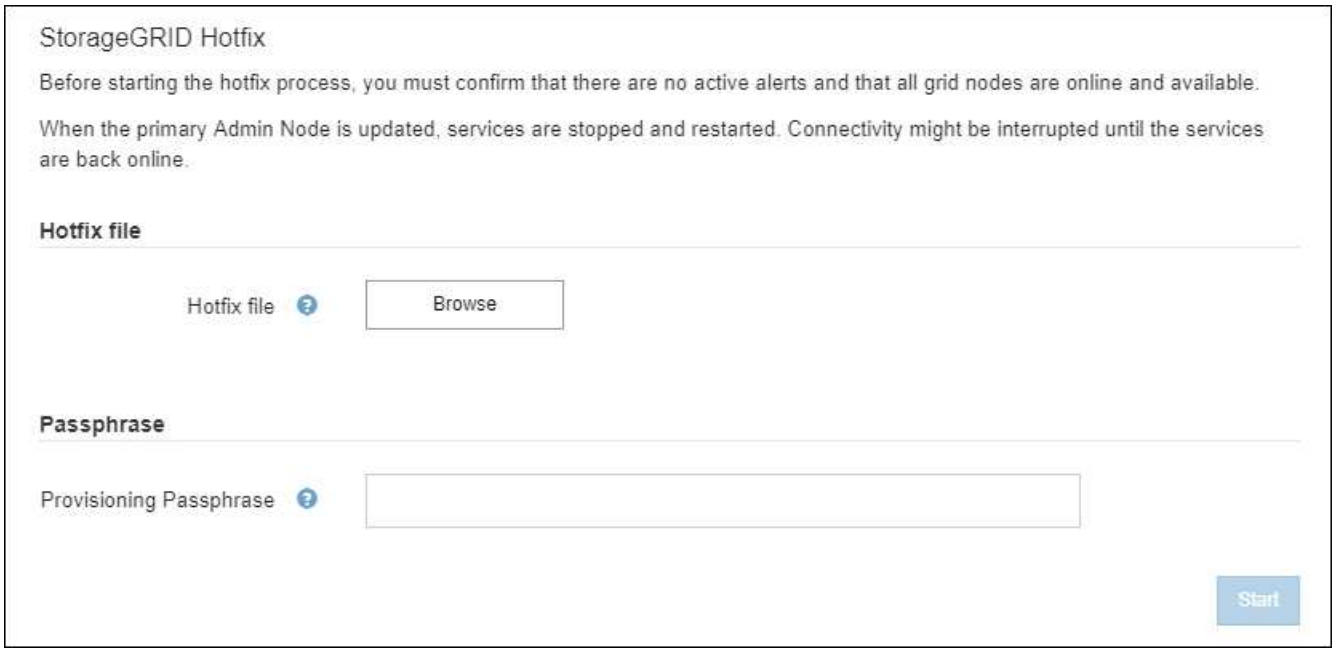
1. Connectez-vous au Grid Manager à l'aide d'un "navigateur web pris en charge".
2. Sélectionnez **MAINTENANCE** > **système** > **mise à jour logicielle**.

   La page mise à jour du logiciel s'affiche.



3. Sélectionnez **appliquer le correctif**.

   La page correctif StorageGRID s'affiche.



4. Sélectionnez le fichier correctif que vous avez téléchargé à partir du site de support NetApp.

   a. Sélectionnez **Parcourir**.

   b. Localisez et sélectionnez le fichier.

      `hotfix-install-`*`version`*

   c. Sélectionnez **Ouvrir**.

      Le fichier est téléchargé. Lorsque le téléchargement est terminé, le nom du fichier s'affiche dans le champ Détails.

      Ne modifiez pas le nom du fichier car il fait partie du processus de vérification.

5. Entrez la phrase de passe de provisionnement dans la zone de texte.

   Le bouton **Démarrer** devient activé.

6. Sélectionnez **Démarrer**.

   Un avertissement s'affiche indiquant que la connexion de votre navigateur peut être perdue temporairement au fur et à mesure que les services sur le nœud d'administration principal sont redémarrés.

7. Sélectionnez **OK** pour commencer à appliquer le correctif au nœud d'administration principal.

   Lorsque le correctif démarre :

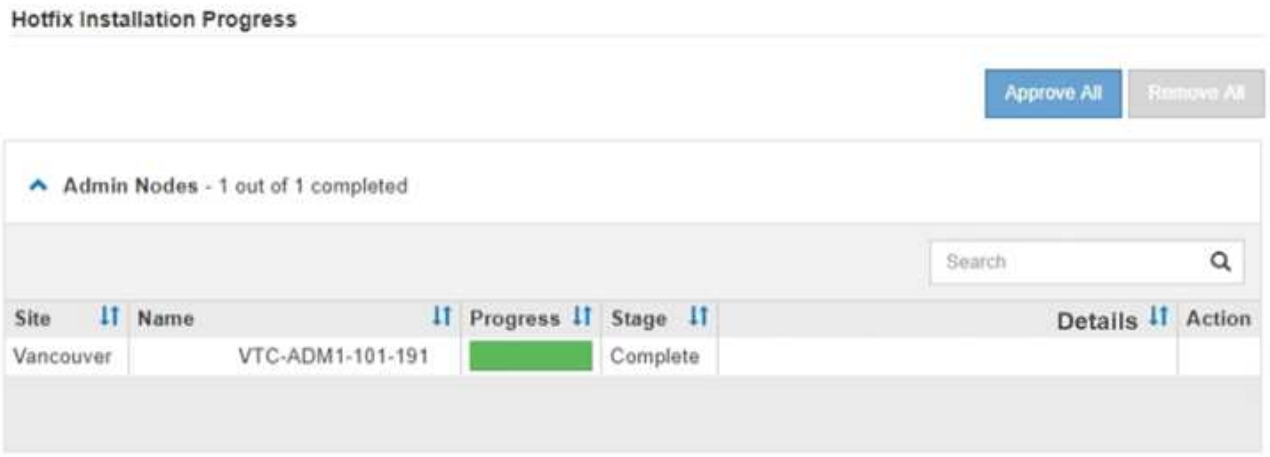
   a. Les validations de correctif sont exécutées.

      Si des erreurs sont signalées, résolvez-les, téléchargez à nouveau le fichier correctif et sélectionnez à nouveau **Démarrer**.

   b. Le tableau de progression de l'installation du correctif s'affiche.

      Ce tableau affiche tous les nœuds de votre grille et l'étape actuelle de l'installation du correctif pour chaque nœud. Les nœuds du tableau sont regroupés par type (nœuds Admin, nœuds de passerelle, nœuds de stockage et nœuds d'archivage).

   c. La barre de progression atteint la fin, puis le nœud d'administration principal est affiché comme « terminé ».



8. Vous pouvez également trier les listes de nœuds de chaque groupe par ordre croissant ou décroissant en fonction de **site**, **Nom**, **progrès**, **étape** ou **Détails**. Vous pouvez également saisir un terme dans la zone **Rechercher** pour rechercher des nœuds spécifiques.
9. Approuver les nœuds grid prêts à être mis à jour. Les nœuds approuvés du même type sont mis à niveau un par un.

> N'approuvez pas le correctif pour un nœud, sauf si vous êtes sûr que le nœud est prêt à être mis à jour. Lorsque le correctif est appliqué à un nœud de grille, certains services sur ce nœud peuvent être redémarrés. Ces opérations peuvent entraîner des interruptions de service pour les clients qui communiquent avec le nœud.

   - Sélectionnez un ou plusieurs boutons **Approve** pour ajouter un ou plusieurs nœuds individuels à la file d'attente du correctif.
   - Sélectionnez le bouton **approuver tout** dans chaque groupe pour ajouter tous les nœuds du même type à la file d'attente du correctif. Si vous avez saisi des critères de recherche dans la zone **recherche**, le bouton **approuver tout** s'applique à tous les nœuds sélectionnés par les critères de recherche.

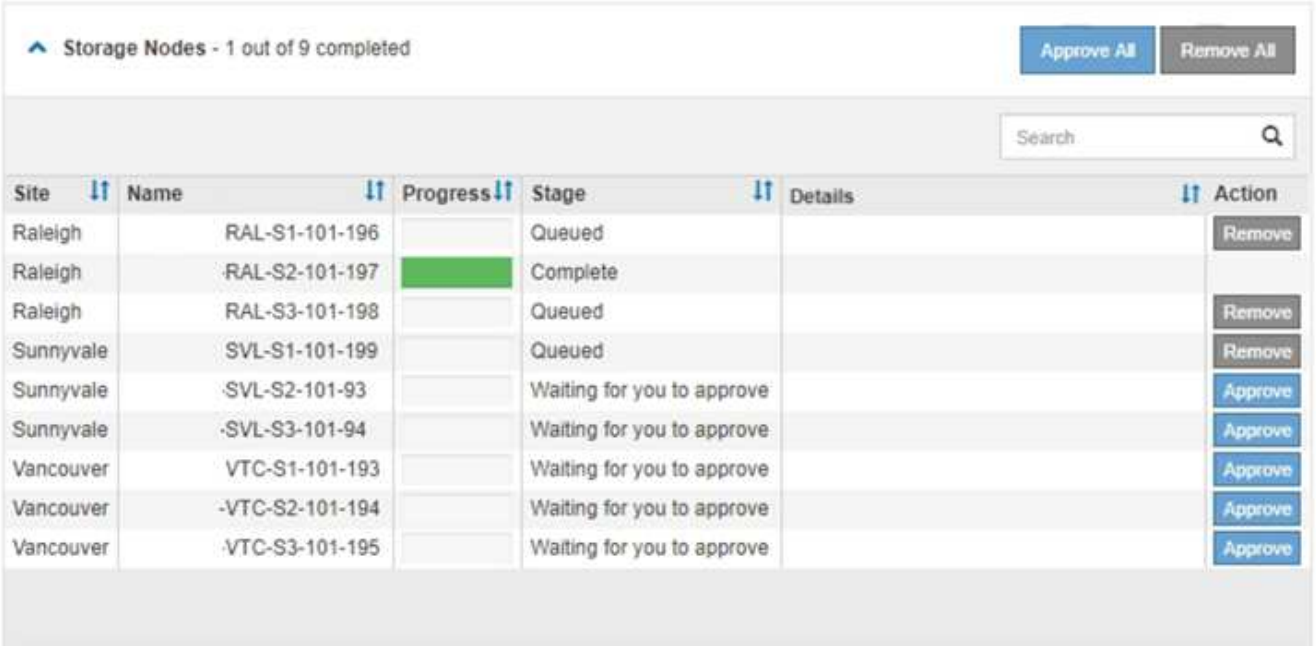
> Le bouton **approuver tout** en haut de la page approuve tous les nœuds répertoriés sur la page, tandis que le bouton **approuver tout** en haut d'un groupe de tables n'approuve que tous les nœuds de ce groupe. Si l'ordre dans lequel les nœuds sont mis à niveau est important, approuvez les nœuds ou les groupes de nœuds un par un et attendez que la mise à niveau soit terminée sur chaque nœud avant d'approuver le ou les nœuds suivants.

   - Sélectionnez le bouton de niveau supérieur **approuver tout** en haut de la page pour ajouter tous les nœuds de la grille à la file d'attente du correctif.

> Vous devez effectuer le correctif StorageGRID avant de lancer une autre mise à jour logicielle. Si vous ne parvenez pas à effectuer le correctif, contactez le support technique.

   - Sélectionnez **Remove** ou **Remove All** pour supprimer un noeud ou tous les noeuds de la file d'attente du correctif.

     Lorsque la scène dépasse « Queued », le bouton **Remove** est masqué et vous ne pouvez plus supprimer le nœud du processus de correctif.



10. Attendez que le correctif soit appliqué à chaque nœud de grille approuvé.

    Lorsque le correctif a été correctement installé sur tous les nœuds, le tableau de progression de l'installation du correctif se ferme. Une bannière verte indique la date et l'heure de fin du correctif.

11. Si le correctif n'a pu être appliqué à aucun nœud, vérifiez l'erreur pour chaque nœud, résolvez le problème et répétez ces étapes.

    La procédure n'est pas terminée tant que le correctif n'a pas été appliqué à tous les nœuds. Vous pouvez réessayer en toute sécurité le processus de correctif autant de fois que nécessaire jusqu'à ce qu'il soit terminé.

Procédures de restauration des nœuds de la grille

Procédures de restauration de nœud de grid : présentation

En cas de défaillance d'un nœud de grille, vous pouvez le restaurer en remplaçant le serveur physique ou virtuel défaillant, en réinstallant le logiciel StorageGRID et en restaurant les données récupérables.

Les nœuds du grid peuvent tomber en panne si une panne matérielle, de virtualisation, de système d'exploitation ou logicielle rend le nœud inutilisable ou peu fiable. Il existe de nombreux types de défaillance pouvant déclencher la restauration d'un nœud grid.

Les étapes de restauration d'un nœud de grid varient en fonction de la plateforme sur laquelle le nœud de grid est hébergé et du type de nœud de grid. Chaque type de nœud de la grille dispose d'une procédure de restauration spécifique, que vous devez suivre exactement.

En général, vous essayez de préserver les données du nœud de grille défaillant dans la mesure du possible, réparez ou remplacez le nœud défaillant, utilisez Grid Manager pour configurer le nœud de remplacement et restaurer les données du nœud.

En cas de défaillance de l'ensemble du site StorageGRID, contactez le support technique. Le support technique vous accompagne pour développer et mettre en œuvre un plan de reprise sur site qui optimise la quantité des données récupérées et répond aux objectifs de l'entreprise. Voir "Comment la reprise sur site est effectuée par le support technique".

Avertissements et considérations relatives à la restauration des nœuds de la grille

En cas de défaillance d'un nœud de la grille, vous devez le restaurer dès que possible. Avant de commencer, vous devez examiner tous les avertissements et considérations relatifs à la restauration du nœud.

StorageGRID est un système distribué composé de plusieurs nœuds qui travaillent les uns avec les autres. N'utilisez pas de snapshots de disque pour restaurer des nœuds de grille. Reportez-vous plutôt aux procédures de restauration et de maintenance pour chaque type de nœud.

Voici quelques-unes des raisons pour lesquelles une restauration d'un nœud de grid a échoué dès que possible :

- Un nœud de grille défaillant peut réduire la redondance des données système et objet, ce qui vous rend vulnérable au risque de perte permanente de données en cas de défaillance d'un autre nœud.
- En cas de défaillance d'un nœud de grid, vous pouvez avoir un impact sur l'efficacité des opérations quotidiennes.
- Un nœud de grid en panne peut vous permettre de surveiller les opérations système.
- Un nœud grid en panne peut entraîner une erreur de serveur interne 500 si des règles ILM strictes sont en place.
- Si un nœud de la grille n'est pas restauré rapidement, le temps de restauration peut augmenter. Par exemple, des files d'attente peuvent se développer et doivent être effacées avant la fin de la restauration.

Suivez toujours la procédure de restauration pour le type spécifique de nœud de grille que vous restaurez. Les procédures de restauration varient selon les nœuds d'administration principal ou non primaire, les nœuds de passerelle, les nœuds d'archivage, les nœuds d'appliance et les nœuds de stockage.

Conditions préalables à la récupération des nœuds de la grille

Les conditions suivantes sont réunies lors de la récupération des nœuds de la grille :

- Le matériel physique ou virtuel en panne a été remplacé et configuré.
- La version du programme d'installation de l'appliance StorageGRID installée sur l'appliance de remplacement correspond à la version logicielle de votre système StorageGRID, comme décrit à la section "Vérifiez et mettez à niveau la version du programme d'installation de l'appliance StorageGRID".
- Si vous récupérez un nœud de grille autre que le nœud d'administration principal, il existe une connectivité entre le nœud de grille en cours de restauration et le nœud d'administration principal.

Ordre de restauration de nœud en cas de défaillance d'un serveur hébergeant plusieurs nœuds de la grille

Si un serveur hébergeant plusieurs nœuds de la grille tombe en panne, vous pouvez récupérer les nœuds dans n'importe quel ordre. Toutefois, si le serveur en panne héberge le nœud d'administration principal, vous devez d'abord restaurer ce nœud. La récupération du nœud d'administration principal empêche les autres restaurations de nœud d'arrêter lorsqu'elles attendent de contacter le nœud d'administration principal.

Adresses IP des nœuds restaurés

N'essayez pas de restaurer un nœud à l'aide d'une adresse IP actuellement attribuée à un autre nœud. Lorsque vous déployez le nouveau nœud, utilisez l'adresse IP actuelle du nœud défaillant ou une adresse IP non utilisée.

Si vous utilisez une nouvelle adresse IP pour déployer le nouveau nœud puis restaurer le nœud, la nouvelle adresse IP continuera à être utilisée pour le nœud restauré. Si vous souhaitez revenir à l'adresse IP d'origine, utilisez l'outil Modifier l'adresse IP une fois la restauration terminée.

Collectez les ressources requises pour la restauration des nœuds du grid

Avant d'effectuer des procédures de maintenance, vous devez vous assurer que vous disposez des matériaux nécessaires pour récupérer un nœud de grille défaillant.

Élément	Remarques
Archive de l'installation de StorageGRID	Si vous devez restaurer un nœud grid, vous devez Téléchargez les fichiers d'installation de StorageGRID pour votre plate-forme. **Remarque :** vous n'avez pas besoin de télécharger des fichiers si vous récupérez des volumes de stockage défectueux sur un noeud de stockage.
L'ordinateur portable de service	L'ordinateur portable de service doit être équipé des éléments suivants : • Port réseau • Client SSH (par exemple, PuTTY) • "Navigateur Web pris en charge"
Package de restauration `.zip` fichier	Obtenir une copie du dernier progiciel de récupération `.zip` fichier : `sgws-recovery-package-`*`id-revision`*`.zip` Le contenu du `.zip` le fichier est mis à jour chaque fois que le système est modifié. Vous êtes invité à stocker la version la plus récente du progiciel de restauration dans un emplacement sécurisé après avoir effectué de telles modifications. Utilisez la copie la plus récente pour récupérer des données suite à des défaillances du grid. Si le nœud d'administration principal fonctionne normalement, vous pouvez télécharger le progiciel de restauration à partir de Grid Manager. Sélectionnez **MAINTENANCE** > **système** > **progiciel de récupération**. Si vous ne parvenez pas à accéder à Grid Manager, vous pouvez trouver des copies chiffrées du progiciel de récupération sur certains nœuds de stockage qui contiennent le service ADC. Sur chaque nœud de stockage, examinez cet emplacement pour le progiciel de restauration : `/var/local/install/sgws-recovery-package-`*`grid-id-revision`*`.zip.gpg` Utilisez le progiciel de restauration avec le numéro de révision le plus élevé.

Élément	Remarques
`Passwords.txt` fichier	Contient les mots de passe requis pour accéder aux nœuds de la grille sur la ligne de commande. Inclus dans le package de restauration.
Phrase secrète pour le provisionnement	La phrase de passe est créée et documentée lors de l'installation initiale du système StorageGRID. La phrase de passe de provisionnement n'est pas dans le `Passwords.txt` fichier.
Documentation actuelle pour votre plate-forme	Rendez-vous sur le site Web du fournisseur de la plate-forme pour obtenir de la documentation. Pour connaître les versions actuelles prises en charge de votre plate-forme, reportez-vous à la section "Matrice d'interopérabilité NetApp".

Téléchargez et extrayez les fichiers d'installation StorageGRID

Téléchargez le logiciel et extrayez les fichiers, sauf si vous l'êtes "Récupération des volumes de stockage défectueux sur un noeud de stockage".

Vous devez utiliser la version de StorageGRID en cours d'exécution sur la grille.

Étapes

1. Déterminez quelle version du logiciel est actuellement installée. Dans la partie supérieure du Gestionnaire de grille, sélectionnez l'icône d'aide et sélectionnez **About**.
2. Accédez au "Page de téléchargements NetApp pour StorageGRID".
3. Sélectionnez la version de StorageGRID en cours d'exécution sur la grille.

   Les versions du logiciel StorageGRID ont le format suivant : `11.x.y`.
4. Connectez-vous avec le nom d'utilisateur et le mot de passe de votre compte NetApp.
5. Lisez le contrat de licence de l'utilisateur final, cochez la case, puis sélectionnez **accepter et continuer**.
6. Dans la colonne **installer StorageGRID** de la page de téléchargement, sélectionnez `.tgz` ou `.zip` fichier pour votre plate-forme.

   La version affichée dans le fichier d'archive d'installation doit correspondre à la version du logiciel actuellement installé.

   Utilisez le `.zip` Fichier si vous exécutez Windows.

Plateforme	Archive d'installation

Red Hat Enterprise Linux ou CentOS	`StorageGRID-Webscale-`*`version`*`-RPM-`*`uniqueID`*`.zip`
	
	`StorageGRID-Webscale-`*`version`*`-RPM-`*`uniqueID`*`.tgz`

Plateforme	Archive d'installation

Ubuntu ou Debian ou Appliances	`StorageGRID-Webscale-version-DEB-uniqueID.zip`
	
	`StorageGRID-Webscale-version-DEB-uniqueID.tgz`

VMware	`StorageGRID-Webscale-version-VMware-uniqueID.zip`
	
	`StorageGRID-Webscale-version-VMware-uniqueID.tgz`

7. Téléchargez et extrayez le fichier d'archive.
8. Suivez l'étape appropriée pour votre plate-forme afin de choisir les fichiers dont vous avez besoin, en fonction de votre plate-forme et des nœuds de grille que vous devez récupérer.

   Les chemins répertoriés dans l'étape pour chaque plate-forme sont relatifs au répertoire de niveau supérieur installé par le fichier d'archive.

9. Si vous récupérez un "Système Red Hat Enterprise Linux ou CentOS", sélectionnez les fichiers appropriés.

Chemin d'accès et nom de fichier	Description
	Fichier texte qui décrit tous les fichiers contenus dans le fichier de téléchargement StorageGRID.
	Licence gratuite qui ne fournit aucun droit d'assistance pour le produit.
	Package RPM pour l'installation des images des nœuds StorageGRID sur vos hôtes RHEL ou CentOS.
	Package RPM pour l'installation du service hôte StorageGRID sur vos hôtes RHEL ou CentOS.
Outil de script de déploiement	Description
	Script Python utilisé pour automatiser la configuration d'un système StorageGRID.
	Script Python utilisé pour automatiser la configuration des appliances StorageGRID.
	Exemple de fichier de configuration à utiliser avec `configure-storagegrid.py` script.

Chemin d'accès et nom de fichier	Description
	Exemple de script Python que vous pouvez utiliser pour vous connecter à l'API Grid Management lorsque l'authentification unique est activée. Vous pouvez également utiliser ce script pour le Federate Ping.
	Un fichier de configuration vierge à utiliser avec le `configure-storagegrid.py` script.
	Exemple de rôle et de manuel de vente Ansible pour la configuration des hôtes RHEL ou CentOS pour le déploiement de conteneurs StorageGRID. Vous pouvez personnaliser le rôle ou le PlayBook selon vos besoins.
	Exemple de script Python que vous pouvez utiliser pour vous connecter à l'API de gestion de grille lorsque l'authentification unique (SSO) est activée à l'aide d'Active Directory ou de Ping Federate.
	Script d'aide appelé par le compagnon `storagegrid-ssoauth-azure.py` Script Python pour effectuer des interactions SSO avec Azure.
	Schémas API pour StorageGRID. **Remarque** : avant d'effectuer une mise à niveau, vous pouvez utiliser ces schémas pour confirmer que tout code que vous avez écrit pour utiliser les API de gestion StorageGRID sera compatible avec la nouvelle version de StorageGRID si vous ne disposez pas d'un environnement StorageGRID non productif pour le test de compatibilité de mise à niveau.

1. Si vous récupérez un "Système Ubuntu ou Debian", sélectionnez les fichiers appropriés.

Chemin d'accès et nom de fichier	Description
	Fichier texte qui décrit tous les fichiers contenus dans le fichier de téléchargement StorageGRID.
	Un fichier de licence NetApp hors production que vous pouvez utiliser pour tester et réaliser des démonstrations de faisabilité.
	DEB paquet pour installer les images de noeud StorageGRID sur des hôtes Ubuntu ou Debian.

Chemin d'accès et nom de fichier	Description
	Somme de contrôle MD5 pour le fichier `/debs/storagegrid-webscale-images-version-SHA.deb`.
	Paquet DEB pour l'installation du service hôte StorageGRID sur des hôtes Ubuntu ou Debian.
Outil de script de déploiement	Description
	Script Python utilisé pour automatiser la configuration d'un système StorageGRID.
	Script Python utilisé pour automatiser la configuration des appliances StorageGRID.
	Exemple de script Python que vous pouvez utiliser pour vous connecter à l'API Grid Management lorsque l'authentification unique est activée. Vous pouvez également utiliser ce script pour le Federate Ping.
	Exemple de fichier de configuration à utiliser avec `configure-storagegrid.py` script.
	Un fichier de configuration vierge à utiliser avec le `configure-storagegrid.py` script.
	Exemple de rôle et de manuel de vente Ansible pour la configuration des hôtes Ubuntu ou Debian pour le déploiement de conteneurs StorageGRID. Vous pouvez personnaliser le rôle ou le PlayBook selon vos besoins.
	Exemple de script Python que vous pouvez utiliser pour vous connecter à l'API de gestion de grille lorsque l'authentification unique (SSO) est activée à l'aide d'Active Directory ou de Ping Federate.
	Script d'aide appelé par le compagnon `storagegrid-ssoauth-azure.py` Script Python pour effectuer des interactions SSO avec Azure.

Chemin d'accès et nom de fichier	Description
	Schémas API pour StorageGRID. **Remarque** : avant d'effectuer une mise à niveau, vous pouvez utiliser ces schémas pour confirmer que tout code que vous avez écrit pour utiliser les API de gestion StorageGRID sera compatible avec la nouvelle version de StorageGRID si vous ne disposez pas d'un environnement StorageGRID non productif pour le test de compatibilité de mise à niveau.

1. Si vous récupérez un "Système VMware", sélectionnez les fichiers appropriés.

Chemin d'accès et nom de fichier	Description
	Fichier texte qui décrit tous les fichiers contenus dans le fichier de téléchargement StorageGRID.
	Licence gratuite qui ne fournit aucun droit d'assistance pour le produit.
	Fichier de disque de machine virtuelle utilisé comme modèle pour créer des machines virtuelles de nœud de grille.
	Fichier modèle du format Open Virtualization (`.ovf`) et fichier manifeste (`.mf`) Pour le déploiement du nœud d'administration principal.
	Le fichier de modèle (`.ovf`) et fichier manifeste (`.mf`) Pour le déploiement de nœuds d'administration non primaires.
	Le fichier de modèle (`.ovf`) et fichier manifeste (`.mf`) Pour le déploiement des nœuds d'archivage.
	Le fichier de modèle (`.ovf`) et fichier manifeste (`.mf`) Pour le déploiement des nœuds de passerelle.
	Le fichier de modèle (`.ovf`) et fichier manifeste (`.mf`) Pour le déploiement de nœuds de stockage basés sur des machines virtuelles.
Outil de script de déploiement	Description
	Script de shell de Bash utilisé pour automatiser le déploiement de nœuds de grille virtuels.

Chemin d'accès et nom de fichier	Description
	Exemple de fichier de configuration à utiliser avec `deploy-vsphere-ovftool.sh` script.
	Script Python utilisé pour automatiser la configuration d'un système StorageGRID.
	Script Python utilisé pour automatiser la configuration des appliances StorageGRID.
	Exemple de script Python que vous pouvez utiliser pour vous connecter à l'API de gestion de grille lorsque l'authentification unique (SSO) est activée. Vous pouvez également utiliser ce script pour le Federate Ping.
	Exemple de fichier de configuration à utiliser avec `configure-storagegrid.py` script.
	Un fichier de configuration vierge à utiliser avec le `configure-storagegrid.py` script.
	Exemple de script Python que vous pouvez utiliser pour vous connecter à l'API de gestion de grille lorsque l'authentification unique (SSO) est activée à l'aide d'Active Directory ou de Ping Federate.
	Script d'aide appelé par le compagnon `storagegrid-ssoauth-azure.py` Script Python pour effectuer des interactions SSO avec Azure.
	Schémas API pour StorageGRID. **Remarque** : avant d'effectuer une mise à niveau, vous pouvez utiliser ces schémas pour confirmer que tout code que vous avez écrit pour utiliser les API de gestion StorageGRID sera compatible avec la nouvelle version de StorageGRID si vous ne disposez pas d'un environnement StorageGRID non productif pour le test de compatibilité de mise à niveau.

1. Si vous récupérez un système basé sur l'appliance StorageGRID, sélectionnez les fichiers appropriés.

Chemin d'accès et nom de fichier	Description
	DEB package pour l'installation des images de noeud StorageGRID sur vos appareils.

Chemin d'accès et nom de fichier	Description
	Somme de contrôle MD5 pour le fichier `/debs/storagegridwebscale-images-version-SHA.deb`.

> Pour l'installation de l'appliance, ces fichiers ne sont nécessaires que si vous devez éviter le trafic réseau. L'appliance peut télécharger les fichiers requis à partir du nœud d'administration principal.

Sélectionnez la procédure de restauration du noeud

Vous devez sélectionner la procédure de restauration correcte pour le type de nœud qui a échoué.

Nœud de grille	Procédure de reprise
Plusieurs nœuds de stockage	Contactez l'assistance technique. Si plusieurs nœuds de stockage sont en panne, le support technique doit vous aider à effectuer la restauration afin d'éviter les incohérences de base de données pouvant entraîner la perte de données. Une procédure de restauration sur site peut être requise. "Comment la reprise sur site est effectuée par le support technique"
Un seul nœud de stockage	La procédure de restauration du nœud de stockage dépend du type et de la durée de l'échec. "Restaurez les données après une panne de nœud de stockage"
Nœud d'administration	La procédure nœud d'administration varie selon que vous devez restaurer le nœud d'administration principal ou un nœud d'administration non primaire. "Restaurez vos données après une panne de nœud d'administration"
Nœud de passerelle	"Restaurez les données à partir d'une défaillance de nœud de passerelle".
Nœud d'archivage	"Échec de la restauration à partir du nœud d'archivage".

> Si un serveur hébergeant plusieurs nœuds de la grille tombe en panne, vous pouvez récupérer les nœuds dans n'importe quel ordre. Toutefois, si le serveur en panne héberge le nœud d'administration principal, vous devez d'abord restaurer ce nœud. La récupération du nœud d'administration principal empêche les autres restaurations de nœud d'arrêter lorsqu'elles attendent de contacter le nœud d'administration principal.

Restaurez les données après une panne de nœud de stockage

Restauration après une panne de nœud de stockage : présentation

La procédure de récupération d'un noeud de stockage défaillant dépend du type de panne et du type de noeud de stockage qui a échoué.

Utilisez ce tableau pour sélectionner la procédure de restauration d'un noeud de stockage défaillant.

Problème	Action	Remarques
• Plusieurs nœuds de stockage ont échoué. • Un second nœud de stockage a échoué moins de 15 jours après une défaillance ou une restauration d'un nœud de stockage. Cela inclut le cas où un nœud de stockage tombe en panne pendant la restauration d'un autre nœud de stockage.	Contactez l'assistance technique.	La récupération de plusieurs nœuds de stockage (ou de plusieurs nœuds de stockage dans un délai de 15 jours) peut affecter l'intégrité de la base de données Cassandra, ce qui peut entraîner la perte de données. Le support technique peut déterminer quand il est possible de commencer la restauration d'un second nœud de stockage. **Remarque** : si plusieurs nœuds de stockage contenant le service ADC échouent sur un site, vous perdez toute demande de service de plate-forme en attente pour ce site.
Plusieurs nœuds de stockage sur un site ont échoué ou l'ensemble d'un site a échoué.	Contactez l'assistance technique. Il peut être nécessaire d'effectuer une procédure de reprise sur site.	L'assistance technique évaluera votre situation et élaborera un plan de reprise. Voir "Comment la reprise sur site est effectuée par le support technique".
Un nœud de stockage a été hors ligne pendant plus de 15 jours.	"Panne d'un nœud de stockage de plus de 15 jours"	Cette procédure est nécessaire pour assurer l'intégrité de la base de données Cassandra.
Un nœud de stockage de l'appliance est défectueux.	"Restaurez le nœud de stockage de l'appliance"	La procédure de restauration des nœuds de stockage de l'appliance est la même pour toutes les défaillances.
Un ou plusieurs volumes de stockage sont en panne, mais le lecteur système est intact	"Restaurez le disque d'après la panne du volume de stockage là où le disque du système est intact"	Cette procédure est utilisée pour les nœuds de stockage basés sur logiciel.

Problème	Action	Remarques
Le lecteur système est défectueux.	"Restaurez les données après une panne de disque système"	La procédure de remplacement des nœuds dépend de la plateforme de déploiement et indique si des volumes de stockage sont également défectueux.

Certaines procédures de restauration StorageGRID utilisent Reaper pour traiter les réparations Cassandra. Les réparations sont effectuées automatiquement dès que les services connexes ou requis ont commencé. Vous remarquerez peut-être des résultats de script mentionnant « couche » ou « réparation Cassandra ». Si un message d'erreur indiquant que la réparation a échoué, exécutez la commande indiquée dans le message d'erreur.

Panne d'un nœud de stockage de plus de 15 jours

Si un seul nœud de stockage a été hors ligne et n'est pas connecté aux autres nœuds de stockage depuis plus de 15 jours, vous devez reconstruire Cassandra sur le nœud.

Avant de commencer

- Vous avez vérifié qu'une mise hors service du nœud de stockage n'est pas en cours ou que vous avez interrompu la procédure de mise hors service du nœud. (Dans le Gestionnaire de grille, sélectionnez **MAINTENANCE** > **tâches** > **désaffectation**.)
- Vous avez vérifié qu'une extension n'est pas en cours. (Dans le Gestionnaire de grille, sélectionnez **MAINTENANCE** > **tâches** > **expansion**.)

Description de la tâche

Les nœuds de stockage disposent d'une base de données Cassandra qui inclut les métadonnées d'objet. Si un nœud de stockage n'a pas pu communiquer avec d'autres nœuds de stockage depuis plus de 15 jours, StorageGRID suppose que la base de données Cassandra du nœud est obsolète. Le nœud de stockage ne peut pas rejoindre la grille tant que Cassandra n'a pas été reconstruite à l'aide d'informations provenant d'autres nœuds de stockage.

Utilisez cette procédure pour reconstruire Cassandra uniquement si un seul nœud de stockage est défaillant. Contactez le support technique si des nœuds de stockage supplémentaires sont hors ligne ou si Cassandra a été reconstruite sur un autre nœud de stockage au cours des 15 derniers jours. Par exemple, Cassandra a peut-être été reconstruite dans le cadre des procédures de restauration des volumes de stockage défaillants ou de restauration d'un nœud de stockage défaillant.

Si plusieurs nœuds de stockage ont échoué (ou sont hors ligne), contactez le support technique. N'effectuez pas la procédure de récupération suivante. Des données peuvent être perdues.

S'il s'agit de la défaillance du deuxième nœud de stockage dans les 15 jours qui suivent la défaillance ou la restauration d'un nœud de stockage, contactez le support technique. N'effectuez pas la procédure de récupération suivante. Des données peuvent être perdues.

Si plusieurs nœuds de stockage d'un site ont échoué, une procédure de restauration de site peut être nécessaire. Voir "Comment la reprise sur site est effectuée par le support technique".

Étapes

1. Si nécessaire, mettez le nœud de stockage sous tension qui doit être restauré.
2. Connectez-vous au nœud grid :
   a. Saisissez la commande suivante : `ssh admin@grid_node_IP`
   b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
   c. Entrez la commande suivante pour passer à la racine : `su -`
   d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

   Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.+

   > Si vous ne parvenez pas à vous connecter au nœud de la grille, il est possible que le disque système ne soit pas intact. Passer à la procédure pour "restauration en cas de panne du lecteur système".

3. Effectuez les vérifications suivantes sur le nœud de stockage :
   a. Exécutez cette commande : `nodetool status`

   La sortie doit être de `Connection refused`

   b. Dans le Gestionnaire de grille, sélectionnez **SUPPORT** > **Outils** > **topologie de grille**.
   c. Sélectionnez ***site*** > **nœud de stockage** > **SSM** > **Services**. Vérifiez que le service Cassandra s'affiche `Not Running`.
   d. Sélectionnez **nœud de stockage** > **SSM** > **Ressources**. Vérifiez qu'il n'y a pas d'état d'erreur dans la section volumes.
   e. Exécutez cette commande : `grep -i Cassandra /var/local/log/servermanager.log`

   Le message suivant doit s'afficher dans la sortie :

```
Cassandra not started because it has been offline for more than 15 day
grace period - rebuild Cassandra
```

4. Exécutez cette commande et surveillez la sortie du script : `check-cassandra-rebuild`
   - Si le service Cassandra, selon le volume 0, est en cours d'exécution, vous serez invité à l'arrêter. Saisissez : **y**

     > Si le service Cassandra est déjà arrêté, vous n'êtes pas invité à le faire. Le service Cassandra est arrêté uniquement pour le volume 0.

   - Vérifiez les avertissements dans le script. Si aucune d'entre elles ne s'applique, confirmez que vous souhaitez reconstruire Cassandra. Saisissez : **y**

Certaines procédures de restauration StorageGRID utilisent Reaper pour traiter les réparations Cassandra. Les réparations sont effectuées automatiquement dès que les services connexes ou requis ont commencé. Vous remarquerez peut-être des résultats de script mentionnant « couche » ou « réparation Cassandra ». Si un message d'erreur indiquant que la réparation a échoué, exécutez la commande indiquée dans le message d'erreur.

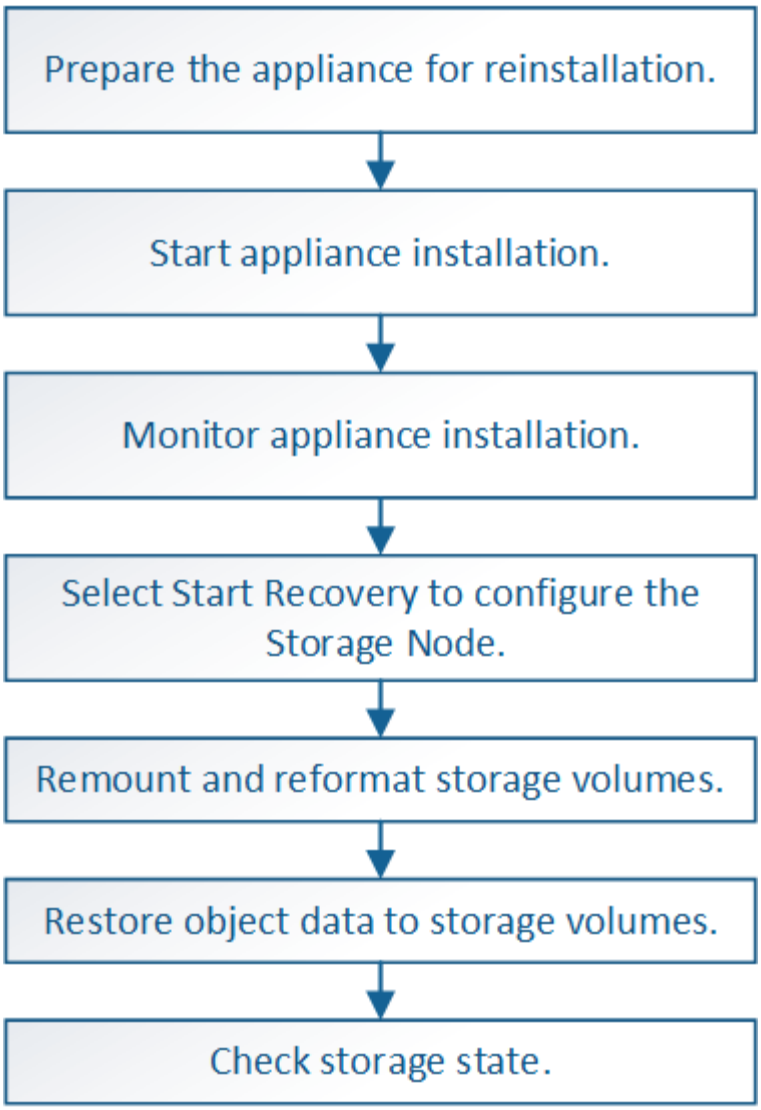
5. Une fois la reconstruction terminée, effectuez les vérifications suivantes :
   a. Dans le Gestionnaire de grille, sélectionnez **SUPPORT** > **Outils** > **topologie de grille**.
   b. Sélectionnez ***site*** > **nœud de stockage récupéré** > **SSM** > **Services**.
   c. Vérifiez que tous les services sont en cours d'exécution.
   d. Sélectionnez **DDS** > **Data Store**.
   e. Confirmez que l'état **Data Store** est « Up » (mise en service) et l'état **Data Store State** est « Normal » (État de stockage de données*).

Restaurez le nœud de stockage de l'appliance

Restaurer le nœud de stockage de l'appliance : workflow

La procédure de restauration d'un nœud de stockage de l'appliance StorageGRID défaillant est identique, que vous soyez en train de récupérer à partir de la perte du disque système ou de la perte de volumes de stockage uniquement.

Comme indiqué dans le schéma de workflow, vous devez préparer l'appliance et réinstaller le logiciel, configurer le nœud pour qu'il rejoigne la grille, reformater le stockage et restaurer les données d'objet.



Mises en garde et remarques concernant la restauration des nœuds de stockage de l'appliance

Si plusieurs nœuds de stockage ont échoué (ou sont hors ligne), contactez le support technique. N'effectuez pas la procédure de récupération suivante. Des données peuvent être perdues.

S'il s'agit de la défaillance du deuxième nœud de stockage dans les 15 jours qui suivent la défaillance ou la restauration d'un nœud de stockage, contactez le support technique. Reconstruire Cassandra sur deux nœuds de stockage ou plus en un délai de 15 jours peut entraîner une perte de données.

Si plusieurs nœuds de stockage d'un site ont échoué, une procédure de restauration de site peut être nécessaire. Voir "Comment la reprise sur site est effectuée par le support technique".

Si les règles ILM sont configurées pour ne stocker qu'une seule copie répliquée, et si cette copie existe sur un volume de stockage défaillant, vous ne pourrez pas restaurer l'objet.

Si vous rencontrez une alarme Services: Status - Cassandra (SVST) pendant la récupération, reportez-vous à la section "Restaurez des volumes de stockage défaillants et reconstruisez la base de données Cassandra". Après la reconstruction de Cassandra, les alarmes doivent être désactivées. Si les alarmes ne s'effacent pas, contactez le support technique.

Pour connaître les procédures de maintenance du matériel, telles que les instructions de remplacement d'un contrôleur ou de réinstallation de SANtricity OS, reportez-vous aux instructions de maintenance de votre dispositif de stockage.

- "Appliances de stockage SGF6112"
- "Dispositifs de stockage SG6000"
- "Appliances de stockage SG5700"

Préparez le nœud de stockage de l'appliance pour la réinstallation

Lors de la restauration d'un nœud de stockage d'appliance, vous devez d'abord préparer l'appliance pour la réinstallation du logiciel StorageGRID.

Étapes

1. Connectez-vous au noeud de stockage défaillant :

   a. Saisissez la commande suivante : `ssh admin@grid_node_IP`

   b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

   c. Entrez la commande suivante pour passer à la racine : `su -`

   d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

   Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

2. Préparez le nœud de stockage de l'appliance pour l'installation du logiciel StorageGRID. `sgareinstall`

3. Lorsque vous êtes invité à continuer, entrez : `y`

   L'appliance redémarre et votre session SSH se termine. La disponibilité du programme d'installation de l'appliance StorageGRID prend généralement 5 minutes environ, même si dans certains cas, vous devrez attendre jusqu'à 30 minutes.

   N'essayez pas d'accélérer le redémarrage en mettant l'appareil hors tension ou en le réinitialisant autrement. Vous pouvez interrompre les mises à niveau automatiques du BIOS, du contrôleur BMC ou d'autres micrologiciels.

   Le nœud de stockage de l'appliance StorageGRID est réinitialisé et les données du nœud de stockage ne sont plus accessibles. Les adresses IP configurées pendant le processus d'installation d'origine doivent rester intactes ; cependant, il est recommandé de confirmer cette opération une fois la procédure terminée.

   Après avoir exécuté le `sgareinstall` Commande : tous les comptes provisionnés par StorageGRID, mots de passe et clés SSH sont supprimés, puis de nouvelles clés hôte sont générées.

Démarrez l'installation de l'appliance StorageGRID

Pour installer StorageGRID sur un nœud de stockage de l'appliance, utilisez le programme d'installation de l'appliance StorageGRID, qui est inclus sur l'appliance.

Avant de commencer

- L'appliance a été installée dans un rack, connectée à vos réseaux et sous tension.
- Les liens réseau et les adresses IP ont été configurés pour l'appliance à l'aide du programme d'installation de l'appliance StorageGRID.
- Vous connaissez l'adresse IP du nœud d'administration principal de la grille de StorageGRID.
- Tous les sous-réseaux de réseau Grid répertoriés sur la page de configuration IP du programme d'installation de l'appliance StorageGRID ont été définis dans la liste de sous-réseaux de réseau de grille sur le nœud d'administration principal.
- Vous avez terminé ces tâches préalables en suivant les instructions d'installation de votre appliance de stockage. Voir "Démarrage rapide pour l'installation du matériel".
- Vous utilisez un "navigateur web pris en charge".
- Vous connaissez l'une des adresses IP attribuées au contrôleur de calcul dans l'appliance. Vous pouvez utiliser l'adresse IP du réseau d'administration (port de gestion 1 sur le contrôleur), du réseau Grid ou du réseau client.

Description de la tâche

Pour installer StorageGRID sur un nœud de stockage d'appliance :

- Vous spécifiez ou confirmez l'adresse IP du nœud d'administration principal et le nom d'hôte (nom du système) du nœud.
- Vous démarrez l'installation et attendez que les volumes soient configurés et que le logiciel soit installé.
- Partway tout au long du processus, l'installation se met en pause. Pour reprendre l'installation, vous devez vous connecter à Grid Manager et configurer le nœud de stockage en attente en remplacement du nœud défaillant.
- Une fois le nœud configuré, le processus d'installation de l'appliance est terminé et l'appliance est redémarrée.

Étapes

1. Ouvrez un navigateur et entrez l'une des adresses IP du contrôleur de calcul de l'appliance.

   `https://Controller_IP:8443`

   La page d'accueil du programme d'installation de l'appliance StorageGRID s'affiche.

2. Dans la section connexion au noeud d'administration principal, déterminez si vous devez spécifier l'adresse IP du noeud d'administration principal.

   Le programme d'installation de l'appliance StorageGRID peut détecter automatiquement cette adresse IP, en supposant que le nœud d'administration principal, ou au moins un autre nœud de grille avec ADMIN_IP configuré, soit présent sur le même sous-réseau.

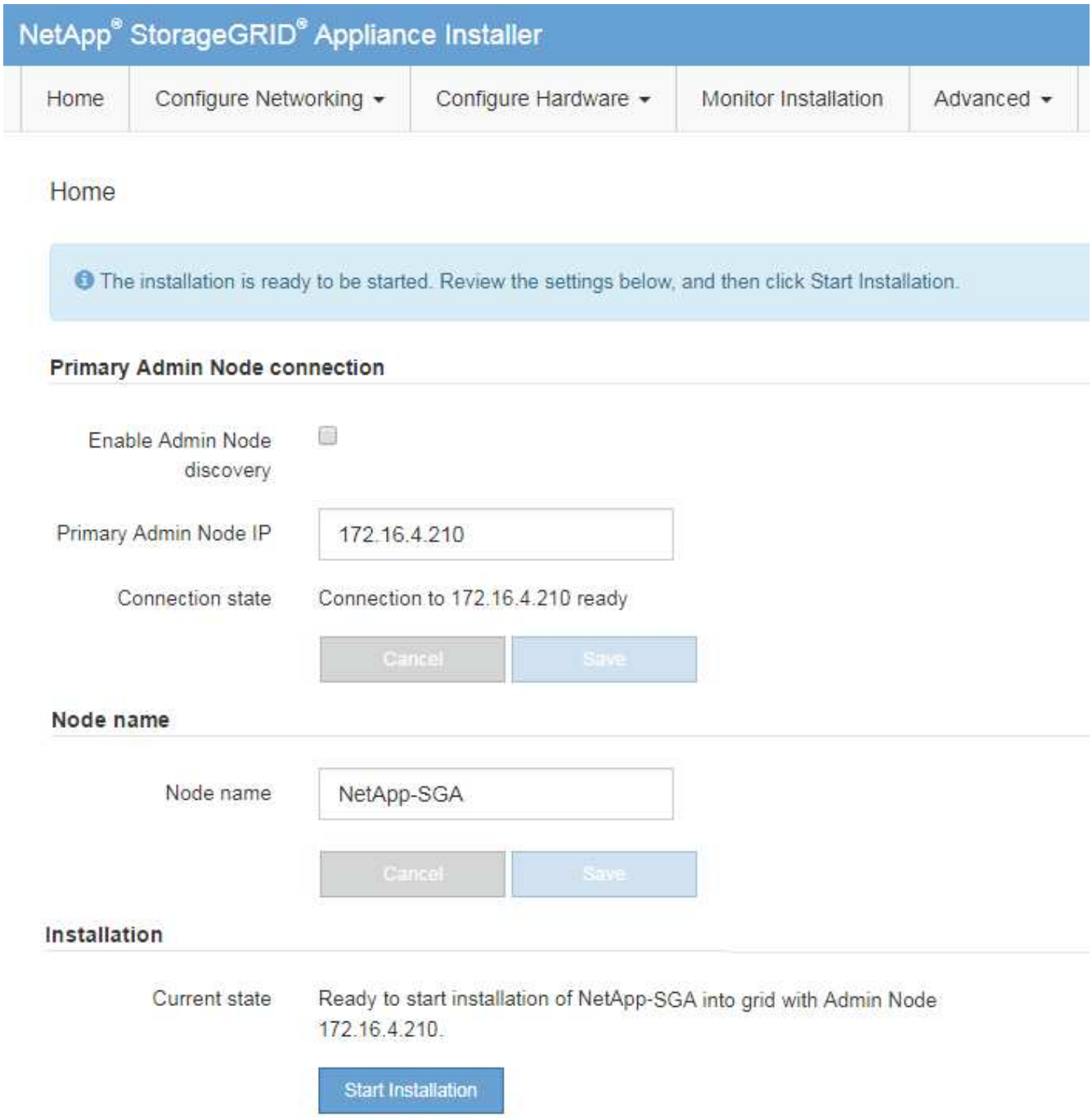
3. Si cette adresse IP n'apparaît pas ou si vous devez la modifier, spécifiez l'adresse :

Option	Étapes
Entrée IP manuelle	a. Décochez la case **Activer la découverte du noeud d'administration**. b. Saisissez l'adresse IP manuellement. c. Cliquez sur **Enregistrer**. d. Attendez que l'état de connexion de la nouvelle adresse IP devienne « prêt ».
Détection automatique de tous les nœuds d'administration principaux connectés	a. Cochez la case **Activer la découverte du noeud d'administration**. b. Dans la liste des adresses IP découvertes, sélectionnez le nœud d'administration principal de la grille sur lequel ce nœud de stockage de l'appliance sera déployé. c. Cliquez sur **Enregistrer**. d. Attendez que l'état de connexion de la nouvelle adresse IP devienne « prêt ».

4. Dans le champ **Node Name**, entrez le même nom d'hôte (nom du système) que celui utilisé pour le nœud que vous êtes en train de récupérer, puis cliquez sur **Save**.
5. Dans la section installation, vérifiez que l'état actuel est « prêt à démarrer l'installation de `node name` Dans la grille avec le noeud Admin principal `*admin_ip*`"` et que le bouton **Start installation** est activé.

   Si le bouton **Start installation** n'est pas activé, vous devrez peut-être modifier la configuration réseau ou les paramètres de port. Pour obtenir des instructions, reportez-vous aux instructions d'entretien de votre appareil.

6. Dans la page d'accueil du programme d'installation de l'appliance StorageGRID, cliquez sur **Démarrer l'installation**.



L'état actuel passe à « installation en cours » et la page installation du moniteur s'affiche.

> Si vous devez accéder manuellement à la page installation du moniteur, cliquez sur **installation du moniteur** dans la barre de menus. Voir "Surveiller l'installation de l'appareil".

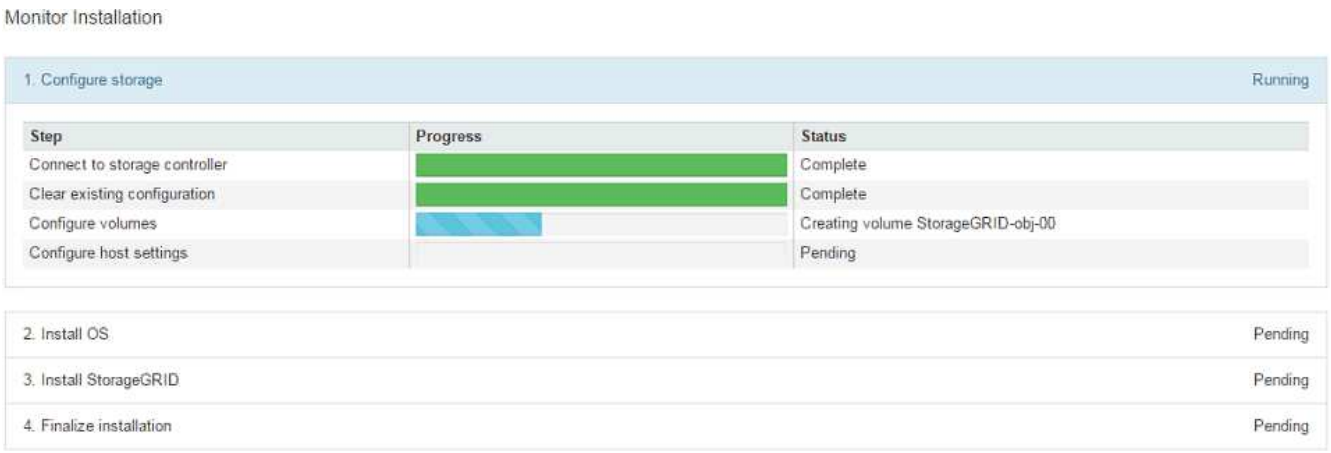
Surveillez l'installation de l'appliance StorageGRID

Le programme d'installation de l'appliance StorageGRID indique l'état jusqu'à ce que l'installation soit terminée. Une fois l'installation du logiciel terminée, l'appliance est redémarrée.

Étapes

1. Pour contrôler la progression de l'installation, cliquez sur **Monitor installation** dans la barre de menus.

   La page installation du moniteur affiche la progression de l'installation.



   La barre d'état bleue indique la tâche en cours. Les barres d'état vertes indiquent que les tâches ont été effectuées avec succès.

   > Le programme d'installation s'assure que les tâches terminées lors d'une installation précédente ne sont pas réexécutées. Si vous exécutez à nouveau une installation, toutes les tâches qui n'ont pas besoin d'être réexécutées s'affichent avec une barre d'état verte et un état de « `barrét' ».

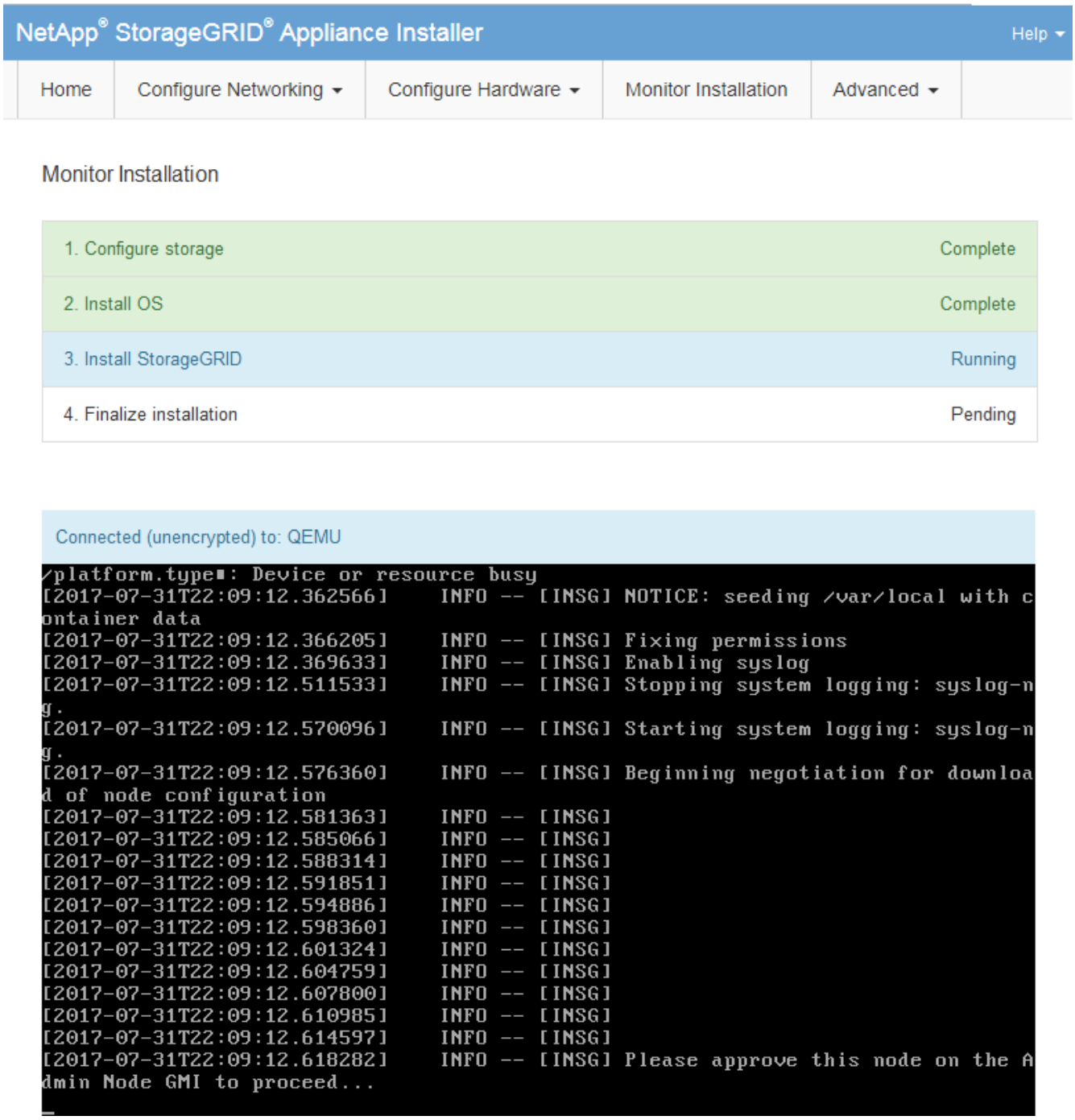
2. Passez en revue l'état d'avancement des deux premières étapes d'installation.
   - **1. Configurer le stockage**

     Au cours de cette étape, le programme d'installation se connecte au contrôleur de stockage, efface toute configuration existante, communique avec SANtricity OS pour configurer des volumes et configure les paramètres de l'hôte.

   - **2. Installez OS**

     Au cours de cette étape, le programme d'installation copie l'image du système d'exploitation de base pour StorageGRID sur l'appliance.

3. Continuez à surveiller la progression de l'installation jusqu'à ce que l'étape **installer StorageGRID** s'arrête et un message s'affiche sur la console intégrée vous invitant à approuver ce nœud sur le nœud d'administration à l'aide du gestionnaire de grille.



4. Accédez à "Sélectionnez Démarrer la restauration pour configurer le nœud de stockage de l'appliance".

Sélectionnez Démarrer la restauration pour configurer le nœud de stockage de l'appliance

Vous devez sélectionner Démarrer la restauration dans Grid Manager pour configurer un noeud de stockage d'appliance en remplacement du noeud défaillant.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous disposez de l'autorisation Maintenance ou accès racine.
- Vous avez la phrase secrète pour le provisionnement.

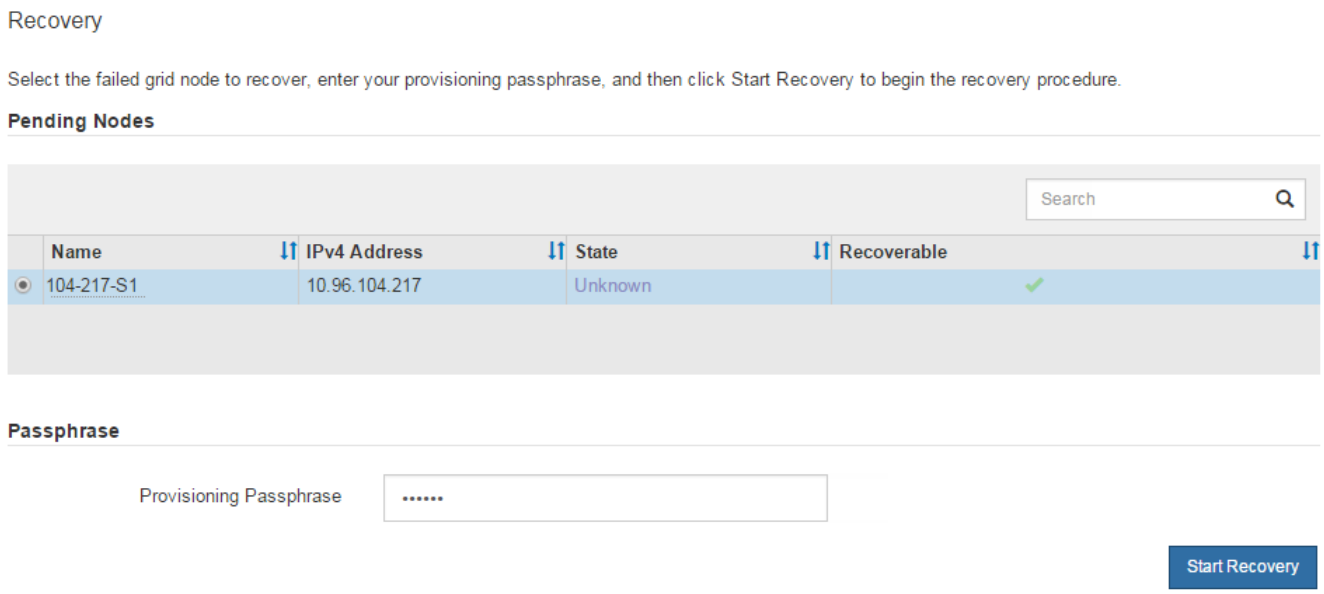
- Vous avez déployé un nœud de stockage d'appliance de restauration.
- Vous disposez de la date de début des travaux de réparation pour les données avec code d'effacement.
- Vous avez vérifié que le nœud de stockage n'a pas été reconstruit au cours des 15 derniers jours.

Étapes

1. Dans le Gestionnaire de grille, sélectionnez **MAINTENANCE** > **tâches** > **récupération**.
2. Sélectionnez le nœud de grille à récupérer dans la liste nœuds en attente.

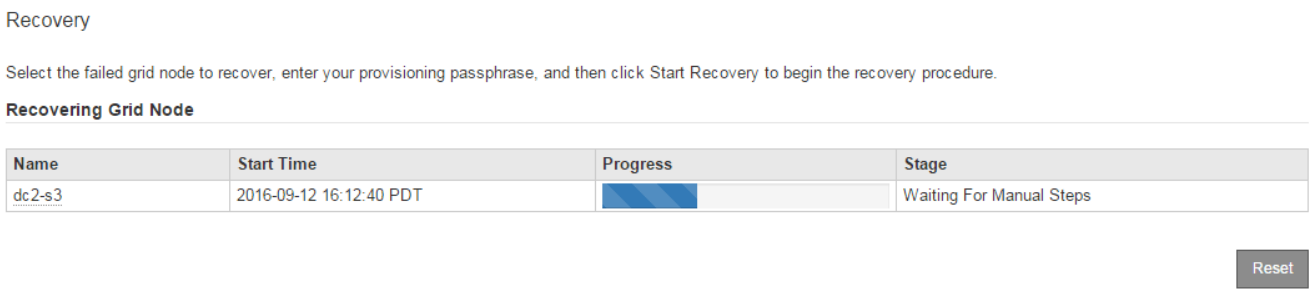
   Les nœuds apparaissent dans la liste après leur échec, mais vous ne pouvez pas sélectionner un nœud tant qu'il n'a pas été réinstallé et qu'il est prêt pour la restauration.

3. Saisissez la phrase de passe de provisionnement *.
4. Cliquez sur **Démarrer la récupération**.

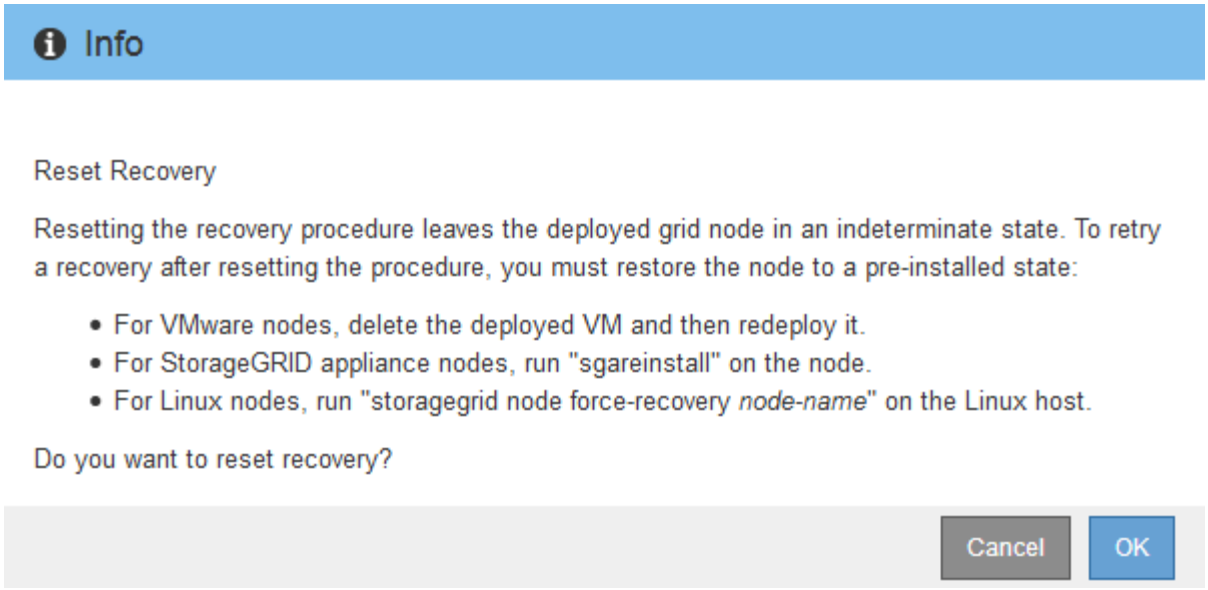


5. Surveiller la progression de la récupération dans le tableau de noeuds de grille de récupération.

   Lorsque le nœud de la grille atteint l'étape « attente des étapes manuelles », passez à la rubrique suivante et effectuez les étapes manuelles pour remonter et reformater les volumes de stockage de l'appliance.



> À tout moment pendant la récupération, vous pouvez cliquer sur **Réinitialiser** pour démarrer une nouvelle restauration. Une boîte de dialogue s'affiche, indiquant que le nœud restera dans un état indéterminé si vous réinitialisez la procédure.



Si vous souhaitez recommencer la restauration après avoir réinitialisé la procédure, vous devez restaurer l'état pré-installé du nœud d'appliance en cours d'exécution `sgareinstall` sur le nœud.

Remontage et reformatage des volumes de stockage de l'appliance (étapes manuelles)

Vous devez exécuter manuellement deux scripts pour remonter les volumes de stockage conservés et reformater les volumes de stockage défaillants. Le premier script monte les volumes au format approprié en tant que volumes de stockage StorageGRID. Le deuxième script reformate tous les volumes démontés, reconstruit la base de données Cassandra si nécessaire et démarre les services.

Avant de commencer

- Vous avez déjà remplacé le matériel de tous les volumes de stockage défectueux que vous savez avoir besoin d'être remplacé.

  Exécution du `sn-remount-volumes` un script peut vous aider à identifier d'autres volumes de stockage ayant échoué.

- Vous avez vérifié qu'une mise hors service du nœud de stockage n'est pas en cours ou que vous avez interrompu la procédure de mise hors service du nœud. (Dans le Gestionnaire de grille, sélectionnez **MAINTENANCE** > **tâches** > **désaffectation**.)
- Vous avez vérifié qu'une extension n'est pas en cours. (Dans le Gestionnaire de grille, sélectionnez **MAINTENANCE** > **tâches** > **expansion**.)

> ⚠ Si plus d'un nœud de stockage est hors ligne ou si un nœud de stockage de cette grille a été reconstruit au cours des 15 derniers jours, contactez le support technique. N'exécutez pas le `sn-recovery-postinstall.sh` script. Reconstruire Cassandra sur deux nœuds de stockage ou plus dans les 15 jours suivant l'arrêt du service peut entraîner une perte de données.

Description de la tâche

Pour effectuer cette procédure, vous devez effectuer les tâches de haut niveau suivantes :

- Connectez-vous au nœud de stockage récupéré.
- Exécutez le `sn-remount-volumes` script pour remonter les volumes de stockage correctement formatés. Lorsque ce script s'exécute, il effectue les opérations suivantes :
  - Monte et démonte chaque volume de stockage pour relire le journal XFS.
  - Effectue une vérification de cohérence de fichier XFS.
  - Si le système de fichiers est cohérent, détermine si le volume de stockage est un volume de stockage StorageGRID correctement formaté.
  - Si le volume de stockage est correctement formaté, remonter le volume de stockage. Toutes les données existantes du volume restent intactes.
- Examinez la sortie du script et résolvez tout problème.
- Exécutez le `sn-recovery-postinstall.sh` script. Lorsque ce script s'exécute, il effectue les opérations suivantes :

> Ne redémarrez pas un nœud de stockage pendant la restauration avant l'exécution `sn-recovery-postinstall.sh` (étape 4) pour reformater les volumes de stockage défaillants et restaurer les métadonnées de l'objet. Redémarrage du nœud de stockage avant `sn-recovery-postinstall.sh` La solution complète provoque des erreurs sur les services qui tentent de démarrer et entraîne la sortie des nœuds d'appliance StorageGRID en mode de maintenance.

  - Reformate tous les volumes de stockage du `sn-remount-volumes` le script n'a pas pu être monté ou a été mal formaté.

> Lorsqu'un volume de stockage est reformaté, toutes les données de ce volume sont perdues. Vous devez effectuer une procédure supplémentaire pour restaurer les données d'objet à partir d'autres emplacements de la grille, en supposant que les règles ILM ont été configurées pour stocker plusieurs copies d'objet.

  - Reconstruit la base de données Cassandra sur le nœud, si nécessaire.
  - Démarre les services sur le nœud de stockage.

Étapes

1. Connectez-vous au nœud de stockage récupéré :
   a. Saisissez la commande suivante : `ssh admin@grid_node_IP`
   b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
   c. Entrez la commande suivante pour passer à la racine : `su -`
   d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

   Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

2. Exécutez le premier script pour remonter tous les volumes de stockage correctement formatés.

> Si tous les volumes de stockage sont nouveaux et doivent être formatés, ou si tous les volumes de stockage ont échoué, vous pouvez ignorer cette étape et exécuter le deuxième script pour reformater tous les volumes de stockage démontés.

a. Exécutez le script : `sn-remount-volumes`

   Ce script peut prendre des heures sur les volumes de stockage qui contiennent des données.

b. Au fur et à mesure de l'exécution du script, vérifiez le résultat et répondez aux invites.

> Si nécessaire, vous pouvez utiliser le `tail -f` commande permettant de contrôler le contenu du fichier journal du script (`/var/local/log/sn-remount-volumes.log`). Le fichier journal contient des informations plus détaillées que la sortie de la ligne de commande.

```
root@SG:~ # sn-remount-volumes
The configured LDR noid is 12632740

====== Device /dev/sdb ======
Mount and unmount device /dev/sdb and checking file system
consistency:
The device is consistent.
Check rangedb structure on device /dev/sdb:
Mount device /dev/sdb to /tmp/sdb-654321 with rangedb mount options
This device has all rangedb directories.
Found LDR node id 12632740, volume number 0 in the volID file
Attempting to remount /dev/sdb
Device /dev/sdb remounted successfully

====== Device /dev/sdc ======
Mount and unmount device /dev/sdc and checking file system
consistency:
Error: File system consistency check retry failed on device /dev/sdc.
You can see the diagnosis information in the /var/local/log/sn-
remount-volumes.log.

This volume could be new or damaged. If you run sn-recovery-
postinstall.sh, this volume and any data on this volume will be
deleted. If you only had two copies of object data, you will
temporarily have only a single copy.
StorageGRID Webscale will attempt to restore data redundancy by
making additional replicated copies or EC fragments, according to the
rules in the active ILM policy.

Don't continue to the next step if you believe that the data
remaining on this volume can't be rebuilt from elsewhere in the grid
(for example, if your ILM policy uses a rule that makes only one copy
or if volumes have failed on multiple nodes). Instead, contact
support to determine how to recover your data.

====== Device /dev/sdd ======
```

```
Mount and unmount device /dev/sdd and checking file system
consistency:
Failed to mount device /dev/sdd
This device could be an uninitialized disk or has corrupted
superblock.
File system check might take a long time. Do you want to continue? (y
or n) [y/N]? y

Error: File system consistency check retry failed on device /dev/sdd.
You can see the diagnosis information in the /var/local/log/sn-
remount-volumes.log.

This volume could be new or damaged. If you run sn-recovery-
postinstall.sh, this volume and any data on this volume will be
deleted. If you only had two copies of object data, you will
temporarily have only a single copy.
StorageGRID Webscale will attempt to restore data redundancy by
making additional replicated copies or EC fragments, according to the
rules in the active ILM policy.

Don't continue to the next step if you believe that the data
remaining on this volume can't be rebuilt from elsewhere in the grid
(for example, if your ILM policy uses a rule that makes only one copy
or if volumes have failed on multiple nodes). Instead, contact
support to determine how to recover your data.

====== Device /dev/sde ======
Mount and unmount device /dev/sde and checking file system
consistency:
The device is consistent.
Check rangedb structure on device /dev/sde:
Mount device /dev/sde to /tmp/sde-654321 with rangedb mount options
This device has all rangedb directories.
Found LDR node id 12000078, volume number 9 in the volID file
Error: This volume does not belong to this node. Fix the attached
volume and re-run this script.
```

Dans l'exemple de sortie, un volume de stockage a été remonté avec succès et trois volumes de stockage ont rencontré des erreurs.

- `/dev/sdb` La vérification de cohérence du système de fichiers XFS a été effectuée et une structure de volume valide a été correctement remontée. Les données sur les périphériques remontés par le script sont conservées.
- `/dev/sdc` Echec de la vérification de cohérence du système de fichiers XFS car le volume de stockage était nouveau ou corrompu.
- `/dev/sdd` impossible de monter car le disque n'a pas été initialisé ou le superbloc du disque a été

corrompu. Lorsque le script ne peut pas monter un volume de stockage, il vous demande si vous souhaitez exécuter le contrôle de cohérence du système de fichiers.

- Si le volume de stockage est relié à un nouveau disque, répondez **N** à l'invite. Vous n'avez pas besoin de vérifier le système de fichiers sur un nouveau disque.
- Si le volume de stockage est relié à un disque existant, répondez **y** à l'invite. Vous pouvez utiliser les résultats de la vérification du système de fichiers pour déterminer la source de la corruption. Les résultats sont enregistrés dans le `/var/local/log/sn-remount-volumes.log` fichier journal.

- `/dev/sde` A réussi la vérification de cohérence du système de fichiers XFS et avait une structure de volume valide ; cependant, l'ID de nœud LDR dans le `volID` Le fichier ne correspond pas à l'ID de ce noeud de stockage (l' `configured LDR noid` affiché en haut). Ce message indique que ce volume appartient à un autre noeud de stockage.

3. Examinez la sortie du script et résolvez tout problème.

> Si un volume de stockage a échoué au contrôle de cohérence du système de fichiers XFS ou ne peut pas être monté, vérifiez attentivement les messages d'erreur dans la sortie. Vous devez comprendre les implications de l'exécution du `sn-recovery-postinstall.sh` créer des scripts sur ces volumes.

a. Vérifiez que les résultats incluent une entrée pour tous les volumes attendus. Si aucun volume n'est répertorié, exécutez à nouveau le script.

b. Consultez les messages de tous les périphériques montés. Assurez-vous qu'il n'y a pas d'erreur indiquant qu'un volume de stockage n'appartient pas à ce noeud de stockage.

Dans l'exemple, la sortie de /dev/sde inclut le message d'erreur suivant :

```
Error: This volume does not belong to this node. Fix the attached
volume and re-run this script.
```

> Si un volume de stockage est signalé comme appartenant à un autre nœud de stockage, contactez le support technique. Si vous exécutez le `sn-recovery-postinstall.sh` script, le volume de stockage sera reformaté, ce qui peut entraîner une perte de données.

c. Si aucun périphérique de stockage n'a pu être monté, notez le nom du périphérique et réparez ou remplacez le périphérique.

> Vous devez réparer ou remplacer tout périphérique de stockage qui n'a pas pu être monté.

Vous utiliserez le nom de l'appareil pour rechercher l'ID de volume, qui est obligatoire lorsque vous exécutez le `repair-data` script permettant de restaurer les données d'objet sur le volume (procédure suivante).

d. Après avoir réparé ou remplacé tous les dispositifs unmountable, exécutez le `sn-remount-volumes` script une nouvelle fois pour confirmer que tous les volumes de stockage pouvant être remontés ont été remontés.

Si un volume de stockage ne peut pas être monté ou est mal formaté et que vous passez à l'étape suivante, le volume et toutes les données du volume seront supprimés. Si vous aviez deux copies de vos données d'objet, vous n'aurez qu'une seule copie jusqu'à la fin de la procédure suivante (restauration des données d'objet).

N'exécutez pas le `sn-recovery-postinstall.sh` Script si vous pensez que les données restantes sur un volume de stockage en panne ne peuvent pas être reconstruites à partir d'un autre emplacement de la grille (par exemple, si votre règle ILM utilise une règle qui effectue une seule copie ou si les volumes ont échoué sur plusieurs nœuds). Contactez plutôt le support technique pour savoir comment récupérer vos données.

4. Exécutez le `sn-recovery-postinstall.sh` script : `sn-recovery-postinstall.sh`

   Ce script reformate tous les volumes de stockage qui n'ont pas pu être montés ou qui n'ont pas été correctement formatés. Reconstruit la base de données Cassandra sur le nœud, si nécessaire, et démarre les services sur le nœud de stockage.

   Gardez à l'esprit les points suivants :

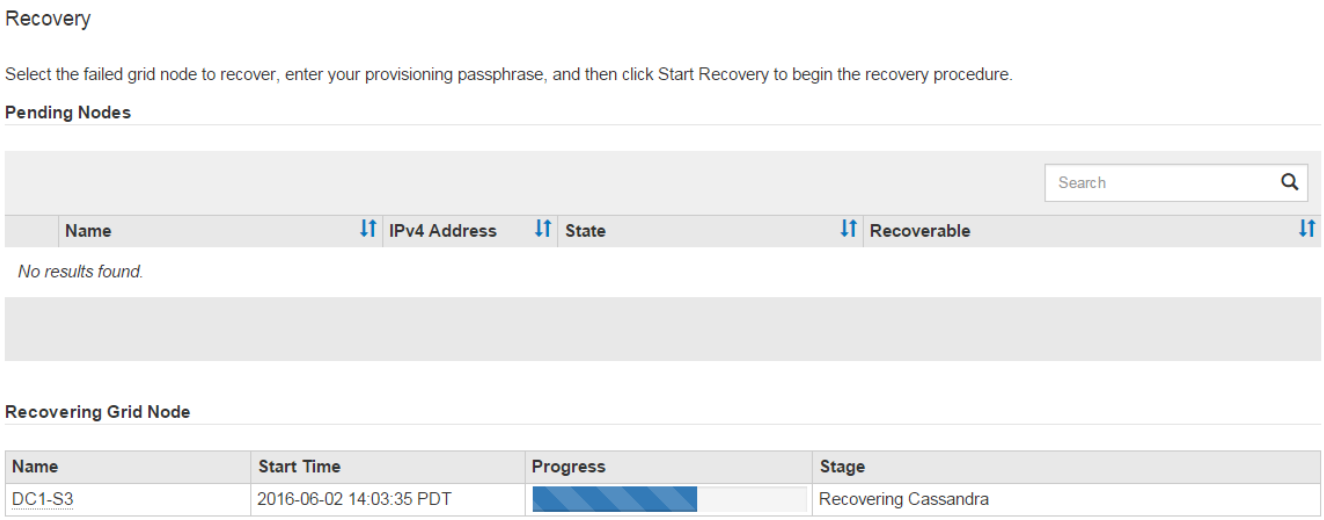
   - L'exécution du script peut prendre des heures.
   - En général, vous devez laisser la session SSH seule pendant que le script est en cours d'exécution.
   - N'appuyez pas sur **Ctrl+C** lorsque la session SSH est active.
   - Le script s'exécute en arrière-plan en cas d'interruption du réseau et met fin à la session SSH, mais vous pouvez afficher la progression à partir de la page récupération.
   - Si le nœud de stockage utilise le service RSM, le script peut sembler bloqué pendant 5 minutes au redémarrage des services de nœud. Ce délai de 5 minutes est prévu lorsque l'entretien du RSM démarre pour la première fois.

     Le service RSM est présent sur les nœuds de stockage qui incluent le service ADC.

   Certaines procédures de restauration StorageGRID utilisent Reaper pour traiter les réparations Cassandra. Les réparations sont effectuées automatiquement dès que les services connexes ou requis ont commencé. Vous remarquerez peut-être des résultats de script mentionnant « couche » ou « réparation Cassandra ». Si un message d'erreur indiquant que la réparation a échoué, exécutez la commande indiquée dans le message d'erreur.

5. Comme le `sn-recovery-postinstall.sh` Exécution du script, surveillez la page récupération dans le Gestionnaire de grille.

   La barre de progression et la colonne Etape de la page récupération fournissent un état de haut niveau du `sn-recovery-postinstall.sh` script.



6. Après le `sn-recovery-postinstall.sh` le script a démarré les services sur le nœud. vous pouvez restaurer les données d'objet sur tous les volumes de stockage formatés par le script.

   Le script vous demande si vous souhaitez restaurer les données d'objet manuellement.

   - Dans la plupart des cas, vous devriez "Restaurez les données d'objet à l'aide de Grid Manager". Réponse `n` Pour utiliser le Gestionnaire de grille.
   - Dans de rares cas, par exemple lorsque le support technique vous y invite, ou lorsque vous savez que le nœud de remplacement dispose de moins de volumes disponibles pour le stockage objet que le nœud d'origine, vous devez "restaurez les données d'objet manuellement" à l'aide du `repair-data` script. Si l'un de ces cas s'applique, répondez `y`.

   > Si vous répondez `y` pour restaurer les données d'objet manuellement :
   >
   > - Vous ne pouvez pas restaurer les données d'objet à l'aide de Grid Manager.
   > - Vous pouvez surveiller la progression des travaux de restauration manuelle à l'aide de Grid Manager.

Restaurez les données d'objet vers un volume de stockage pour l'appliance

Après avoir restauré des volumes de stockage pour le nœud de stockage de l'appliance, vous pouvez restaurer les données d'objet répliquées ou avec code d'effacement qui ont été perdues en cas de défaillance du nœud de stockage.

Quelle procédure dois-je utiliser ?

Dans la mesure du possible, restaurez les données d'objet à l'aide de la page **Restauration de volume** du gestionnaire de grille.

- Si les volumes sont répertoriés sous **MAINTENANCE** > **Restauration de volume** > **nœuds à restaurer**, restaurez les données d'objet à l'aide de l' "Page de restauration de volume dans le Gestionnaire de grille".
- Si les volumes ne sont pas répertoriés dans **MAINTENANCE** > **Restauration du volume** > **nœuds à restaurer**, suivez les étapes ci-dessous pour utiliser le `repair-data` script de restauration des données d'objet.

Si le nœud de stockage restauré contient moins de volumes que le nœud qu'il remplace, vous devez utiliser le `repair-data` script.

Utilisez le `repair-data` script de restauration des données d'objet

Avant de commencer

- Vous devez avoir confirmé que le noeud de stockage récupéré possède un état de connexion * connecté* Dans l'onglet **NODES** > **Présentation** du Gestionnaire de grille.

Description de la tâche

Les données d'objet peuvent être restaurées depuis d'autres nœuds de stockage, un nœud d'archivage ou un pool de stockage cloud, en supposant que les règles ILM de la grille soient configurées de manière à ce que les copies d'objet soient disponibles.

Notez ce qui suit :

- Si une règle ILM a été configurée pour stocker une seule copie répliquée, et que cette copie existait sur un volume de stockage défaillant, vous ne pourrez pas restaurer l'objet.
- Si la seule copie restante d'un objet se trouve dans un pool de stockage cloud, StorageGRID doit émettre plusieurs demandes vers le terminal de pool de stockage cloud pour restaurer les données d'objet. Avant d'effectuer cette procédure, contactez le support technique pour obtenir de l'aide pour estimer le délai de restauration et les coûts associés.
- Si la seule copie restante d'un objet se trouve sur un noeud d'archivage, les données d'objet sont extraites du noeud d'archivage. La restauration de données d'objet sur un nœud de stockage à partir d'un nœud d'archivage prend plus de temps que la restauration de copies à partir d'autres nœuds de stockage en raison de la latence associée aux récupérations à partir de systèmes de stockage d'archives externes.

À propos du `repair-data` script

Pour restaurer les données d'objet, exécutez le `repair-data` script. Ce script commence le processus de restauration des données d'objet et fonctionne avec l'analyse ILM pour s'assurer que les règles ILM sont respectées.

Sélectionnez **données répliquées** ou **données codées par effacement (EC)** ci-dessous pour apprendre les différentes options du `repair-data` script, basé sur la restauration des données répliquées ou des données avec code d'effacement. Si vous devez restaurer les deux types de données, vous devez exécuter les deux ensembles de commandes.

> Pour plus d'informations sur le `repair-data` script, entrez `repair-data --help` Dans la ligne de commande du nœud d'administration principal.

Les données répliquées

Deux commandes sont disponibles pour la restauration des données répliquées, et ce, selon que vous devez réparer le nœud entier ou uniquement certains volumes sur le nœud :

```
repair-data start-replicated-node-repair

repair-data start-replicated-volume-repair
```

Vous pouvez suivre les réparations des données répliquées avec cette commande :

```
repair-data show-replicated-repair-status
```

Données avec code d'effacement (EC)

Deux commandes sont disponibles pour la restauration des données avec code d'effacement, selon que vous devez réparer le nœud entier ou uniquement certains volumes sur le nœud :

```
repair-data start-ec-node-repair

repair-data start-ec-volume-repair
```

Vous pouvez suivre les réparations des données codées par effacement à l'aide de cette commande :

```
repair-data show-ec-repair-status
```

> Les réparations des données codées peuvent commencer alors que certains nœuds de stockage sont hors ligne. Toutefois, si toutes les données avec code d'effacement ne peuvent pas être prises en compte, la réparation ne peut pas être effectuée. La réparation s'effectuera une fois que tous les nœuds sont disponibles.

> Le travail de réparation EC réserve temporairement une grande quantité de stockage. Les alertes de stockage peuvent être déclenchées, mais elles seront résolus une fois la réparation terminée. S'il n'y a pas assez de stockage pour la réservation, la tâche de réparation EC échouera. Les réservations de stockage sont libérées lorsque la tâche de réparation EC est terminée, que la tâche ait échoué ou a réussi.

Rechercher le nom d'hôte pour le noeud de stockage

1. Connectez-vous au nœud d'administration principal :
   a. Saisissez la commande suivante : `ssh admin@primary_Admin_Node_IP`
   b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
   c. Entrez la commande suivante pour passer à la racine : `su -`
   d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

   Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

2. Utilisez le `/etc/hosts` Fichier pour trouver le nom d'hôte du noeud de stockage pour les volumes de stockage restaurés. Pour afficher la liste de tous les nœuds de la grille, saisissez les éléments suivants : `cat /etc/hosts`.

Réparez les données si tous les volumes ont échoué

Si tous les volumes de stockage sont en panne, réparez l'intégralité du nœud. Suivez les instructions pour les données **répliquées**, **codées par effacement (EC)**, ou les deux, selon que vous utilisez ou non des données répliquées, des données codées par effacement (EC), ou les deux.

Si seuls certains volumes ont échoué, accédez à Réparer les données si seulement certains volumes ont échoué.

> Vous ne pouvez pas courir `repair-data` opérations simultanément pour plusieurs nœuds. Pour restaurer plusieurs nœuds, contactez le support technique.

Les données répliquées

Si votre grid inclut des données répliquées, utilisez le `repair-data start-replicated-node-repair` commande avec `--nodes` option, où `--nodes` Est le nom d'hôte (nom du système), pour réparer la totalité du nœud de stockage.

Cette commande répare les données répliquées sur un nœud de stockage nommé SG-DC-SN3 :

```
repair-data start-replicated-node-repair --nodes SG-DC-SN3
```

> Lorsque les données d'objet sont restaurées, l'alerte **objets perdus** est déclenchée si le système StorageGRID ne peut pas localiser les données d'objet répliquées. Des alertes peuvent être déclenchées sur les nœuds de stockage dans le système. Vous devez déterminer la cause de la perte et si la récupération est possible. Voir "Rechercher les objets perdus".

Données avec code d'effacement (EC)

Si votre grid contient des données avec code d'effacement, utilisez la `repair-data start-ec-node-repair` commande avec `--nodes` option, où `--nodes` Est le nom d'hôte (nom du système), pour réparer la totalité du nœud de stockage.

Cette commande répare les données codées de l'effacement sur un nœud de stockage appelé SG-DC-SN3 :

```
repair-data start-ec-node-repair --nodes SG-DC-SN3
```

L'opération renvoie un seul `repair ID` qui l'identifie `repair_data` fonctionnement. Utilisez-le `repair ID` pour suivre la progression et le résultat du `repair_data` fonctionnement. Aucun autre retour n'est renvoyé à la fin du processus de récupération.

> Les réparations des données codées peuvent commencer alors que certains nœuds de stockage sont hors ligne. La réparation s'effectuera une fois que tous les nœuds sont disponibles.

Réparer les données si seulement certains volumes ont échoué

Si seulement certains volumes ont échoué, réparez les volumes affectés. Suivez les instructions pour les données **répliquées**, **codées par effacement (EC)**, ou les deux, selon que vous utilisez ou non des données répliquées, des données codées par effacement (EC), ou les deux.

Si tous les volumes ont échoué, accédez à Réparez les données si tous les volumes ont échoué.

Saisissez les ID de volume en hexadécimal. Par exemple : `0000` est le premier volume et `000F` est le seizième volume. Vous pouvez spécifier un volume, une plage de volumes ou plusieurs volumes qui ne sont pas dans une séquence.

Tous les volumes doivent se trouver sur le même nœud de stockage. Si vous devez restaurer des volumes pour plusieurs nœuds de stockage, contactez le support technique.

Les données répliquées

Si votre grid contient des données répliquées, utilisez le `start-replicated-volume-repair` commande avec `--nodes` option permettant d'identifier le nœud (où `--nodes` est le nom d'hôte du nœud). Ajoutez ensuite l'une ou l'autre des `--volumes` ou `--volume-range` comme indiqué dans les exemples suivants.

Volume unique : cette commande restaure les données répliquées vers le volume `0002` Sur un nœud de stockage nommé SG-DC-SN3 :

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volumes 0002
```

Plage de volumes : cette commande restaure les données répliquées vers tous les volumes de la plage `0003` à `0009` Sur un nœud de stockage nommé SG-DC-SN3 :

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volume-range
0003,0009
```

Volumes multiples non compris dans une séquence : cette commande restaure les données répliquées vers des volumes `0001`, `0005`, et `0008` Sur un nœud de stockage nommé SG-DC-SN3 :

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volumes
0001,0005,0008
```

> Lorsque les données d'objet sont restaurées, l'alerte **objets perdus** est déclenchée si le système StorageGRID ne peut pas localiser les données d'objet répliquées. Des alertes peuvent être déclenchées sur les nœuds de stockage dans le système. Notez la description de l'alerte et les actions recommandées pour déterminer la cause de la perte et si la récupération est possible.

Données avec code d'effacement (EC)

Si votre grid contient des données avec code d'effacement, utilisez la `start-ec-volume-repair` commande avec `--nodes` option permettant d'identifier le nœud (où `--nodes` est le nom d'hôte du nœud). Ajoutez ensuite l'une ou l'autre des `--volumes` ou `--volume-range` comme indiqué dans les exemples suivants.

Volume unique : cette commande restaure les données codées par effacement dans un volume `0007` Sur un nœud de stockage nommé SG-DC-SN3 :

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 0007
```

Plage de volumes : cette commande restaure les données avec code d'effacement sur tous les volumes de la plage `0004` à `0006` Sur un nœud de stockage nommé SG-DC-SN3 :

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volume-range 0004,0006
```

Plusieurs volumes non dans une séquence : cette commande restaure les données codées par effacement dans des volumes `000A`, `000C`, et `000E` Sur un nœud de stockage nommé SG-DC-SN3 :

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 000A,000C,000E
```

Le `repair-data` l'opération renvoie un seul `repair ID` qui l'identifie `repair_data` fonctionnement.

Utilisez-le `repair ID` pour suivre la progression et le résultat du `repair_data` fonctionnement. Aucun autre retour n'est renvoyé à la fin du processus de récupération.

> Les réparations des données codées peuvent commencer alors que certains nœuds de stockage sont hors ligne. La réparation s'effectuera une fois que tous les nœuds sont disponibles.

Surveiller les réparations

Surveiller l'état des travaux de réparation, en fonction de l'utilisation ou non des données **répliquées**, **données codées par effacement (EC)**, ou des deux.

Vous pouvez également surveiller l'état des travaux de restauration de volume en cours et afficher un historique des travaux de restauration effectués dans"Gestionnaire de grille".

Les données répliquées

- Pour obtenir une estimation du pourcentage d'achèvement de la réparation répliquée, ajoutez le `show-replicated-repair-status` option de la commande repair-data.

  ```
  repair-data show-replicated-repair-status
  ```

- Pour déterminer si les réparations sont terminées :
  a. Sélectionnez **NŒUDS** > ***nœud de stockage en cours de réparation*** > **ILM**.
  b. Vérifiez les attributs dans la section évaluation. Lorsque les réparations sont terminées, l'attribut **attente - tous** indique 0 objets.
- Pour surveiller la réparation plus en détail :
  a. Sélectionnez **SUPPORT** > **Outils** > **topologie de grille**.
  b. Sélectionnez ***GRID*** > ***Storage Node en cours de réparation*** > **LDR** > **Data Store**.
  c. Utilisez une combinaison des attributs suivants pour déterminer, autant que possible, si les réparations répliquées sont terminées.

  > Cassandra présente peut-être des incohérences et les réparations échouées ne sont pas suivies.

  - **Réparations tentées (XRPA)** : utilisez cet attribut pour suivre la progression des réparations répliquées. Cet attribut augmente chaque fois qu'un nœud de stockage tente de réparer un objet à haut risque. Lorsque cet attribut n'augmente pas pendant une période plus longue que la période d'acquisition actuelle (fournie par l'attribut **période d'analyse — estimation**), cela signifie que l'analyse ILM n'a trouvé aucun objet à haut risque qui doit être réparé sur n'importe quel nœud.

    > Les objets à haut risque sont des objets qui risquent d'être complètement perdus. Cela n'inclut pas les objets qui ne répondent pas à leur configuration ILM.

  - **Période d'acquisition — estimée (XSCM)** : utilisez cet attribut pour estimer quand une modification de règle sera appliquée aux objets précédemment ingérés. Si l'attribut **réparations tentées** n'augmente pas pendant une période supérieure à la période d'acquisition actuelle, il est probable que les réparations répliquées soient effectuées. Notez que la période d'acquisition peut changer. L'attribut **période d'acquisition — estimée (XSCM)** s'applique à la grille entière et est le maximum de toutes les périodes d'acquisition de nœud. Vous pouvez interroger l'historique d'attributs **période de balayage — estimation** de la grille pour déterminer une période appropriée.

Données avec code d'effacement (EC)

Pour surveiller la réparation des données codées d'effacement et réessayer toute demande qui pourrait avoir échoué :

1. Déterminez l'état des réparations des données par code d'effacement :
   - Sélectionnez **SUPPORT** > **Tools** > **Metrics** pour afficher le temps de réalisation estimé et le pourcentage de réalisation de la tâche en cours. Sélectionnez ensuite **EC Overview** dans la section Grafana. Examinez les tableaux de bord **Grid EC Job estimé Time to Completion** et **Grid EC Job Percentage Finted**.

- Utilisez cette commande pour afficher le statut d'un spécifique `repair-data` fonctionnement :

  ```
  repair-data show-ec-repair-status --repair-id repair ID
  ```

- Utilisez cette commande pour lister toutes les réparations :

  ```
  repair-data show-ec-repair-status
  ```

Les informations de sortie sont affichées, notamment `repair ID`, pour toutes les réparations précédentes et en cours.

2. Si le résultat indique que l'opération de réparation a échoué, utilisez le `--repair-id` option permettant de réessayer la réparation.

   Cette commande relance une réparation de nœud ayant échoué à l'aide de l'ID de réparation 6949309319275667690 :

   ```
   repair-data start-ec-node-repair --repair-id 6949309319275667690
   ```

   Cette commande relance une réparation de volume en échec à l'aide de l'ID de réparation 6949309319275667690 :

   ```
   repair-data start-ec-volume-repair --repair-id 6949309319275667690
   ```

Vérifiez l'état de stockage après la récupération du nœud de stockage de l'appliance

Après avoir restauré un noeud de stockage d'appliance, vous devez vérifier que l'état souhaité du noeud de stockage de l'appliance est défini sur en ligne et vous assurer que l'état est en ligne par défaut à chaque redémarrage du serveur de noeud de stockage.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Le nœud de stockage a été restauré et la restauration des données est terminée.

Étapes

1. Sélectionnez **SUPPORT** > **Outils** > **topologie de grille**.
2. Vérifiez les valeurs de **nœud de stockage récupéré** > **LDR** > **Storage** > **Storage State de stockage — désiré** et **Storage State — Current**.

   La valeur des deux attributs doit être en ligne.

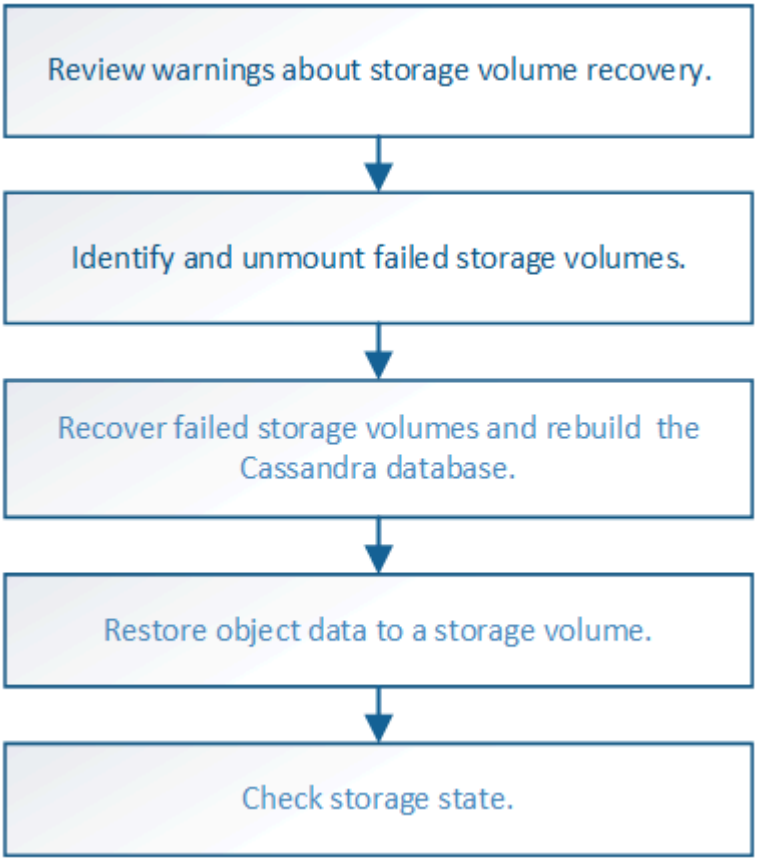
3. Si l'état de stockage — souhaité est défini sur lecture seule, procédez comme suit :
   a. Cliquez sur l'onglet **Configuration**.
   b. Dans la liste déroulante **État de stockage — désiré**, sélectionnez **en ligne**.
   c. Cliquez sur **appliquer les modifications**.
   d. Cliquez sur l'onglet **Présentation** et confirmez que les valeurs de **État de stockage — désiré** et **État de stockage — actuel** sont mises à jour en ligne.

Restaurez les données après une panne du volume de stockage, où le disque système est intact : flux de travail

Vous devez effectuer une série de tâches pour restaurer un nœud de stockage logiciel dans lequel un ou plusieurs volumes de stockage du nœud de stockage sont défaillants, mais le lecteur système est intact. Si seuls les volumes de stockage ont échoué, le nœud de stockage est toujours disponible pour le système StorageGRID.

> Cette procédure de restauration s'applique uniquement aux nœuds de stockage basés sur logiciel. Si les volumes de stockage ont échoué sur un nœud de stockage de l'appliance, suivez la procédure ci-dessous : "Restaurez le nœud de stockage de l'appliance".

Comme indiqué dans le schéma de workflow, vous devez identifier et démonter les volumes de stockage défaillants, restaurer les volumes, reconstruire la base de données Cassandra et restaurer les données d'objet.



Examinez les avertissements concernant la restauration des volumes de stockage

Avant de récupérer des volumes de stockage défaillants pour un noeud de stockage, vous devez vérifier les avertissements suivants.

Les volumes de stockage (ou rangedbs) d'un noeud de stockage sont identifiés par un nombre hexadécimal, appelé ID de volume. Par exemple, 0000 est le premier volume et 000F est le seizième volume. Le premier magasin d'objets (volume 0) sur chaque nœud de stockage utilise jusqu'à 4 To d'espace pour les métadonnées d'objet et les opérations des bases de données Cassandra, tout espace restant sur ce volume

est utilisé pour les données d'objet. Tous les autres volumes de stockage sont utilisés exclusivement pour les données d'objet.

Si le volume 0 échoue et doit être récupéré, la base de données Cassandra peut être reconstruite dans le cadre de la procédure de récupération du volume. Cassandra peut également être reconstruite dans les cas suivants :

- Un nœud de stockage est remis en ligne après avoir été hors ligne pendant plus de 15 jours.
- Le lecteur système et un ou plusieurs volumes de stockage sont défectueux et restaurés.

Lorsque Cassandra est reconstruite, le système utilise les informations d'autres nœuds de stockage. Si trop de nœuds de stockage sont hors ligne, il se peut que certaines données Cassandra ne soient pas disponibles. Si Cassandra a été récemment reconstruite, les données Cassandra ne peuvent pas encore être cohérentes sur l'ensemble de la grille. Cette perte peut se produire si Cassandra est reconstruite lorsque trop de nœuds de stockage sont hors ligne ou si deux nœuds de stockage ou plus sont reconstruites dans les 15 jours restants.

Si plusieurs nœuds de stockage ont échoué (ou sont hors ligne), contactez le support technique. N'effectuez pas la procédure de récupération suivante. Des données peuvent être perdues.

S'il s'agit de la défaillance du deuxième nœud de stockage dans les 15 jours qui suivent la défaillance ou la restauration d'un nœud de stockage, contactez le support technique. Reconstruire Cassandra sur deux nœuds de stockage ou plus en un délai de 15 jours peut entraîner une perte de données.

Si plusieurs nœuds de stockage d'un site ont échoué, une procédure de restauration de site peut être nécessaire. Voir "Comment la reprise sur site est effectuée par le support technique".

Si les règles ILM sont configurées pour ne stocker qu'une seule copie répliquée, et si cette copie existe sur un volume de stockage défaillant, vous ne pourrez pas restaurer l'objet.

Si vous rencontrez une alarme Services: Status - Cassandra (SVST) pendant la récupération, reportez-vous à la section "Restaurez des volumes de stockage défaillants et reconstruisez la base de données Cassandra". Après la reconstruction de Cassandra, les alarmes doivent être désactivées. Si les alarmes ne s'effacent pas, contactez le support technique.

Informations associées

"Avertissements et considérations relatives à la restauration des nœuds de la grille"

Identifiez et démontez les volumes de stockage défectueux

Lors de la restauration d'un nœud de stockage dont les volumes de stockage sont en panne, vous devez identifier et démonter les volumes en panne. Vous devez vérifier que seuls les volumes de stockage défaillants sont reformatés dans le cadre de la procédure de restauration.

Avant de commencer

Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".

Description de la tâche

Vous devriez récupérer les volumes de stockage défaillants dès que possible.

La première étape du processus de restauration consiste à détecter les volumes qui se sont détachés, qui doivent être démontés ou qui présentent des erreurs d'E/S. Si les volumes défaillants sont toujours attachés mais qu'un système de fichiers est corrompu de façon aléatoire, le système risque de ne pas détecter de corruption dans les pièces non utilisées ou non attribuées du disque.

> Vous devez terminer cette procédure avant d'effectuer manuellement les étapes de restauration des volumes, telles que l'ajout ou la reconfiguration des disques, l'arrêt du nœud, le démarrage du nœud ou le redémarrage. Sinon, lorsque vous exécutez le `reformat_storage_block_devices.rb` script, vous pouvez rencontrer une erreur du système de fichiers qui entraîne l'arrêt ou l'échec du script.

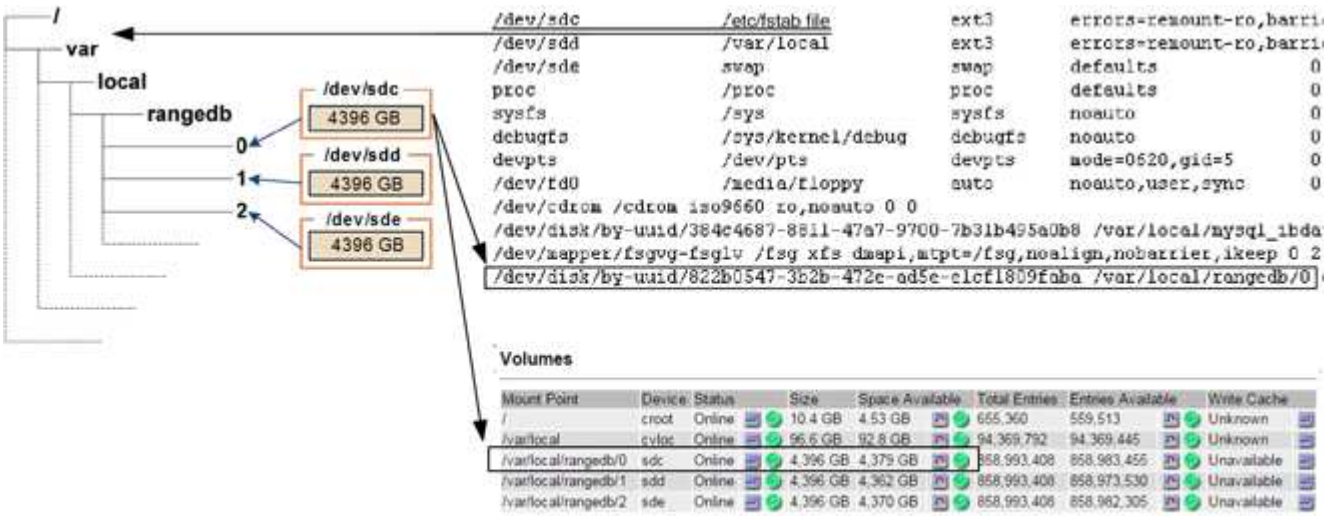
> Réparez le matériel et fixez correctement les disques avant de faire fonctionner le `reboot` commande.

> Identifiez minutieusement les volumes de stockage défaillants. Ces informations vous permettront de vérifier quels volumes doivent être reformatés. Une fois qu'un volume a été reformaté, les données du volume ne peuvent pas être récupérées.

Pour récupérer correctement les volumes de stockage défectueux, vous devez connaître à la fois les noms des périphériques des volumes de stockage défaillants et leurs ID de volume.

Lors de l'installation, un identifiant unique universel du système de fichiers (UUID) est attribué à chaque périphérique de stockage et il est monté dans un répertoire rangedb du nœud de stockage à l'aide de l'UUID attribué au système de fichiers. L'UUID du système de fichiers et le répertoire rangedb sont répertoriés dans le `/etc/fstab` fichier. Le nom du périphérique, le répertoire rangedb et la taille du volume monté sont affichés dans le Gestionnaire de grille.

Dans l'exemple suivant, périphérique `/dev/sdc` A une taille de volume de 4 To, est monté sur `/var/local/rangedb/0`, en utilisant le nom du périphérique `/dev/disk/by-uuid/822b0547-3b2b-472e-ad5e-e1cf1809faba` dans le `/etc/fstab` fichier :



Étapes

1. Procédez comme suit pour enregistrer les volumes de stockage défaillants et leurs noms de périphériques :

   a. Sélectionnez **SUPPORT** > **Outils** > **topologie de grille**.

   b. Sélectionnez **site** > **noeud de stockage défaillant** > **LDR** > **Storage** > **Présentation** > **main** et recherchez des magasins d'objets avec alarmes.

Object Stores

ID	Total	Available	Stored Data	Stored (%)	Health
0000	96.6 GB	96.6 GB	823 KB	0.001 %	Error
0001	107 GB	107 GB	0 B	0 %	No Errors
0002	107 GB	107 GB	0 B	0 %	No Errors

   c. Sélectionnez **site** > **noeud de stockage défaillant** > **SSM** > **Ressources** > **Présentation** > **main**. Déterminez la taille du point de montage et du volume de chaque volume de stockage défectueux identifié à l'étape précédente.

   Les magasins d'objets sont numérotés en notation hexadécimale. Par exemple, 0000 est le premier volume et 000F est le seizième volume. Dans l'exemple, le magasin d'objets avec un ID de 0000 correspond à `/var/local/rangedb/0` Avec le nom de périphérique sdc et une taille de 107 Go.

Volumes

Mount Point	Device	Status	Size	Space Available	Total Entries	Entries Available	Write Cache
/	croot	Online	10.4 GB	4.17 GB	655,360	554,806	Unknown
/var/local	cvloc	Online	96.6 GB	96.1 GB	94,369,792	94,369,423	Unknown
/var/local/rangedb/0	sdc	Online	107 GB	107 GB	104,857,600	104,856,202	Enabled
/var/local/rangedb/1	sdd	Online	107 GB	107 GB	104,857,600	104,856,536	Enabled
/var/local/rangedb/2	sde	Online	107 GB	107 GB	104,857,600	104,856,536	Enabled

2. Connectez-vous au noeud de stockage défaillant :

   a. Saisissez la commande suivante : `ssh admin@grid_node_IP`

   b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

   c. Entrez la commande suivante pour passer à la racine : `su -`

   d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

   Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

3. Exécutez le script suivant pour démonter un volume de stockage défaillant :

   ```
   sn-unmount-volume object_store_ID
   ```

   Le `object_store_ID` Est l'ID du volume de stockage défaillant. Par exemple, spécifiez `0` Dans la commande pour un magasin d'objets avec l'ID 0000.

4. Si vous y êtes invité, appuyez sur **y** pour arrêter le service Cassandra en fonction du volume de stockage 0.

Si le service Cassandra est déjà arrêté, vous n'êtes pas invité à le faire. Le service Cassandra est arrêté uniquement pour le volume 0.

```
root@Storage-180:~/var/local/tmp/storage~ # sn-unmount-volume 0
Services depending on storage volume 0 (cassandra) aren't down.
Services depending on storage volume 0 must be stopped before running
this script.
Stop services that require storage volume 0 [y/N]? y
Shutting down services that require storage volume 0.
Services requiring storage volume 0 stopped.
Unmounting /var/local/rangedb/0
/var/local/rangedb/0 is unmounted.
```

Le volume est démonté en quelques secondes. Des messages s'affichent indiquant chaque étape du processus. Le dernier message indique que le volume est démonté.

5. Si le démontage échoue parce que le volume est occupé, vous pouvez forcer le démontage à l'aide du `--use-umountof` option :

Forcer un démontage à l'aide du `--use-umountof` peut provoquer un comportement inattendu ou une panne des processus ou services utilisant le volume.

```
root@Storage-180:~ # sn-unmount-volume --use-umountof
/var/local/rangedb/2
Unmounting /var/local/rangedb/2 using umountof
/var/local/rangedb/2 is unmounted.
Informing LDR service of changes to storage volumes
```

Restaurez des volumes de stockage défaillants et reconstruisez la base de données Cassandra

Vous devez exécuter un script qui reformate et remonte le stockage sur les volumes de stockage défaillants, puis rereconstruit la base de données Cassandra sur le nœud de stockage si le système détermine qu'elle est nécessaire.

Avant de commencer

- Vous avez le `Passwords.txt` fichier.
- Les lecteurs système du serveur sont intacts.
- La cause de la défaillance a été identifiée et, si nécessaire, le matériel de stockage de remplacement a déjà été acquis.
- La taille totale du stockage de remplacement est la même que celle de l'original.
- Vous avez vérifié qu'une mise hors service du nœud de stockage n'est pas en cours ou que vous avez interrompu la procédure de mise hors service du nœud. (Dans le Gestionnaire de grille, sélectionnez **MAINTENANCE** > **tâches** > **désaffectation**.)

- Vous avez vérifié qu'une extension n'est pas en cours. (Dans le Gestionnaire de grille, sélectionnez **MAINTENANCE** > **tâches** > **expansion**.)
- Vous avez "vérifié les avertissements concernant la restauration du volume de stockage".

Étapes

1. Si nécessaire, remplacez le stockage physique ou virtuel défectueux associé aux volumes de stockage défectueux que vous avez identifiés et démontés précédemment.

   Ne remontez pas les volumes lors de cette étape. Le stockage est remonté et ajouté à `/etc/fstab` dans une étape ultérieure.

2. Dans le Gestionnaire de grille, accédez à **NODES** > **`appliance Storage Node`** > **matériel**. Dans la section dispositif StorageGRID de la page, vérifiez que le mode RAID de stockage fonctionne correctement.
3. Connectez-vous au noeud de stockage défaillant :
   a. Saisissez la commande suivante : `ssh admin@grid_node_IP`
   b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
   c. Entrez la commande suivante pour passer à la racine : `su -`
   d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

      Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

4. Utilisez un éditeur de texte (vi ou vim) pour supprimer les volumes ayant échoué du `/etc/fstab` puis enregistrez le fichier.

   > Ajout d'un commentaire sur un volume en panne dans le `/etc/fstab` le fichier est insuffisant. Le volume doit être supprimé de `fstab` pendant que le processus de récupération vérifie que toutes les lignes de l' `fstab` les fichiers correspondent aux systèmes de fichiers montés.

5. Reformatez les volumes de stockage défaillants et reconstruisez la base de données Cassandra si nécessaire. Entrez : `reformat_storage_block_devices.rb`
   - Lorsque le volume de stockage 0 est démonté, des invites et des messages indiquent que le service Cassandra est en cours d'arrêt.
   - Si nécessaire, vous serez invité à reconstruire la base de données Cassandra.
     - Examinez les avertissements. Si aucune d'entre elles ne s'applique, reconstruisez la base de données Cassandra. Saisissez : **y**
     - Si plus d'un nœud de stockage est hors ligne ou si un autre nœud de stockage a été reconstruit au cours des 15 derniers jours. Saisissez : **n**

       Le script s'quittera sans reconstruire Cassandra. Contactez l'assistance technique.
   - Pour chaque lecteur de rancedb sur le nœud de stockage, lorsque vous êtes invité à : `Reformat the rangedb drive <name> (device <major number>:<minor number>)? [y/n]?`, entrez l'une des réponses suivantes :
     - **y** pour reformater un lecteur qui a eu des erreurs. Cette opération reformate le volume de stockage et ajoute le volume de stockage reformaté à la `/etc/fstab` fichier.

- **n** si le lecteur ne contient aucune erreur et que vous ne voulez pas le reformater.

> La sélection de **n** ferme le script. Montez le lecteur (si vous pensez que les données du lecteur doivent être conservées et que le lecteur a été démonté par erreur) ou retirez le lecteur. Ensuite, exécutez le `reformat_storage_block_devices.rb` commande de nouveau.

> Certaines procédures de restauration StorageGRID utilisent Reaper pour traiter les réparations Cassandra. Les réparations sont effectuées automatiquement dès que les services connexes ou requis ont commencé. Vous remarquerez peut-être des résultats de script mentionnant « couche » ou « réparation Cassandra ». Si un message d'erreur indiquant que la réparation a échoué, exécutez la commande indiquée dans le message d'erreur.

Dans l'exemple de sortie suivant, le lecteur `/dev/sdf` Reformaté. Cassandra n'a pas besoin d'être reconstruite :

```
root@DC1-S1:~ # reformat_storage_block_devices.rb
Formatting devices that are not in use...
Skipping in use device /dev/sdc
Skipping in use device /dev/sdd
Skipping in use device /dev/sde
Reformat the rangedb drive /dev/sdf (device 8:64)? [Y/n]? y
Successfully formatted /dev/sdf with UUID b951bfcb-4804-41ad-b490-
805dfd8df16c
All devices processed
Running: /usr/local/ldr/setup_rangedb.sh 12368435
Cassandra does not need rebuilding.
Starting services.
Informing storage services of new volume

Reformatting done.  Now do manual steps to
restore copies of data.
```

Une fois les volumes de stockage reformatés et remontés et les opérations Cassandra nécessaires terminées, vous pouvez le faire "Restaurez les données d'objet à l'aide de Grid Manager".

Restaurez les données d'objet vers le volume de stockage sur lequel le disque système est intact

Après avoir restauré un volume de stockage sur un nœud de stockage sur lequel le disque système est intact, vous pouvez restaurer les données d'objet répliquées ou avec code d'effacement qui ont été perdues en cas de défaillance du volume de stockage.

Quelle procédure dois-je utiliser ?

Dans la mesure du possible, restaurez les données d'objet à l'aide de la page **Restauration de volume** du gestionnaire de grille.

- Si les volumes sont répertoriés sous **MAINTENANCE** > **Restauration de volume** > **nœuds à restaurer**, restaurez les données d'objet à l'aide de l' "Page de restauration de volume dans le Gestionnaire de grille".
- Si les volumes ne sont pas répertoriés dans **MAINTENANCE** > **Restauration du volume** > **nœuds à restaurer**, suivez les étapes ci-dessous pour utiliser le `repair-data` script de restauration des données d'objet.

  Si le nœud de stockage restauré contient moins de volumes que le nœud qu'il remplace, vous devez utiliser le `repair-data` script.

Utilisez le `repair-data` script de restauration des données d'objet

Avant de commencer

- Vous devez avoir confirmé que le noeud de stockage récupéré possède un état de connexion * connecté* Dans l'onglet **NODES** > **Présentation** du Gestionnaire de grille.

Description de la tâche

Les données d'objet peuvent être restaurées depuis d'autres nœuds de stockage, un nœud d'archivage ou un pool de stockage cloud, en supposant que les règles ILM de la grille soient configurées de manière à ce que les copies d'objet soient disponibles.

Notez ce qui suit :

- Si une règle ILM a été configurée pour stocker une seule copie répliquée, et que cette copie existait sur un volume de stockage défaillant, vous ne pourrez pas restaurer l'objet.
- Si la seule copie restante d'un objet se trouve dans un pool de stockage cloud, StorageGRID doit émettre plusieurs demandes vers le terminal de pool de stockage cloud pour restaurer les données d'objet. Avant d'effectuer cette procédure, contactez le support technique pour obtenir de l'aide pour estimer le délai de restauration et les coûts associés.
- Si la seule copie restante d'un objet se trouve sur un noeud d'archivage, les données d'objet sont extraites du noeud d'archivage. La restauration de données d'objet sur un nœud de stockage à partir d'un nœud d'archivage prend plus de temps que la restauration de copies à partir d'autres nœuds de stockage en raison de la latence associée aux récupérations à partir de systèmes de stockage d'archives externes.

À propos du `repair-data` script

Pour restaurer les données d'objet, exécutez le `repair-data` script. Ce script commence le processus de restauration des données d'objet et fonctionne avec l'analyse ILM pour s'assurer que les règles ILM sont respectées.

Sélectionnez **données répliquées** ou **données codées par effacement (EC)** ci-dessous pour apprendre les différentes options du `repair-data` script, basé sur la restauration des données répliquées ou des données avec code d'effacement. Si vous devez restaurer les deux types de données, vous devez exécuter les deux ensembles de commandes.

> Pour plus d'informations sur le `repair-data` script, entrez `repair-data --help` Dans la ligne de commande du nœud d'administration principal.

Les données répliquées

Deux commandes sont disponibles pour la restauration des données répliquées, et ce, selon que vous devez réparer le nœud entier ou uniquement certains volumes sur le nœud :

```
repair-data start-replicated-node-repair

repair-data start-replicated-volume-repair
```

Vous pouvez suivre les réparations des données répliquées avec cette commande :

```
repair-data show-replicated-repair-status
```

Données avec code d'effacement (EC)

Deux commandes sont disponibles pour la restauration des données avec code d'effacement, selon que vous devez réparer le nœud entier ou uniquement certains volumes sur le nœud :

```
repair-data start-ec-node-repair

repair-data start-ec-volume-repair
```

Vous pouvez suivre les réparations des données codées par effacement à l'aide de cette commande :

```
repair-data show-ec-repair-status
```

> Les réparations des données codées peuvent commencer alors que certains nœuds de stockage sont hors ligne. Toutefois, si toutes les données avec code d'effacement ne peuvent pas être prises en compte, la réparation ne peut pas être effectuée. La réparation s'effectuera une fois que tous les nœuds sont disponibles.

> Le travail de réparation EC réserve temporairement une grande quantité de stockage. Les alertes de stockage peuvent être déclenchées, mais elles seront résolus une fois la réparation terminée. S'il n'y a pas assez de stockage pour la réservation, la tâche de réparation EC échouera. Les réservations de stockage sont libérées lorsque la tâche de réparation EC est terminée, que la tâche ait échoué ou a réussi.

Rechercher le nom d'hôte pour le noeud de stockage

1. Connectez-vous au nœud d'administration principal :
   a. Saisissez la commande suivante : `ssh admin@primary_Admin_Node_IP`
   b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
   c. Entrez la commande suivante pour passer à la racine : `su -`
   d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

   Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

2. Utilisez le `/etc/hosts` Fichier pour trouver le nom d'hôte du noeud de stockage pour les volumes de stockage restaurés. Pour afficher la liste de tous les nœuds de la grille, saisissez les éléments suivants : `cat /etc/hosts`.

Réparez les données si tous les volumes ont échoué

Si tous les volumes de stockage sont en panne, réparez l'intégralité du nœud. Suivez les instructions pour les données **répliquées**, **codées par effacement (EC)**, ou les deux, selon que vous utilisez ou non des données répliquées, des données codées par effacement (EC), ou les deux.

Si seuls certains volumes ont échoué, accédez à Réparer les données si seulement certains volumes ont échoué.

> Vous ne pouvez pas courir `repair-data` opérations simultanément pour plusieurs nœuds. Pour restaurer plusieurs nœuds, contactez le support technique.

Les données répliquées

Si votre grid inclut des données répliquées, utilisez le `repair-data start-replicated-node-repair` commande avec `--nodes` option, où `--nodes` Est le nom d'hôte (nom du système), pour réparer la totalité du nœud de stockage.

Cette commande répare les données répliquées sur un nœud de stockage nommé SG-DC-SN3 :

```
repair-data start-replicated-node-repair --nodes SG-DC-SN3
```

> Lorsque les données d'objet sont restaurées, l'alerte **objets perdus** est déclenchée si le système StorageGRID ne peut pas localiser les données d'objet répliquées. Des alertes peuvent être déclenchées sur les nœuds de stockage dans le système. Vous devez déterminer la cause de la perte et si la récupération est possible. Voir "Rechercher les objets perdus".

Données avec code d'effacement (EC)

Si votre grid contient des données avec code d'effacement, utilisez la `repair-data start-ec-node-repair` commande avec `--nodes` option, où `--nodes` Est le nom d'hôte (nom du système), pour réparer la totalité du nœud de stockage.

Cette commande répare les données codées de l'effacement sur un nœud de stockage appelé SG-DC-SN3 :

```
repair-data start-ec-node-repair --nodes SG-DC-SN3
```

L'opération renvoie un seul `repair ID` qui l'identifie `repair_data` fonctionnement. Utilisez-le `repair ID` pour suivre la progression et le résultat du `repair_data` fonctionnement. Aucun autre retour n'est renvoyé à la fin du processus de récupération.

> Les réparations des données codées peuvent commencer alors que certains nœuds de stockage sont hors ligne. La réparation s'effectuera une fois que tous les nœuds sont disponibles.

Réparer les données si seulement certains volumes ont échoué

Si seulement certains volumes ont échoué, réparez les volumes affectés. Suivez les instructions pour les données **répliquées**, **codées par effacement (EC)**, ou les deux, selon que vous utilisez ou non des données répliquées, des données codées par effacement (EC), ou les deux.

Si tous les volumes ont échoué, accédez à Réparez les données si tous les volumes ont échoué.

Saisissez les ID de volume en hexadécimal. Par exemple : `0000` est le premier volume et `000F` est le seizième volume. Vous pouvez spécifier un volume, une plage de volumes ou plusieurs volumes qui ne sont pas dans une séquence.

Tous les volumes doivent se trouver sur le même nœud de stockage. Si vous devez restaurer des volumes pour plusieurs nœuds de stockage, contactez le support technique.

Les données répliquées

Si votre grid contient des données répliquées, utilisez le `start-replicated-volume-repair` commande avec `--nodes` option permettant d'identifier le nœud (où `--nodes` est le nom d'hôte du nœud). Ajoutez ensuite l'une ou l'autre des `--volumes` ou `--volume-range` comme indiqué dans les exemples suivants.

Volume unique : cette commande restaure les données répliquées vers le volume `0002` Sur un nœud de stockage nommé SG-DC-SN3 :

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volumes 0002
```

Plage de volumes : cette commande restaure les données répliquées vers tous les volumes de la plage `0003` à `0009` Sur un nœud de stockage nommé SG-DC-SN3 :

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volume-range
0003,0009
```

Volumes multiples non compris dans une séquence : cette commande restaure les données répliquées vers des volumes `0001`, `0005`, et `0008` Sur un nœud de stockage nommé SG-DC-SN3 :

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volumes
0001,0005,0008
```

> Lorsque les données d'objet sont restaurées, l'alerte **objets perdus** est déclenchée si le système StorageGRID ne peut pas localiser les données d'objet répliquées. Des alertes peuvent être déclenchées sur les nœuds de stockage dans le système. Notez la description de l'alerte et les actions recommandées pour déterminer la cause de la perte et si la récupération est possible.

Données avec code d'effacement (EC)

Si votre grid contient des données avec code d'effacement, utilisez la `start-ec-volume-repair` commande avec `--nodes` option permettant d'identifier le nœud (où `--nodes` est le nom d'hôte du nœud). Ajoutez ensuite l'une ou l'autre des `--volumes` ou `--volume-range` comme indiqué dans les exemples suivants.

Volume unique : cette commande restaure les données codées par effacement dans un volume `0007` Sur un nœud de stockage nommé SG-DC-SN3 :

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 0007
```

Plage de volumes : cette commande restaure les données avec code d'effacement sur tous les volumes de la plage `0004` à `0006` Sur un nœud de stockage nommé SG-DC-SN3 :

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volume-range 0004,0006
```

Plusieurs volumes non dans une séquence : cette commande restaure les données codées par effacement dans des volumes `000A`, `000C`, et `000E` Sur un nœud de stockage nommé SG-DC-SN3 :

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 000A,000C,000E
```

Le `repair-data` l'opération renvoie un seul `repair ID` qui l'identifie `repair_data` fonctionnement.

Utilisez-le `repair ID` pour suivre la progression et le résultat du `repair_data` fonctionnement. Aucun autre retour n'est renvoyé à la fin du processus de récupération.

> Les réparations des données codées peuvent commencer alors que certains nœuds de stockage sont hors ligne. La réparation s'effectuera une fois que tous les nœuds sont disponibles.

Surveiller les réparations

Surveiller l'état des travaux de réparation, en fonction de l'utilisation ou non des données **répliquées**, **données codées par effacement (EC)**, ou des deux.

Vous pouvez également surveiller l'état des travaux de restauration de volume en cours et afficher un historique des travaux de restauration effectués dans"Gestionnaire de grille".

Les données répliquées

- Pour obtenir une estimation du pourcentage d'achèvement de la réparation répliquée, ajoutez le `show-replicated-repair-status` option de la commande repair-data.

  ```
  repair-data show-replicated-repair-status
  ```

- Pour déterminer si les réparations sont terminées :
  a. Sélectionnez **NŒUDS** > ***nœud de stockage en cours de réparation*** > **ILM**.
  b. Vérifiez les attributs dans la section évaluation. Lorsque les réparations sont terminées, l'attribut **attente - tous** indique 0 objets.
- Pour surveiller la réparation plus en détail :
  a. Sélectionnez **SUPPORT** > **Outils** > **topologie de grille**.
  b. Sélectionnez ***GRID*** > ***Storage Node en cours de réparation*** > **LDR** > **Data Store**.
  c. Utilisez une combinaison des attributs suivants pour déterminer, autant que possible, si les réparations répliquées sont terminées.

  > Cassandra présente peut-être des incohérences et les réparations échouées ne sont pas suivies.

  - **Réparations tentées (XRPA)** : utilisez cet attribut pour suivre la progression des réparations répliquées. Cet attribut augmente chaque fois qu'un nœud de stockage tente de réparer un objet à haut risque. Lorsque cet attribut n'augmente pas pendant une période plus longue que la période d'acquisition actuelle (fournie par l'attribut **période d'analyse — estimation**), cela signifie que l'analyse ILM n'a trouvé aucun objet à haut risque qui doit être réparé sur n'importe quel nœud.

    > Les objets à haut risque sont des objets qui risquent d'être complètement perdus. Cela n'inclut pas les objets qui ne répondent pas à leur configuration ILM.

  - **Période d'acquisition — estimée (XSCM)** : utilisez cet attribut pour estimer quand une modification de règle sera appliquée aux objets précédemment ingérés. Si l'attribut **réparations tentées** n'augmente pas pendant une période supérieure à la période d'acquisition actuelle, il est probable que les réparations répliquées soient effectuées. Notez que la période d'acquisition peut changer. L'attribut **période d'acquisition — estimée (XSCM)** s'applique à la grille entière et est le maximum de toutes les périodes d'acquisition de nœud. Vous pouvez interroger l'historique d'attributs **période de balayage — estimation** de la grille pour déterminer une période appropriée.

Données avec code d'effacement (EC)

Pour surveiller la réparation des données codées d'effacement et réessayer toute demande qui pourrait avoir échoué :

1. Déterminez l'état des réparations des données par code d'effacement :
   - Sélectionnez **SUPPORT** > **Tools** > **Metrics** pour afficher le temps de réalisation estimé et le pourcentage de réalisation de la tâche en cours. Sélectionnez ensuite **EC Overview** dans la section Grafana. Examinez les tableaux de bord **Grid EC Job estimé Time to Completion** et **Grid EC Job Percentage Finted**.

- Utilisez cette commande pour afficher le statut d'un spécifique `repair-data` fonctionnement :

  ```
  repair-data show-ec-repair-status --repair-id repair ID
  ```

- Utilisez cette commande pour lister toutes les réparations :

  ```
  repair-data show-ec-repair-status
  ```

Les informations de sortie sont affichées, notamment `repair ID`, pour toutes les réparations précédentes et en cours.

2. Si le résultat indique que l'opération de réparation a échoué, utilisez le `--repair-id` option permettant de réessayer la réparation.

   Cette commande relance une réparation de nœud ayant échoué à l'aide de l'ID de réparation 6949309319275667690 :

   ```
   repair-data start-ec-node-repair --repair-id 6949309319275667690
   ```

   Cette commande relance une réparation de volume en échec à l'aide de l'ID de réparation 6949309319275667690 :

   ```
   repair-data start-ec-volume-repair --repair-id 6949309319275667690
   ```

Vérifier l'état du stockage après la récupération des volumes de stockage

Après la récupération des volumes de stockage, vous devez vérifier que l'état souhaité du noeud de stockage est défini sur en ligne et vous assurer que l'état sera en ligne par défaut à chaque redémarrage du serveur du noeud de stockage.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Le nœud de stockage a été restauré et la restauration des données est terminée.

Étapes

1. Sélectionnez **SUPPORT** > **Outils** > **topologie de grille**.
2. Vérifiez les valeurs de **nœud de stockage récupéré** > **LDR** > **Storage** > **Storage State de stockage — désiré** et **Storage State — Current**.

   La valeur des deux attributs doit être en ligne.

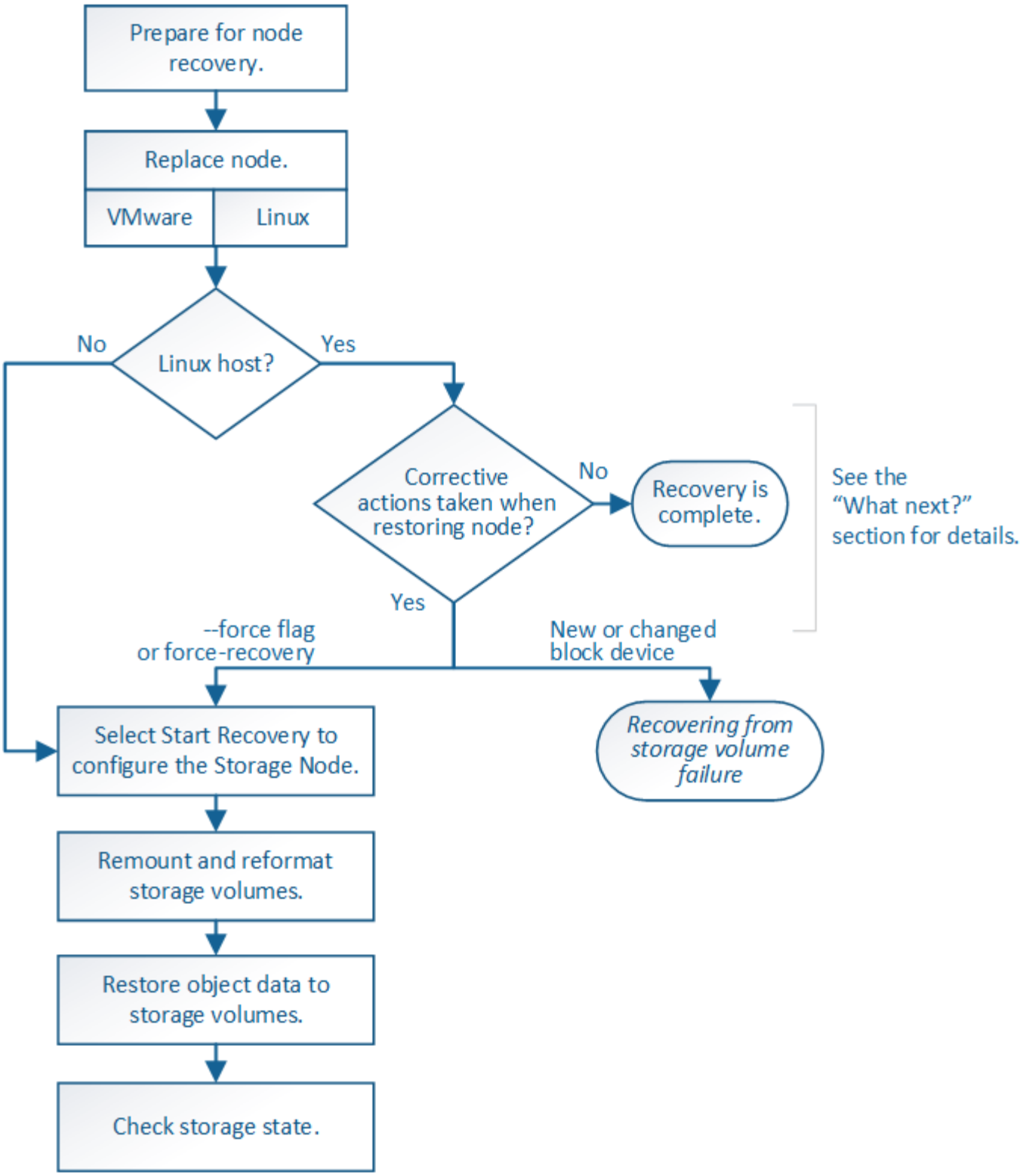
3. Si l'état de stockage — souhaité est défini sur lecture seule, procédez comme suit :
   a. Cliquez sur l'onglet **Configuration**.
   b. Dans la liste déroulante **État de stockage — désiré**, sélectionnez **en ligne**.
   c. Cliquez sur **appliquer les modifications**.
   d. Cliquez sur l'onglet **Présentation** et confirmez que les valeurs de **État de stockage — désiré** et **État de stockage — actuel** sont mises à jour en ligne.

Restauration après une panne de disque système : workflow

Si le lecteur système d'un nœud de stockage logiciel est défectueux, le nœud de stockage n'est pas disponible pour le système StorageGRID. Vous devez effectuer un ensemble spécifique de tâches pour effectuer une restauration en cas de panne de disque système.

Utilisez cette procédure pour effectuer une restauration après une panne de lecteur système sur un nœud de stockage logiciel. Cette procédure comprend les étapes à suivre si des volumes de stockage sont également défaillants ou ne peuvent pas être remontés.

> Cette procédure s'applique uniquement aux nœuds de stockage basés sur logiciel. Vous devez suivre une procédure différente de "Restaurez un nœud de stockage d'appliance".



Consultez les avertissements relatifs à la restauration du lecteur système du nœud de stockage

Avant de restaurer un lecteur système en panne d'un nœud de stockage, consultez la section général"avertissements et remarques concernant la restauration d'un nœud grid" et les avertissements spécifiques suivants.

Les nœuds de stockage disposent d'une base de données Cassandra qui inclut les métadonnées d'objet. La base de données Cassandra peut être reconstruite dans les cas suivants :

- Un nœud de stockage est remis en ligne après avoir été hors ligne pendant plus de 15 jours.
- Un volume de stockage a échoué et a été récupéré.
- Le lecteur système et un ou plusieurs volumes de stockage sont défectueux et restaurés.

Lorsque Cassandra est reconstruite, le système utilise les informations d'autres nœuds de stockage. Si trop de nœuds de stockage sont hors ligne, il se peut que certaines données Cassandra ne soient pas disponibles. Si Cassandra a été récemment reconstruite, les données Cassandra ne peuvent pas encore être cohérentes sur l'ensemble de la grille. Cette perte peut se produire si Cassandra est reconstruite lorsque trop de nœuds de stockage sont hors ligne ou si deux nœuds de stockage ou plus sont reconstruites dans les 15 jours restants.

Si plusieurs nœuds de stockage ont échoué (ou sont hors ligne), contactez le support technique. N'effectuez pas la procédure de récupération suivante. Des données peuvent être perdues.

S'il s'agit de la défaillance du deuxième nœud de stockage dans les 15 jours qui suivent la défaillance ou la restauration d'un nœud de stockage, contactez le support technique. Reconstruire Cassandra sur deux nœuds de stockage ou plus en un délai de 15 jours peut entraîner une perte de données.

Si plusieurs nœuds de stockage d'un site ont échoué, une procédure de restauration de site peut être nécessaire. Voir "Comment la reprise sur site est effectuée par le support technique".

Si ce nœud de stockage est en mode de maintenance en lecture seule pour permettre la récupération d'objets par un autre nœud de stockage avec des volumes de stockage défaillants, récupérez les volumes du nœud de stockage avec des volumes de stockage défaillants avant de récupérer ce noeud de stockage défaillant. Voir les instructions à "effectuez des restaurations après une panne du volume de stockage, là où le disque système est intact".

Si les règles ILM sont configurées pour ne stocker qu'une seule copie répliquée, et si cette copie existe sur un volume de stockage défaillant, vous ne pourrez pas restaurer l'objet.

Si vous rencontrez une alarme Services: Status - Cassandra (SVST) pendant la récupération, reportez-vous à la section "Restaurez des volumes de stockage défaillants et reconstruisez la base de données Cassandra". Après la reconstruction de Cassandra, les alarmes doivent être désactivées. Si les alarmes ne s'effacent pas, contactez le support technique.

Remplacez le nœud de stockage

Si le lecteur du système est défectueux, vous devez d'abord remplacer le nœud de stockage.

Vous devez sélectionner la procédure de remplacement de nœuds pour votre plate-forme. Les étapes à suivre pour remplacer un nœud sont les mêmes pour tous les types de nœuds de la grille.

Cette procédure s'applique uniquement aux nœuds de stockage basés sur logiciel. Vous devez suivre une procédure différente de "Restaurez un nœud de stockage d'appliance".

Linux: si vous n'êtes pas sûr que votre lecteur système est en panne, suivez les instructions pour remplacer le nœud afin de déterminer les étapes de récupération requises.

Plateforme	Procédure
VMware	"Remplacement d'un noeud VMware"
Linux	"Remplacer un noeud Linux"
OpenStack	Les fichiers et scripts de disques de machine virtuelle fournis par NetApp pour OpenStack ne sont plus pris en charge pour les opérations de restauration. Si vous devez restaurer un nœud exécuté dans un déploiement OpenStack, téléchargez les fichiers du système d'exploitation Linux. Suivre ensuite la procédure pour "Remplacement d'un nœud Linux".

Sélectionnez Démarrer la restauration pour configurer le nœud de stockage

Après avoir remplacé un noeud de stockage, vous devez sélectionner Démarrer la restauration dans Grid Manager pour configurer le nouveau noeud en remplacement du noeud défaillant.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous disposez de l'autorisation Maintenance ou accès racine.
- Vous avez la phrase secrète pour le provisionnement.
- Vous avez déployé et configuré le nœud de remplacement.
- Vous disposez de la date de début des travaux de réparation pour les données avec code d'effacement.
- Vous avez vérifié que le nœud de stockage n'a pas été reconstruit au cours des 15 derniers jours.

Description de la tâche

Si le nœud de stockage est installé en tant que conteneur sur un hôte Linux, vous devez effectuer cette étape uniquement si l'un d'entre eux est vrai :

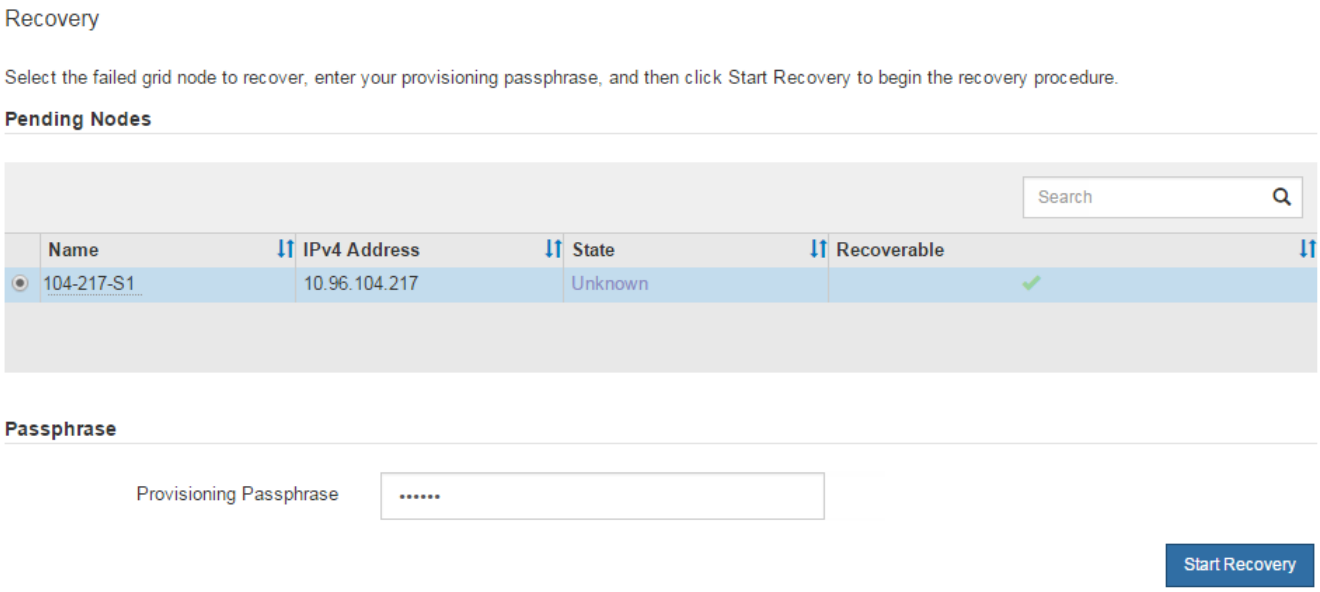
- Il fallait utiliser le `--force` indicateur pour importer le nœud, ou vous avez émis `storagegrid node force-recovery` *`node-name`*
- Vous deviez réinstaller un nœud complet ou restaurer /var/local.

Étapes

1. Dans le Gestionnaire de grille, sélectionnez **MAINTENANCE** > **tâches** > **récupération**.
2. Sélectionnez le nœud de grille à récupérer dans la liste nœuds en attente.

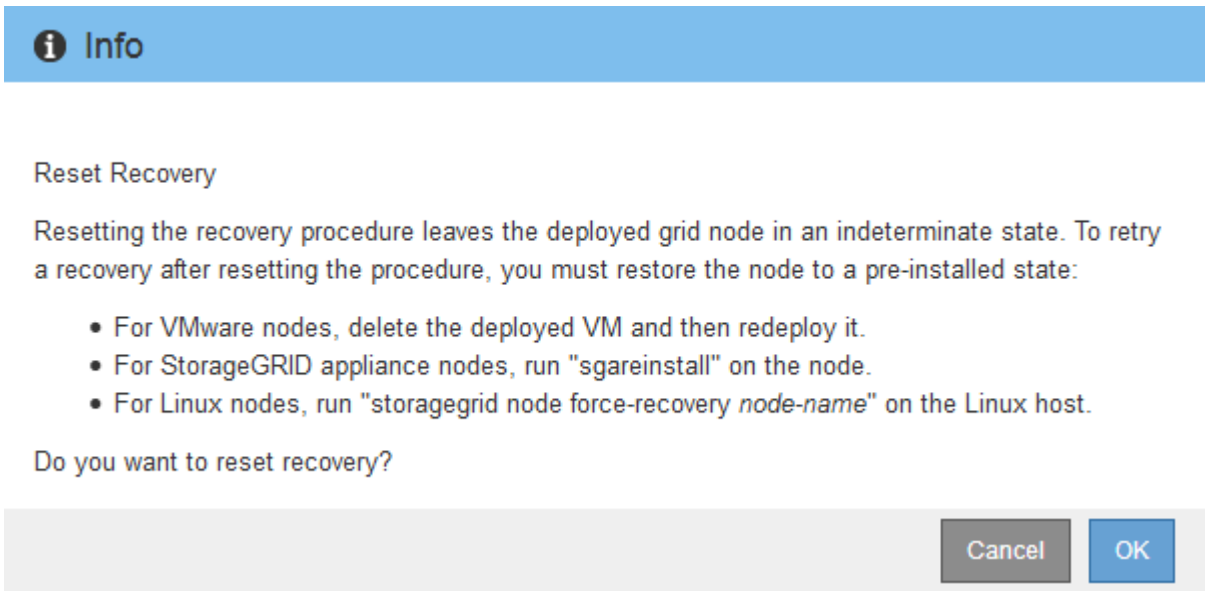
   Les nœuds apparaissent dans la liste après leur échec, mais vous ne pouvez pas sélectionner un nœud tant qu'il n'a pas été réinstallé et qu'il est prêt pour la restauration.

3. Saisissez la phrase de passe de provisionnement *.
4. Cliquez sur **Démarrer la récupération**.



5. Surveiller la progression de la récupération dans le tableau de noeuds de grille de récupération.

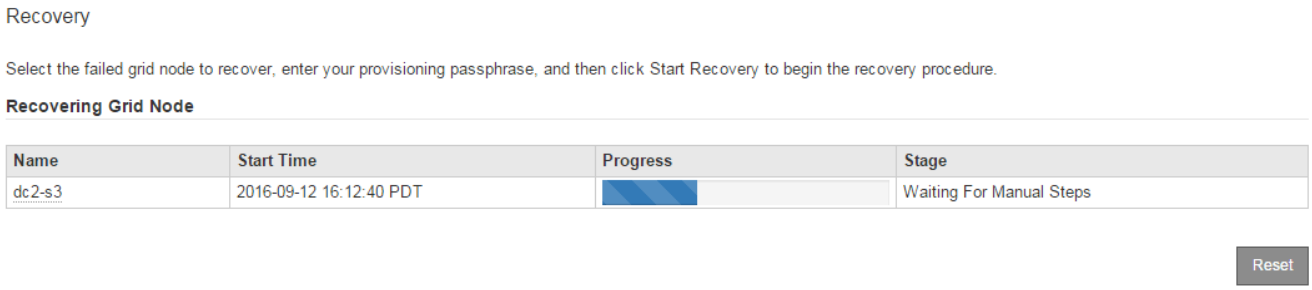
> Pendant l'exécution de la procédure de récupération, vous pouvez cliquer sur **Réinitialiser** pour lancer une nouvelle restauration. Une boîte de dialogue s'affiche, indiquant que le nœud restera dans un état indéterminé si vous réinitialisez la procédure.



Si vous souhaitez relancer la restauration après avoir réinitialisé la procédure, vous devez restaurer l'état pré-installé du nœud, comme suit :

- **VMware** : supprimez le nœud de grille virtuelle déployé. Ensuite, lorsque vous êtes prêt à redémarrer la restauration, redéployez le nœud.
- **Linux** : redémarrez le nœud en exécutant cette commande sur l'hôte Linux : `storagegrid node force-recovery node-name`

6. Lorsque le nœud de stockage atteint l'étape « en attente d'étapes manuelles », passer à "Remontage et reformatage des volumes de stockage (étapes manuelles)".



Remontage et reformatage des volumes de stockage (étapes manuelles)

Vous devez exécuter manuellement deux scripts pour remonter les volumes de stockage conservés et reformater les volumes de stockage défaillants. Le premier script monte les volumes au format approprié en tant que volumes de stockage StorageGRID. Le deuxième script reformate tous les volumes démontés, reconstruit Cassandra si nécessaire et démarre les services.

Avant de commencer

- Vous avez déjà remplacé le matériel de tous les volumes de stockage défectueux que vous savez avoir besoin d'être remplacé.

  Exécution du `sn-remount-volumes` un script peut vous aider à identifier d'autres volumes de stockage ayant échoué.

- Vous avez vérifié qu'une mise hors service du nœud de stockage n'est pas en cours ou que vous avez interrompu la procédure de mise hors service du nœud. (Dans le Gestionnaire de grille, sélectionnez **MAINTENANCE** > **tâches** > **désaffectation**.)
- Vous avez vérifié qu'une extension n'est pas en cours. (Dans le Gestionnaire de grille, sélectionnez **MAINTENANCE** > **tâches** > **expansion**.)
- Vous avez "Consultez les avertissements relatifs à la restauration du lecteur du système du nœud de stockage".

> Si plus d'un nœud de stockage est hors ligne ou si un nœud de stockage de cette grille a été reconstruit au cours des 15 derniers jours, contactez le support technique. N'exécutez pas le `sn-recovery-postinstall.sh` script. Reconstruire Cassandra sur deux nœuds de stockage ou plus dans les 15 jours suivant l'arrêt du service peut entraîner une perte de données.

Description de la tâche

Pour effectuer cette procédure, vous devez effectuer les tâches de haut niveau suivantes :

- Connectez-vous au nœud de stockage récupéré.
- Exécutez le `sn-remount-volumes` script pour remonter les volumes de stockage correctement formatés. Lorsque ce script s'exécute, il effectue les opérations suivantes :
  - Monte et démonte chaque volume de stockage pour relire le journal XFS.
  - Effectue une vérification de cohérence de fichier XFS.
  - Si le système de fichiers est cohérent, détermine si le volume de stockage est un volume de stockage StorageGRID correctement formaté.

- Si le volume de stockage est correctement formaté, remonter le volume de stockage. Toutes les données existantes du volume restent intactes.

- Examinez la sortie du script et résolvez tout problème.
- Exécutez le `sn-recovery-postinstall.sh` script. Lorsque ce script s'exécute, il effectue les opérations suivantes :

> Ne redémarrez pas un nœud de stockage pendant la restauration avant l'exécution `sn-recovery-postinstall.sh` pour reformater les volumes de stockage défaillants et restaurer les métadonnées de l'objet. Redémarrage du nœud de stockage avant `sn-recovery-postinstall.sh` La solution complète provoque des erreurs sur les services qui tentent de démarrer et entraîne la sortie des nœuds d'appliance StorageGRID en mode de maintenance. Voir l'étape pour script post-installation.

  - Reformate tous les volumes de stockage du `sn-remount-volumes` le script n'a pas pu être monté ou a été mal formaté.

> Lorsqu'un volume de stockage est reformaté, toutes les données de ce volume sont perdues. Vous devez effectuer une procédure supplémentaire pour restaurer les données d'objet à partir d'autres emplacements de la grille, en supposant que les règles ILM ont été configurées pour stocker plusieurs copies d'objet.

  - Reconstruit la base de données Cassandra sur le nœud, si nécessaire.
  - Démarre les services sur le nœud de stockage.

Étapes

1. Connectez-vous au nœud de stockage récupéré :
   a. Saisissez la commande suivante : `ssh admin@grid_node_IP`
   b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
   c. Entrez la commande suivante pour passer à la racine : `su -`
   d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

   Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

2. Exécutez le premier script pour remonter tous les volumes de stockage correctement formatés.

> Si tous les volumes de stockage sont nouveaux et doivent être formatés, ou si tous les volumes de stockage ont échoué, vous pouvez ignorer cette étape et exécuter le deuxième script pour reformater tous les volumes de stockage démontés.

   a. Exécutez le script : `sn-remount-volumes`

      Ce script peut prendre des heures sur les volumes de stockage qui contiennent des données.

   b. Au fur et à mesure de l'exécution du script, vérifiez le résultat et répondez aux invites.

Si nécessaire, vous pouvez utiliser le `tail -f` commande permettant de contrôler le contenu du fichier journal du script (`/var/local/log/sn-remount-volumes.log`). Le fichier journal contient des informations plus détaillées que la sortie de la ligne de commande.

```
root@SG:~ # sn-remount-volumes
The configured LDR noid is 12632740

====== Device /dev/sdb ======
Mount and unmount device /dev/sdb and checking file system
consistency:
The device is consistent.
Check rangedb structure on device /dev/sdb:
Mount device /dev/sdb to /tmp/sdb-654321 with rangedb mount options
This device has all rangedb directories.
Found LDR node id 12632740, volume number 0 in the volID file
Attempting to remount /dev/sdb
Device /dev/sdb remounted successfully

====== Device /dev/sdc ======
Mount and unmount device /dev/sdc and checking file system
consistency:
Error: File system consistency check retry failed on device /dev/sdc.
You can see the diagnosis information in the /var/local/log/sn-
remount-volumes.log.

This volume could be new or damaged. If you run sn-recovery-
postinstall.sh,
this volume and any data on this volume will be deleted. If you only
had two
copies of object data, you will temporarily have only a single copy.
StorageGRID Webscale will attempt to restore data redundancy by
making
additional replicated copies or EC fragments, according to the rules
in
the active ILM policy.

Don't continue to the next step if you believe that the data
remaining on
this volume can't be rebuilt from elsewhere in the grid (for example,
if
your ILM policy uses a rule that makes only one copy or if volumes
have
failed on multiple nodes). Instead, contact support to determine how
to
recover your data.
```

```
====== Device /dev/sdd ======
Mount and unmount device /dev/sdd and checking file system
consistency:
Failed to mount device /dev/sdd
This device could be an uninitialized disk or has corrupted
superblock.
File system check might take a long time. Do you want to continue? (y
or n) [y/N]? y

Error: File system consistency check retry failed on device /dev/sdd.
You can see the diagnosis information in the /var/local/log/sn-
remount-volumes.log.

This volume could be new or damaged. If you run sn-recovery-
postinstall.sh,
this volume and any data on this volume will be deleted. If you only
had two
copies of object data, you will temporarily have only a single copy.
StorageGRID Webscale will attempt to restore data redundancy by
making
additional replicated copies or EC fragments, according to the rules
in
the active ILM policy.

Don't continue to the next step if you believe that the data
remaining on
this volume can't be rebuilt from elsewhere in the grid (for example,
if
your ILM policy uses a rule that makes only one copy or if volumes
have
failed on multiple nodes). Instead, contact support to determine how
to
recover your data.

====== Device /dev/sde ======
Mount and unmount device /dev/sde and checking file system
consistency:
The device is consistent.
Check rangedb structure on device /dev/sde:
Mount device /dev/sde to /tmp/sde-654321 with rangedb mount options
This device has all rangedb directories.
Found LDR node id 12000078, volume number 9 in the volID file
Error: This volume does not belong to this node. Fix the attached
volume and re-run this script.
```

Dans l'exemple de sortie, un volume de stockage a été remonté avec succès et trois volumes de stockage ont rencontré des erreurs.

- `/dev/sdb` La vérification de cohérence du système de fichiers XFS a été effectuée et une structure de volume valide a été correctement remontée. Les données sur les périphériques remontés par le script sont conservées.
- `/dev/sdc` Echec de la vérification de cohérence du système de fichiers XFS car le volume de stockage était nouveau ou corrompu.
- `/dev/sdd` impossible de monter car le disque n'a pas été initialisé ou le superbloc du disque a été corrompu. Lorsque le script ne peut pas monter un volume de stockage, il vous demande si vous souhaitez exécuter le contrôle de cohérence du système de fichiers.
  - Si le volume de stockage est relié à un nouveau disque, répondez **N** à l'invite. Vous n'avez pas besoin de vérifier le système de fichiers sur un nouveau disque.
  - Si le volume de stockage est relié à un disque existant, répondez **y** à l'invite. Vous pouvez utiliser les résultats de la vérification du système de fichiers pour déterminer la source de la corruption. Les résultats sont enregistrés dans le `/var/local/log/sn-remount-volumes.log` fichier journal.
- `/dev/sde` A réussi la vérification de cohérence du système de fichiers XFS et avait une structure de volume valide ; cependant, l'ID de nœud LDR du fichier volID ne correspond pas à l'ID de ce noeud de stockage (l' `configured LDR noid` affiché en haut). Ce message indique que ce volume appartient à un autre noeud de stockage.

3. Examinez la sortie du script et résolvez tout problème.

> Si un volume de stockage a échoué au contrôle de cohérence du système de fichiers XFS ou ne peut pas être monté, vérifiez attentivement les messages d'erreur dans la sortie. Vous devez comprendre les implications de l'exécution du `sn-recovery-postinstall.sh` créer des scripts sur ces volumes.

a. Vérifiez que les résultats incluent une entrée pour tous les volumes attendus. Si aucun volume n'est répertorié, exécutez à nouveau le script.

b. Consultez les messages de tous les périphériques montés. Assurez-vous qu'il n'y a pas d'erreur indiquant qu'un volume de stockage n'appartient pas à ce noeud de stockage.

   Dans l'exemple, la sortie de `/dev/sde` inclut le message d'erreur suivant :

```
Error: This volume does not belong to this node. Fix the attached
volume and re-run this script.
```

> Si un volume de stockage est signalé comme appartenant à un autre nœud de stockage, contactez le support technique. Si vous exécutez le `sn-recovery-postinstall.sh` script, le volume de stockage sera reformaté, ce qui peut entraîner une perte de données.

c. Si aucun périphérique de stockage n'a pu être monté, notez le nom du périphérique et réparez ou remplacez le périphérique.

Vous devez réparer ou remplacer tout périphérique de stockage qui n'a pas pu être monté.

Vous utiliserez le nom de l'appareil pour rechercher l'ID de volume, qui est obligatoire lorsque vous exécutez le `repair-data` script permettant de restaurer les données d'objet sur le volume (procédure suivante).

d. Après avoir réparé ou remplacé tous les dispositifs unmountable, exécutez le `sn-remount-volumes` script une nouvelle fois pour confirmer que tous les volumes de stockage pouvant être remontés ont été remontés.

Si un volume de stockage ne peut pas être monté ou est mal formaté et que vous passez à l'étape suivante, le volume et toutes les données du volume seront supprimés. Si vous aviez deux copies de vos données d'objet, vous n'aurez qu'une seule copie jusqu'à la fin de la procédure suivante (restauration des données d'objet).

N'exécutez pas le `sn-recovery-postinstall.sh` Script si vous pensez que les données restantes sur un volume de stockage en panne ne peuvent pas être reconstruites à partir d'un autre emplacement de la grille (par exemple, si votre règle ILM utilise une règle qui effectue une seule copie ou si les volumes ont échoué sur plusieurs nœuds). Contactez plutôt le support technique pour savoir comment récupérer vos données.

4. Exécutez le `sn-recovery-postinstall.sh` script : `sn-recovery-postinstall.sh`

Ce script reformate tous les volumes de stockage qui n'ont pas pu être montés ou qui n'ont pas été correctement formatés. Reconstruit la base de données Cassandra sur le nœud, si nécessaire, et démarre les services sur le nœud de stockage.

Gardez à l'esprit les points suivants :

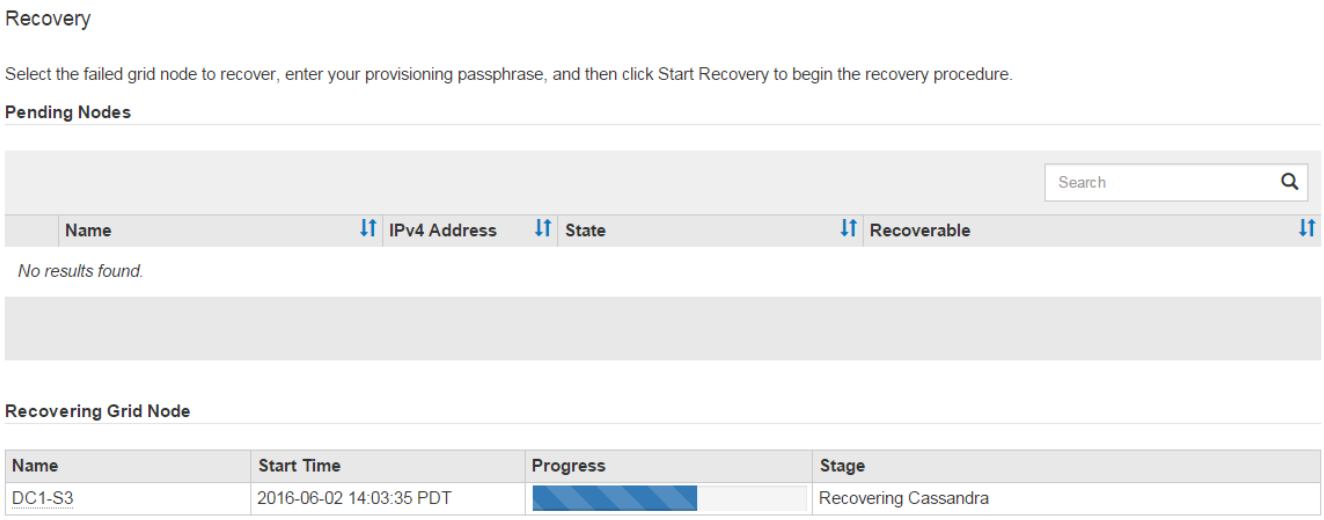
- L'exécution du script peut prendre des heures.
- En général, vous devez laisser la session SSH seule pendant que le script est en cours d'exécution.
- N'appuyez pas sur **Ctrl+C** lorsque la session SSH est active.
- Le script s'exécute en arrière-plan en cas d'interruption du réseau et met fin à la session SSH, mais vous pouvez afficher la progression à partir de la page récupération.
- Si le nœud de stockage utilise le service RSM, le script peut sembler bloqué pendant 5 minutes au redémarrage des services de nœud. Ce délai de 5 minutes est prévu lorsque l'entretien du RSM démarre pour la première fois.

Le service RSM est présent sur les nœuds de stockage qui incluent le service ADC.

Certaines procédures de restauration StorageGRID utilisent Reaper pour traiter les réparations Cassandra. Les réparations sont effectuées automatiquement dès que les services connexes ou requis ont commencé. Vous remarquerez peut-être des résultats de script mentionnant « couche » ou « réparation Cassandra ». Si un message d'erreur indiquant que la réparation a échoué, exécutez la commande indiquée dans le message d'erreur.

5. comme l' `sn-recovery-postinstall.sh` Exécution du script, surveillez la page récupération dans le Gestionnaire de grille.

La barre de progression et la colonne Etape de la page récupération fournissent un état de haut niveau du `sn-recovery-postinstall.sh` script.



6. Après le `sn-recovery-postinstall.sh` le script a démarré les services sur le nœud. vous pouvez restaurer les données d'objet sur tous les volumes de stockage formatés par le script.

   Le script vous demande si vous souhaitez restaurer les données d'objet manuellement.

   - Dans la plupart des cas, vous devriez "Restaurez les données d'objet à l'aide de Grid Manager". Réponse `n` Pour utiliser le Gestionnaire de grille.
   - Dans de rares cas, par exemple lorsque le support technique vous y invite, ou lorsque vous savez que le nœud de remplacement dispose de moins de volumes disponibles pour le stockage objet que le nœud d'origine, vous devez "restaurez les données d'objet manuellement" à l'aide du `repair-data` script. Si l'un de ces cas s'applique, répondez `y`.

   > Si vous répondez `y` pour restaurer les données d'objet manuellement :
   >
   > - Vous ne pouvez pas restaurer les données d'objet à l'aide de Grid Manager.
   > - Vous pouvez surveiller la progression des travaux de restauration manuelle à l'aide de Grid Manager.

Restauration des données d'objet sur le volume de stockage (panne de disque système)

Après avoir restauré des volumes de stockage sur un nœud de stockage non appliance, vous pouvez restaurer les données d'objet répliquées ou codées en effacement qui ont été perdues en cas de défaillance du nœud de stockage.

Quelle procédure dois-je utiliser ?

Dans la mesure du possible, restaurez les données d'objet à l'aide de la page **Restauration de volume** du gestionnaire de grille.

- Si les volumes sont répertoriés sous **MAINTENANCE** > **Restauration de volume** > **nœuds à restaurer**, restaurez les données d'objet à l'aide de l' "Page de restauration de volume dans le Gestionnaire de grille".

- Si les volumes ne sont pas répertoriés dans **MAINTENANCE** > **Restauration du volume** > **nœuds à restaurer**, suivez les étapes ci-dessous pour utiliser le `repair-data` script de restauration des données d'objet.

  Si le nœud de stockage restauré contient moins de volumes que le nœud qu'il remplace, vous devez utiliser le `repair-data` script.

Utilisez le `repair-data` script de restauration des données d'objet

Avant de commencer

- Vous devez avoir confirmé que le noeud de stockage récupéré possède un état de connexion * connecté* Dans l'onglet **NODES** > **Présentation** du Gestionnaire de grille.

Description de la tâche

Les données d'objet peuvent être restaurées depuis d'autres nœuds de stockage, un nœud d'archivage ou un pool de stockage cloud, en supposant que les règles ILM de la grille soient configurées de manière à ce que les copies d'objet soient disponibles.

Notez ce qui suit :

- Si une règle ILM a été configurée pour stocker une seule copie répliquée, et que cette copie existait sur un volume de stockage défaillant, vous ne pourrez pas restaurer l'objet.
- Si la seule copie restante d'un objet se trouve dans un pool de stockage cloud, StorageGRID doit émettre plusieurs demandes vers le terminal de pool de stockage cloud pour restaurer les données d'objet. Avant d'effectuer cette procédure, contactez le support technique pour obtenir de l'aide pour estimer le délai de restauration et les coûts associés.
- Si la seule copie restante d'un objet se trouve sur un noeud d'archivage, les données d'objet sont extraites du noeud d'archivage. La restauration de données d'objet sur un nœud de stockage à partir d'un nœud d'archivage prend plus de temps que la restauration de copies à partir d'autres nœuds de stockage en raison de la latence associée aux récupérations à partir de systèmes de stockage d'archives externes.

À propos du `repair-data` script

Pour restaurer les données d'objet, exécutez le `repair-data` script. Ce script commence le processus de restauration des données d'objet et fonctionne avec l'analyse ILM pour s'assurer que les règles ILM sont respectées.

Sélectionnez **données répliquées** ou **données codées par effacement (EC)** ci-dessous pour apprendre les différentes options du `repair-data` script, basé sur la restauration des données répliquées ou des données avec code d'effacement. Si vous devez restaurer les deux types de données, vous devez exécuter les deux ensembles de commandes.

> Pour plus d'informations sur le `repair-data` script, entrez `repair-data --help` Dans la ligne de commande du nœud d'administration principal.

Les données répliquées

Deux commandes sont disponibles pour la restauration des données répliquées, et ce, selon que vous devez réparer le nœud entier ou uniquement certains volumes sur le nœud :

```
repair-data start-replicated-node-repair

repair-data start-replicated-volume-repair
```

Vous pouvez suivre les réparations des données répliquées avec cette commande :

```
repair-data show-replicated-repair-status
```

Données avec code d'effacement (EC)

Deux commandes sont disponibles pour la restauration des données avec code d'effacement, selon que vous devez réparer le nœud entier ou uniquement certains volumes sur le nœud :

```
repair-data start-ec-node-repair

repair-data start-ec-volume-repair
```

Vous pouvez suivre les réparations des données codées par effacement à l'aide de cette commande :

```
repair-data show-ec-repair-status
```

> Les réparations des données codées peuvent commencer alors que certains nœuds de stockage sont hors ligne. Toutefois, si toutes les données avec code d'effacement ne peuvent pas être prises en compte, la réparation ne peut pas être effectuée. La réparation s'effectuera une fois que tous les nœuds sont disponibles.

> Le travail de réparation EC réserve temporairement une grande quantité de stockage. Les alertes de stockage peuvent être déclenchées, mais elles seront résolus une fois la réparation terminée. S'il n'y a pas assez de stockage pour la réservation, la tâche de réparation EC échouera. Les réservations de stockage sont libérées lorsque la tâche de réparation EC est terminée, que la tâche ait échoué ou a réussi.

Rechercher le nom d'hôte pour le noeud de stockage

1. Connectez-vous au nœud d'administration principal :
   a. Saisissez la commande suivante : `ssh admin@primary_Admin_Node_IP`
   b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
   c. Entrez la commande suivante pour passer à la racine : `su -`
   d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

   Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

2. Utilisez le `/etc/hosts` Fichier pour trouver le nom d'hôte du noeud de stockage pour les volumes de stockage restaurés. Pour afficher la liste de tous les nœuds de la grille, saisissez les éléments suivants : `cat /etc/hosts`.

Réparez les données si tous les volumes ont échoué

Si tous les volumes de stockage sont en panne, réparez l'intégralité du nœud. Suivez les instructions pour les données **répliquées**, **codées par effacement (EC)**, ou les deux, selon que vous utilisez ou non des données répliquées, des données codées par effacement (EC), ou les deux.

Si seuls certains volumes ont échoué, accédez à Réparer les données si seulement certains volumes ont échoué.

> Vous ne pouvez pas courir `repair-data` opérations simultanément pour plusieurs nœuds. Pour restaurer plusieurs nœuds, contactez le support technique.

Les données répliquées

Si votre grid inclut des données répliquées, utilisez le `repair-data start-replicated-node-repair` commande avec `--nodes` option, où `--nodes` Est le nom d'hôte (nom du système), pour réparer la totalité du nœud de stockage.

Cette commande répare les données répliquées sur un nœud de stockage nommé SG-DC-SN3 :

```
repair-data start-replicated-node-repair --nodes SG-DC-SN3
```

> Lorsque les données d'objet sont restaurées, l'alerte **objets perdus** est déclenchée si le système StorageGRID ne peut pas localiser les données d'objet répliquées. Des alertes peuvent être déclenchées sur les nœuds de stockage dans le système. Vous devez déterminer la cause de la perte et si la récupération est possible. Voir "Rechercher les objets perdus".

Données avec code d'effacement (EC)

Si votre grid contient des données avec code d'effacement, utilisez la `repair-data start-ec-node-repair` commande avec `--nodes` option, où `--nodes` Est le nom d'hôte (nom du système), pour réparer la totalité du nœud de stockage.

Cette commande répare les données codées de l'effacement sur un nœud de stockage appelé SG-DC-SN3 :

```
repair-data start-ec-node-repair --nodes SG-DC-SN3
```

L'opération renvoie un seul `repair ID` qui l'identifie `repair_data` fonctionnement. Utilisez-le `repair ID` pour suivre la progression et le résultat du `repair_data` fonctionnement. Aucun autre retour n'est renvoyé à la fin du processus de récupération.

> Les réparations des données codées peuvent commencer alors que certains nœuds de stockage sont hors ligne. La réparation s'effectuera une fois que tous les nœuds sont disponibles.

Réparer les données si seulement certains volumes ont échoué

Si seulement certains volumes ont échoué, réparez les volumes affectés. Suivez les instructions pour les données **répliquées**, **codées par effacement (EC)**, ou les deux, selon que vous utilisez ou non des données répliquées, des données codées par effacement (EC), ou les deux.

Si tous les volumes ont échoué, accédez à Réparez les données si tous les volumes ont échoué.

Saisissez les ID de volume en hexadécimal. Par exemple : `0000` est le premier volume et `000F` est le seizième volume. Vous pouvez spécifier un volume, une plage de volumes ou plusieurs volumes qui ne sont pas dans une séquence.

Tous les volumes doivent se trouver sur le même nœud de stockage. Si vous devez restaurer des volumes pour plusieurs nœuds de stockage, contactez le support technique.

Les données répliquées

Si votre grid contient des données répliquées, utilisez le `start-replicated-volume-repair` commande avec `--nodes` option permettant d'identifier le nœud (où `--nodes` est le nom d'hôte du nœud). Ajoutez ensuite l'une ou l'autre des `--volumes` ou `--volume-range` comme indiqué dans les exemples suivants.

Volume unique : cette commande restaure les données répliquées vers le volume `0002` Sur un nœud de stockage nommé SG-DC-SN3 :

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volumes 0002
```

Plage de volumes : cette commande restaure les données répliquées vers tous les volumes de la plage `0003` à `0009` Sur un nœud de stockage nommé SG-DC-SN3 :

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volume-range
0003,0009
```

Volumes multiples non compris dans une séquence : cette commande restaure les données répliquées vers des volumes `0001`, `0005`, et `0008` Sur un nœud de stockage nommé SG-DC-SN3 :

```
repair-data start-replicated-volume-repair --nodes SG-DC-SN3 --volumes
0001,0005,0008
```

> Lorsque les données d'objet sont restaurées, l'alerte **objets perdus** est déclenchée si le système StorageGRID ne peut pas localiser les données d'objet répliquées. Des alertes peuvent être déclenchées sur les nœuds de stockage dans le système. Notez la description de l'alerte et les actions recommandées pour déterminer la cause de la perte et si la récupération est possible.

Données avec code d'effacement (EC)

Si votre grid contient des données avec code d'effacement, utilisez la `start-ec-volume-repair` commande avec `--nodes` option permettant d'identifier le nœud (où `--nodes` est le nom d'hôte du nœud). Ajoutez ensuite l'une ou l'autre des `--volumes` ou `--volume-range` comme indiqué dans les exemples suivants.

Volume unique : cette commande restaure les données codées par effacement dans un volume `0007` Sur un nœud de stockage nommé SG-DC-SN3 :

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 0007
```

Plage de volumes : cette commande restaure les données avec code d'effacement sur tous les volumes de la plage `0004` à `0006` Sur un nœud de stockage nommé SG-DC-SN3 :

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volume-range 0004,0006
```

Plusieurs volumes non dans une séquence : cette commande restaure les données codées par effacement dans des volumes `000A`, `000C`, et `000E` Sur un nœud de stockage nommé SG-DC-SN3 :

```
repair-data start-ec-volume-repair --nodes SG-DC-SN3 --volumes 000A,000C,000E
```

Le `repair-data` l'opération renvoie un seul `repair ID` qui l'identifie `repair_data` fonctionnement.

Utilisez-le `repair ID` pour suivre la progression et le résultat du `repair_data` fonctionnement. Aucun autre retour n'est renvoyé à la fin du processus de récupération.

> Les réparations des données codées peuvent commencer alors que certains nœuds de stockage sont hors ligne. La réparation s'effectuera une fois que tous les nœuds sont disponibles.

Surveiller les réparations

Surveiller l'état des travaux de réparation, en fonction de l'utilisation ou non des données **répliquées**, **données codées par effacement (EC)**, ou des deux.

Vous pouvez également surveiller l'état des travaux de restauration de volume en cours et afficher un historique des travaux de restauration effectués dans"Gestionnaire de grille".

Les données répliquées

- Pour obtenir une estimation du pourcentage d'achèvement de la réparation répliquée, ajoutez le `show-replicated-repair-status` option de la commande repair-data.

  ```
  repair-data show-replicated-repair-status
  ```

- Pour déterminer si les réparations sont terminées :
  a. Sélectionnez **NŒUDS** > ***nœud de stockage en cours de réparation*** > **ILM**.
  b. Vérifiez les attributs dans la section évaluation. Lorsque les réparations sont terminées, l'attribut **attente - tous** indique 0 objets.
- Pour surveiller la réparation plus en détail :
  a. Sélectionnez **SUPPORT** > **Outils** > **topologie de grille**.
  b. Sélectionnez ***GRID*** > ***Storage Node en cours de réparation*** > **LDR** > **Data Store**.
  c. Utilisez une combinaison des attributs suivants pour déterminer, autant que possible, si les réparations répliquées sont terminées.

  > Cassandra présente peut-être des incohérences et les réparations échouées ne sont pas suivies.

  - **Réparations tentées (XRPA)** : utilisez cet attribut pour suivre la progression des réparations répliquées. Cet attribut augmente chaque fois qu'un nœud de stockage tente de réparer un objet à haut risque. Lorsque cet attribut n'augmente pas pendant une période plus longue que la période d'acquisition actuelle (fournie par l'attribut **période d'analyse — estimation**), cela signifie que l'analyse ILM n'a trouvé aucun objet à haut risque qui doit être réparé sur n'importe quel nœud.

    > Les objets à haut risque sont des objets qui risquent d'être complètement perdus. Cela n'inclut pas les objets qui ne répondent pas à leur configuration ILM.

  - **Période d'acquisition — estimée (XSCM)** : utilisez cet attribut pour estimer quand une modification de règle sera appliquée aux objets précédemment ingérés. Si l'attribut **réparations tentées** n'augmente pas pendant une période supérieure à la période d'acquisition actuelle, il est probable que les réparations répliquées soient effectuées. Notez que la période d'acquisition peut changer. L'attribut **période d'acquisition — estimée (XSCM)** s'applique à la grille entière et est le maximum de toutes les périodes d'acquisition de nœud. Vous pouvez interroger l'historique d'attributs **période de balayage — estimation** de la grille pour déterminer une période appropriée.

Données avec code d'effacement (EC)

Pour surveiller la réparation des données codées d'effacement et réessayer toute demande qui pourrait avoir échoué :

1. Déterminez l'état des réparations des données par code d'effacement :
   - Sélectionnez **SUPPORT** > **Tools** > **Metrics** pour afficher le temps de réalisation estimé et le pourcentage de réalisation de la tâche en cours. Sélectionnez ensuite **EC Overview** dans la section Grafana. Examinez les tableaux de bord **Grid EC Job estimé Time to Completion** et **Grid EC Job Percentage Finted**.

- Utilisez cette commande pour afficher le statut d'un spécifique `repair-data` fonctionnement :

  ```
  repair-data show-ec-repair-status --repair-id repair ID
  ```

- Utilisez cette commande pour lister toutes les réparations :

  ```
  repair-data show-ec-repair-status
  ```

Les informations de sortie sont affichées, notamment `repair ID`, pour toutes les réparations précédentes et en cours.

2. Si le résultat indique que l'opération de réparation a échoué, utilisez le `--repair-id` option permettant de réessayer la réparation.

   Cette commande relance une réparation de nœud ayant échoué à l'aide de l'ID de réparation 6949309319275667690 :

   ```
   repair-data start-ec-node-repair --repair-id 6949309319275667690
   ```

   Cette commande relance une réparation de volume en échec à l'aide de l'ID de réparation 6949309319275667690 :

   ```
   repair-data start-ec-volume-repair --repair-id 6949309319275667690
   ```

Vérifiez l'état du stockage après avoir restauré le lecteur système du nœud de stockage

Après avoir restauré le lecteur système d'un noeud de stockage, vous devez vérifier que l'état souhaité du noeud de stockage est défini sur en ligne et vous assurer que l'état est en ligne par défaut à chaque redémarrage du serveur de noeud de stockage.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Le nœud de stockage a été restauré et la restauration des données est terminée.

Étapes

1. Sélectionnez **SUPPORT** > **Outils** > **topologie de grille**.
2. Vérifiez les valeurs de **nœud de stockage récupéré** > **LDR** > **Storage** > **Storage State de stockage — désiré** et **Storage State — Current**.

   La valeur des deux attributs doit être en ligne.

3. Si l'état de stockage — souhaité est défini sur lecture seule, procédez comme suit :
   a. Cliquez sur l'onglet **Configuration**.
   b. Dans la liste déroulante **État de stockage — désiré**, sélectionnez **en ligne**.
   c. Cliquez sur **appliquer les modifications**.
   d. Cliquez sur l'onglet **Présentation** et confirmez que les valeurs de **État de stockage — désiré** et **État de stockage — actuel** sont mises à jour en ligne.

Restaurez les données d'objet à l'aide de Grid Manager

Vous pouvez restaurer les données d'objet d'un volume de stockage ou d'un nœud de stockage défaillant à l'aide de Grid Manager. Vous pouvez également utiliser Grid Manager pour surveiller les processus de restauration en cours et afficher un historique de restauration.

Avant de commencer

- Vous avez effectué l'une des procédures suivantes pour formater les volumes défaillants :
  - "Remontage et reformatage des volumes de stockage de l'appliance (étapes manuelles)"
  - "Remontage et reformatage des volumes de stockage (étapes manuelles)"
- Vous avez confirmé que le noeud de stockage sur lequel vous restaurez les objets a un état de connexion **connecté** Dans l'onglet **NODES** > **Présentation** du Gestionnaire de grille.
- Vous avez confirmé ce qui suit :
  - Une extension de grille pour ajouter un nœud de stockage n'est pas en cours.
  - La mise hors service d'un nœud de stockage n'est pas en cours ou a échoué.
  - La restauration d'un volume de stockage défaillant n'est pas en cours.
  - La restauration d'un nœud de stockage avec un disque système en panne n'est pas en cours.
  - Un travail de rééquilibrage EC n'est pas en cours.
  - Le clonage des nœuds de l'appliance n'est pas en cours.

Description de la tâche

Après avoir remplacé les lecteurs et effectué les étapes manuelles de formatage des volumes, Grid Manager affiche les volumes comme candidats à la restauration dans l'onglet **MAINTENANCE** > **Restauration du volume** > **nœuds à restaurer**.

Dans la mesure du possible, restaurez les données d'objet à l'aide de la page **Restauration de volume** du gestionnaire de grille. Suivez ces instructions :

- Si les volumes sont répertoriés dans **MAINTENANCE** > **Restauration de volume** > **nœuds à restaurer**, restaurez les données d'objet comme décrit dans les étapes ci-dessous. Les volumes seront répertoriés si :
  - Certains volumes de stockage d'un nœud sont en panne, mais pas tous
  - Tous les volumes de stockage d'un nœud sont en panne et sont remplacés par le même nombre de volumes ou plus

  La page de restauration de volume du gestionnaire de grille vous permet également de le faire surveiller le processus de restauration des volumes et afficher l'historique de restauration.
- Si les volumes ne sont pas répertoriés dans le gestionnaire de grille comme candidats à la restauration, suivez les étapes appropriées pour utiliser le `repair-data` script de restauration des données d'objet :
  - "Restauration des données d'objet sur le volume de stockage (panne de disque système)"
  - "Restaurez les données d'objet vers le volume de stockage sur lequel le disque système est intact"
  - "Restaurez les données d'objet vers un volume de stockage pour l'appliance"

  Si le nœud de stockage restauré contient moins de volumes que le nœud qu'il remplace, vous devez

utiliser le `repair-data` script.

Vous pouvez restaurer deux types de données d'objet :

- Les objets de données répliqués sont restaurés à partir d'autres emplacements, dans la mesure où les règles ILM de la grille ont été configurées de façon à rendre disponibles les copies objet.
  - Si une règle ILM a été configurée pour stocker une seule copie répliquée, et que cette copie existait sur un volume de stockage défaillant, vous ne pourrez pas restaurer l'objet.
  - Si la seule copie restante d'un objet se trouve dans un pool de stockage cloud, StorageGRID doit émettre plusieurs demandes vers le terminal de pool de stockage cloud pour restaurer les données d'objet.
  - Si la seule copie restante d'un objet se trouve sur un noeud d'archivage, les données d'objet sont extraites du noeud d'archivage. La restauration des données d'objet vers un nœud de stockage à partir d'un nœud d'archivage prend plus de temps que la restauration des copies d'objet à partir d'autres nœuds de stockage.
- Les objets de données avec code d'effacement (EC) sont restaurés en réassemblez les fragments stockés. Les fragments corrompus ou perdus sont recréés par l'algorithme de code d'effacement à partir des fragments de données et de parité restants.

> La restauration des volumes dépend de la disponibilité des ressources dans lesquelles les copies objet sont stockées. La progression de la restauration des volumes n'est pas linéaire et peut prendre des jours ou des semaines.

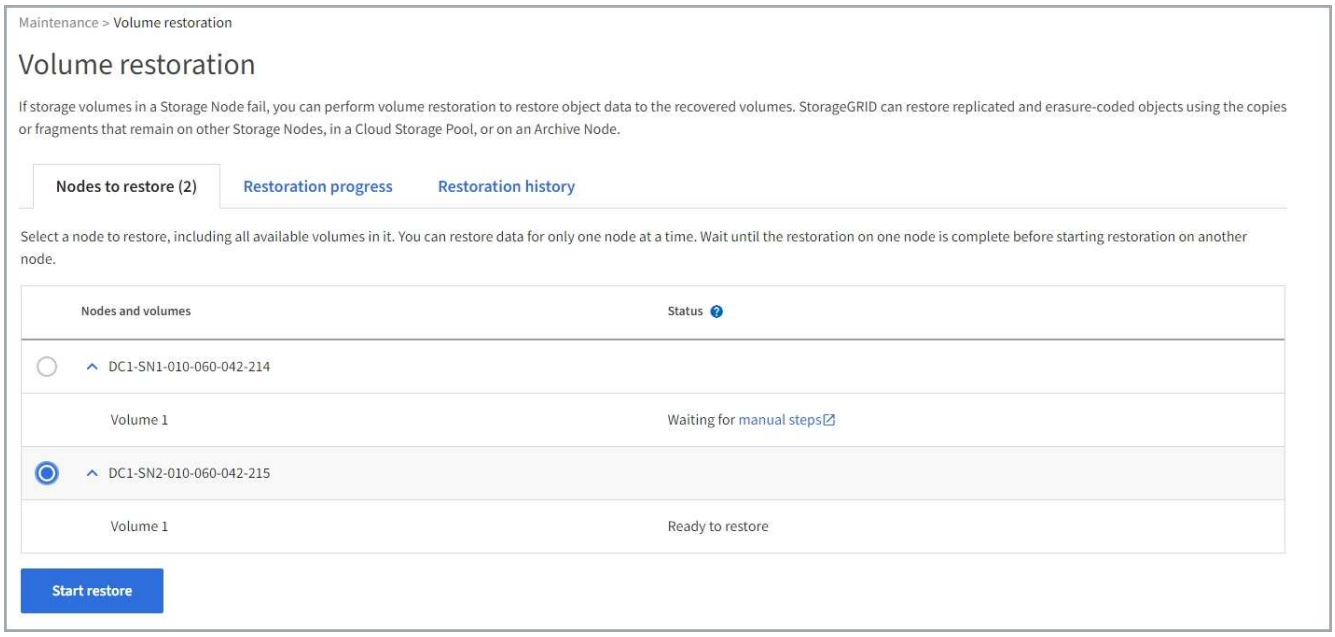
Restauration d'un volume ou d'un nœud défaillant

Procédez comme suit pour restaurer un volume ou un nœud défaillant.

Étapes

1. Dans Grid Manager, accédez à **MAINTENANCE** > **Restauration de volume**.
2. Sélectionnez l'onglet **nœuds à restaurer**.

   Le numéro de l'onglet indique le nombre de nœuds pour lesquels des volumes nécessitent une restauration.



3. Développez chaque nœud pour afficher les volumes qui nécessitent une restauration, ainsi que leur état.
4. Corrigez tous les problèmes empêchant la restauration de chaque volume qui sont indiqués lorsque vous sélectionnez attendre les étapes manuelles, s'il s'affiche comme état du volume.
5. Sélectionnez un nœud à restaurer où tous les volumes indiquent l'état prêt pour la restauration.

   Vous ne pouvez restaurer les volumes que pour un nœud à la fois.

   Chaque volume du nœud doit indiquer qu'il est prêt pour la restauration.

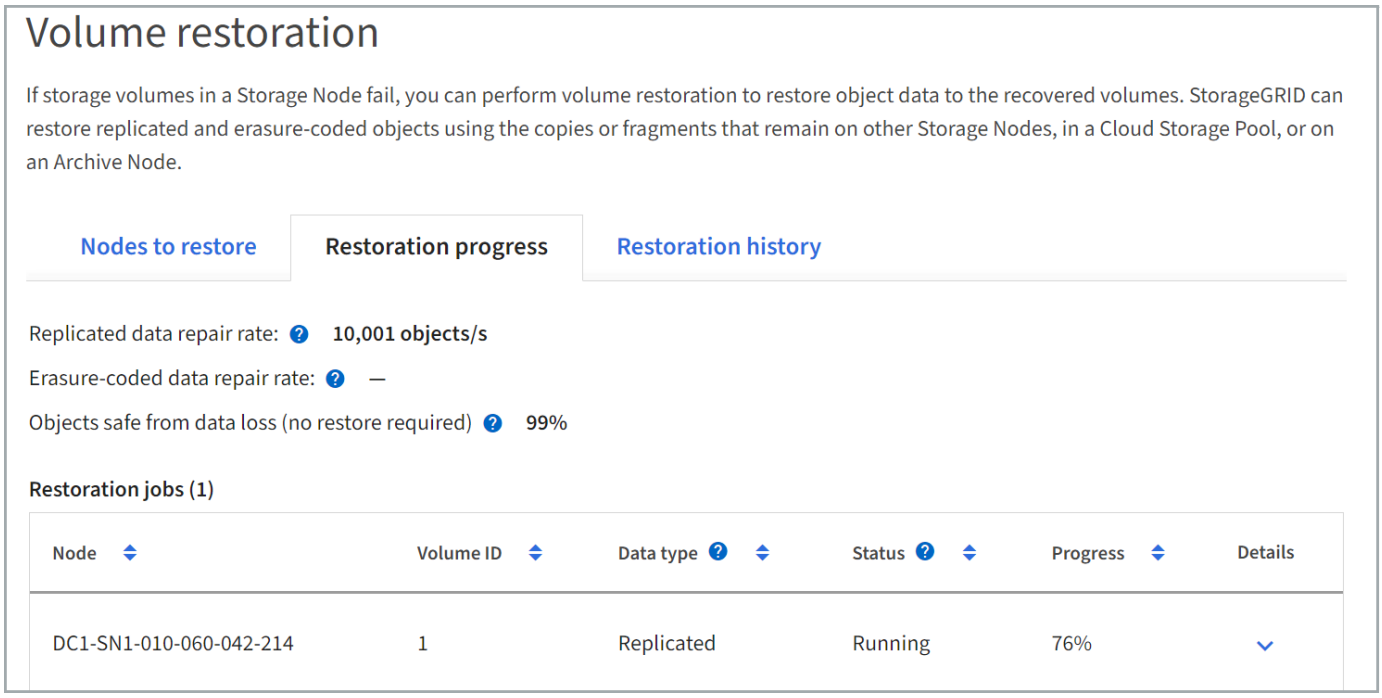
6. Sélectionnez **Démarrer la restauration**.
7. Réglez les avertissements qui peuvent apparaître ou sélectionnez **Démarrer malgré tout** pour ignorer les avertissements et lancer la restauration.

Les nœuds sont déplacés de l'onglet **nœuds à restaurer** vers l'onglet **progression de la restauration** au démarrage de la restauration.

Si une restauration de volume ne peut pas être démarrée, le nœud revient à l'onglet **noeuds à restaurer**.

Afficher la progression de la restauration

L'onglet **progression de la restauration** affiche l'état du processus de restauration du volume et des informations sur les volumes d'un nœud restauré.



Dans tous les volumes, les taux de réparation des données pour les objets répliqués et soumis au code d'effacement constituent des moyennes résumant toutes les restaurations en cours, y compris les restaurations initiées à l'aide du `repair-data` script. Le pourcentage d'objets de ces volumes qui sont intacts et ne nécessitent pas de restauration est également indiqué.

> La restauration des données répliquées dépend de la disponibilité des ressources dans lesquelles les copies répliquées sont stockées. La progression de la restauration des données répliquées n'est pas linéaire et peut prendre des jours ou des semaines.

La section tâches de restauration affiche des informations sur les restaurations de volume démarrées à partir du Gestionnaire de grille.

- Le nombre indiqué dans l'en-tête de la section travaux de restauration indique le nombre de volumes en cours de restauration ou en file d'attente de restauration.
- Le tableau affiche des informations sur chaque volume d'un nœud en cours de restauration ainsi que sa progression.
  - La progression de chaque nœud affiche le pourcentage pour chaque travail.
  - Développez la colonne Détails pour afficher l'heure de début de la restauration et l'ID du travail.
- En cas d'échec de la restauration d'un volume :
  - La colonne État indique échec.
  - Une erreur s'affiche, indiquant la cause de la défaillance.

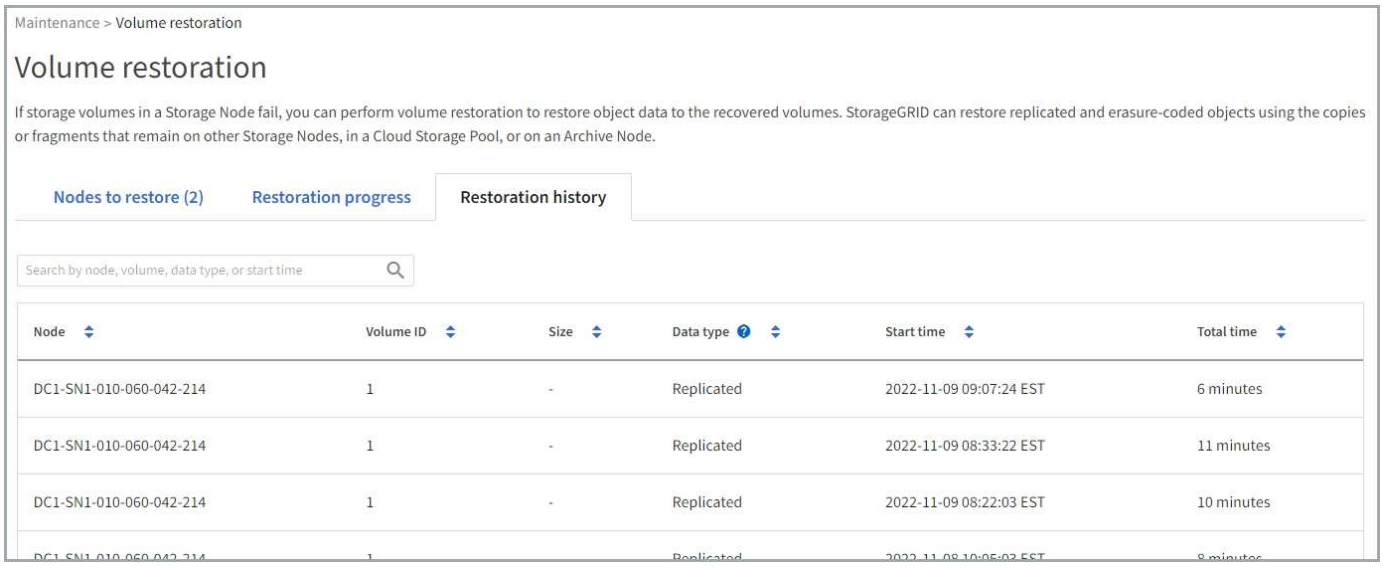
    Corrigez les problèmes indiqués dans l'erreur. Sélectionnez **Réessayer** pour relancer la restauration du volume.

  Si plusieurs travaux de restauration ont échoué, la sélection de **Réessayer** lance le travail ayant échoué le plus récemment.

Afficher l’historique de restauration

L’onglet **Historique de restauration** affiche des informations sur toutes les restaurations de volume effectuées avec succès.

> Les tailles ne s’appliquent pas aux objets répliqués. Elles s’affichent uniquement pour les restaurations contenant des objets de données avec code d’effacement (EC).



Surveiller les tâches de réparation des données

Vous pouvez surveiller l’état des travaux de réparation à l’aide de `repair-data` script à partir de la ligne de commande.

Il s’agit notamment des tâches que vous avez initiées manuellement ou des tâches que StorageGRID a initiées automatiquement dans le cadre d’une procédure de mise hors service.

> Si vous exécutez des tâches de restauration de volume, "Surveillez la progression et affichez un historique de ces travaux dans le Gestionnaire de grille" à la place.

Surveiller l’état de `repair-data` Travaux basés sur l’utilisation de **données répliquées**, **données avec code d’effacement (EC)** ou les deux.

Les données répliquées

- Pour obtenir une estimation du pourcentage d'achèvement de la réparation répliquée, ajoutez le `show-replicated-repair-status` option de la commande repair-data.

  ```
  repair-data show-replicated-repair-status
  ```

- Pour déterminer si les réparations sont terminées :
  a. Sélectionnez **NŒUDS** > ***nœud de stockage en cours de réparation*** > **ILM**.
  b. Vérifiez les attributs dans la section évaluation. Lorsque les réparations sont terminées, l'attribut **attente - tous** indique 0 objets.
- Pour surveiller la réparation plus en détail :
  a. Sélectionnez **SUPPORT** > **Outils** > **topologie de grille**.
  b. Sélectionnez ***GRID*** > ***Storage Node en cours de réparation*** > **LDR** > **Data Store**.
  c. Utilisez une combinaison des attributs suivants pour déterminer, autant que possible, si les réparations répliquées sont terminées.

  > Cassandra présente peut-être des incohérences et les réparations échouées ne sont pas suivies.

  - **Réparations tentées (XRPA)** : utilisez cet attribut pour suivre la progression des réparations répliquées. Cet attribut augmente chaque fois qu'un nœud de stockage tente de réparer un objet à haut risque. Lorsque cet attribut n'augmente pas pendant une période plus longue que la période d'acquisition actuelle (fournie par l'attribut **période d'analyse — estimation**), cela signifie que l'analyse ILM n'a trouvé aucun objet à haut risque qui doit être réparé sur n'importe quel nœud.

    > Les objets à haut risque sont des objets qui risquent d'être complètement perdus. Cela n'inclut pas les objets qui ne répondent pas à leur configuration ILM.

  - **Période d'acquisition — estimée (XSCM)** : utilisez cet attribut pour estimer quand une modification de règle sera appliquée aux objets précédemment ingérés. Si l'attribut **réparations tentées** n'augmente pas pendant une période supérieure à la période d'acquisition actuelle, il est probable que les réparations répliquées soient effectuées. Notez que la période d'acquisition peut changer. L'attribut **période d'acquisition — estimée (XSCM)** s'applique à la grille entière et est le maximum de toutes les périodes d'acquisition de nœud. Vous pouvez interroger l'historique d'attributs **période de balayage — estimation** de la grille pour déterminer une période appropriée.

Données avec code d'effacement (EC)

Pour surveiller la réparation des données codées d'effacement et réessayer toute demande qui pourrait avoir échoué :

1. Déterminez l'état des réparations des données par code d'effacement :
   - Sélectionnez **SUPPORT** > **Tools** > **Metrics** pour afficher le temps de réalisation estimé et le pourcentage de réalisation de la tâche en cours. Sélectionnez ensuite **EC Overview** dans la section Grafana. Examinez les tableaux de bord **Grid EC Job estimé Time to Completion** et **Grid EC Job Percentage Finted**.

- Utilisez cette commande pour afficher le statut d'un spécifique `repair-data` fonctionnement :

  ```
  repair-data show-ec-repair-status --repair-id repair ID
  ```

- Utilisez cette commande pour lister toutes les réparations :

  ```
  repair-data show-ec-repair-status
  ```

Les informations de sortie sont affichées, notamment `repair ID`, pour toutes les réparations précédentes et en cours.

2. Si le résultat indique que l'opération de réparation a échoué, utilisez le `--repair-id` option permettant de réessayer la réparation.

   Cette commande relance une réparation de nœud ayant échoué à l'aide de l'ID de réparation 6949309319275667690 :

   ```
   repair-data start-ec-node-repair --repair-id 6949309319275667690
   ```

   Cette commande relance une réparation de volume en échec à l'aide de l'ID de réparation 6949309319275667690 :

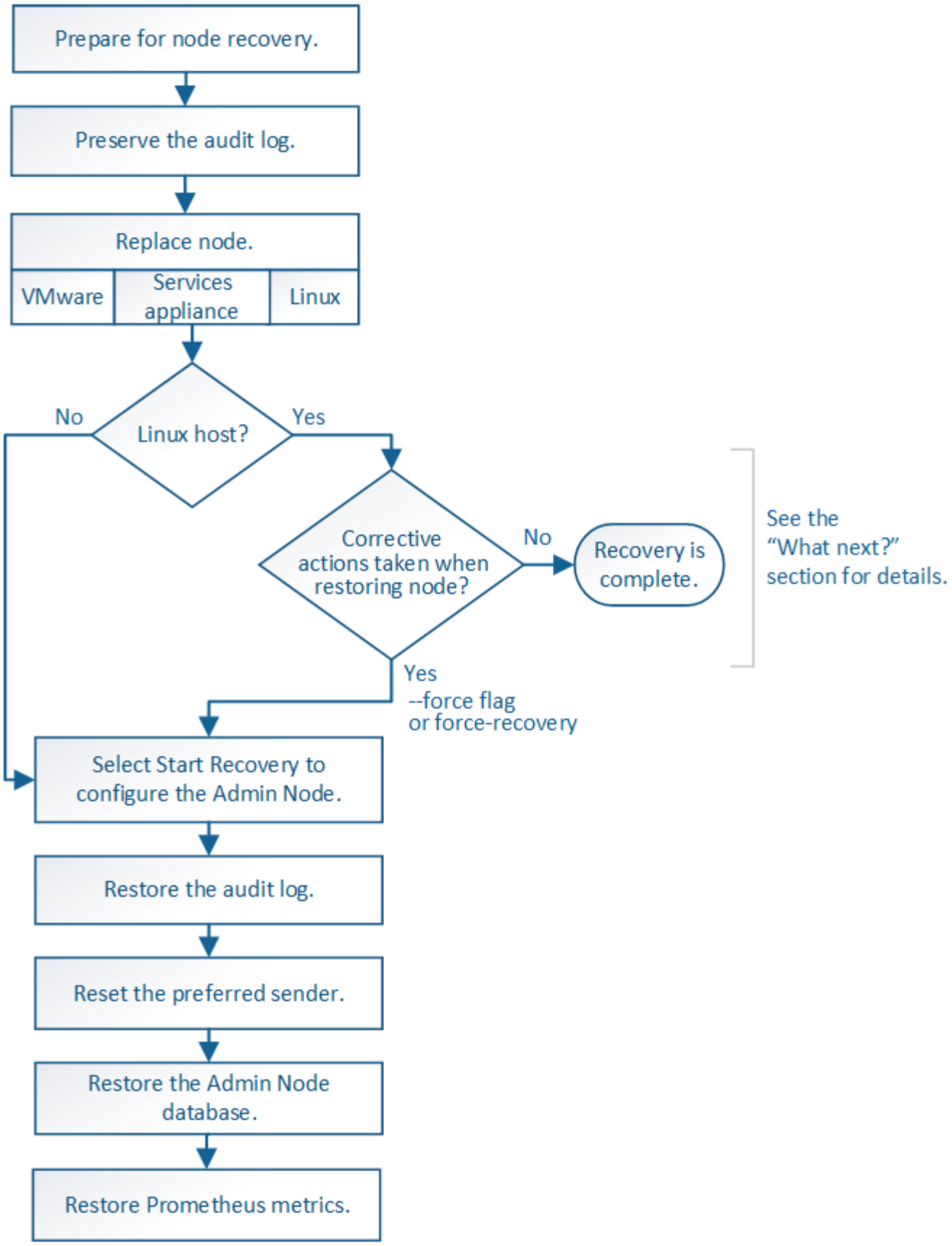
   ```
   repair-data start-ec-volume-repair --repair-id 6949309319275667690
   ```

Restaurez vos données après une panne de nœud d'administration

Échec de la restauration à partir d'un nœud d'administration : workflow

Le processus de restauration d'un noeud d'administration dépend du noeud d'administration principal ou non primaire.

Les étapes générales de restauration d'un nœud d'administration principal ou non primaire sont les mêmes, bien que les détails de la procédure diffèrent.



Suivez toujours la procédure de récupération correcte pour le nœud d'administration que vous restaurez. Les procédures semblent identiques à un niveau élevé, mais diffèrent dans les détails.

Choix

- "Restaurez vos données après une panne de nœud d'administration principal"
- "Restaurez vos données en cas de défaillance d'un nœud d'administration non principal"

Restaurez vos données après une panne de nœud d'administration principal

Restauration après les pannes de nœud d'administration principal : présentation

Vous devez effectuer un ensemble spécifique de tâches pour effectuer une restauration suite à une défaillance d'un nœud d'administration principal. Le nœud d'administration principal héberge le service de nœud de gestion de la configuration (CMN) pour la grille.

Un nœud d'administration principal défectueux doit être remplacé rapidement. Le service de nœud de gestion de la configuration (CMN) sur le nœud d'administration principal est responsable de l'émission de blocs d'identifiants d'objets pour la grille. Ces identificateurs sont attribués aux objets lors de leur ingestion. Les nouveaux objets ne peuvent pas être ingérés à moins que des identifiants soient disponibles. L'ingestion d'objet peut se poursuivre pendant que le CMN n'est pas disponible car la quantité d'identifiants d'un mois environ est mise en cache dans la grille. Cependant, une fois les identificateurs mis en cache épuisés, aucun nouvel objet ne peut être ajouté.

> Vous devez réparer ou remplacer un nœud d'administration principal défectueux dans un délai d'environ un mois. Dans ce cas, la grille risque de perdre sa capacité à ingérer de nouveaux objets. La période exacte dépend de votre taux d'acquisition de l'objet : si vous avez besoin d'une évaluation plus précise de la durée de votre grille, contactez le support technique.

La copie des journaux d'audit à partir d'un nœud d'administration principal a échoué

Si vous pouvez copier les journaux d'audit à partir du nœud d'administration principal défaillant, conservez-les pour conserver l'enregistrement de l'activité et de l'utilisation du système dans la grille. Vous pouvez restaurer les journaux d'audit conservés sur le nœud d'administration principal restauré une fois qu'il est en cours d'exécution.

Description de la tâche

Cette procédure copie les fichiers journaux d'audit du nœud d'administration défaillant vers un emplacement temporaire sur un nœud de grille distinct. Ces journaux conservés peuvent ensuite être copiés sur le nœud d'administration de remplacement. Les journaux d'audit ne sont pas automatiquement copiés sur le nouveau nœud d'administration.

Selon le type de défaillance, il se peut que vous ne puissiez pas copier les journaux d'audit à partir d'un nœud d'administration défaillant. Si le déploiement ne comporte qu'un seul nœud d'administration, le nœud d'administration restauré commence à enregistrer les événements dans le journal d'audit d'un nouveau fichier vide et les données précédemment enregistrées sont perdues. Si le déploiement inclut plusieurs nœuds d'administration, vous pouvez récupérer les journaux d'audit à partir d'un autre nœud d'administration.

> Si les journaux d'audit ne sont pas accessibles sur le nœud d'administration défaillant maintenant, vous pourrez peut-être y accéder ultérieurement, par exemple après la restauration de l'hôte.

Étapes

1. Si possible, connectez-vous au nœud d'administration défaillant. Sinon, connectez-vous au nœud d'administration principal ou à un autre nœud d'administration, le cas échéant.

a. Saisissez la commande suivante : `ssh admin@grid_node_IP`

b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

c. Entrez la commande suivante pour passer à la racine : `su -`

d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

2. Arrêtez le service AMS pour l'empêcher de créer un nouveau fichier journal :`service ams stop`
3. Renommez le fichier audit.log de sorte qu'il ne remplace pas le fichier existant lorsque vous le copiez sur le nœud d'administration restauré.

   Renommez audit.log en un nom de fichier numéroté unique. Par exemple, renommez le fichier audit.log en `2023-10-25.txt.1`.

   ```
   cd /var/local/audit/export
   ls -l
   mv audit.log 2023-10-25.txt.1
   ```

4. Redémarrez le service AMS : `service ams start`
5. Créez le répertoire pour copier tous les fichiers journaux d'audit vers un emplacement temporaire sur un nœud de grille distinct : `ssh admin@grid_node_IP mkdir -p /var/local/tmp/saved-audit-logs`

   Lorsque vous y êtes invité, entrez le mot de passe pour l'administrateur.

6. Copier tous les fichiers journaux d'audit : `scp -p * admin@grid_node_IP:/var/local/tmp/saved-audit-logs`

   Lorsque vous y êtes invité, entrez le mot de passe pour l'administrateur.

7. Se déconnecter en tant que racine : `exit`

Remplacez le nœud d'administration principal

Pour restaurer un noeud d'administration principal, vous devez d'abord remplacer le matériel physique ou virtuel.

Vous pouvez remplacer un nœud d'administration principal défectueux par un nœud d'administration principal s'exécutant sur la même plate-forme, ou remplacer un nœud d'administration principal s'exécutant sur VMware ou un hôte Linux par un nœud d'administration principal hébergé sur une appliance de services.

Utilisez la procédure qui correspond à la plate-forme de remplacement que vous sélectionnez pour le nœud. Après avoir effectué la procédure de remplacement des nœuds (adaptée à tous les types de nœuds), cette procédure vous dirige vers l'étape suivante pour la restauration du nœud d'administration principal.

Et de remplacement	Procédure
VMware	"Remplacement d'un noeud VMware"
Linux	"Remplacer un noeud Linux"
Appareils de services SG100 et SG1000	"Remplacer une appliance de services"
OpenStack	Les fichiers et scripts de disques de machine virtuelle fournis par NetApp pour OpenStack ne sont plus pris en charge pour les opérations de restauration. Si vous devez restaurer un nœud exécuté dans un déploiement OpenStack, téléchargez les fichiers du système d'exploitation Linux. Suivre ensuite la procédure pour "Remplacement d'un nœud Linux".

Configurez le nœud d'administration principal de remplacement

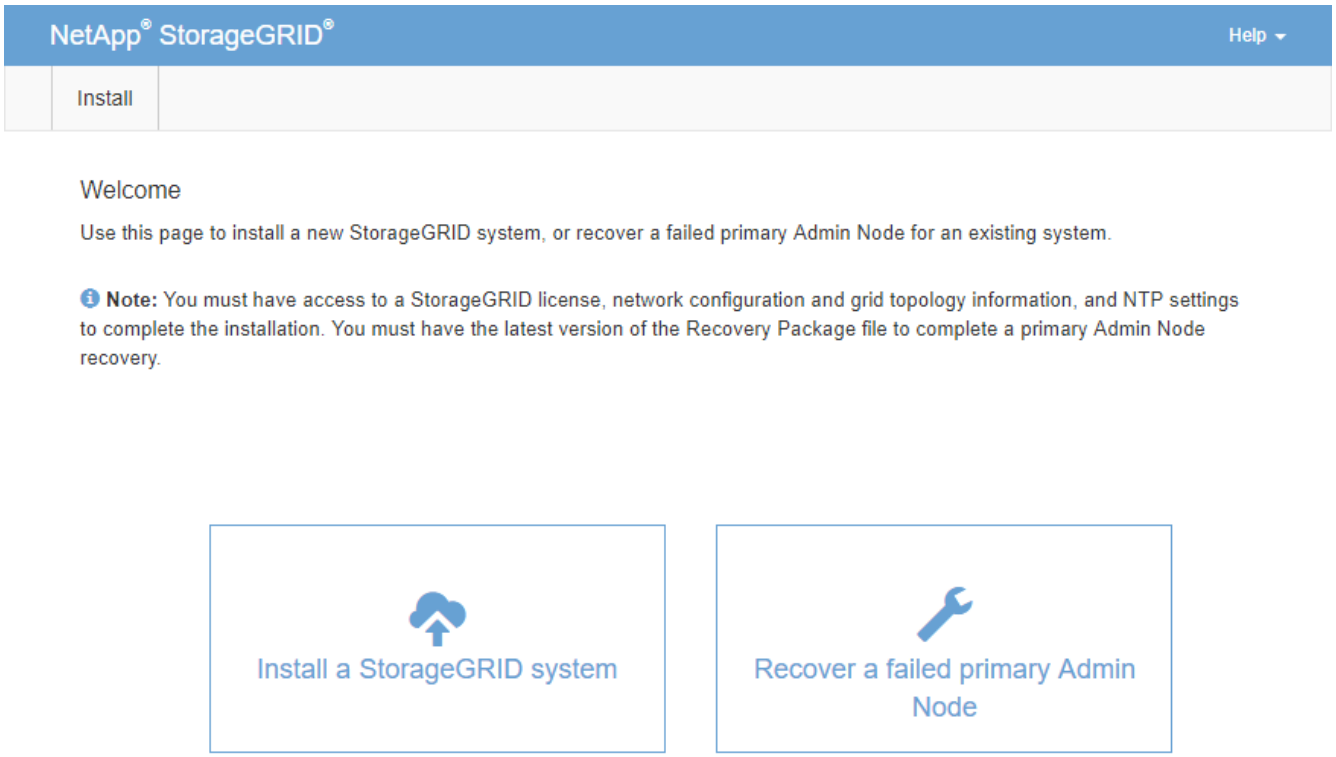
Le nœud de remplacement doit être configuré en tant que nœud d'administration principal de votre système StorageGRID.

Avant de commencer

- Pour les nœuds d'administration principaux hébergés sur des machines virtuelles, la machine virtuelle a été déployée, mise sous tension et initialisée.
- Pour les nœuds d'administration primaires hébergés sur une appliance de services, vous avez remplacé l'appliance et installé le logiciel. Voir la "instructions d'installation de votre appareil".
- Vous disposez de la dernière sauvegarde du fichier du progiciel de récupération (`sgws-recovery-package-id-revision.zip`).
- Vous avez la phrase secrète pour le provisionnement.

Étapes

1. Ouvrez votre navigateur Web et accédez à `https://primary_admin_node_ip`.



2. Cliquez sur **récupérer un noeud d'administration principal ayant échoué**.
3. Téléchargez la sauvegarde la plus récente du progiciel de restauration :
   a. Cliquez sur **Parcourir**.
   b. Recherchez le fichier de progiciel de récupération le plus récent pour votre système StorageGRID et cliquez sur **Ouvrir**.
4. Saisissez la phrase secrète pour le provisionnement.
5. Cliquez sur **Démarrer la récupération**.

   Le processus de récupération commence. Le Grid Manager peut devenir indisponible pendant quelques minutes lorsque les services requis démarrent. Une fois la récupération terminée, la page de connexion s'affiche.

6. Si l'authentification unique (SSO) est activée pour votre système StorageGRID et que l'approbation du composant de confiance pour le nœud d'administration que vous avez récupéré a été configurée pour utiliser le certificat d'interface de gestion par défaut, mettre à jour (ou supprimer et recréer) l'approbation du nœud dans Active Directory Federation Services (AD FS). Utilisez le nouveau certificat de serveur par défaut qui a été généré pendant le processus de restauration du noeud d'administration.

   > Pour configurer une confiance de partie utilisatrice, reportez-vous à la section "Configurer l'authentification unique". Pour accéder au certificat de serveur par défaut, connectez-vous au shell de commande du noeud d'administration. Accédez au `/var/local/mgmt-api` et sélectionnez `server.crt` fichier.

7. Déterminez si vous devez appliquer un correctif.
   a. Connectez-vous au Grid Manager à l'aide d'un "navigateur web pris en charge".
   b. Sélectionnez **NOEUDS**.

c. Dans la liste de gauche, sélectionnez le nœud d'administration principal.

d. Dans l'onglet vue d'ensemble, notez la version affichée dans le champ **version du logiciel**.

e. Sélectionnez un autre nœud de grille.

f. Dans l'onglet vue d'ensemble, notez la version affichée dans le champ **version du logiciel**.

- Si les versions affichées dans les champs **version du logiciel** sont identiques, vous n'avez pas besoin d'appliquer un correctif.
- Si les versions affichées dans les champs **version du logiciel** sont différentes, vous devez le faire "appliquer un correctif" Pour mettre à jour le nœud d'administration principal restauré vers la même version.

Restaurez le journal d'audit sur le nœud d'administration principal restauré

Si vous avez pu conserver le journal d'audit à partir du nœud d'administration principal défaillant, vous pouvez le copier sur le nœud d'administration principal en cours de restauration.

Avant de commencer

- Le nœud d'administration récupéré est installé et en cours d'exécution.
- Vous avez copié les journaux d'audit à un autre emplacement après l'échec du nœud d'administration d'origine.

Description de la tâche

En cas de panne d'un nœud d'administration, les journaux d'audit enregistrés sur ce nœud d'administration sont potentiellement perdus. Vous pouvez préserver les données contre la perte en copiant les journaux d'audit à partir du nœud d'administration défaillant, puis en les restaurant vers le nœud d'administration restauré. En fonction de la panne, il peut être impossible de copier les journaux d'audit à partir du nœud d'administration défaillant. Dans ce cas, si le déploiement comporte plusieurs nœuds d'administration, vous pouvez récupérer les journaux d'audit à partir d'un autre nœud d'administration, car les journaux d'audit sont répliqués sur tous les nœuds d'administration.

S'il n'y a qu'un seul nœud d'administration et que le journal d'audit ne peut pas être copié depuis le nœud défaillant, le nœud d'administration récupéré commence à enregistrer les événements dans le journal d'audit comme si l'installation était nouvelle.

Vous devez restaurer un noeud d'administration dès que possible pour restaurer la fonctionnalité de journalisation.

> Par défaut, les informations d'audit sont envoyées au journal d'audit des nœuds d'administration. Vous pouvez ignorer ces étapes si l'une des conditions suivantes s'applique :
>
> - Un serveur syslog externe et des journaux d'audit sont maintenant envoyés au serveur syslog au lieu de vers les nœuds d'administration.
> - Vous avez explicitement indiqué que les messages d'audit doivent être enregistrés uniquement sur les nœuds locaux qui les ont générés.
>
> Voir "Configurez les messages d'audit et les destinations des journaux" pour plus d'informations.

Étapes

1. Connectez-vous au nœud d'administration restauré :

a. Saisissez la commande suivante : `ssh admin@recovery_Admin_Node_IP`

b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

c. Entrez la commande suivante pour passer à la racine : `su -`

d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

Une fois que vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

2. Vérifiez quels fichiers d'audit ont été conservés : `cd /var/local/audit/export`
3. Copiez les fichiers journaux d'audit conservés sur le nœud d'administration restauré : `scp admin@grid_node_IP:/var/local/tmp/saved-audit-logs/YYYY* .`

   Lorsque vous y êtes invité, entrez le mot de passe pour l'administrateur.

4. Pour plus de sécurité, supprimez les journaux d'audit du nœud de grille défaillant après avoir vérifié qu'ils ont bien été copiés sur le nœud d'administration restauré.
5. Mettez à jour les paramètres utilisateur et groupe des fichiers journaux d'audit sur le nœud d'administration restauré : `chown ams-user: bycast *`
6. Se déconnecter en tant que racine : `exit`

Vous devez également restaurer tout accès client existant au partage d'audit. Pour plus d'informations, voir "Configurez l'accès client d'audit".

Restaurez la base de données du nœud d'administration lors de la récupération du nœud d'administration principal

Si vous souhaitez conserver les informations historiques sur les attributs, les alarmes et les alertes sur un noeud d'administration principal ayant échoué, vous pouvez restaurer la base de données du noeud d'administration. Vous ne pouvez restaurer cette base de données que si votre système StorageGRID inclut un autre noeud d'administration.

Avant de commencer

- Le nœud d'administration récupéré est installé et en cours d'exécution.
- Le système StorageGRID comprend au moins deux nœuds d'administration.
- Vous avez le `Passwords.txt` fichier.
- Vous avez la phrase secrète pour le provisionnement.

Description de la tâche

En cas de défaillance d'un nœud d'administration, les informations historiques stockées dans sa base de données de nœud d'administration sont perdues. Cette base de données contient les informations suivantes :

- Historique des alertes
- Historique des alarmes
- Les données d'attributs historiques, qui sont utilisées dans les graphiques et les rapports texte disponibles à partir de la page **SUPPORT** > **Outils** > **topologie de grille**.

Lorsque vous restaurez un noeud d'administration, le processus d'installation du logiciel crée une base de données de noeud d'administration vide sur le noeud récupéré. Toutefois, la nouvelle base de données

comprend uniquement les informations pour les serveurs et services qui font actuellement partie du système ou qui sont ajoutés ultérieurement.

Si vous avez restauré un noeud d'administration principal et que votre système StorageGRID dispose d'un autre noeud d'administration, vous pouvez restaurer les informations historiques en copiant la base de données du noeud d'administration d'un noeud d'administration non primaire (le *source Admin Node*) vers le noeud d'administration principal récupéré. Si votre système ne dispose que d'un nœud d'administration principal, vous ne pouvez pas restaurer la base de données du nœud d'administration.

> La copie de la base de données du nœud d'administration peut prendre plusieurs heures. Certaines fonctionnalités de Grid Manager ne seront pas disponibles lorsque les services sont arrêtés sur le nœud d'administration source.

Étapes

1. Connectez-vous au nœud d'administration source :
   a. Saisissez la commande suivante : `ssh admin@grid_node_IP`
   b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
   c. Entrez la commande suivante pour passer à la racine : `su -`
   d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
2. Depuis le nœud d'administration source, arrêtez le service MI : `service mi stop`
3. Depuis le nœud d'administration source, arrêtez le service Management application Program interface (mgapi) : `service mgmt-api stop`
4. Effectuez les étapes suivantes sur le nœud d'administration restauré :
   a. Connectez-vous au nœud d'administration restauré :
      i. Saisissez la commande suivante : `ssh admin@grid_node_IP`
      ii. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
      iii. Entrez la commande suivante pour passer à la racine : `su -`
      iv. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
   b. Arrêtez le service MI : `service mi stop`
   c. Arrêt du service mgmt-api : `service mgmt-api stop`
   d. Ajoutez la clé privée SSH à l'agent SSH. Entrez :`ssh-add`
   e. Entrez le mot de passe d'accès SSH répertorié dans le `Passwords.txt` fichier.
   f. Copiez la base de données du nœud d'administration source vers le nœud d'administration restauré : `/usr/local/mi/bin/mi-clone-db.sh Source_Admin_Node_IP`
   g. Lorsque vous y êtes invité, confirmez que vous souhaitez remplacer la base DE données MI sur le nœud d'administration restauré.

      La base de données et ses données historiques sont copiées dans le nœud d'administration restauré. Une fois l'opération de copie effectuée, le script démarre le nœud d'administration restauré.

   h. Lorsque vous n'avez plus besoin d'un accès sans mot de passe à d'autres serveurs, supprimez la clé privée de l'agent SSH. Entrez :`ssh-add -D`
5. Redémarrez les services sur le nœud d'administration source : `service servermanager start`

Restaurez les metrics Prometheus lors de la récupération du nœud d'administration principal

Vous pouvez également conserver les metrics historiques gérés par Prometheus sur un nœud d'administration principal défaillant. Les metrics de Prometheus ne peuvent être restaurés que si votre système StorageGRID inclut un autre nœud d'administration.

Avant de commencer

- Le nœud d'administration récupéré est installé et en cours d'exécution.
- Le système StorageGRID comprend au moins deux nœuds d'administration.
- Vous avez le `Passwords.txt` fichier.
- Vous avez la phrase secrète pour le provisionnement.

Description de la tâche

En cas de panne d'un nœud d'administration, les metrics gérés dans la base de données Prometheus sur le nœud d'administration sont perdus. Lorsque vous restaurez le nœud d'administration, un processus d'installation logicielle crée une nouvelle base de données Prometheus. Une fois le nœud d'administration restauré démarré, il enregistre les metrics comme si vous aviez déjà effectué une nouvelle installation du système StorageGRID.

Si vous avez restauré un nœud d'administration principal et que votre système StorageGRID dispose d'un autre nœud d'administration, vous pouvez restaurer les metrics historiques en copiant la base de données Prometheus à partir d'un nœud d'administration non primaire (le *source Admin Node*) vers le nœud d'administration principal récupéré. Si votre système ne dispose que d'un nœud d'administration principal, vous ne pouvez pas restaurer la base de données Prometheus.

> La copie de la base de données Prometheus peut prendre une heure ou plus. Certaines fonctionnalités de Grid Manager ne seront pas disponibles lorsque les services sont arrêtés sur le nœud d'administration source.

Étapes

1. Connectez-vous au nœud d'administration source :
   a. Saisissez la commande suivante : `ssh admin@grid_node_IP`
   b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
   c. Entrez la commande suivante pour passer à la racine : `su -`
   d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
2. Depuis le nœud d'administration source, arrêter le service Prometheus : `service prometheus stop`
3. Effectuez les étapes suivantes sur le nœud d'administration restauré :
   a. Connectez-vous au nœud d'administration restauré :
      i. Saisissez la commande suivante : `ssh admin@grid_node_IP`
      ii. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
      iii. Entrez la commande suivante pour passer à la racine : `su -`
      iv. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
   b. Arrêtez le service Prometheus : `service prometheus stop`

c. Ajoutez la clé privée SSH à l'agent SSH. Entrez `:ssh-add`

d. Entrez le mot de passe d'accès SSH répertorié dans le `Passwords.txt` fichier.

e. Copiez la base de données Prometheus du nœud d'administration source vers le nœud d'administration restauré : `/usr/local/prometheus/bin/prometheus-clone-db.sh Source_Admin_Node_IP`

f. Lorsque vous y êtes invité, appuyez sur **Enter** pour confirmer que vous souhaitez détruire la nouvelle base de données Prometheus sur le noeud d'administration restauré.

La base de données Prometheus d'origine et ses données historiques sont copiées sur le nœud d'administration restauré. Une fois l'opération de copie effectuée, le script démarre le nœud d'administration restauré. L'état suivant apparaît :

Base de données clonée, démarrage des services

a. Lorsque vous n'avez plus besoin d'un accès sans mot de passe à d'autres serveurs, supprimez la clé privée de l'agent SSH. Entrez `:ssh-add -D`

4. Redémarrez le service Prometheus sur le nœud d'administration source.`service prometheus start`

Restaurez vos données en cas de défaillance d'un nœud d'administration non principal

Restauration après des pannes de nœud d'administration non principal : présentation

Vous devez effectuer les tâches suivantes pour effectuer une restauration à partir d'une panne de nœud d'administration non primaire. Un nœud d'administration héberge le service de nœud de gestion de la configuration (CMN) et est appelé nœud d'administration principal. Bien que vous puissiez avoir plusieurs nœuds d'administration, chaque système StorageGRID n'inclut qu'un seul nœud d'administration principal. Tous les autres nœuds d'administration sont des nœuds d'administration non primaires.

Copie des journaux d'audit à partir d'un nœud d'administration non primaire ayant échoué

Si vous pouvez copier les journaux d'audit depuis le nœud d'administration défaillant, conservez-les pour conserver l'enregistrement de l'activité et de l'utilisation du système dans la grille. Vous pouvez restaurer les journaux d'audit conservés sur le nœud d'administration non primaire restauré après son exécution.

Cette procédure copie les fichiers journaux d'audit du nœud d'administration défaillant vers un emplacement temporaire sur un nœud de grille distinct. Ces journaux conservés peuvent ensuite être copiés sur le nœud d'administration de remplacement. Les journaux d'audit ne sont pas automatiquement copiés sur le nouveau nœud d'administration.

Selon le type de défaillance, il se peut que vous ne puissiez pas copier les journaux d'audit à partir d'un nœud d'administration défaillant. Si le déploiement ne comporte qu'un seul nœud d'administration, le nœud d'administration restauré commence à enregistrer les événements dans le journal d'audit d'un nouveau fichier vide et les données précédemment enregistrées sont perdues. Si le déploiement inclut plusieurs nœuds d'administration, vous pouvez récupérer les journaux d'audit à partir d'un autre nœud d'administration.

Si les journaux d'audit ne sont pas accessibles sur le nœud d'administration défaillant maintenant, vous pourrez peut-être y accéder ultérieurement, par exemple après la restauration de l'hôte.

1. Si possible, connectez-vous au nœud d'administration défaillant. Sinon, connectez-vous au nœud d'administration principal ou à un autre nœud d'administration, le cas échéant.
   a. Saisissez la commande suivante : `ssh admin@grid_node_IP`
   b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
   c. Entrez la commande suivante pour passer à la racine : `su -`
   d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

   Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.
2. Arrêtez le service AMS pour l'empêcher de créer un nouveau fichier journal :`service ams stop`
3. Renommez le fichier audit.log de sorte qu'il ne remplace pas le fichier existant lorsque vous le copiez sur le nœud d'administration restauré.

   Renommez audit.log en un nom de fichier numéroté unique. Par exemple, renommez le fichier audit.log en `2023-10-25.txt.1`.

   ```
   cd /var/local/audit/export
   ls -l
   mv audit.log 2023-10-25.txt.1
   ```
4. Redémarrez le service AMS : `service ams start`
5. Créez le répertoire pour copier tous les fichiers journaux d'audit vers un emplacement temporaire sur un nœud de grille distinct : `ssh admin@grid_node_IP mkdir -p /var/local/tmp/saved-audit-logs`

   Lorsque vous y êtes invité, entrez le mot de passe pour l'administrateur.
6. Copier tous les fichiers journaux d'audit : `scp -p * admin@grid_node_IP:/var/local/tmp/saved-audit-logs`

   Lorsque vous y êtes invité, entrez le mot de passe pour l'administrateur.
7. Se déconnecter en tant que racine : `exit`

Remplacez un nœud d'administration non primaire

Pour restaurer un noeud d'administration non primaire, vous devez d'abord remplacer le matériel physique ou virtuel.

Vous pouvez remplacer un noeud d'administration non primaire défaillant par un noeud d'administration non primaire exécuté sur la même plate-forme, ou remplacer un noeud d'administration non primaire exécuté sur VMware ou un hôte Linux par un noeud d'administration non primaire hébergé sur une appliance de services.

Utilisez la procédure qui correspond à la plate-forme de remplacement que vous sélectionnez pour le nœud. Après avoir effectué la procédure de remplacement de nœud (adaptée à tous les types de nœuds), cette procédure vous dirige vers l'étape suivante pour la restauration de nœud d'administration non primaire.

Et de remplacement	Procédure
VMware	"Remplacement d'un noeud VMware"
Linux	"Remplacer un noeud Linux"
Appareils de services SG100 et SG1000	"Remplacer une appliance de services"
OpenStack	Les fichiers et scripts de disques de machine virtuelle fournis par NetApp pour OpenStack ne sont plus pris en charge pour les opérations de restauration. Si vous devez restaurer un nœud exécuté dans un déploiement OpenStack, téléchargez les fichiers du système d'exploitation Linux. Suivre ensuite la procédure pour "Remplacement d'un nœud Linux".

Sélectionnez Démarrer la restauration pour configurer un noeud d'administration non primaire

Après avoir remplacé un noeud d'administration non primaire, vous devez sélectionner Démarrer la restauration dans Grid Manager pour configurer le nouveau noeud en remplacement du noeud défaillant.

Avant de commencer

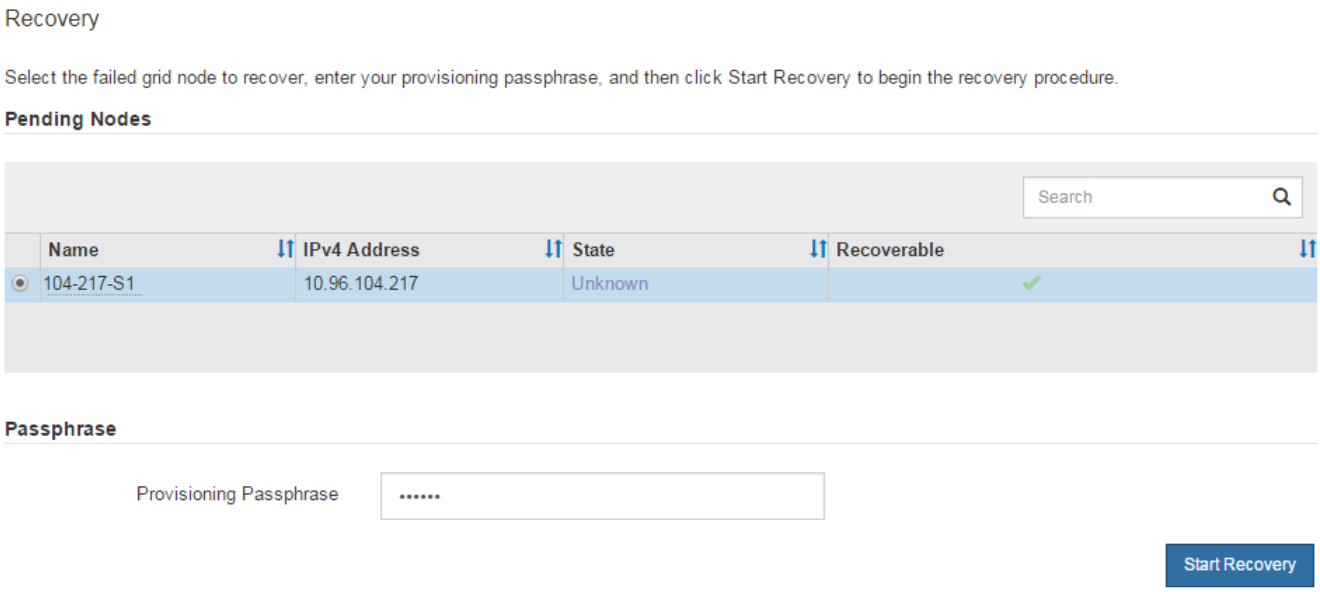
- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous disposez de l'autorisation Maintenance ou accès racine.
- Vous avez la phrase secrète pour le provisionnement.
- Vous avez déployé et configuré le nœud de remplacement.

Étapes

1. Dans le Gestionnaire de grille, sélectionnez **MAINTENANCE** > **tâches** > **récupération**.
2. Sélectionnez le nœud de grille à récupérer dans la liste nœuds en attente.

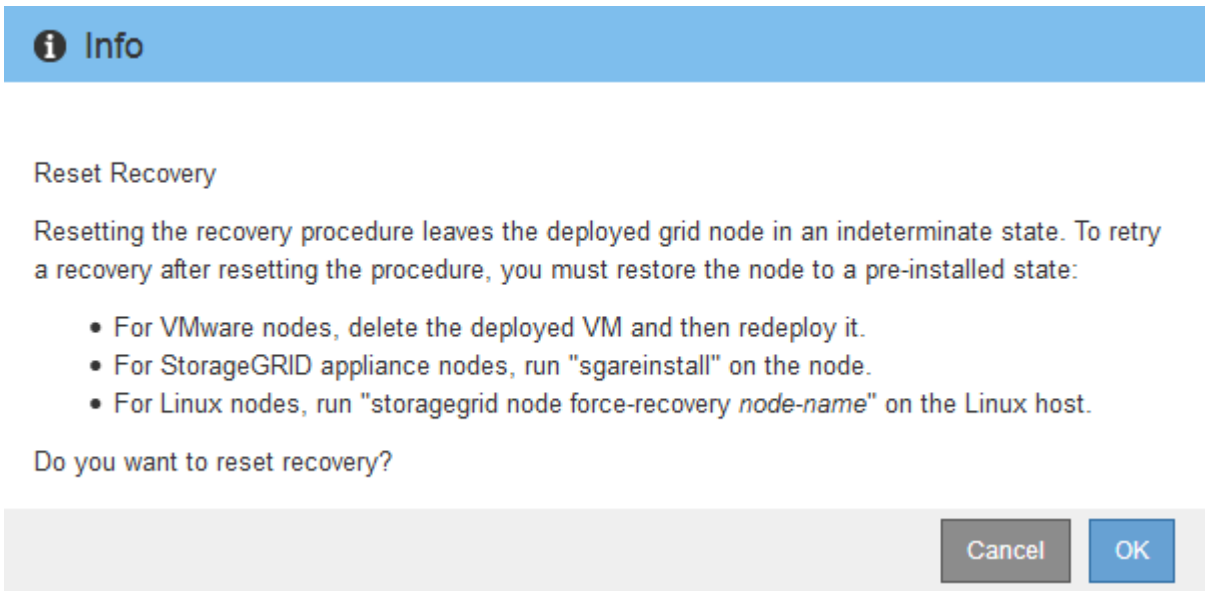
   Les nœuds apparaissent dans la liste après leur échec, mais vous ne pouvez pas sélectionner un nœud tant qu'il n'a pas été réinstallé et qu'il est prêt pour la restauration.

3. Saisissez la phrase de passe de provisionnement *.
4. Cliquez sur **Démarrer la récupération**.



5. Surveiller la progression de la récupération dans le tableau de noeuds de grille de récupération.

> Pendant l'exécution de la procédure de récupération, vous pouvez cliquer sur **Réinitialiser** pour lancer une nouvelle restauration. Une boîte de dialogue s'affiche, indiquant que le nœud restera dans un état indéterminé si vous réinitialisez la procédure.



Si vous souhaitez relancer la restauration après avoir réinitialisé la procédure, vous devez restaurer l'état pré-installé du nœud, comme suit :

- **VMware** : supprimez le nœud de grille virtuelle déployé. Ensuite, lorsque vous êtes prêt à redémarrer la restauration, redéployez le nœud.
- **Linux** : redémarrez le nœud en exécutant cette commande sur l'hôte Linux : `storagegrid node force-recovery node-name`
- **Appliance** : si vous souhaitez réessayer la récupération après la réinitialisation de la procédure, vous devez restaurer le nœud de l'appliance à un état préinstallé en cours d'exécution `sgareinstall` sur le nœud. Voir "Préparez l'appareil pour la réinstallation (remplacement de la plate-forme uniquement)".

6. Si l'authentification unique (SSO) est activée pour votre système StorageGRID et que l'approbation du composant de confiance pour le nœud d'administration que vous avez récupéré a été configurée pour utiliser le certificat d'interface de gestion par défaut, mettre à jour (ou supprimer et recréer) l'approbation du nœud dans Active Directory Federation Services (AD FS). Utilisez le nouveau certificat de serveur par défaut qui a été généré pendant le processus de restauration du noeud d'administration.

> Pour configurer une confiance de partie utilisatrice, reportez-vous à la section "Configurer l'authentification unique". Pour accéder au certificat de serveur par défaut, connectez-vous au shell de commande du noeud d'administration. Accédez au `/var/local/mgmt-api` et sélectionnez `server.crt` fichier.

Restaurez le journal d'audit sur un nœud d'administration non primaire restauré

Si vous avez pu conserver le journal d'audit à partir du noeud d'administration non primaire défaillant, de sorte que les informations du journal d'audit historique soient conservées, vous pouvez le copier sur le noeud d'administration non primaire que vous êtes en train de récupérer.

Avant de commencer

- Le nœud d'administration récupéré est installé et en cours d'exécution.
- Vous avez copié les journaux d'audit à un autre emplacement après l'échec du nœud d'administration d'origine.

Description de la tâche

En cas de panne d'un nœud d'administration, les journaux d'audit enregistrés sur ce nœud d'administration sont potentiellement perdus. Vous pouvez préserver les données contre la perte en copiant les journaux d'audit à partir du nœud d'administration défaillant, puis en les restaurant vers le nœud d'administration restauré. En fonction de la panne, il peut être impossible de copier les journaux d'audit à partir du nœud d'administration défaillant. Dans ce cas, si le déploiement comporte plusieurs nœuds d'administration, vous pouvez récupérer les journaux d'audit à partir d'un autre nœud d'administration, car les journaux d'audit sont répliqués sur tous les nœuds d'administration.

S'il n'y a qu'un seul nœud d'administration et que le journal d'audit ne peut pas être copié depuis le nœud défaillant, le nœud d'administration récupéré commence à enregistrer les événements dans le journal d'audit comme si l'installation était nouvelle.

Vous devez restaurer un noeud d'administration dès que possible pour restaurer la fonctionnalité de journalisation.

> Par défaut, les informations d'audit sont envoyées au journal d'audit des nœuds d'administration. Vous pouvez ignorer ces étapes si l'une des conditions suivantes s'applique :
>
> - Un serveur syslog externe et des journaux d'audit sont maintenant envoyés au serveur syslog au lieu de vers les nœuds d'administration.
> - Vous avez explicitement indiqué que les messages d'audit doivent être enregistrés uniquement sur les nœuds locaux qui les ont générés.
>
> Voir "Configurez les messages d'audit et les destinations des journaux" pour plus d'informations.

Étapes

1. Connectez-vous au nœud d'administration restauré :

   a. Saisissez la commande suivante :
   `ssh admin@recovery_Admin_Node_IP`

   b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

   c. Entrez la commande suivante pour passer à la racine : `su -`

   d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

   Une fois que vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

2. Vérifiez quels fichiers d'audit ont été conservés :

   ```
   cd /var/local/audit/export
   ```

3. Copiez les fichiers journaux d'audit conservés sur le nœud d'administration restauré :

   ```
   scp admin@grid_node_IP:/var/local/tmp/saved-audit-logs/YYYY*
   ```

   Lorsque vous y êtes invité, entrez le mot de passe pour l'administrateur.

4. Pour plus de sécurité, supprimez les journaux d'audit du nœud de grille défaillant après avoir vérifié qu'ils ont bien été copiés sur le nœud d'administration restauré.
5. Mettez à jour les paramètres utilisateur et groupe des fichiers journaux d'audit sur le nœud d'administration restauré :

   ```
   chown ams-user:bycast *
   ```

6. Se déconnecter en tant que racine : `exit`

Vous devez également restaurer tout accès client existant au partage d'audit. Pour plus d'informations, voir "Configurez l'accès client d'audit".

Restaurez la base de données du nœud d'administration lors de la restauration d'un nœud d'administration non primaire

Si vous souhaitez conserver les informations historiques relatives aux attributs, aux alarmes et aux alertes sur un nœud d'administration non primaire qui a échoué, vous pouvez restaurer la base de données du nœud d'administration à partir du nœud d'administration principal.

Avant de commencer

- Le nœud d'administration récupéré est installé et en cours d'exécution.
- Le système StorageGRID comprend au moins deux nœuds d'administration.
- Vous avez le `Passwords.txt` fichier.
- Vous avez la phrase secrète pour le provisionnement.

Description de la tâche

En cas de défaillance d'un nœud d'administration, les informations historiques stockées dans sa base de données de nœud d'administration sont perdues. Cette base de données contient les informations suivantes :

- Historique des alertes
- Historique des alarmes
- Les données d'attributs historiques, qui sont utilisées dans les graphiques et les rapports texte disponibles à partir de la page **SUPPORT** > **Outils** > **topologie de grille**.

Lorsque vous restaurez un noeud d'administration, le processus d'installation du logiciel crée une base de données de noeud d'administration vide sur le noeud récupéré. Toutefois, la nouvelle base de données comprend uniquement les informations pour les serveurs et services qui font actuellement partie du système ou qui sont ajoutés ultérieurement.

Si vous avez restauré un noeud d'administration non primaire, vous pouvez restaurer les informations d'historique en copiant la base de données du noeud d'administration principal (le noeud d'administration *source*) vers le noeud récupéré.

> La copie de la base de données du nœud d'administration peut prendre plusieurs heures. Certaines fonctions de Grid Manager ne seront pas disponibles lorsque les services sont arrêtés sur le nœud source.

Étapes

1. Connectez-vous au nœud d'administration source :
   a. Saisissez la commande suivante : `ssh admin@grid_node_IP`
   b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
   c. Entrez la commande suivante pour passer à la racine : `su -`
   d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
2. Exécutez la commande suivante depuis le nœud d'administration source. Saisissez ensuite la phrase de passe de provisionnement si vous y êtes invité. `recover-access-points`
3. Depuis le nœud d'administration source, arrêtez le service MI : `service mi stop`
4. Depuis le nœud d'administration source, arrêtez le service Management application Program interface (mgapi) : `service mgmt-api stop`
5. Effectuez les étapes suivantes sur le nœud d'administration restauré :
   a. Connectez-vous au nœud d'administration restauré :
      i. Saisissez la commande suivante : `ssh admin@grid_node_IP`
      ii. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
      iii. Entrez la commande suivante pour passer à la racine : `su -`
      iv. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
   b. Arrêtez le service MI : `service mi stop`
   c. Arrêt du service mgmt-api : `service mgmt-api stop`
   d. Ajoutez la clé privée SSH à l'agent SSH. Entrez :`ssh-add`
   e. Entrez le mot de passe d'accès SSH répertorié dans le `Passwords.txt` fichier.
   f. Copiez la base de données du nœud d'administration source vers le nœud d'administration restauré : `/usr/local/mi/bin/mi-clone-db.sh Source_Admin_Node_IP`

g. Lorsque vous y êtes invité, confirmez que vous souhaitez remplacer la base DE données MI sur le nœud d'administration restauré.

   La base de données et ses données historiques sont copiées dans le nœud d'administration restauré. Une fois l'opération de copie effectuée, le script démarre le nœud d'administration restauré.

h. Lorsque vous n'avez plus besoin d'un accès sans mot de passe à d'autres serveurs, supprimez la clé privée de l'agent SSH. Entrez `:ssh-add -D`

6. Redémarrez les services sur le nœud d'administration source : `service servermanager start`

Restaurez des metrics Prometheus lors de la récupération d'un nœud d'administration non primaire

Vous pouvez également conserver les metrics historiques gérés par Prometheus sur un nœud d'administration non primaire qui a échoué.

Avant de commencer

- Le nœud d'administration récupéré est installé et en cours d'exécution.
- Le système StorageGRID comprend au moins deux nœuds d'administration.
- Vous avez le `Passwords.txt` fichier.
- Vous avez la phrase secrète pour le provisionnement.

Description de la tâche

En cas de panne d'un nœud d'administration, les metrics gérés dans la base de données Prometheus sur le nœud d'administration sont perdus. Lorsque vous restaurez le nœud d'administration, un processus d'installation logicielle crée une nouvelle base de données Prometheus. Une fois le nœud d'administration restauré démarré, il enregistre les metrics comme si vous aviez déjà effectué une nouvelle installation du système StorageGRID.

Si vous avez restauré un noeud d'administration non primaire, vous pouvez restaurer les metrics historiques en copiant la base de données Prometheus du noeud d'administration principal (le *source Admin Node*) vers le noeud d'administration récupéré.

> La copie de la base de données Prometheus peut prendre une heure ou plus. Certaines fonctionnalités de Grid Manager ne seront pas disponibles lorsque les services sont arrêtés sur le nœud d'administration source.

Étapes

1. Connectez-vous au nœud d'administration source :
   a. Saisissez la commande suivante : `ssh admin@grid_node_IP`
   b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
   c. Entrez la commande suivante pour passer à la racine : `su -`
   d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
2. Depuis le nœud d'administration source, arrêter le service Prometheus : `service prometheus stop`
3. Effectuez les étapes suivantes sur le nœud d'administration restauré :
   a. Connectez-vous au nœud d'administration restauré :

i. Saisissez la commande suivante : `ssh admin@grid_node_IP`

ii. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

iii. Entrez la commande suivante pour passer à la racine : `su -`

iv. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

b. Arrêtez le service Prometheus : `service prometheus stop`

c. Ajoutez la clé privée SSH à l'agent SSH. Entrez :`ssh-add`

d. Entrez le mot de passe d'accès SSH répertorié dans le `Passwords.txt` fichier.

e. Copiez la base de données Prometheus du nœud d'administration source vers le nœud d'administration restauré : `/usr/local/prometheus/bin/prometheus-clone-db.sh Source_Admin_Node_IP`

f. Lorsque vous y êtes invité, appuyez sur **Enter** pour confirmer que vous souhaitez détruire la nouvelle base de données Prometheus sur le noeud d'administration restauré.

La base de données Prometheus d'origine et ses données historiques sont copiées sur le nœud d'administration restauré. Une fois l'opération de copie effectuée, le script démarre le nœud d'administration restauré. L'état suivant apparaît :

Base de données clonée, démarrage des services

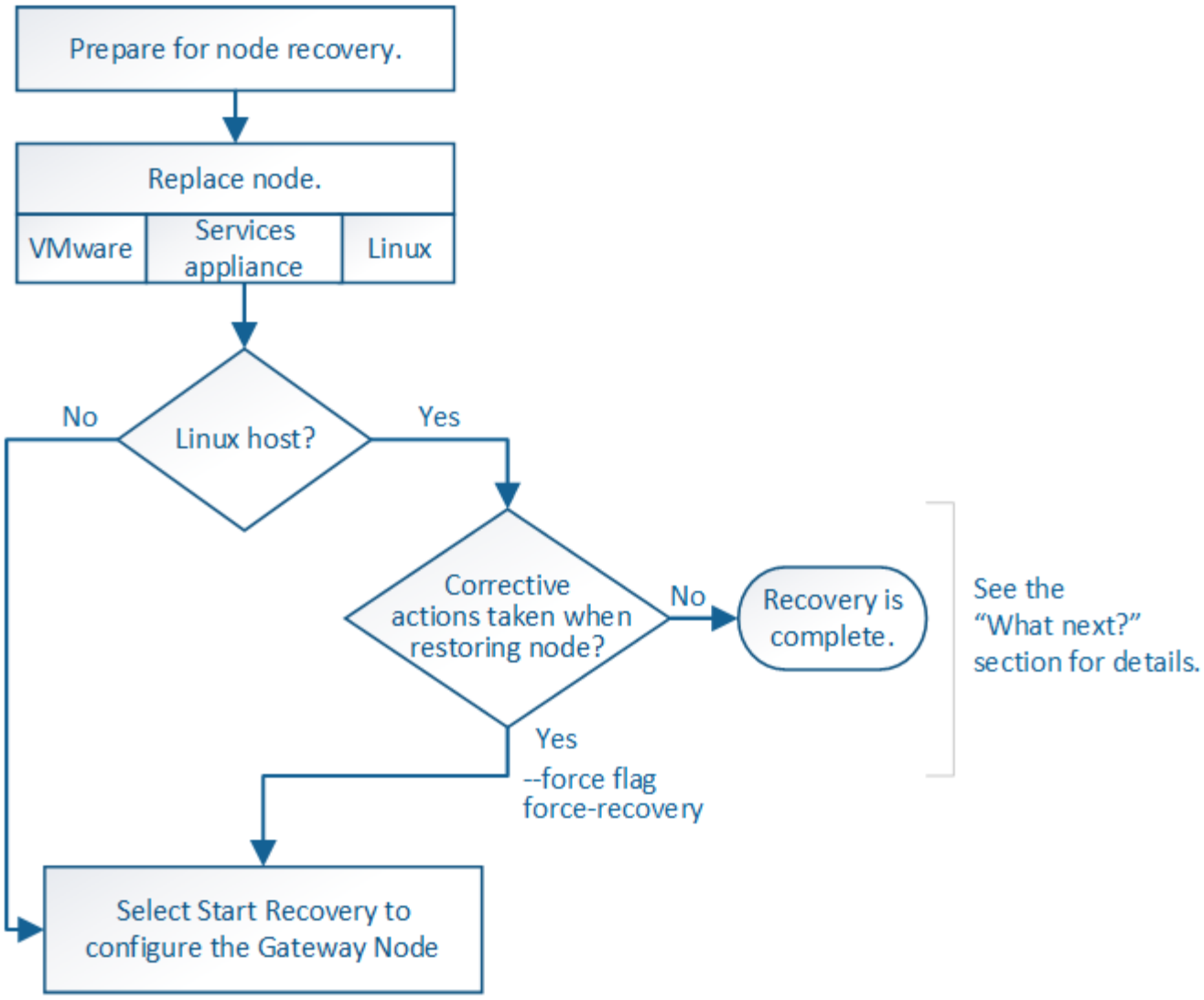
a. Lorsque vous n'avez plus besoin d'un accès sans mot de passe à d'autres serveurs, supprimez la clé privée de l'agent SSH. Entrez :`ssh-add -D`

4. Redémarrez le service Prometheus sur le nœud d'administration source.`service prometheus start`

Restaurez les données à partir d'une défaillance de nœud de passerelle

Défaillances de restauration à partir du nœud de passerelle : workflow

Vous devez effectuer une séquence de tâches afin de pouvoir effectuer une restauration suite à une défaillance du noeud de passerelle.



Remplacer le nœud de passerelle

Vous pouvez remplacer un nœud de passerelle défaillant par un nœud de passerelle exécuté sur le même matériel physique ou virtuel, ou remplacer un nœud de passerelle exécuté sur VMware ou un hôte Linux par un nœud de passerelle hébergé sur une appliance de services.

La procédure de remplacement des nœuds que vous devez suivre dépend de la plateforme à utiliser par le nœud de remplacement. Une fois la procédure de remplacement de nœud terminée, qui convient à tous les types de nœud, cette procédure vous dirige vers l'étape suivante pour la restauration du nœud de passerelle.

Et de remplacement	Procédure
VMware	"Remplacement d'un noeud VMware"
Linux	"Remplacer un noeud Linux"
Appareils de services SG100 et SG1000	"Remplacer une appliance de services"

Et de remplacement	Procédure
OpenStack	Les fichiers et scripts de disques de machine virtuelle fournis par NetApp pour OpenStack ne sont plus pris en charge pour les opérations de restauration. Si vous devez restaurer un nœud exécuté dans un déploiement OpenStack, téléchargez les fichiers du système d'exploitation Linux. Suivre ensuite la procédure pour "Remplacement d'un nœud Linux".

Sélectionnez Démarrer la récupération pour configurer le nœud de passerelle

Après avoir remplacé un noeud de passerelle, vous devez sélectionner Démarrer la restauration dans Grid Manager pour configurer le nouveau noeud en remplacement du noeud défaillant.

Avant de commencer

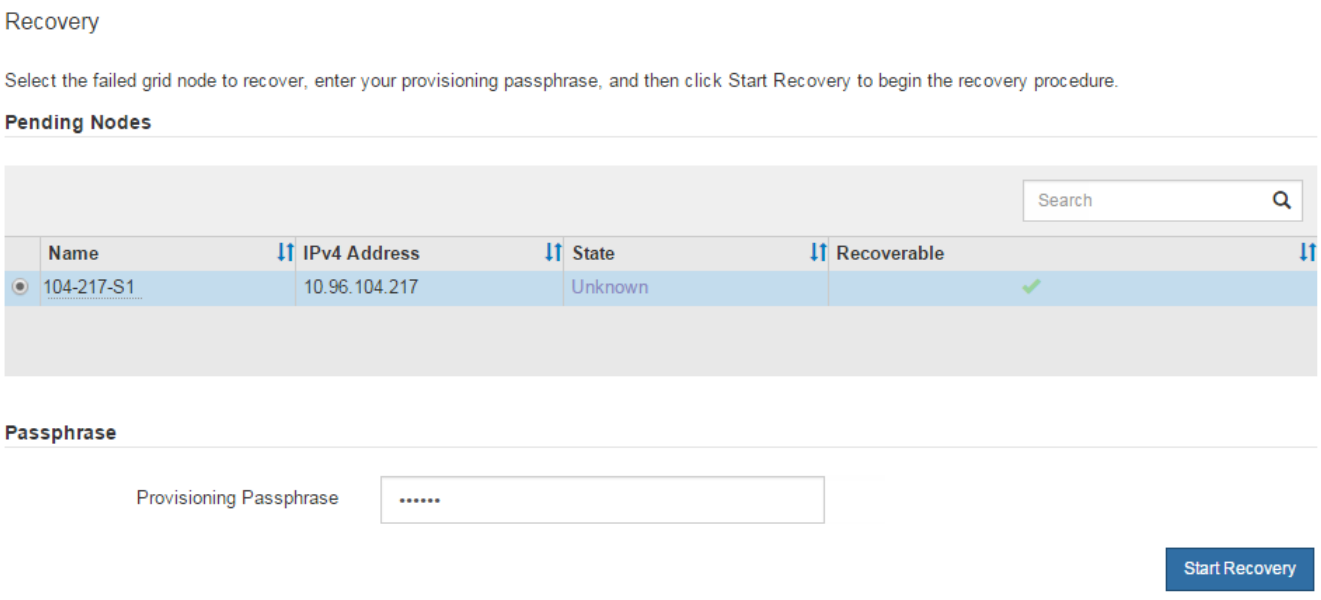
- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous disposez de l'autorisation Maintenance ou accès racine.
- Vous avez la phrase secrète pour le provisionnement.
- Vous avez déployé et configuré le nœud de remplacement.

Étapes

1. Dans le Gestionnaire de grille, sélectionnez **MAINTENANCE** > **tâches** > **récupération**.
2. Sélectionnez le nœud de grille à récupérer dans la liste nœuds en attente.

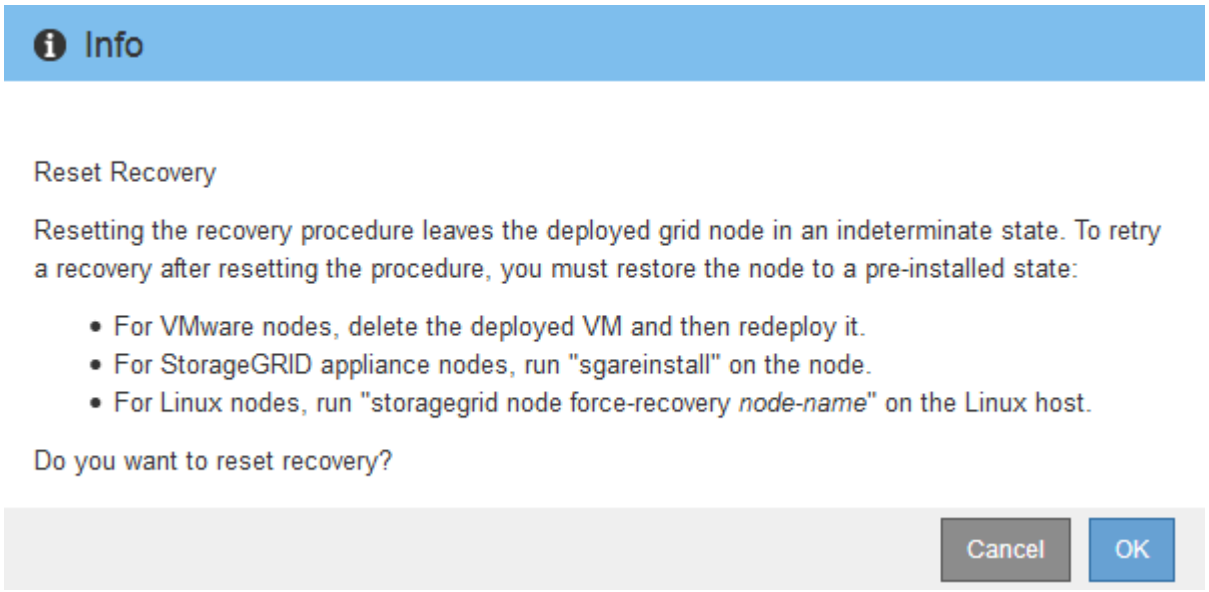
   Les nœuds apparaissent dans la liste après leur échec, mais vous ne pouvez pas sélectionner un nœud tant qu'il n'a pas été réinstallé et qu'il est prêt pour la restauration.

3. Saisissez la phrase de passe de provisionnement *.
4. Cliquez sur **Démarrer la récupération**.



5. Surveiller la progression de la récupération dans le tableau de noeuds de grille de récupération.

> Pendant l'exécution de la procédure de récupération, vous pouvez cliquer sur **Réinitialiser** pour lancer une nouvelle restauration. Une boîte de dialogue s'affiche, indiquant que le nœud restera dans un état indéterminé si vous réinitialisez la procédure.



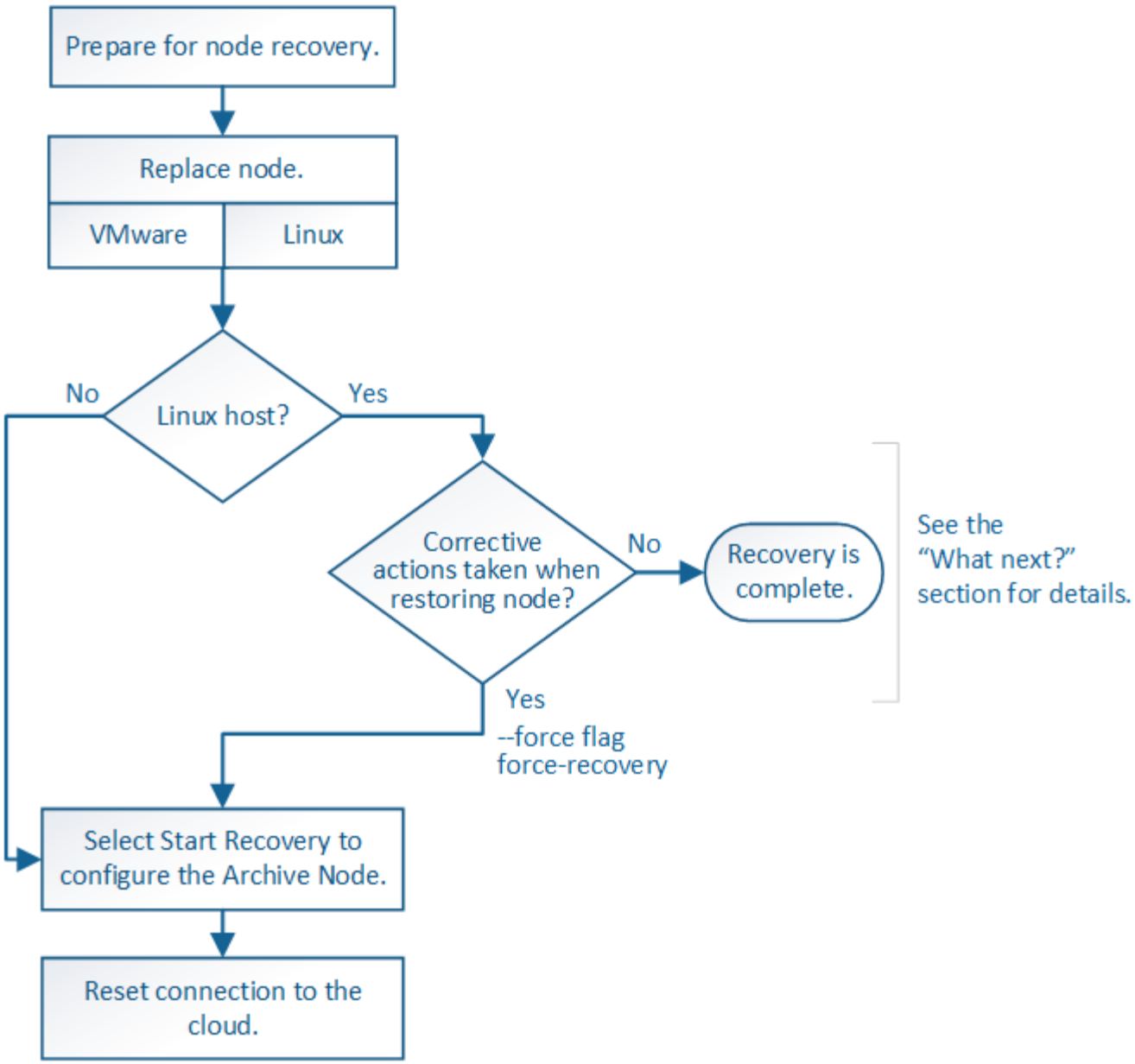
Si vous souhaitez relancer la restauration après avoir réinitialisé la procédure, vous devez restaurer l'état pré-installé du nœud, comme suit :

- **VMware** : supprimez le nœud de grille virtuelle déployé. Ensuite, lorsque vous êtes prêt à redémarrer la restauration, redéployez le nœud.
- **Linux** : redémarrez le nœud en exécutant cette commande sur l'hôte Linux : `storagegrid node force-recovery node-name`
- **Appliance** : si vous souhaitez réessayer la récupération après la réinitialisation de la procédure, vous devez restaurer le nœud de l'appliance à un état préinstallé en cours d'exécution `sgareinstall` sur le nœud. Voir "Préparez l'appareil pour la réinstallation (remplacement de la plate-forme uniquement)".

Échec de la restauration à partir du nœud d'archivage

Échec de la restauration à partir du nœud d'archivage : workflow

Vous devez effectuer une séquence de tâches pour pouvoir effectuer une restauration suite à un échec de nœud d'archivage.



La restauration du nœud d'archivage est affectée par les problèmes suivants :

- Si la règle ILM est configurée pour répliquer une seule copie.

  Dans un système StorageGRID configuré pour créer une seule copie des objets, une défaillance de nœud d'archivage peut entraîner une perte irrécupérable de données. En cas d'échec, tous ces objets sont perdus ; cependant, vous devez toujours exécuter des procédures de restauration pour « nettoyer » votre système StorageGRID et purger les informations d'objet perdues de la base de données.

- En cas de défaillance d'un nœud d'archivage lors de la restauration du nœud de stockage.

  Si le nœud d'archivage échoue lors du traitement des récupérations en bloc dans le cadre d'une restauration de nœud de stockage, Vous devez répéter la procédure pour récupérer des copies de données d'objet sur le nœud de stockage depuis le début pour vous assurer que toutes les données d'objet extraites du nœud d'archivage sont restaurées sur le nœud de stockage.

Remplacer le nœud d'archivage

Pour restaurer un noeud d'archivage, vous devez d'abord remplacer le noeud.

Vous devez sélectionner la procédure de remplacement de nœuds pour votre plate-forme. Les étapes à suivre pour remplacer un nœud sont les mêmes pour tous les types de nœuds de la grille.

Plateforme	Procédure
VMware	"Remplacement d'un noeud VMware"
Linux	"Remplacer un noeud Linux"
OpenStack	Les fichiers et scripts de disques de machine virtuelle fournis par NetApp pour OpenStack ne sont plus pris en charge pour les opérations de restauration. Si vous devez restaurer un nœud exécuté dans un déploiement OpenStack, téléchargez les fichiers du système d'exploitation Linux. Suivre ensuite la procédure pour "Remplacement d'un nœud Linux".

Sélectionnez Démarrer la restauration pour configurer le nœud d'archivage

Après avoir remplacé un noeud d'archivage, vous devez sélectionner Démarrer la restauration dans le Gestionnaire de grille pour configurer le nouveau noeud en remplacement du noeud défaillant.

Avant de commencer

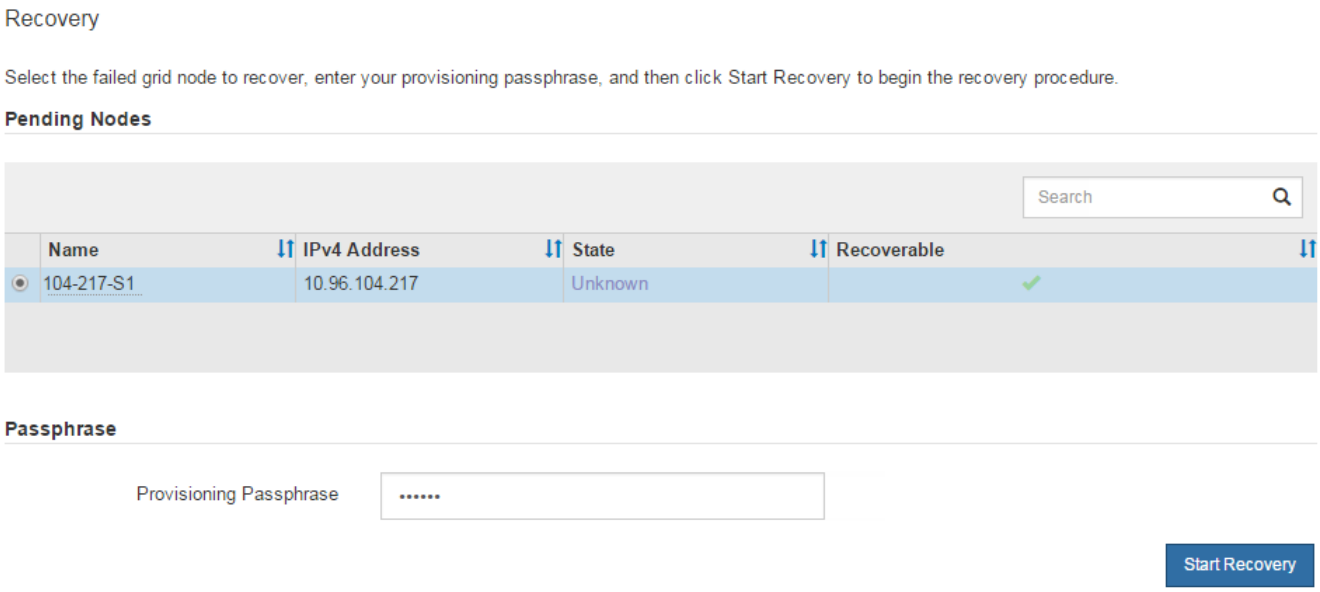
- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous disposez de l'autorisation Maintenance ou accès racine.
- Vous avez la phrase secrète pour le provisionnement.
- Vous avez déployé et configuré le nœud de remplacement.

Étapes

1. Dans le Gestionnaire de grille, sélectionnez **MAINTENANCE** > **tâches** > **récupération**.
2. Sélectionnez le nœud de grille à récupérer dans la liste nœuds en attente.

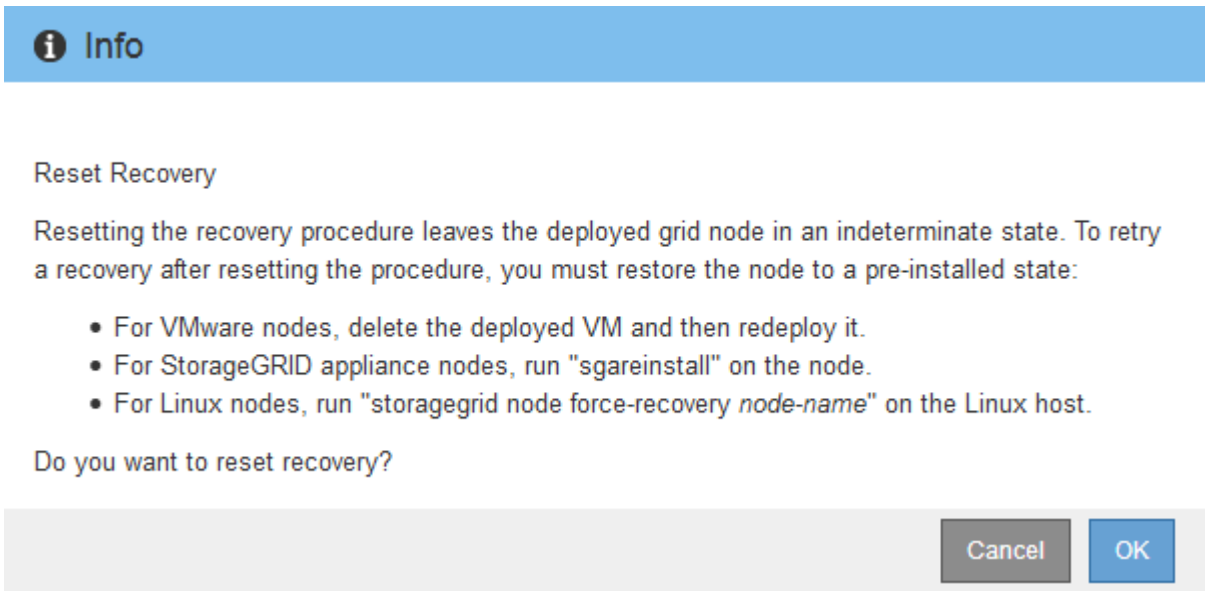
   Les nœuds apparaissent dans la liste après leur échec, mais vous ne pouvez pas sélectionner un nœud tant qu'il n'a pas été réinstallé et qu'il est prêt pour la restauration.

3. Saisissez la phrase de passe de provisionnement *.
4. Cliquez sur **Démarrer la récupération**.



5. Surveiller la progression de la récupération dans le tableau de noeuds de grille de récupération.

> Pendant l'exécution de la procédure de récupération, vous pouvez cliquer sur **Réinitialiser** pour lancer une nouvelle restauration. Une boîte de dialogue s'affiche, indiquant que le nœud restera dans un état indéterminé si vous réinitialisez la procédure.



Si vous souhaitez relancer la restauration après avoir réinitialisé la procédure, vous devez restaurer l'état pré-installé du nœud, comme suit :

- **VMware** : supprimez le nœud de grille virtuelle déployé. Ensuite, lorsque vous êtes prêt à redémarrer la restauration, redéployez le nœud.
- **Linux** : redémarrez le nœud en exécutant cette commande sur l'hôte Linux : `storagegrid node force-recovery node-name`

Réinitialisez la connexion du nœud d'archivage au cloud

Après avoir restaurez un nœud d'archivage qui cible le cloud via l'API S3, vous devez modifier les paramètres de configuration pour réinitialiser les connexions. Une alarme ORSU (Outbound Replication Status) est déclenchée si le nœud d'archivage ne parvient pas à récupérer les données d'objet.

> Si votre nœud d'archivage se connecte au stockage externe via le middleware TSM, le nœud se réinitialise automatiquement et vous n'avez pas besoin de le reconfigurer.

Avant de commencer

Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".

Étapes

1. Sélectionnez **SUPPORT** > **Outils** > **topologie de grille**.
2. Sélectionnez **Archive Node** > **ARC** > **Target**.
3. Modifiez le champ **Access Key** en saisissant une valeur incorrecte et cliquez sur **Apply Changes**.
4. Modifiez le champ **Access Key** en saisissant la valeur correcte et cliquez sur **Apply Changes**.

Tous les types de nœuds de la grille : remplacent les nœuds VMware

Lorsque vous restaurez un nœud StorageGRID en panne hébergé sur VMware, vous supprimez le nœud en panne et déployez un nœud de restauration.

Avant de commencer

Vous avez déterminé que la machine virtuelle ne peut pas être restaurée et doit être remplacée.

Description de la tâche

Utilisez le client Web VMware vSphere pour supprimer d'abord la machine virtuelle associée au nœud de grille défaillant. Vous pouvez ensuite déployer une nouvelle machine virtuelle.

Cette procédure ne représente qu'une étape du processus de restauration du nœud grid. La procédure de suppression et de déploiement des nœuds est la même pour tous les nœuds VMware, y compris les nœuds d'administration, les nœuds de stockage, les nœuds de passerelle et les nœuds d'archivage.

Étapes

1. Connectez-vous au client Web VMware vSphere.
2. Accédez à la machine virtuelle du nœud de grille qui a échoué.
3. Notez toutes les informations nécessaires au déploiement du noeud de restauration.
   a. Cliquez avec le bouton droit de la souris sur la machine virtuelle, sélectionnez l'onglet **Modifier les paramètres** et notez les paramètres utilisés.
   b. Sélectionnez l'onglet **vApp Options** pour afficher et enregistrer les paramètres réseau du nœud de grille.
4. Si le nœud de grille défaillant est un nœud de stockage, déterminez si l'un des disques durs virtuels utilisés pour le stockage des données n'est pas endommagé et conservez-le pour qu'il soit reconnecté au nœud de grille récupéré.
5. Mise hors tension de la machine virtuelle

6. Sélectionnez **actions** > **toutes les actions vCenter** > **Supprimer du disque** pour supprimer la machine virtuelle.
7. Déployez une nouvelle machine virtuelle en tant que nœud de remplacement et connectez-la à un ou plusieurs réseaux StorageGRID. Pour obtenir des instructions, voir "Déploiement d'un nœud StorageGRID en tant que machine virtuelle".

   Lorsque vous déployez le nœud, vous pouvez remappage les ports de nœud ou augmenter les paramètres de processeur ou de mémoire.

   > Après le déploiement du nouveau nœud, vous pouvez ajouter de nouveaux disques virtuels en fonction de vos besoins de stockage, rattacher tout disque dur virtuel conservé à partir du noeud de grille défaillant précédemment retiré, ou les deux.

8. Suivez la procédure de restauration des nœuds, en fonction du type de nœud que vous restaurez.

Type de nœud	Accédez à
Nœud d'administration principal	"Configurez le nœud d'administration principal de remplacement"
Nœud d'administration non primaire	"Sélectionnez Démarrer la restauration pour configurer un noeud d'administration non primaire"
Nœud de passerelle	"Sélectionnez Démarrer la récupération pour configurer le nœud de passerelle"
Nœud de stockage	"Sélectionnez Démarrer la restauration pour configurer le nœud de stockage"
Nœud d'archivage	"Sélectionnez Démarrer la restauration pour configurer le nœud d'archivage"

Tous les types de nœuds grid : remplacez le nœud Linux

Tous les types de nœuds grid : remplacez le nœud Linux

Si une défaillance nécessite le déploiement d'un ou de plusieurs nouveaux hôtes physiques ou virtuels ou la réinstallation de Linux sur un hôte existant, déployez et configurez l'hôte de remplacement avant de pouvoir restaurer le nœud de grille. Cette procédure constitue une étape du processus de restauration des nœuds grid pour tous les types de nœuds.

« Linux » désigne un déploiement Red Hat® Enterprise Linux®, Ubuntu®, CentOS ou Debian®. Utilisez le "Matrice d'interopérabilité NetApp (IMT)" pour obtenir une liste des versions prises en charge.

Cette procédure s'effectue uniquement en une étape du processus de restauration des nœuds de stockage Software-based, des nœuds d'administration principal ou non principaux, des nœuds de passerelle ou des nœuds d'archivage. Les étapes sont identiques quel que soit le type de nœud de grille que vous récupérez.

Si plusieurs nœuds de grille sont hébergés sur un hôte Linux physique ou virtuel, vous pouvez récupérer les nœuds de la grille dans n'importe quel ordre. Toutefois, la restauration d'un nœud d'administration principal, le

cas échéant, empêche la restauration des autres nœuds de la grille lorsqu'ils tentent de contacter le nœud d'administration principal pour s'inscrire à la restauration.

Déploiement de nouveaux hôtes Linux

À quelques exceptions près, vous préparez les nouveaux hôtes comme vous l'avez fait lors du processus d'installation initiale.

Pour déployer de nouveaux hôtes Linux physiques ou virtuels ou les réinstaller, suivez la procédure de préparation des hôtes dans les instructions d'installation de StorageGRID pour votre système d'exploitation Linux :

- "Installation de Linux (Red Hat Enterprise Linux ou CentOS)"
- "Installer Linux (Ubuntu ou Debian)"

Cette procédure comprend les étapes permettant d'effectuer les tâches suivantes :

1. Installez Linux.
2. Configurez le réseau hôte.
3. Configurer le stockage de l'hôte
4. Installer le moteur de mise en conteneurs.
5. Installez le service hôte StorageGRID.

> Arrêtez-vous après avoir terminé la tâche « installer le service hôte StorageGRID » dans les instructions d'installation. Ne démarrez pas la tâche « nœuds grid de déploiement ».

À mesure que vous effectuez ces étapes, prenez note des consignes importantes suivantes :

- Veillez à utiliser les mêmes noms d'interface hôte que ceux utilisés sur l'hôte d'origine.
- Si vous utilisez un stockage partagé pour prendre en charge vos nœuds StorageGRID, ou si vous avez déplacé tout ou partie des disques ou disques SSD de vers les nœuds de remplacement, vous devez rétablir les mêmes mappages du stockage que ceux présents sur l'hôte d'origine. Par exemple, si vous avez utilisé des WWID et des alias dans `/etc/multipath.conf` Comme recommandé dans les instructions d'installation, veillez à utiliser les mêmes paires alias/WWID dans `/etc/multipath.conf` sur l'hôte de remplacement.
- Si le nœud StorageGRID utilise le stockage affecté à un système NetApp ONTAP, vérifiez que cette FabricPool règle n'est pas activée pour le volume. La désactivation du Tiering FabricPool pour les volumes utilisés avec des nœuds StorageGRID simplifie la résolution des problèmes et les opérations de stockage.

> N'utilisez jamais FabricPool pour transférer automatiquement toutes les données liées à StorageGRID vers StorageGRID. Le Tiering des données StorageGRID vers StorageGRID augmente la complexité opérationnelle et la résolution des problèmes.

Restaurez les nœuds de la grille sur l'hôte

Pour restaurer un nœud de grille défaillant sur un nouvel hôte Linux, procédez comme suit afin de restaurer le fichier de configuration du nœud.

1. Restaurer et valider le nœud en restaurant le fichier de configuration du nœud. Pour une nouvelle

installation, vous créez un fichier de configuration de nœud pour chaque nœud de grille à installer sur un hôte. Lors de la restauration d'un nœud de grille sur un hôte de remplacement, vous restaurez ou remplacez le fichier de configuration de nœud pour les nœuds de grille défaillants.

2. Démarrez le service d'hôte StorageGRID.
3. Si nécessaire, restaurez tous les nœuds qui ne démarrent pas.

Si des volumes de stockage en blocs ont été préservés à partir de l'hôte précédent, vous devrez peut-être effectuer des procédures de restauration supplémentaires. Les commandes de cette section vous aident à déterminer les procédures supplémentaires requises.

Restaurez et validez les nœuds de la grille

Vous devez restaurer les fichiers de configuration de la grille de tout nœud de grille ayant échoué, puis valider les fichiers de configuration de la grille et résoudre les erreurs éventuelles.

Description de la tâche

Vous pouvez importer tout nœud de grille qui doit être présent sur l'hôte, tant que son `/var/local` le volume n'a pas été perdu suite à la défaillance de l'hôte précédent. Par exemple, le `/var/local` Il se peut que le volume existe toujours si vous utilisez le stockage partagé pour les volumes de données du système StorageGRID, comme décrit dans les instructions d'installation de StorageGRID pour votre système d'exploitation Linux. L'importation du nœud restaure son fichier de configuration de nœud vers l'hôte.

S'il n'est pas possible d'importer des nœuds manquants, vous devez recréer leurs fichiers de configuration de grille.

Vous devez ensuite valider le fichier de configuration de la grille et résoudre tous les problèmes de réseau ou de stockage qui pourraient se produire avant de redémarrer StorageGRID. Lorsque vous recréez le fichier de configuration d'un nœud, vous devez utiliser le même nom pour le nœud de remplacement utilisé pour le nœud en cours de restauration.

Reportez-vous aux instructions d'installation pour plus d'informations sur l'emplacement du `/var/local` volume pour un nœud.

- "Installez Red Hat Enterprise Linux ou CentOS"
- "Installez Ubuntu ou Debian"

Étapes

1. Sur la ligne de commande de l'hôte restauré, répertoriez tous les nœuds grid StorageGRID actuellement configurés :`sudo storagegrid node list`

   Si aucun nœud de grille n'est configuré, il n'y aura pas de sortie. Si certains nœuds de grid sont configurés, la sortie doit être au format suivant :

```
Name               Metadata-Volume
=============================================================
dc1-adm1           /dev/mapper/sgws-adm1-var-local
dc1-gw1            /dev/mapper/sgws-gw1-var-local
dc1-sn1            /dev/mapper/sgws-sn1-var-local
dc1-arc1           /dev/mapper/sgws-arc1-var-local
```

Si certains ou tous les nœuds de grille qui doivent être configurés sur l'hôte ne sont pas répertoriés, vous devez restaurer les nœuds de grille manquants.

2. Pour importer des nœuds de grille dotés d'un `/var/local` volume :

   a. Exécutez la commande suivante pour chaque nœud à importer :`sudo storagegrid node import node-var-local-volume-path`

      Le `storagegrid node import` la commande ne réussit que si le nœud cible a été arrêté correctement sur l'hôte sur lequel il a été exécuté pour la dernière fois. Si ce n'est pas le cas, vous observez une erreur semblable à ce qui suit :

      ```
      This node (node-name) appears to be owned by another host (UUID host-uuid).

      Use the --force flag if you are sure import is safe.
      ```

   a. Si vous voyez l'erreur relative au nœud qui appartient à un autre hôte, exécutez de nouveau la commande avec le `--force` indicateur pour terminer l'importation :`sudo storagegrid --force node import node-var-local-volume-path`

      > ⓘ Tous les nœuds importés avec le `--force` flag nécessitera des étapes de récupération supplémentaires avant qu'elles ne puissent rejoindre la grille, comme décrit dans "Qu'est-ce qui suit : effectuez d'autres étapes de restauration, le cas échéant".

3. Pour les nœuds grid n'ont pas de `/var/local` volume, recréez le fichier de configuration du nœud pour le restaurer sur l'hôte. Pour obtenir des instructions, reportez-vous à la section :

   - "Créez des fichiers de configuration de nœuds pour Red Hat Enterprise Linux ou CentOS"
   - "Créez des fichiers de configuration de nœud pour Ubuntu ou Debian"

   > ⓘ Lorsque vous recréez le fichier de configuration d'un nœud, vous devez utiliser le même nom pour le nœud de remplacement utilisé pour le nœud en cours de restauration. Pour les déploiements Linux, assurez-vous que le nom du fichier de configuration contient le nom du nœud. Lorsque cela est possible, vous devez utiliser les mêmes interfaces réseau, les mêmes mappages de périphériques de bloc et les mêmes adresses IP. Cette pratique réduit la quantité de données à copier sur le nœud lors de la restauration, ce qui peut accélérer la restauration (dans certains cas, quelques minutes au lieu de plusieurs semaines).

   > ⓘ Si vous utilisez de nouveaux périphériques de bloc (périphériques que le nœud StorageGRID n'utilisait pas auparavant) comme valeurs pour l'une des variables de configuration commençant par `BLOCK_DEVICE_` lorsque vous recréez le fichier de configuration d'un nœud, suivez les instructions de la section Corrigez les erreurs de périphérique de bloc manquantes.

4. Exécutez la commande suivante sur l'hôte restauré pour lister tous les nœuds StorageGRID.

   ```
   sudo storagegrid node list
   ```

5. Valider le fichier de configuration de nœud pour chaque nœud de la grille dont le nom s'affiche dans la sortie de la liste des nœuds StorageGRID :

`sudo storagegrid node validate node-name`

Vous devez corriger toute erreur ou avertissement avant de démarrer le service hôte StorageGRID. Les sections suivantes donnent plus de détails sur les erreurs susceptibles d'avoir une importance particulière pendant la récupération.

Corrigez les erreurs d'interface réseau manquantes

Si le réseau hôte n'est pas configuré correctement ou si un nom est mal orthographié, une erreur se produit lorsque StorageGRID vérifie le mappage spécifié dans l' `/etc/storagegrid/nodes/node-name.conf` fichier.

Une erreur ou un avertissement correspondant à ce modèle peut s'afficher :

```
Checking configuration file /etc/storagegrid/nodes/<node-name>.conf for
node <node-name>...
ERROR: <node-name>: GRID_NETWORK_TARGET = <host-interface-name>
       <node-name>: Interface <host-interface-name>' does not exist
```

L'erreur peut être signalée pour le réseau Grid, le réseau Admin ou le réseau client. Cette erreur signifie que le `/etc/storagegrid/nodes/node-name.conf` Le fichier mappe le réseau StorageGRID indiqué sur l'interface hôte nommée *`host-interface-name`*, mais il n'y a pas d'interface avec ce nom sur l'hôte actuel.

Si vous recevez cette erreur, vérifiez que vous avez terminé les étapes de la section "Déploiement de nouveaux hôtes Linux". Utilisez les mêmes noms pour toutes les interfaces hôtes que ceux utilisés sur l'hôte d'origine.

Si vous ne parvenez pas à nommer les interfaces hôtes pour qu'elles correspondent au fichier de configuration du nœud, vous pouvez modifier le fichier de configuration du nœud et modifier la valeur de GRID_NETWORK_TARGET, ADMIN_NETWORK_TARGET ou client_NETWORK_TARGET pour qu'elle corresponde à une interface hôte existante.

Assurez-vous que l'interface hôte donne accès au port réseau physique ou au VLAN approprié et que l'interface ne fait pas directement référence à un périphérique de liaison ou de pont. Vous devez soit configurer un VLAN (soit une autre interface virtuelle) sur le périphérique de liaison de l'hôte, soit utiliser un pont et une paire Ethernet virtuelle (veth).

Corrigez les erreurs de périphérique de bloc manquantes

Le système vérifie que chaque nœud récupéré est associé à un fichier spécial de périphérique de bloc valide ou à un lien logiciel valide vers un fichier spécial de périphérique de bloc. Si StorageGRID trouve un mappage non valide dans le `/etc/storagegrid/nodes/node-name.conf` fichier, une erreur de périphérique de bloc manquant s'affiche.

Si vous observez une erreur correspondant à ce modèle :

```
Checking configuration file /etc/storagegrid/nodes/<node-name>.conf for
node <node-name>...
ERROR: <node-name>: BLOCK_DEVICE_PURPOSE = <path-name>
       <node-name>: <path-name> does not exist
```

Cela signifie que `/etc/storagegrid/nodes/node-name.conf` mappe le périphérique de bloc utilisé par *nom-nœud* pour `PURPOSE` Au nom de chemin indiqué dans le système de fichiers Linux, mais il n'existe pas de fichier spécial de périphérique de bloc valide, ou de lien logiciel vers un fichier spécial de périphérique de bloc, à cet emplacement.

Vérifiez que vous avez terminé les étapes de la section "Déploiement de nouveaux hôtes Linux". Utilisez les mêmes noms de périphériques persistants pour tous les périphériques de bloc que ceux utilisés sur l'hôte d'origine.

Si vous ne parvenez pas à restaurer ou à recréer le fichier spécial de périphérique de bloc manquant, vous pouvez attribuer un nouveau périphérique de bloc de la taille et de la catégorie de stockage appropriées et modifier le fichier de configuration de nœud pour modifier la valeur de `BLOCK_DEVICE_PURPOSE` pour pointer vers le nouveau fichier spécial de périphérique de bloc.

Déterminez la taille et la catégorie de stockage appropriées à l'aide des tableaux correspondant à votre système d'exploitation Linux :

- "Exigences de stockage et de performance pour Red Hat Enterprise Linux ou CentOS"
- "Exigences en matière de stockage et de performances pour Ubuntu ou Debian"

Consultez les recommandations de configuration du stockage hôte avant de procéder au remplacement du périphérique de bloc :

- "Configurez le stockage hôte pour Red Hat Enterprise Linux ou CentOS"
- "Configurer le stockage hôte pour Ubuntu ou Debian"

> Si vous devez fournir une nouvelle unité de stockage bloc pour l'une des variables de fichier de configuration commençant par `BLOCK_DEVICE_` comme le périphérique de bloc d'origine a été perdu avec l'hôte défaillant, assurez-vous que le nouveau périphérique de bloc n'est pas formaté avant de tenter d'autres procédures de récupération. Le nouveau périphérique de bloc n'est pas formaté si vous utilisez un stockage partagé et que vous avez créé un nouveau volume. Si vous n'êtes pas certain, exécutez la commande suivante sur tout nouveau fichier spécial de périphérique de stockage en mode bloc.

> Exécutez la commande suivante uniquement pour les nouveaux périphériques de stockage en mode bloc. N'exécutez pas cette commande si vous pensez que le stockage en mode bloc contient toujours des données valides pour le nœud en cours de restauration, car toutes les données du périphérique seront perdues.
>
> ```
> sudo dd if=/dev/zero of=/dev/mapper/my-block-device-name bs=1G count=1
> ```

Démarrez le service d'hôte StorageGRID

Pour démarrer vos nœuds StorageGRID et s'assurer qu'ils redémarrent après un redémarrage de l'hôte, vous devez activer et démarrer le service hôte StorageGRID.

Étapes

1. Exécutez les commandes suivantes sur chaque hôte :

```
sudo systemctl enable storagegrid
sudo systemctl start storagegrid
```

2. Exécutez la commande suivante pour vérifier que le déploiement se déroule :

```
sudo storagegrid node status node-name
```

3. Si un nœud renvoie le statut « Not running » ou « Ssured, », exécutez la commande suivante :

```
sudo storagegrid node start node-name
```

4. Si vous avez déjà activé et démarré le service hôte StorageGRID (ou si vous n'êtes pas sûr que le service a été activé et démarré), exécutez également la commande suivante :

```
sudo systemctl reload-or-restart storagegrid
```

Restaurez les nœuds qui ne démarrent pas normalement

Si un nœud StorageGRID ne rejoint pas la grille normalement et qu'il n'apparaît pas comme récupérable, il est possible qu'il soit corrompu. Vous pouvez forcer le nœud en mode de récupération.

Étapes

1. Vérifiez que la configuration réseau du nœud est correcte.

   Le nœud n'a peut-être pas pu rejoindre la grille en raison de mappages d'interface réseau incorrects ou d'une adresse IP ou d'une passerelle de réseau Grid incorrecte.

2. Si la configuration réseau est correcte, exécutez le `force-recovery` commande :

   `sudo storagegrid node force-recovery` *`node-name`*

3. Effectuez les étapes de restauration supplémentaires pour le nœud. Voir "Qu'est-ce qui suit : effectuez d'autres étapes de restauration, le cas échéant".

Qu'est-ce qui suit : effectuez des étapes de récupération supplémentaires, si nécessaire

En fonction des actions spécifiques que vous avez effectuées pour exécuter les nœuds StorageGRID sur l'hôte de remplacement, vous devrez peut-être effectuer des étapes de restauration supplémentaires pour chaque nœud.

La récupération de nœud est terminée si vous n'avez pas besoin d'effectuer d'actions correctives pendant que vous avez remplacé l'hôte Linux ou restauré le nœud de grille défaillant vers le nouvel hôte.

Actions correctives et étapes suivantes

Lors du remplacement d'un nœud, vous devrez peut-être effectuer l'une des actions correctives suivantes :

- Il fallait utiliser le `--force` indicateur pour importer le nœud.
- Pour tous `<PURPOSE>`, la valeur de l' `BLOCK_DEVICE_<PURPOSE>` la variable de fichier de configuration fait référence à un périphérique de bloc qui ne contient pas les mêmes données qu'avant l'échec de l'hôte.
- Vous avez émis `storagegrid node force-recovery node-name` pour le nœud.
- Vous avez ajouté un nouveau périphérique de bloc.

Si vous avez pris **l'une** de ces actions correctives, vous devez effectuer des étapes de récupération supplémentaires.

Type de restauration	Étape suivante
Nœud d'administration principal	"Configurez le nœud d'administration principal de remplacement"
Nœud d'administration non primaire	"Sélectionnez Démarrer la restauration pour configurer un noeud d'administration non primaire"
Nœud de passerelle	"Sélectionnez Démarrer la récupération pour configurer le nœud de passerelle"
Nœud d'archivage	"Sélectionnez Démarrer la restauration pour configurer le nœud d'archivage"
Nœud de stockage (basé sur logiciel) : • Si vous devez utiliser le `--force` indicateur pour importer le nœud, ou vous avez émis `storagegrid node force-recovery node-name` • Si vous deviez effectuer une réinstallation complète du nœud, ou si vous deviez restaurer /var/local	"Sélectionnez Démarrer la restauration pour configurer le nœud de stockage"
Nœud de stockage (basé sur logiciel) : • Si vous avez ajouté un nouveau périphérique de bloc. • Le cas échéant `<PURPOSE>`, la valeur de l' `BLOCK_DEVICE_<PURPOSE>` la variable de fichier de configuration fait référence à un périphérique de bloc qui ne contient pas les mêmes données qu'avant l'échec de l'hôte.	"Restaurez le disque d'après la panne du volume de stockage là où le disque du système est intact"

Remplacez le nœud défectueux par l'appliance de services

Remplacement d'un nœud défaillant par une appliance de services : présentation

Vous pouvez utiliser une appliance de services SG100 ou SG1000 pour récupérer un nœud de passerelle défaillant, un nœud d'administration non primaire défaillant ou un nœud d'administration principal défaillant hébergé sur VMware, un hôte Linux ou une appliance de services. Cette procédure constitue une étape de la procédure de restauration des nœuds de la grille.

Avant de commencer

- Vous avez déterminé que l'une des situations suivantes est vraie :
  - Impossible de restaurer la machine virtuelle hébergeant le nœud.
  - L'hôte Linux physique ou virtuel du nœud grid a échoué et doit être remplacé.
  - L'appliance de services qui héberge le nœud de grid doit être remplacée.
- Vous avez confirmé que la version du programme d'installation de l'appliance StorageGRID installée sur l'appliance de services correspond à la version logicielle de votre système StorageGRID. Voir "Vérifiez et mettez à niveau la version du programme d'installation de l'appliance StorageGRID".

> Ne déployez pas à la fois une appliance de services SG100 et SG1000 sur le même site. Cela peut entraîner des performances imprévisibles.

Description de la tâche

Vous pouvez utiliser une appliance de services SG100 ou SG1000 pour restaurer un nœud de grille défaillant dans les cas suivants :

- Le nœud défaillant était hébergé sur VMware ou Linux ("changement de plateforme")
- Le nœud défaillant était hébergé sur une appliance de services ("remplacement de la plate-forme")

Installer l'appliance de services (changement de plateforme uniquement)

Lorsque vous récupérez un nœud de grid en panne hébergé sur VMware ou un hôte Linux et que vous utilisez une appliance de services pour le nœud de remplacement, vous devez d'abord installer le nouveau matériel de l'appliance en utilisant le même nom de nœud (nom du système) que le nœud en panne.

Avant de commencer

Vous disposez des informations suivantes sur le nœud défaillant :

- **Nom du noeud** : vous devez installer l'appliance de services en utilisant le même nom de noeud que le noeud défaillant. Le nom du nœud est le nom d'hôte (nom du système).
- **Adresses IP** : vous pouvez attribuer à l'appliance de services les mêmes adresses IP que le nœud défaillant, qui est l'option préférée, ou sélectionner une nouvelle adresse IP inutilisée sur chaque réseau.

Description de la tâche

Effectuez cette procédure uniquement si vous récupérez un noeud défaillant hébergé sur VMware ou Linux et que vous le remplacez par un noeud hébergé sur une appliance de services.

Étapes

1. Suivez les instructions d'installation d'un nouvel appareil de services SG100 ou SG1000. Voir "Démarrage rapide pour l'installation du matériel".
2. Lorsqu'un nom de nœud est demandé, utilisez le nom du nœud correspondant à l'échec.

Préparez l'appareil pour la réinstallation (remplacement de la plate-forme uniquement)

Lorsque vous récupérez un nœud de grid hébergé sur une appliance de services, vous devez d'abord préparer l'appliance pour la réinstallation du logiciel StorageGRID.

Effectuez cette procédure uniquement si vous remplacez un noeud défaillant hébergé sur une appliance de services. Ne suivez pas ces étapes si le nœud défaillant était initialement hébergé sur un hôte VMware ou Linux.

Étapes

1. Connectez-vous au nœud de grille ayant échoué :
   a. Saisissez la commande suivante : `ssh admin@grid_node_IP`
   b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
   c. Entrez la commande suivante pour passer à la racine : `su -`
   d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

   Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.
2. Préparez l'appliance pour l'installation du logiciel StorageGRID. Entrez : `sgareinstall`
3. Lorsque vous êtes invité à continuer, entrez : `y`

   L'appliance redémarre et votre session SSH se termine. La disponibilité du programme d'installation de l'appliance StorageGRID prend généralement 5 minutes environ, même si dans certains cas, vous devrez attendre jusqu'à 30 minutes.

   L'appliance de services est réinitialisée et les données du nœud grid n'sont plus accessibles. Les adresses IP configurées pendant le processus d'installation d'origine doivent rester intactes ; cependant, il est recommandé de confirmer cette opération une fois la procédure terminée.

   Après avoir exécuté le `sgareinstall` Commande : tous les comptes provisionnés par StorageGRID, mots de passe et clés SSH sont supprimés, puis de nouvelles clés hôte sont générées.

Démarrez l'installation du logiciel sur l'appliance des services

Pour installer un nœud de passerelle ou un nœud d'administration sur une appliance de services SG100 ou SG1000, utilisez le programme d'installation de l'appliance StorageGRID inclus sur l'appliance.

Avant de commencer

- L'appliance est installée dans un rack, connectée à vos réseaux et sous tension.
- Les liaisons réseau et les adresses IP sont configurées pour l'appliance à l'aide du programme d'installation de l'appliance StorageGRID.
- Si vous installez un nœud de passerelle ou un nœud d'administration non primaire, vous connaissez l'adresse IP du nœud d'administration principal de la grille StorageGRID.

- Tous les sous-réseaux de réseau de la grille répertoriés sur la page Configuration IP du programme d'installation de l'appliance StorageGRID sont définis dans la liste de sous-réseaux de réseau de la grille sur le nœud d'administration principal.

  Voir "Démarrage rapide pour l'installation du matériel".

- Vous utilisez un "navigateur web pris en charge".
- L'une des adresses IP est attribuée à l'appliance. Vous pouvez utiliser l'adresse IP du réseau Admin, du réseau Grid ou du réseau client.
- Si vous installez un nœud d'administration principal, vous disposez des fichiers d'installation Ubuntu ou Debian pour cette version de StorageGRID.

> Une version récente du logiciel StorageGRID est préchargée sur l'appliance de services pendant la fabrication. Si la version préchargée du logiciel correspond à la version utilisée dans votre déploiement StorageGRID, vous n'avez pas besoin des fichiers d'installation.

Description de la tâche

Pour installer le logiciel StorageGRID sur une appliance de services SG100 ou SG1000 :

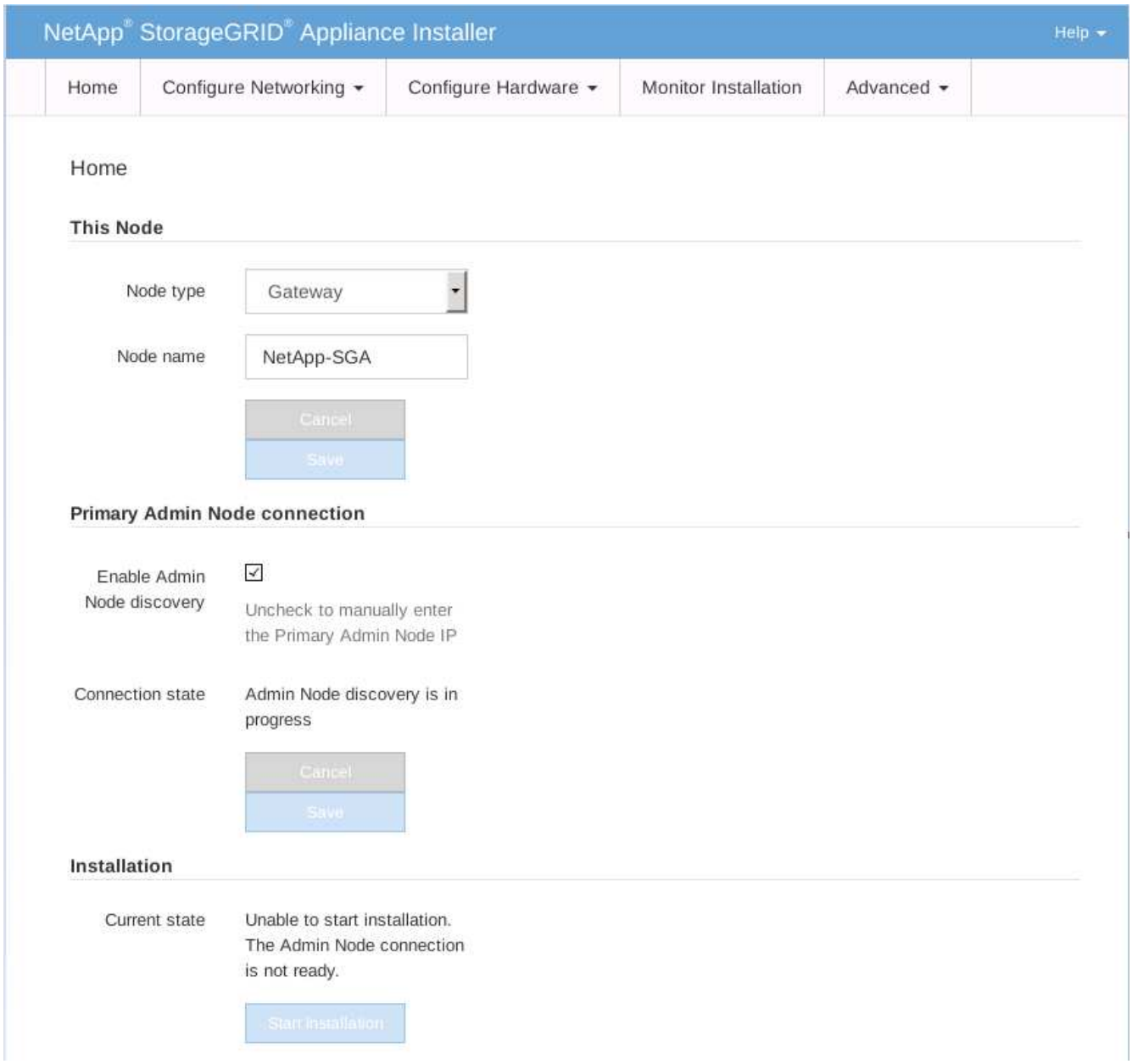
- Pour un nœud d'administration principal, vous spécifiez le nom du nœud, puis téléchargez les packs logiciels appropriés (le cas échéant).
- Pour un noeud d'administration non primaire ou un noeud de passerelle, vous spécifiez ou confirmez l'adresse IP du noeud d'administration principal et le nom du noeud.
- Vous démarrez l'installation et attendez que les volumes soient configurés et que le logiciel soit installé.
- Partway tout au long du processus, l'installation se met en pause. Pour reprendre l'installation, vous devez vous connecter à Grid Manager et configurer le nœud en attente en remplacement du nœud ayant échoué.
- Une fois le nœud configuré, le processus d'installation de l'appliance est terminé et l'appliance est redémarrée.

Étapes

1. Ouvrez un navigateur et saisissez l'une des adresses IP de l'appliance de services SG100 ou SG1000.

   `https://Controller_IP:8443`

   La page d'accueil du programme d'installation de l'appliance StorageGRID s'affiche.



2. Pour installer un nœud d'administration principal :

   a. Dans la section noeud, pour **Type de noeud**, sélectionnez **Administrateur principal**.

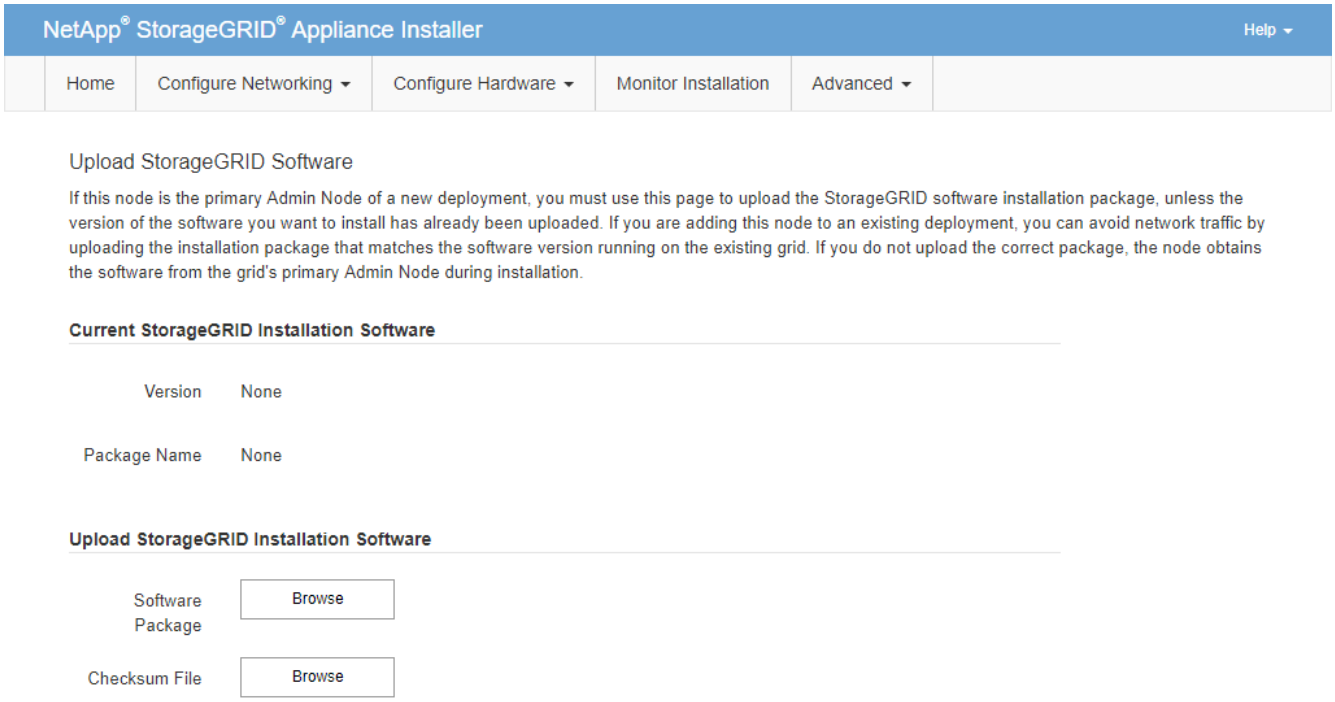
   b. Dans le champ **Nom du noeud**, entrez le même nom que celui utilisé pour le noeud que vous êtes en train de récupérer, puis cliquez sur **Enregistrer**.

   c. Dans la section installation, vérifiez la version du logiciel répertoriée sous l'état actuel

      Si la version du logiciel prêt à être installée est correcte, passez à l'étape Étape d'installation.

   d. Si vous devez télécharger une autre version du logiciel, dans le menu **Avancé**, sélectionnez **Télécharger le logiciel StorageGRID**.

      La page Télécharger le logiciel StorageGRID s'affiche.



a. Cliquez sur **Parcourir** pour télécharger le **progiciel** et le **fichier de somme de contrôle** pour le logiciel StorageGRID.

   Les fichiers sont automatiquement chargés après leur sélection.

b. Cliquez sur **Accueil** pour revenir à la page d'accueil du programme d'installation de l'appliance StorageGRID.

3. Pour installer un nœud de passerelle ou un nœud d'administration non primaire :

   a. Dans la section noeud, pour **Type de noeud**, sélectionnez **passerelle** ou **non-administrateur principal**, selon le type de noeud que vous restaurez.

   b. Dans le champ **Nom du noeud**, entrez le même nom que celui utilisé pour le noeud que vous êtes en train de récupérer, puis cliquez sur **Enregistrer**.

   c. Dans la section connexion au noeud d'administration principal, déterminez si vous devez spécifier l'adresse IP du noeud d'administration principal.

      Le programme d'installation de l'appliance StorageGRID peut détecter automatiquement cette adresse IP, en supposant que le nœud d'administration principal, ou au moins un autre nœud de grille avec ADMIN_IP configuré, soit présent sur le même sous-réseau.

   d. Si cette adresse IP n'apparaît pas ou si vous devez la modifier, spécifiez l'adresse :

Option	Description
Entrée IP manuelle	a. Décochez la case **Activer la découverte du noeud d'administration**. b. Saisissez l'adresse IP manuellement. c. Cliquez sur **Enregistrer**. d. Attendez que l'état de connexion de la nouvelle adresse IP devienne « prêt ».

Option	Description
Détection automatique de tous les nœuds d'administration principaux connectés	a. Cochez la case **Activer la découverte du noeud d'administration**. b. Dans la liste des adresses IP découvertes, sélectionnez le nœud d'administration principal de la grille sur lequel cette appliance de services sera déployée. c. Cliquez sur **Enregistrer**. d. Attendez que l'état de connexion de la nouvelle adresse IP devienne « prêt ».

4. dans la section installation, vérifiez que l'état actuel est prêt à démarrer l'installation du nom du noeud et que le bouton **Démarrer l'installation** est activé.

   Si le bouton **Start installation** n'est pas activé, vous devrez peut-être modifier la configuration réseau ou les paramètres de port. Pour obtenir des instructions, reportez-vous aux instructions d'entretien de votre appareil.

5. Dans la page d'accueil du programme d'installation de l'appliance StorageGRID, cliquez sur **Démarrer l'installation**.

   L'état actuel passe à « installation en cours » et la page installation du moniteur s'affiche.

   Si vous devez accéder manuellement à la page installation du moniteur, cliquez sur **installation du moniteur** dans la barre de menus.

Informations associées

"Maintenance des appliances SG100 et SG1000"

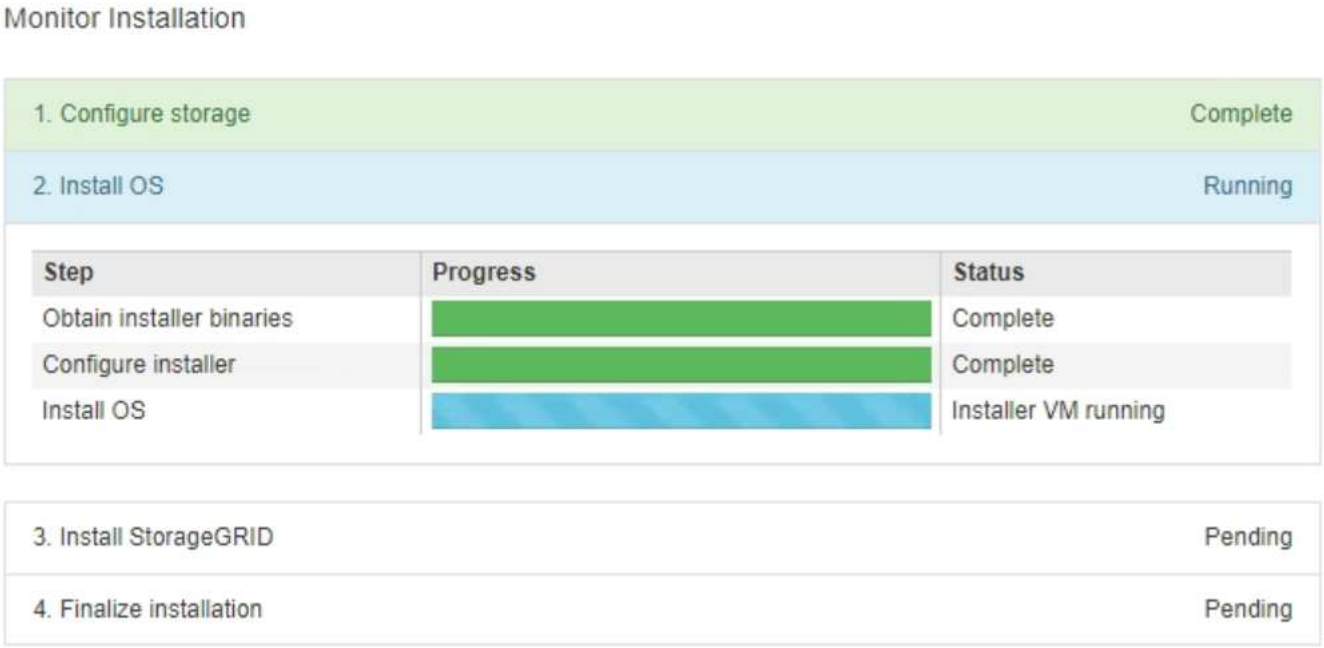
Installation de l'appareil des services du moniteur

Le programme d'installation de l'appliance StorageGRID indique l'état jusqu'à ce que l'installation soit terminée. Une fois l'installation du logiciel terminée, l'appliance est redémarrée.

Étapes

1. Pour contrôler la progression de l'installation, cliquez sur **Monitor installation** dans la barre de menus.

   La page installation du moniteur affiche la progression de l'installation.



La barre d'état bleue indique la tâche en cours. Les barres d'état vertes indiquent que les tâches ont été effectuées avec succès.

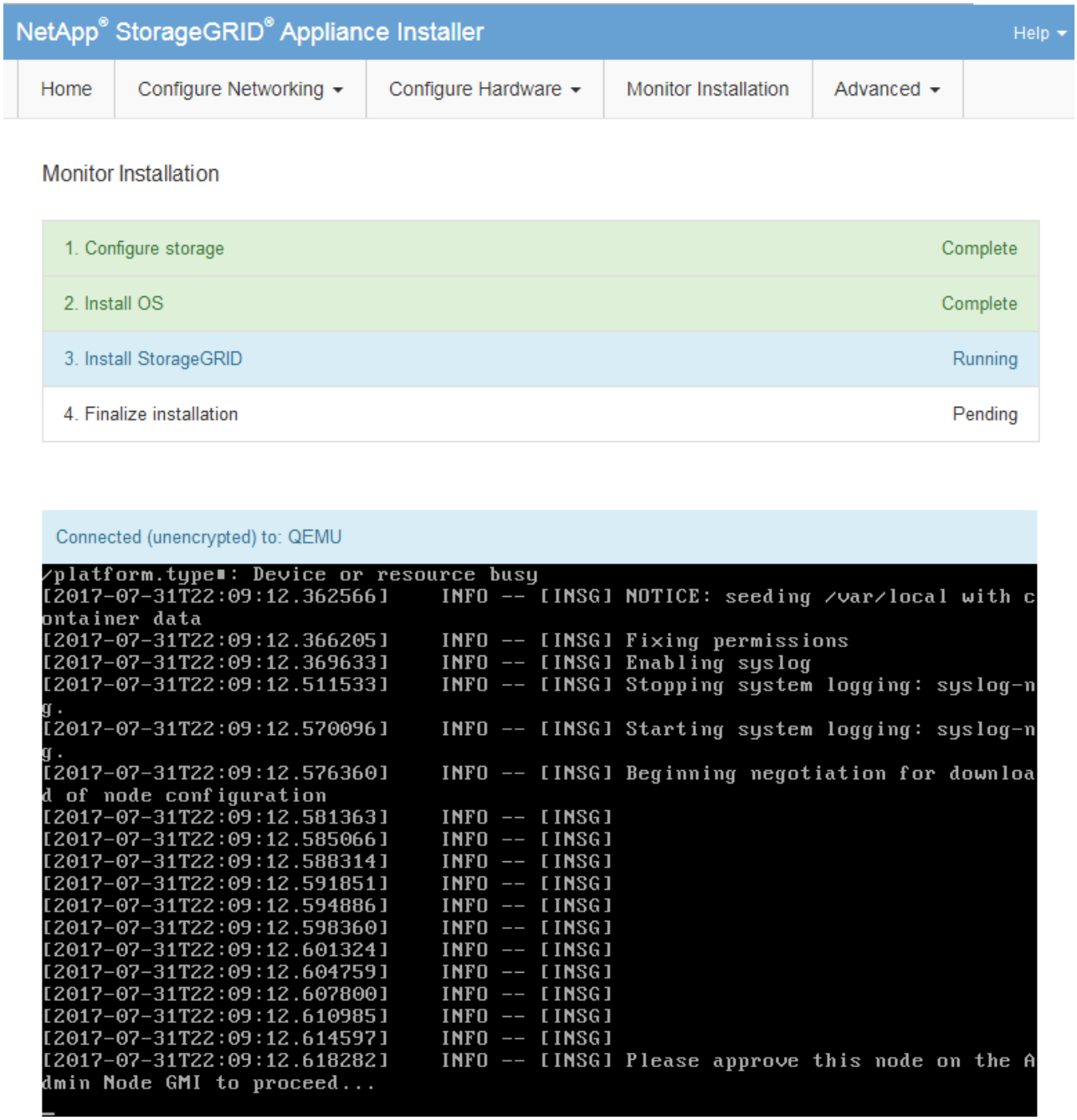
> Le programme d'installation s'assure que les tâches terminées lors d'une installation précédente ne sont pas réexécutées. Si vous exécutez à nouveau une installation, toutes les tâches qui n'ont pas besoin d'être réexécutées s'affichent avec une barre d'état verte et un état de « `barrét' ».

2. Passez en revue l'état d'avancement des deux premières étapes d'installation.
   - **1. Configurer le stockage**

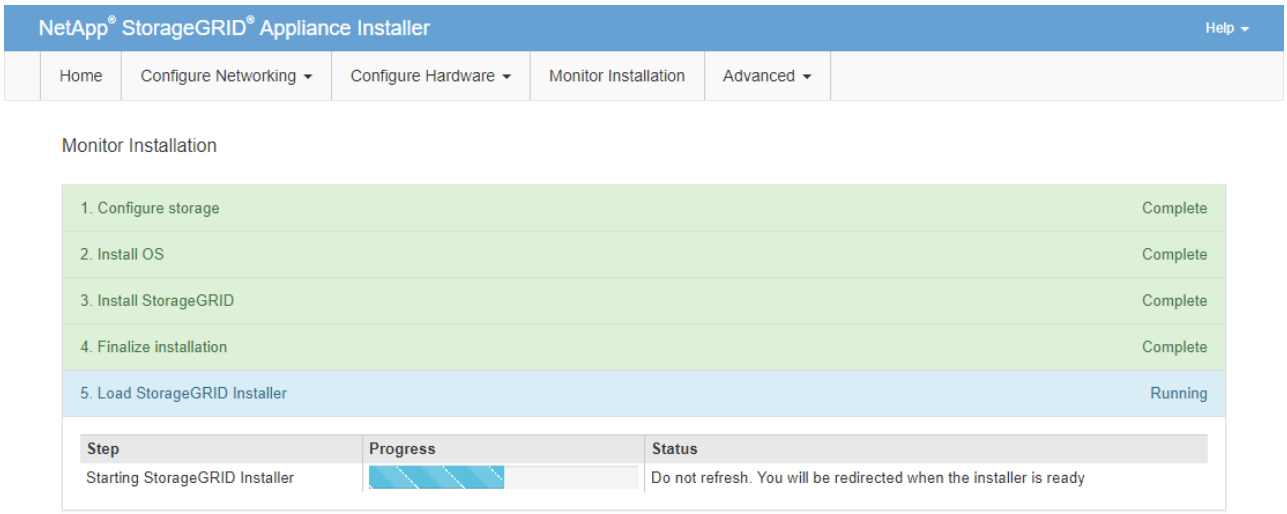
     Au cours de cette étape, le programme d'installation efface toute configuration existante des disques et configure les paramètres hôte.

   - **2. Installez OS**

     Au cours de cette étape, le programme d'installation copie l'image de base du système d'exploitation pour StorageGRID du nœud d'administration principal vers l'appliance ou installe le système d'exploitation de base à partir du package d'installation du nœud d'administration principal.
3. Continuez à surveiller la progression de l'installation jusqu'à ce que l'un des événements suivants se produise :
   - Pour les nœuds de passerelle d'appliance ou les nœuds d'administration de l'appliance non primaire, l'étape **installer StorageGRID** s'interrompt et un message s'affiche sur la console intégrée, vous invitant à approuver ce nœud sur le nœud d'administration à l'aide du Gestionnaire de grille.



- Pour les nœuds d'administration principaux de l'appliance, une cinquième phase (Load StorageGRID installer) s'affiche. Si la cinquième phase est en cours pendant plus de 10 minutes, actualisez la page manuellement.



4. Passez à l'étape suivante du processus de restauration pour le type de nœud de grille d'appliance que vous restaurez.

Type de restauration	Référence
Nœud de passerelle	"Sélectionnez Démarrer la récupération pour configurer le nœud de passerelle"
Nœud d'administration non primaire	"Sélectionnez Démarrer la restauration pour configurer un noeud d'administration non primaire"
Nœud d'administration principal	"Configurez le nœud d'administration principal de remplacement"

Comment la reprise sur site est effectuée par le support technique

Si l'ensemble du site StorageGRID tombe en panne ou si plusieurs nœuds de stockage tombent en panne, vous devez contacter le support technique. Le support technique évalue votre situation, développe un plan de reprise, puis restaure les nœuds ou le site en panne en fonction des objectifs de votre entreprise, optimise le délai de restauration et évite les pertes de données inutiles.

La restauration du site ne peut être effectuée que par le support technique.

Les systèmes StorageGRID sont résilients pour de nombreuses défaillances et vous pouvez réaliser vous-même de nombreuses procédures de reprise et de maintenance. Cependant, il est difficile de créer une procédure simple et généralisée de récupération du site parce que les étapes détaillées dépendent de facteurs spécifiques à votre situation. Par exemple :

- **Vos objectifs d'entreprise**: Après la perte complète d'un site StorageGRID, vous devriez évaluer la meilleure façon d'atteindre vos objectifs d'entreprise. Par exemple, voulez-vous reconstruire le site perdu en place? Voulez-vous remplacer le site StorageGRID perdu à un nouvel emplacement ? La situation de chaque client est différente, et votre plan de reprise doit être conçu pour répondre à vos priorités.
- **Nature exacte de la défaillance** : avant de commencer une récupération de site, déterminez si des nœuds du site défaillant sont intacts ou si des nœuds de stockage contiennent des objets récupérables. Si

vous reconstruisez des nœuds ou des volumes de stockage contenant des données valides, vous risquez de perdre des données superflues.

- **Politique ILM active** : le nombre, le type et l'emplacement des copies d'objet dans votre grille sont contrôlés par votre politique ILM active. Les spécificités de votre politique ILM peuvent affecter la quantité de données récupérables, ainsi que les techniques spécifiques requises pour la restauration.

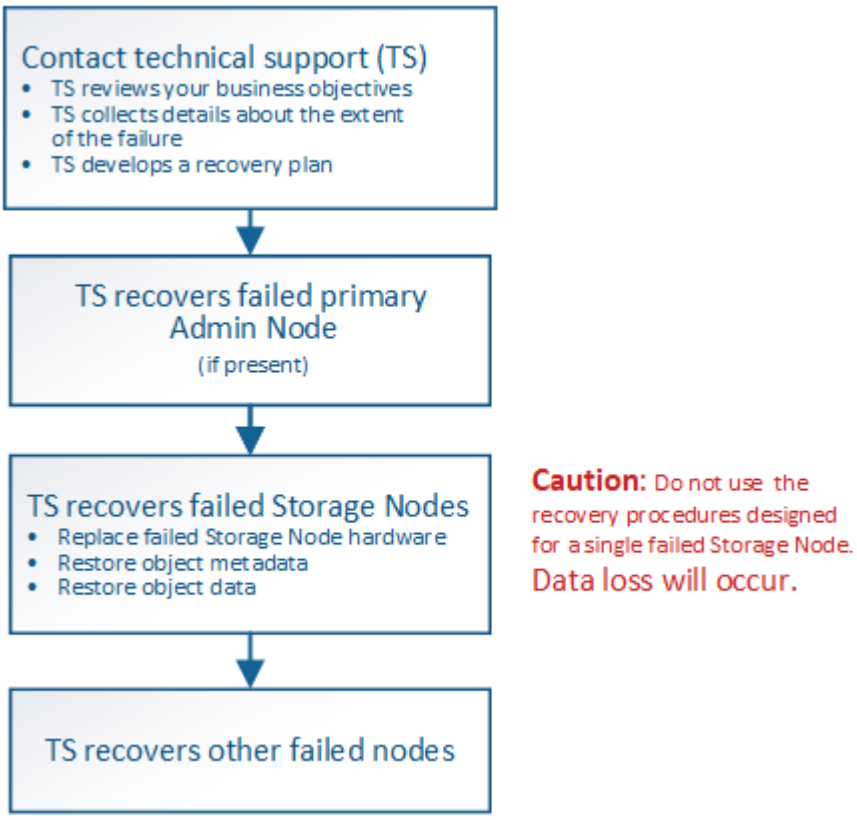
  Si un site contient la seule copie d'un objet et que le site est perdu, l'objet est perdu.

- **Cohérence du compartiment (ou du conteneur)** : le niveau de cohérence appliqué à un compartiment (ou à un conteneur) affecte si StorageGRID réplique intégralement les métadonnées d'objet vers tous les nœuds et sites avant de dire à un client que l'ingestion de l'objet a réussi. Si votre niveau de cohérence permet une éventuelle cohérence, certaines métadonnées d'objet peuvent être perdues en cas de défaillance du site. Cela peut avoir un impact sur la quantité de données récupérables et éventuellement sur les détails de la procédure de restauration.
- **Historique des changements récents**: Les détails de votre procédure de récupération peuvent être affectés par la question de savoir si des procédures de maintenance étaient en cours au moment de l'échec ou si des modifications récentes ont été apportées à votre politique ILM. Le support technique doit évaluer l'historique récent de votre grille ainsi que sa situation actuelle avant de commencer une récupération de site.

Présentation de la récupération de site

Il s'agit d'une présentation générale de la procédure utilisée par le support technique pour restaurer un site en panne.

La restauration du site ne peut être effectuée que par le support technique.



1. Contactez l'assistance technique.

Le support technique évalue en détail la défaillance et travaille avec vous pour examiner les objectifs de votre entreprise. Sur la base de ces informations, le support technique développe un plan de reprise sur incident adapté à votre situation.

2. Le support technique restaure le nœud d'administration principal s'il est défectueux.
3. Support technique pour la restauration de tous les nœuds de stockage, voici les grandes lignes :

   a. Remplacez le matériel ou les machines virtuelles du nœud de stockage selon les besoins.
   b. Restaurez les métadonnées d'objet sur le site défaillant.
   c. Restaurez les données d'objet vers les nœuds de stockage récupérés.

   > La perte de données se produit si les procédures de restauration d'un seul nœud de stockage défaillant sont utilisées.

   > Lorsqu'un site entier présente une défaillance, des commandes spécialisées sont nécessaires pour restaurer correctement les objets et les métadonnées d'objet.

4. Le support technique restaure les autres nœuds défaillants.

   Une fois les métadonnées et les données d'objet restaurées, des nœuds de passerelle défaillants, ainsi que des nœuds d'administration non primaires et des nœuds d'archivage peuvent être restaurés à l'aide des procédures standard.

Informations associées

"Mise hors service du site"

Procédure de mise hors service

Procédure de mise hors service : présentation

Vous pouvez effectuer une procédure de mise hors service pour supprimer définitivement les nœuds grid ou un site entier du système StorageGRID.

Pour supprimer un nœud de grille ou un site, effectuez l'une des procédures de mise hors service suivantes :

- Exécutez un "désaffectation du nœud grid" pour supprimer un ou plusieurs nœuds, qui peuvent se trouver sur un ou plusieurs sites. Les nœuds que vous supprimez peuvent être en ligne et connectés au système StorageGRID, ou encore hors ligne et déconnectés.
- Exécutez un "désaffectation du site" pour supprimer un site. Vous effectuez une **Désaffected site** si tous les nœuds sont connectés à StorageGRID. Vous effectuez une **Désaffected site** si tous les nœuds sont déconnectés de StorageGRID.

> Avant d'effectuer une désaffectation du site déconnecté, vous devez contacter votre ingénieur commercial NetApp. NetApp évaluera vos besoins avant d'activer toutes les étapes de l'assistant Decommission site. N'essayez pas de désaffecter le site si vous pensez qu'il est possible de récupérer le site ou de récupérer les données d'objet à partir du site.

Si un site contient un mélange de connecté ( ) et noeuds déconnectés (ou), vous devez remettre

tous les nœuds hors ligne en ligne.

> Si vous devez effectuer une deuxième procédure de maintenance, vous pouvez "Mettez en pause la procédure de mise hors service pendant le retrait des nœuds de stockage". Le bouton **Pause** n'est activé que lorsque les étapes d'évaluation ILM ou de déclassement des données avec code d'effacement sont atteintes. Cependant, l'évaluation ILM (migration des données) continue à s'exécuter en arrière-plan. Une fois la deuxième procédure d'entretien terminée, vous pouvez reprendre la mise hors service.

Mise hors service du nœud de la grille

Désaffectation du nœud Grid : présentation

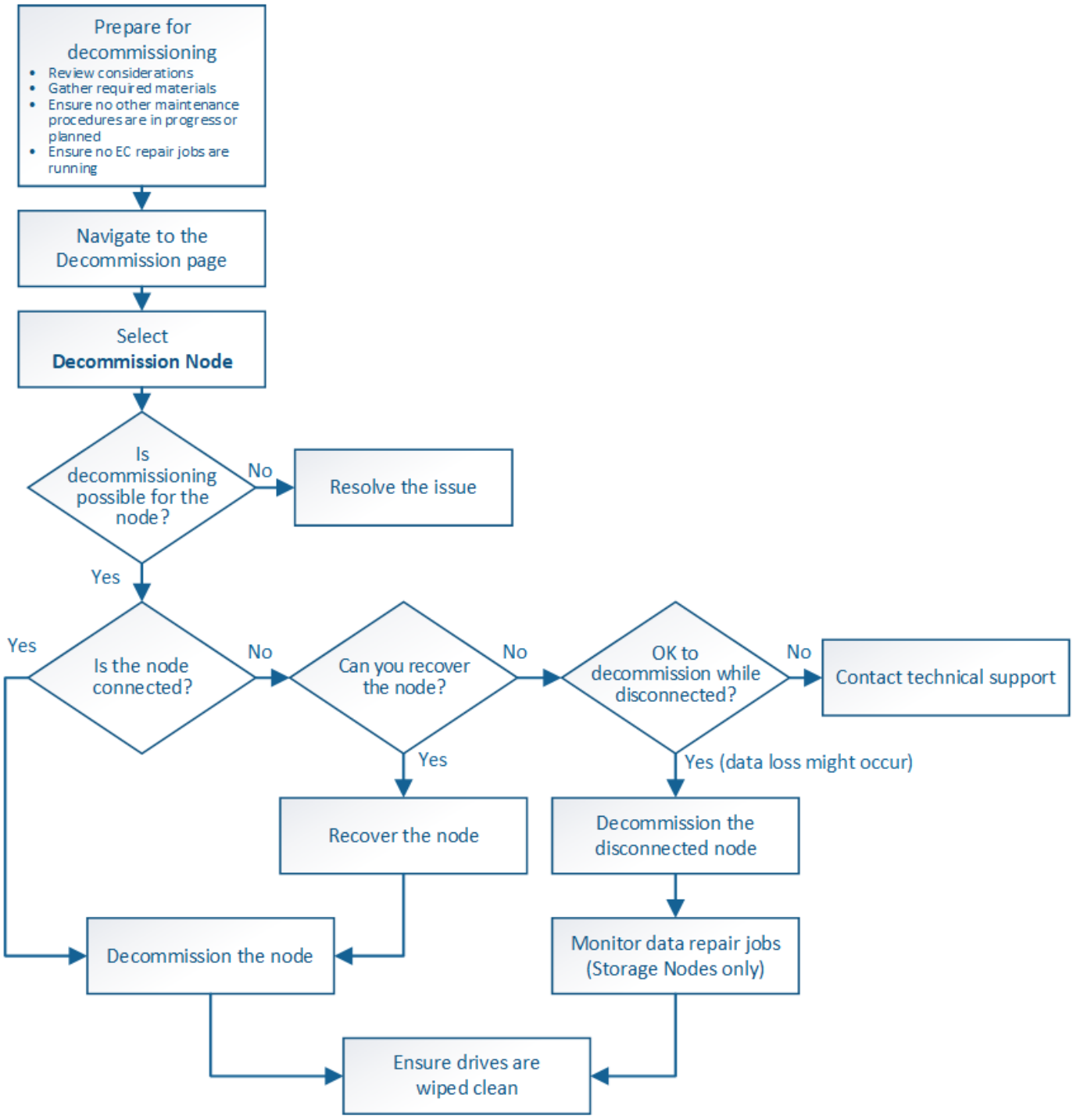
Vous pouvez utiliser la procédure de mise hors service des nœuds pour supprimer un ou plusieurs nœuds de stockage, nœuds de passerelle ou nœuds d'administration non primaires sur un ou plusieurs sites. Vous ne pouvez pas désaffecter le nœud d'administration principal ou un nœud d'archivage.

En général, vous devez mettre hors service les nœuds de la grille uniquement lorsqu'ils sont connectés au système StorageGRID et que tous les nœuds sont en état de santé normal (icônes vertes sur les pages **NOEUDS** et sur la page **nœuds de décomposition**). Toutefois, si nécessaire, vous pouvez désaffecter un nœud de grille qui est déconnecté. Avant de supprimer un nœud déconnecté, assurez-vous de bien comprendre les implications et les restrictions de ce processus.

Utilisez la procédure de mise hors service du nœud lorsque l'un des cas suivants est vrai :

- Vous avez ajouté un nœud de stockage plus grand au système et souhaitez supprimer un ou plusieurs nœuds de stockage plus petits, tout en préservant les objets.
- Vous avez besoin de moins de stockage total.
- Vous n'avez plus besoin d'un nœud de passerelle.
- Vous n'avez plus besoin d'un nœud d'administration non primaire.
- Votre grille inclut un nœud déconnecté que vous ne pouvez pas restaurer ni remettre en ligne.

L'organigramme présente les étapes générales de mise hors service des nœuds de la grille.



Facteurs à prendre en compte lors de la mise hors service des nœuds

Considérations générales concernant la désaffectation de nœud Grid

Avant de commencer cette procédure pour désaffecter un ou plusieurs nœuds, vous devez comprendre les implications que peut avoir la suppression de chaque type de nœud. Lors de la mise hors service d'un nœud, ses services sont désactivés et le nœud est automatiquement arrêté.

Vous ne pouvez pas désaffecter un nœud si cela entraîne un état StorageGRID non valide. Les règles suivantes sont appliquées :

- Vous ne pouvez pas désaffecter le nœud d'administration principal.
- Vous ne pouvez pas désaffecter les nœuds d'archivage.
- Vous ne pouvez pas désaffecter un nœud d'administration ou un nœud de passerelle si l'une de ses interfaces réseau fait partie d'un groupe haute disponibilité (HA).
- Vous ne pouvez pas désaffecter un nœud de stockage si sa suppression affecterait le quorum ADC.
- Vous ne pouvez pas désaffecter un nœud de stockage si cela est nécessaire pour la règle ILM active.
- Vous ne devez pas désaffecter plus de 10 nœuds de stockage dans une procédure de nœud de mise hors service unique.
- Vous ne pouvez pas désaffecter un nœud connecté si votre grid inclut des nœuds déconnectés (nœuds dont l'état de santé est inconnu ou dont l'état de santé est administratif désactivé). Vous devez d'abord mettre hors service ou récupérer les nœuds déconnectés.
- Si votre grille contient plusieurs nœuds déconnectés, le logiciel requiert que vous les désinsaffectez tous en même temps, ce qui augmente le risque de résultats inattendus.
- Si un nœud déconnecté ne peut pas être supprimé (par exemple, un nœud de stockage requis pour le quorum ADC), aucun autre nœud déconnecté ne peut être supprimé.
- Si vous souhaitez remplacer une ancienne appliance par une nouvelle, envisagez "clonage du nœud d'appliance" évite également de désaffecter l'ancien nœud et de ajouter le nouveau nœud dans une extension.

> Ne supprimez pas la machine virtuelle ou d'autres ressources d'un nœud de grille avant d'y être invité dans les procédures de mise hors service.

Considérations relatives à la désaffectation des nœuds de passerelle ou d'administration

Vérifiez les points suivants avant de désaffecter un nœud d'administration ou un nœud de passerelle.

- La procédure de mise hors service nécessite un accès exclusif à certaines ressources système. Vous devez donc confirmer qu'aucune autre procédure de maintenance n'est en cours d'exécution.
- Vous ne pouvez pas désaffecter le nœud d'administration principal.
- Vous ne pouvez pas désaffecter un nœud d'administration ou un nœud de passerelle si l'une de ses interfaces réseau fait partie d'un groupe haute disponibilité (HA). Vous devez d'abord supprimer les interfaces réseau du groupe haute disponibilité. Reportez-vous aux instructions pour "La gestion des groupes de haute disponibilité".
- Vous pouvez modifier la règle ILM en toute sécurité lors de la désaffectation d'un nœud de passerelle ou d'un nœud d'administration.
- Si vous désaffectez un nœud d'administration et que l'authentification unique (SSO) est activée pour votre système StorageGRID, n'oubliez pas de supprimer la confiance de l'interlocuteur du nœud de Active Directory Federation Services (AD FS).
- Si vous utilisez "fédération des grilles", Assurez-vous que l'adresse IP du nœud que vous désaffecterez n'a pas été spécifiée pour une connexion de fédération de grille.

Nœuds de stockage

Facteurs à prendre en compte concernant la désaffectation des nœuds de stockage

Si vous prévoyez de désactiver un nœud de stockage, vous devez comprendre comment StorageGRID gère les données d'objet et les métadonnées sur ce nœud.

Lors de la mise hors service des nœuds de stockage, les facteurs et restrictions suivants s'appliquent :

- Le système doit en permanence inclure suffisamment de nœuds de stockage pour répondre aux exigences opérationnelles, notamment le quorum ADC et la politique ILM active. Pour satisfaire à cette restriction, vous devrez peut-être ajouter un nouveau nœud de stockage dans une opération d'extension avant de pouvoir désactiver un nœud de stockage existant.
- Si le nœud de stockage est déconnecté lors de la mise hors service, le système doit reconstruire les données à l'aide des données des nœuds de stockage connectés, ce qui peut entraîner une perte de données.
- Lorsque vous supprimez un nœud de stockage, de grands volumes de données d'objet doivent être transférés sur le réseau. Bien que ces transferts ne puissent pas affecter le fonctionnement normal du système, ils peuvent avoir un impact sur la quantité totale de bande passante réseau consommée par le système StorageGRID.
- Les tâches associées à la mise hors service des nœuds de stockage ont une priorité inférieure aux tâches associées aux opérations normales du système. Cette mise hors service n'interfère pas avec le fonctionnement normal du système StorageGRID et n'a pas besoin d'être planifiée pour une période d'inactivité du système. Comme le déclassement est effectué en arrière-plan, il est difficile d'estimer la durée du processus. En général, la mise hors service s'effectue plus rapidement lorsque le système est silencieux, ou lorsqu'un seul nœud de stockage est retiré à la fois.
- La mise hors service d'un nœud de stockage peut prendre plusieurs jours, voire des semaines. Planifier cette procédure en conséquence. Bien que le processus de mise hors service soit conçu pour ne pas affecter le fonctionnement du système, il peut limiter d'autres procédures. En général, les mises à niveau ou les extensions du système doivent être effectuées avant de supprimer les nœuds grid.
- Les procédures de mise hors service qui impliquent des nœuds de stockage peuvent être suspendues au cours de certaines étapes pour permettre à d'autres procédures de maintenance de s'exécuter si nécessaire, et reprises une fois terminées.
- Vous ne pouvez pas exécuter les opérations de réparation des données sur des nœuds de grille lorsqu'une tâche de désaffectation est en cours d'exécution.
- Vous ne devez pas apporter de modifications à la règle ILM pendant la désaffectation d'un nœud de stockage.
- Lorsque vous supprimez un nœud de stockage, les données du nœud sont migrées vers d'autres nœuds de la grille. Toutefois, ces données ne sont pas entièrement supprimées du nœud mis hors service. Pour supprimer les données de manière permanente et sécurisée, vous devez effacer les disques du nœud de la grille désaffectée une fois la procédure de mise hors service terminée.
- Lorsque vous désaffectez un nœud de stockage, les alertes et alarmes suivantes peuvent être émises et vous recevrez peut-être des notifications SNMP et des e-mails connexes :
  - **Impossible de communiquer avec l'alerte Node**. Cette alerte est déclenchée lorsque vous désaffectez un nœud de stockage qui inclut le service ADC. L'alerte est résolue une fois l'opération de mise hors service terminée.
  - Alarme VSTU (Etat de vérification d'objet). Cette alarme de niveau de notification indique que le nœud de stockage passe en mode maintenance pendant le processus de mise hors service.
  - Alarme CASA (État de la banque de données). Cette alarme de niveau majeur indique que la base de données Cassandra est en panne parce que les services ont cessé.

Informations associées

"Restaurez les données d'objet sur le volume de stockage"

Comprendre le quorum ADC

Vous ne pourrez peut-être pas désaffecter certains nœuds de stockage sur un site de data Center si trop peu de services ADC (administrative Domain Controller) seront conservés après la mise hors service. Ce service, qui se trouve sur certains nœuds de stockage, conserve les informations de topologie grid et fournit les services de configuration à la grille. Le système StorageGRID nécessite que le quorum des services ADC soit disponible sur chaque site et à tout moment.

Vous ne pouvez pas désaffecter un nœud de stockage si le retrait du nœud entraînerait la non-conformité du quorum ADC. Pour satisfaire le quorum ADC lors d'une mise hors service, un minimum de trois nœuds de stockage doivent être disponibles sur chaque site de data Center. Si un site de data Center dispose de plus de trois nœuds de stockage avec le service ADC, la majorité simple de ces nœuds doit rester disponible après la désaffectation ((0.5 * `Storage Nodes with ADC`) + 1).

Supposons par exemple qu'un site de data Center inclut actuellement six nœuds de stockage avec des services ADC et que vous voulez désaffecter trois nœuds de stockage. En raison de l'exigence de quorum ADC, vous devez effectuer deux procédures de mise hors service, comme suit :

- Lors de la première procédure de mise hors service, vous devez vous assurer que quatre nœuds de stockage avec services ADC restent disponibles ((0.5 * 6) +1) . Cela signifie que vous ne pouvez désaffecter que deux nœuds de stockage au départ.
- Dans la deuxième procédure de mise hors service, vous pouvez supprimer le troisième nœud de stockage car le quorum ADC ne requiert désormais que trois services ADC pour rester disponibles ((0.5 * 4) + 1).

Si vous devez désaffecter un nœud de stockage mais que vous ne pouvez pas le faire en raison de l'exigence de quorum ADC, vous devez ajouter un nouveau nœud de stockage dans une extension et spécifier qu'il doit disposer d'un service ADC. Vous pouvez ensuite désaffecter le nœud de stockage existant.

Informations associées

"Développez votre grille"

Examiner la règle ILM et la configuration du stockage

Si vous prévoyez de désaffecter un nœud de stockage, nous vous recommandons de consulter la politique ILM de votre système StorageGRID avant de lancer le processus de désaffectation.

Pendant la mise hors service, toutes les données d'objet sont migrées du nœud de stockage hors service vers d'autres nœuds de stockage.

> La politique ILM que vous avez *pendant* la mise hors service sera celle utilisée *après* la mise hors service. Vous devez vous assurer que cette règle répond à vos besoins en matière de données avant la mise hors service et une fois la mise hors service terminée.

Nous vous recommandons de lire les règles de la politique ILM active pour vous assurer que le système StorageGRID continuera d'avoir une capacité suffisante pour le type et les emplacements appropriés afin de prendre en charge la désaffectation d'un nœud de stockage.

Tenez compte des points suivants :

- Sera-t-il possible que les services d'évaluation ILM copient les données d'objet si les règles ILM sont respectées ?
- Que se passe-t-il si un site devient temporairement indisponible pendant la mise hors service ? Des copies supplémentaires peuvent-elles être effectuées dans un autre emplacement ?
- En quoi le processus de mise hors service aura-t-il une incidence sur la distribution finale du contenu? Comme décrit dans "Consolidez les nœuds de stockage", Vous devez ajouter de nouveaux nœuds de stockage avant d'en supprimer les anciens. Si vous ajoutez un nœud de stockage de remplacement plus grand après avoir désaffectant un nœud de stockage plus petit, les anciens nœuds de stockage peuvent être proches de leur capacité et le nouveau nœud de stockage n'aurait presque pas de contenu. La plupart des opérations d'écriture des nouvelles données d'objet sont ensuite dirigées vers le nouveau nœud de stockage, ce qui réduit l'efficacité globale des opérations système.
- Le système inclura-t-il en permanence suffisamment de nœuds de stockage pour satisfaire la politique ILM active ?

> Une politique ILM insatisfaisante entraîne des backlogs et des alarmes, et peut arrêter le fonctionnement du système StorageGRID.

Vérifier que la topologie proposée résultant du processus de mise hors service respecte la politique ILM en évaluant les facteurs répertoriés dans le tableau.

Domaine à évaluer	Remarques
Capacité disponible	Aura-t-il suffisamment de capacité de stockage pour prendre en charge toutes les données d'objet stockées dans le système StorageGRID, Y compris les copies permanentes des données d'objet stockées sur le nœud de stockage à désaffecter?y a-t-il suffisamment de capacité pour gérer la croissance anticipée des données d'objet stockées pendant un intervalle raisonnable une fois le déclassement terminé ?
Emplacement de stockage	Si la capacité reste dans l'ensemble du système StorageGRID, la capacité est-elle suffisante aux bons emplacements afin de satisfaire aux règles métier du système StorageGRID ?
Type de stockage	Y aura-t-il suffisamment de stockage pour le type approprié une fois la mise hors service terminée ? Par exemple, les règles ILM régissent le déplacement du contenu d'un type de stockage à un autre, à mesure que son contenu vieillit. Si c'est le cas, vous devez vous assurer qu'un espace de stockage suffisant est disponible dans la configuration finale du système StorageGRID.

Informations associées

"Gestion des objets avec ILM"

"Développez votre grille"

Désaffectation des nœuds de stockage déconnectés

Vous devez comprendre ce qui peut se produire si vous mettez hors service un nœud de

stockage alors qu'il est déconnecté (état de santé inconnu ou panne administrative).

Lorsque vous désaffectez un nœud de stockage déconnecté de la grille, StorageGRID utilise les données des autres nœuds de stockage pour reconstruire les données d'objet et les métadonnées qui se trouvent sur le nœud déconnecté. Pour ce faire, il lance automatiquement les travaux de réparation des données à la fin du processus de mise hors service.

Avant de désaffecter un nœud de stockage déconnecté, tenez compte des points suivants :

- Vous ne devez jamais désaffecter un nœud déconnecté à moins d'être sûr qu'il ne peut pas être mis en ligne ou restauré.

> ⓘ N'effectuez pas cette procédure si vous pensez qu'il est possible de récupérer des données d'objet à partir du nœud. Contactez plutôt le support technique pour déterminer si la restauration du nœud est possible.

- Si un nœud de stockage déconnecté contient la seule copie d'un objet, cet objet sera perdu lorsque vous mettez le nœud hors service. Les tâches de réparation des données ne peuvent reconstruire et récupérer que des objets si au moins une copie répliquée ou suffisamment de fragments avec code d'effacement existent sur les nœuds de stockage actuellement connectés.
- Lorsque vous désaffectez un nœud de stockage déconnecté, la procédure de mise hors service se termine relativement rapidement. Cependant, les tâches de réparation des données peuvent prendre des jours ou des semaines et ne sont pas surveillées par la procédure de mise hors service. Vous devez contrôler ces travaux manuellement et les redémarrer au besoin. Voir "Vérifier les travaux de réparation des données".
- Si vous désaffectez plusieurs nœuds de stockage déconnectés à la fois, des pertes de données peuvent se produire. Il se peut que le système ne puisse pas reconstruire les données si le nombre de copies de données d'objet, de métadonnées ou de fragments avec code d'effacement reste disponible.

> ⓘ Si vous ne pouvez pas restaurer plusieurs nœuds de stockage déconnectés, contactez le support technique pour déterminer la meilleure solution.

Consolidez les nœuds de stockage

Vous pouvez consolider les nœuds de stockage pour réduire le nombre de nœuds de stockage sur un site ou un déploiement, tout en augmentant la capacité de stockage.

Lorsque vous consolidez les nœuds de stockage, étendez le système StorageGRID pour ajouter des nœuds de stockage de plus grande capacité, puis désaffectez des nœuds de stockage anciens et plus petits. Pendant la procédure de mise hors service, les objets sont migrés entre les anciens nœuds de stockage et les nouveaux nœuds de stockage.

> ⓘ Si vous consolidez des appliances plus anciennes ou plus petites avec de nouveaux modèles ou des appliances plus grande capacité, vous utilisez souvent la fonction de clone de nœud ou la procédure de clonage de nœud, ainsi que la procédure de désaffectation si vous ne remplacez pas les appliances un-à-un.

Par exemple, vous pouvez ajouter deux nouveaux nœuds de stockage de plus grande capacité pour remplacer trois nœuds de stockage plus anciens. Vous devez d'abord utiliser la procédure d'extension pour ajouter les deux nouveaux nœuds de stockage de plus grande capacité, puis éliminer les trois anciens nœuds de stockage de plus grande capacité.

Lorsque vous ajoutez de la capacité supplémentaire avant de supprimer les nœuds de stockage, vous assurez une distribution plus équilibrée des données sur le système StorageGRID. Vous réduisez également la possibilité qu'un nœud de stockage existant soit repoussé au-delà du niveau du filigrane.

Informations associées

"Développez votre grille"

Désaffectation de plusieurs nœuds de stockage

Si vous devez supprimer plusieurs nœuds de stockage, vous pouvez les désaffecter de manière séquentielle ou parallèle.

- Si vous mettez hors service les nœuds de stockage de façon séquentielle, vous devez attendre la fin du déclassement du premier nœud de stockage avant de procéder à la mise hors service du prochain nœud de stockage.
- Si vous mettez hors service les nœuds de stockage en parallèle, les nœuds de stockage traitent simultanément les tâches de désaffectation de tous les nœuds de stockage qui sont désaffectés. Cela peut entraîner la désactivation temporaire de la suppression dans les grilles lorsque cette fonctionnalité est activée de toutes les copies permanentes d'un fichier.

Vérifier les travaux de réparation des données

Avant de mettre un nœud de grille hors service, vous devez confirmer qu'aucun travail de réparation de données n'est actif. Si des réparations ont échoué, vous devez les redémarrer et leur permettre d'effectuer la procédure de mise hors service.

Si vous devez désaffecter un nœud de stockage déconnecté, vous devrez également effectuer ces étapes une fois la procédure de mise hors service terminée pour vous assurer que la réparation des données s'est terminée correctement. Vous devez vous assurer que tous les fragments avec code d'effacement qui se trouvaient sur le nœud supprimé ont été restaurés correctement.

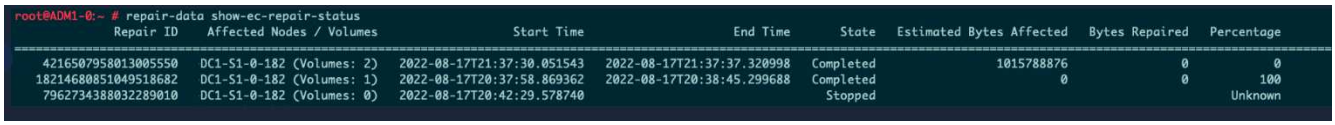
Ces étapes s'appliquent uniquement aux systèmes dotés d'objets avec code d'effacement.

1. Connectez-vous au nœud d'administration principal :
   a. Saisissez la commande suivante : `ssh admin@grid_node_IP`

      Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

   b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
   c. Entrez la commande suivante pour passer à la racine : `su -`
   d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
2. Vérifier l'exécution des réparations : `repair-data show-ec-repair-status`
   - Si vous n'avez jamais exécuté de tâche de réparation de données, la sortie est `No job found`. Vous n'avez pas besoin de redémarrer les travaux de réparation.
   - Si la tâche de réparation de données a été exécutée précédemment ou est en cours d'exécution, la sortie répertorie les informations relatives à la réparation. Chaque réparation possède un ID de réparation unique. Passez à l'étape suivante.
   - Vous pouvez également surveiller l'état des travaux de restauration en cours et afficher un historique

des travaux de restauration effectués dans"Gestionnaire de grille".



3. Si l'état pour toutes les réparations est `Completed`, vous n'avez pas besoin de redémarrer les travaux de réparation.
4. Si l'état pour une réparation est `Stopped`, vous devez redémarrer cette réparation.
   a. Obtenir l'ID de réparation pour la réparation ayant échoué à partir du résultat.
   b. Exécutez le `repair-data start-ec-node-repair` commande.

      Utilisez le `--repair-id` Pour spécifier l'ID de réparation. Par exemple, si vous souhaitez réessayer une réparation avec l'ID de réparation 949292, exécutez la commande suivante : `repair-data start-ec-node-repair --repair-id 949292`

   c. Continuer à suivre l'état des réparations de données EC jusqu'à ce que l'état pour toutes les réparations soit `Completed`.

Rassembler les matériaux nécessaires

Avant d'effectuer la mise hors service d'un nœud de la grille, vous devez obtenir les informations suivantes.

Élément	Remarques
Package de restauration `.zip` fichier	Vous devez "Téléchargez le dernier progiciel de restauration" `.zip` fichier (`sgws-recovery-package-`*`id-revision`*`.zip`). Vous pouvez utiliser le fichier du progiciel de récupération pour restaurer le système en cas de défaillance.
`Passwords.txt` fichier	Ce fichier contient les mots de passe requis pour accéder aux nœuds de la grille sur la ligne de commande et est inclus dans le progiciel de récupération.
Phrase secrète pour le provisionnement	La phrase de passe est créée et documentée lors de l'installation initiale du système StorageGRID. La phrase de passe de provisionnement n'est pas dans le `Passwords.txt` fichier.
Description de la topologie du système StorageGRID avant la mise hors service	Le cas échéant, procurez-vous toute documentation décrivant la topologie actuelle du système.

Informations associées

"Navigateurs Web pris en charge"

Accédez à la page nœuds de mise hors service

Lorsque vous accédez à la page Decommission Nodes dans Grid Manager, vous pouvez voir en un coup d'œil quels nœuds peuvent être désaffectés.

Avant de commencer

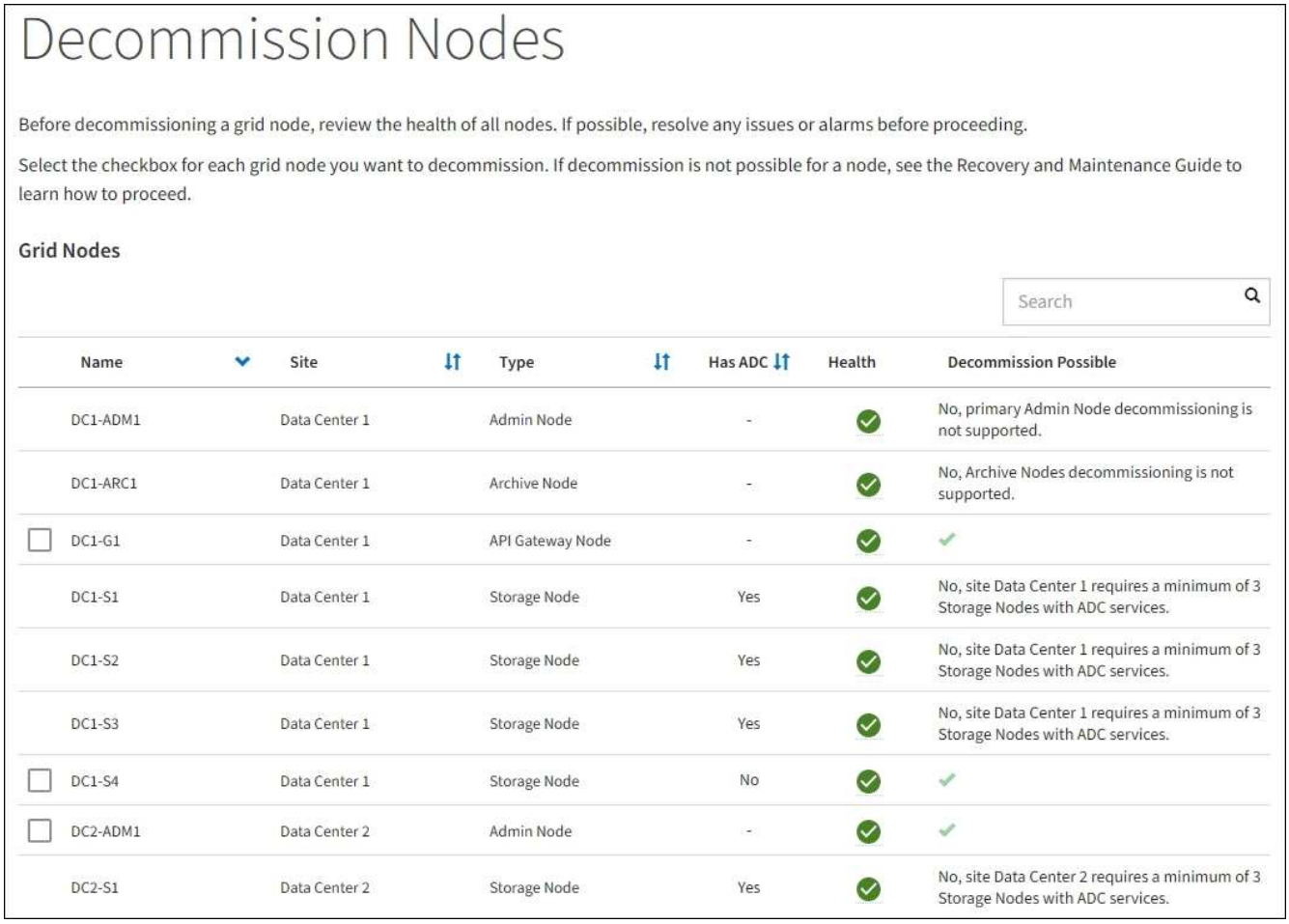
- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous disposez de l'autorisation Maintenance ou accès racine.

Étapes

1. Sélectionnez **MAINTENANCE** > **tâches** > **désaffectation**.
2. Sélectionnez **nœuds de mise hors service**.

   La page nœuds de mise hors service s'affiche. À partir de cette page, vous pouvez :

   - Déterminez les nœuds de la grille qui peuvent être désaffectés.
   - Voir l'état de santé de tous les nœuds de la grille
   - Triez la liste par ordre croissant ou décroissant en fonction de **Nom**, **site**, **Type** ou **a ADC**.
   - Entrez des termes de recherche pour trouver rapidement des nœuds spécifiques. Par exemple, cette page affiche les nœuds grid dans deux data centers. La colonne Decommission possible indique que vous pouvez désaffecter le nœud de passerelle, l'un des cinq nœuds de stockage et le nœud d'administration non primaire.



3. Consultez la colonne **Decommission possible** pour chaque nœud que vous souhaitez désaffecter.

   Si un nœud de grid peut être désaffecté, cette colonne est cochée en vert, et la colonne de gauche inclut une case à cocher. Si un nœud ne peut pas être désaffecté, cette colonne décrit le problème. S'il existe plusieurs raisons pour lesquelles un nœud ne peut pas être désaffecté, la raison la plus critique s'affiche.

Motif de mise hors service possible	Description	Étapes à résoudre
Non, la mise hors service du type de nœud n'est pas prise en charge.	Vous ne pouvez pas désaffecter le nœud d'administration principal ou un nœud d'archivage.	Aucune.
Non, au moins un nœud de la grille est déconnecté. **Remarque :** ce message s'affiche uniquement pour les nœuds de grille connectés.	Vous ne pouvez pas désaffecter un nœud de grid connecté si un nœud de grid est déconnecté. La colonne **Santé** comprend l'une des icônes suivantes pour les nœuds de grille déconnectés : • (Gris) : arrêt administratif • (Bleu) : inconnu	Accédez au étape qui répertorie les choix de procédure de mise hors service.
Non, un ou plusieurs nœuds requis sont actuellement déconnectés et doivent être restaurés. **Remarque :** ce message s'affiche uniquement pour les nœuds de grille déconnectés.	Vous ne pouvez pas désaffecter un nœud de grille déconnecté si un ou plusieurs nœuds requis sont également déconnectés (par exemple, un nœud de stockage requis pour le quorum ADC).	a. Consultez les messages de mise hors service possibles pour tous les nœuds déconnectés. b. Déterminez les nœuds qui ne peuvent pas être désaffectés, car ils sont requis. ◦ Si l'état de santé d'un nœud requis est désactivé d'un point de vue administratif, remettre le nœud en ligne. ◦ Si l'état de santé d'un nœud requis n'est pas connu, effectuez une procédure de restauration de nœud pour restaurer le nœud requis.
Non, membre du(des) groupe(s) HA: *X*. Avant de pouvoir désaffecter ce nœud, vous devez le supprimer de tous les groupes haute disponibilité.	Vous ne pouvez pas désaffecter un nœud d'administration ou un nœud de passerelle si une interface de nœud appartient à un groupe haute disponibilité (HA).	Modifiez le groupe haute disponibilité pour supprimer l'interface du nœud ou supprimer l'ensemble du groupe haute disponibilité. Reportez-vous aux instructions pour "Administration d'StorageGRID".

Motif de mise hors service possible	Description	Étapes à résoudre
Non, site *x* nécessite au moins *n* nœuds de stockage avec services ADC.	**Nœuds de stockage uniquement.** vous ne pouvez pas désaffecter un nœud de stockage si un nombre insuffisant de nœuds resterait sur le site pour prendre en charge les exigences de quorum ADC.	Procédez à une extension. Ajoutez un nouveau nœud de stockage au site et spécifiez qu'il doit disposer d'un service ADC. Voir les informations sur le "Quorum ADC".
Non, un ou plusieurs profils de code d'effacement nécessitent au moins *n* nœuds de stockage. Si le profil n'est pas utilisé dans une règle ILM, vous pouvez le désactiver.	**Nœuds de stockage uniquement.** vous ne pouvez pas désaffecter un nœud de stockage à moins qu'il ne reste suffisamment de nœuds pour les profils de code d'effacement existants. Par exemple, si un profil de code d'effacement existe pour un code d'effacement 4+2, au moins 6 nœuds de stockage doivent rester.	Pour chaque profil de code d'effacement concerné, effectuez l'une des opérations suivantes en fonction de l'utilisation du profil : • **Utilisé dans la politique ILM active** : réaliser une expansion. Ajoutez suffisamment de nœuds de stockage pour que le code d'effacement puisse continuer. Reportez-vous aux instructions pour "extension de votre grille". • **Utilisé dans une règle ILM mais pas dans la règle ILM active** : modifiez ou supprimez la règle, puis désactivez le profil de code d'effacement. • **Non utilisé dans une règle ILM** : désactive le profil de code d'effacement. **Remarque :** un message d'erreur s'affiche si vous tentez de désactiver un profil de code d'effacement et que les données d'objet sont toujours associées au profil. Vous devrez peut-être attendre plusieurs semaines avant d'essayer à nouveau le processus de désactivation. Pour en savoir plus sur la désactivation d'un profil de code d'effacement, reportez-vous aux instructions de "Gestion des objets avec ILM".

4. si le déclassement est possible pour le nœud, déterminez quelle procédure vous devez effectuer :

Si votre grille inclut…	Aller à…
Tous les nœuds de la grille déconnectés	"Désaffectation des nœuds de la grille déconnectés"
Nœuds grid connectés uniquement	"Désaffectation des nœuds connectés"

Désaffectation des nœuds de la grille déconnectés

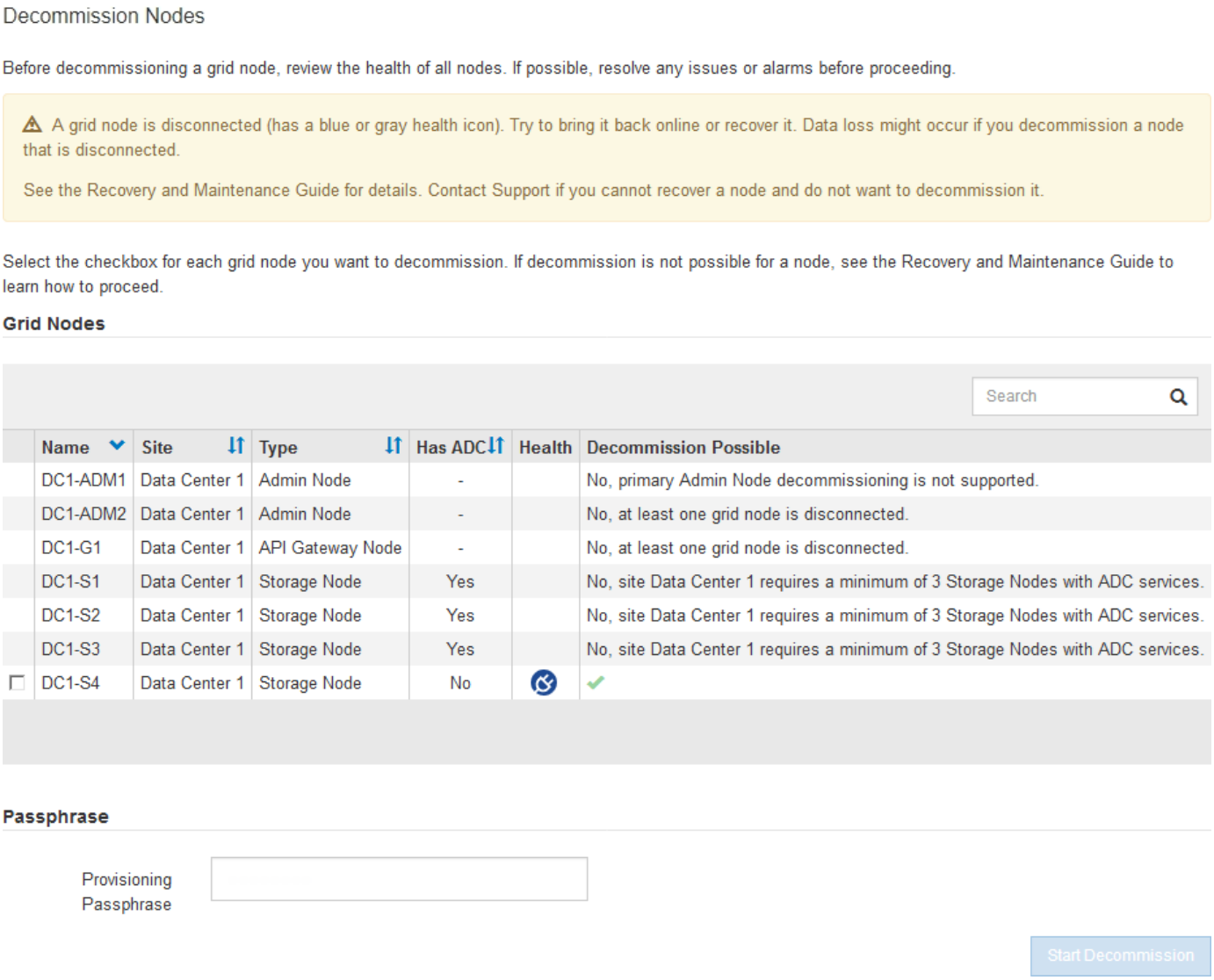
Vous devrez peut-être désaffecter un nœud qui n'est pas actuellement connecté à la grille (dont l'état de santé est inconnu ou désactivé d'un point de vue administratif).

Avant de commencer

- Vous comprenez les exigences et "facteurs à prendre en compte lors de la mise hors service des nœuds".
- Vous avez obtenu tous les éléments prérequis.
- Vous avez vérifié qu'aucun travail de réparation de données n'est actif. Voir "Vérifier les travaux de réparation des données".
- Vous avez confirmé que la restauration du nœud de stockage n'est pas en cours dans la grille. Si c'est le cas, vous devez attendre que la reconstruction Cassandra soit terminée. Vous pouvez ensuite procéder au déclassement.
- Vous avez vérifié que d'autres procédures de maintenance ne seront pas exécutées alors que la procédure de mise hors service du nœud est en cours d'exécution, à moins que la procédure de mise hors service du nœud soit interrompue.
- La colonne **Decommission possible** pour le ou les nœuds déconnectés que vous souhaitez désaffecter contient une coche verte.
- Vous avez la phrase secrète pour le provisionnement.

Description de la tâche

Vous pouvez identifier les nœuds déconnectés en recherchant des icônes inconnues (bleu) ou administrativement déconnectées (gris) dans la colonne **Santé**. Dans l'exemple, le nœud de stockage nommé DC1-S4 est déconnecté ; tous les autres nœuds sont connectés.



Avant de désaffecter un nœud déconnecté, notez ce qui suit :

- Cette procédure est principalement destinée à supprimer un seul nœud déconnecté. Si votre grille contient plusieurs nœuds déconnectés, le logiciel requiert que vous les désinsaffectez tous en même temps, ce qui augmente le risque de résultats inattendus.

> Soyez prudent lors de la mise hors service de plusieurs nœuds de grid déconnectés à la fois, en particulier si vous sélectionnez plusieurs nœuds de stockage déconnectés.

- Si un nœud déconnecté ne peut pas être supprimé (par exemple, un nœud de stockage requis pour le quorum ADC), aucun autre nœud déconnecté ne peut être supprimé.

Avant de désaffecter un **noeud de stockage** déconnecté, notez ce qui suit

- Vous ne devez jamais désaffecter un nœud de stockage déconnecté à moins d'être sûr qu'il ne peut pas être mis en ligne ou restauré.

> Si vous pensez que les données d'objet peuvent toujours être restaurées à partir du nœud, n'effectuez pas cette procédure. Contactez plutôt le support technique pour déterminer si la restauration du nœud est possible.

- Si vous désaffectez plusieurs nœuds de stockage déconnectés, une perte de données peut se produire. Il se peut que le système ne puisse pas reconstruire les données si les copies d'objet, les fragments avec code d'effacement ou les métadonnées d'objet restent disponibles.

> Si vous ne pouvez pas restaurer plusieurs nœuds de stockage déconnectés, contactez le support technique pour déterminer la meilleure solution.

- Lorsque vous désaffectez un nœud de stockage déconnecté, StorageGRID démarre les tâches de réparation des données à la fin du processus de désaffectation. Ces travaux tentent de reconstruire les données d'objet et les métadonnées stockées sur le nœud déconnecté.
- Lorsque vous désaffectez un nœud de stockage déconnecté, la procédure de mise hors service se termine relativement rapidement. Cependant, les tâches de réparation des données peuvent prendre des jours ou des semaines et ne sont pas surveillées par la procédure de mise hors service. Vous devez contrôler ces travaux manuellement et les redémarrer au besoin. Voir "Vérifier les travaux de réparation des données".
- Si vous désaffectez un nœud de stockage déconnecté qui contient la seule copie d'un objet, celui-ci sera perdu. Les tâches de réparation des données ne peuvent reconstruire et récupérer que des objets si au moins une copie répliquée ou suffisamment de fragments avec code d'effacement existent sur les nœuds de stockage actuellement connectés.

Avant de désaffecter un **noeud d'administration** ou **noeud de passerelle** déconnecté, notez ce qui suit :

- Lorsque vous désaffectez un nœud d'administration déconnecté, vous perdrez les journaux d'audit de ce nœud. Cependant, ces journaux doivent également exister sur le nœud d'administration principal.
- Vous pouvez désactiver un nœud de passerelle en toute sécurité lorsqu'il est déconnecté.

Étapes

1. Essayez de remettre en ligne ou de restaurer les nœuds de la grille déconnectée.

   Reportez-vous aux procédures de récupération pour obtenir des instructions.

2. Si vous ne pouvez pas restaurer un nœud de grid déconnecté et que vous souhaitez le désaffecter alors qu'il est déconnecté, cochez la case correspondant à ce nœud.

> Si votre grille contient plusieurs nœuds déconnectés, le logiciel requiert que vous les désinsaffectez tous en même temps, ce qui augmente le risque de résultats inattendus.

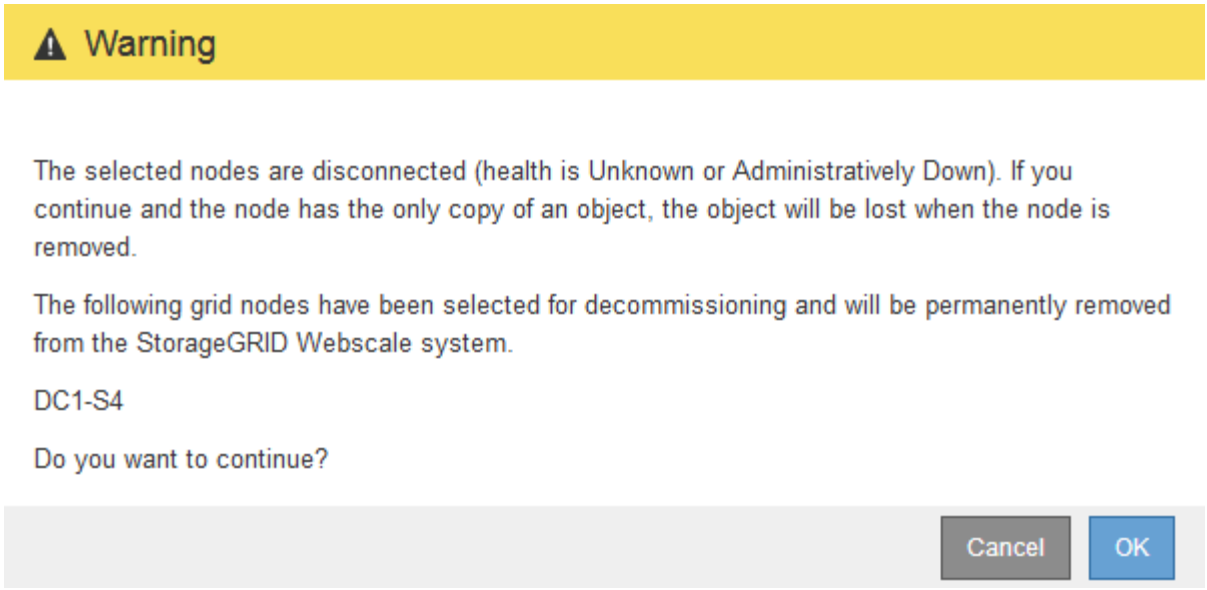
> Soyez prudent lorsque vous choisissez de désaffecter plusieurs nœuds de grid déconnectés à la fois, en particulier si vous sélectionnez plusieurs nœuds de stockage déconnectés. Si vous ne pouvez pas restaurer plusieurs nœuds de stockage déconnectés, contactez le support technique pour déterminer la meilleure solution.

3. Saisissez la phrase secrète pour le provisionnement.

   Le bouton **Start Decommission** est activé.

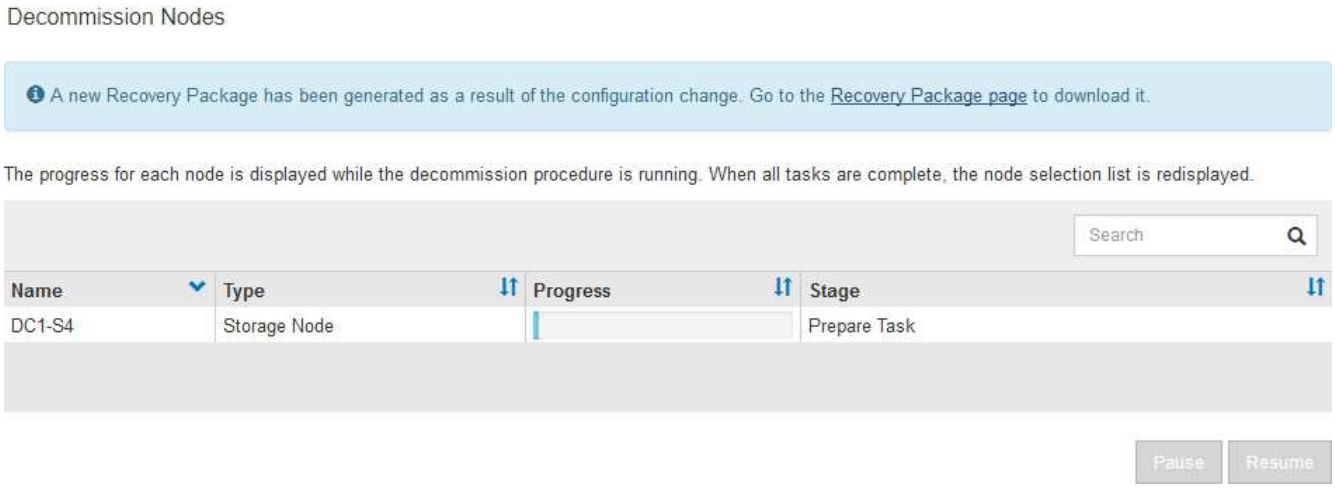
4. Cliquez sur **Start Decommission**.

   Un avertissement apparaît, indiquant que vous avez sélectionné un nœud déconnecté et que ces données d'objet seront perdues si le nœud possède la seule copie d'un objet.



5. Consultez la liste des nœuds et cliquez sur **OK**.

   La procédure de mise hors service démarre et la progression est affichée pour chaque nœud. Au cours de la procédure, un nouveau progiciel de récupération est généré contenant le changement de configuration de la grille.



6. Dès que le nouveau progiciel de récupération est disponible, cliquez sur le lien ou sélectionnez **MAINTENANCE** > **système** > **paquet de récupération** pour accéder à la page du progiciel de récupération. Ensuite, téléchargez le `.zip` fichier.

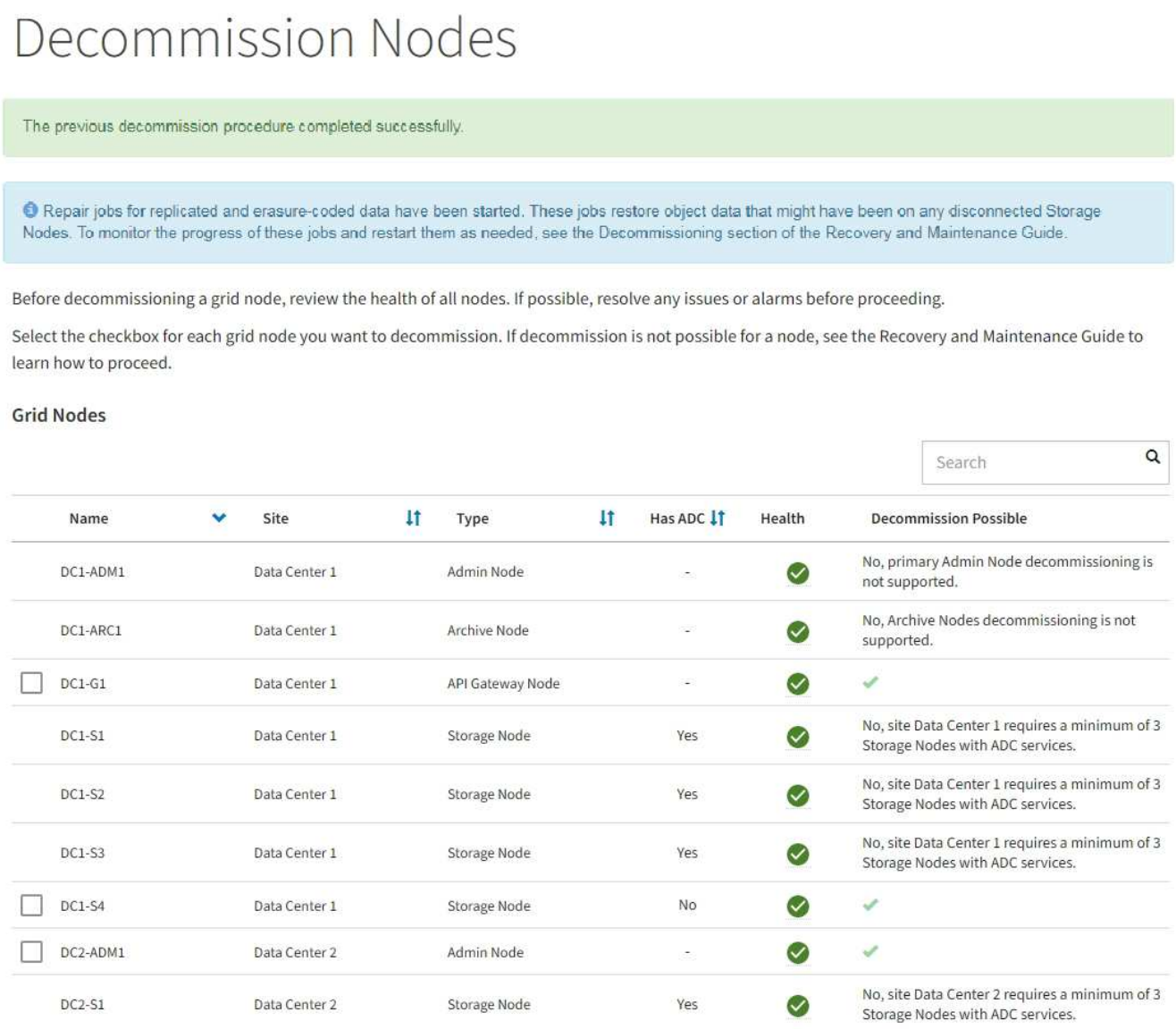
   Reportez-vous aux instructions pour "Téléchargement du progiciel de restauration".

   Téléchargez le progiciel de récupération dès que possible pour vous assurer que vous pouvez récupérer votre grille si un problème survient pendant la procédure de mise hors service.

   Le fichier du progiciel de récupération doit être sécurisé car il contient des clés de cryptage et des mots de passe qui peuvent être utilisés pour obtenir des données du système StorageGRID.

7. Surveillez régulièrement la page mise hors service pour vous assurer que tous les nœuds sélectionnés sont correctement mis hors service.

   La désaffectation des nœuds de stockage peut prendre plusieurs jours ou semaines. Lorsque toutes les tâches sont terminées, la liste de sélection de nœud apparaît à nouveau avec un message de réussite. Si vous avez désactivé un nœud de stockage déconnecté, un message d'information indique que les tâches de réparation ont été lancées.



8. Une fois les nœuds arrêtés automatiquement dans le cadre de la procédure de mise hors service, supprimez les machines virtuelles restantes ou d'autres ressources associées au nœud mis hors service.

   > N'effectuez pas cette étape tant que les nœuds ne s'arrêtent pas automatiquement.

9. Si vous désaffectez un nœud de stockage, surveillez l'état des tâches de réparation **données répliquées** et **données codées d'effacement (EC)** qui sont automatiquement lancées pendant le processus de mise hors service.

Les données répliquées

- Pour obtenir une estimation du pourcentage d'achèvement de la réparation répliquée, ajoutez le `show-replicated-repair-status` option de la commande repair-data.

  ```
  repair-data show-replicated-repair-status
  ```

- Pour déterminer si les réparations sont terminées :
  a. Sélectionnez **NŒUDS** > ***nœud de stockage en cours de réparation*** > **ILM**.
  b. Vérifiez les attributs dans la section évaluation. Lorsque les réparations sont terminées, l'attribut **attente - tous** indique 0 objets.
- Pour surveiller la réparation plus en détail :
  a. Sélectionnez **SUPPORT** > **Outils** > **topologie de grille**.
  b. Sélectionnez ***GRID*** > ***Storage Node en cours de réparation*** > **LDR** > **Data Store**.
  c. Utilisez une combinaison des attributs suivants pour déterminer, autant que possible, si les réparations répliquées sont terminées.

  > Cassandra présente peut-être des incohérences et les réparations échouées ne sont pas suivies.

  - **Réparations tentées (XRPA)** : utilisez cet attribut pour suivre la progression des réparations répliquées. Cet attribut augmente chaque fois qu'un nœud de stockage tente de réparer un objet à haut risque. Lorsque cet attribut n'augmente pas pendant une période plus longue que la période d'acquisition actuelle (fournie par l'attribut **période d'analyse — estimation**), cela signifie que l'analyse ILM n'a trouvé aucun objet à haut risque qui doit être réparé sur n'importe quel nœud.

    > Les objets à haut risque sont des objets qui risquent d'être complètement perdus. Cela n'inclut pas les objets qui ne répondent pas à leur configuration ILM.

  - **Période d'acquisition — estimée (XSCM)** : utilisez cet attribut pour estimer quand une modification de règle sera appliquée aux objets précédemment ingérés. Si l'attribut **réparations tentées** n'augmente pas pendant une période supérieure à la période d'acquisition actuelle, il est probable que les réparations répliquées soient effectuées. Notez que la période d'acquisition peut changer. L'attribut **période d'acquisition — estimée (XSCM)** s'applique à la grille entière et est le maximum de toutes les périodes d'acquisition de nœud. Vous pouvez interroger l'historique d'attributs **période de balayage — estimation** de la grille pour déterminer une période appropriée.

Données avec code d'effacement (EC)

Pour surveiller la réparation des données codées d'effacement et réessayer toute demande qui pourrait avoir échoué :

1. Déterminez l'état des réparations des données par code d'effacement :
   - Sélectionnez **SUPPORT** > **Tools** > **Metrics** pour afficher le temps de réalisation estimé et le pourcentage de réalisation de la tâche en cours. Sélectionnez ensuite **EC Overview** dans la section Grafana. Examinez les tableaux de bord **Grid EC Job estimé Time to Completion** et **Grid EC Job Percentage Finted**.

- Utilisez cette commande pour afficher le statut d'un spécifique `repair-data` fonctionnement :

  ```
  repair-data show-ec-repair-status --repair-id repair ID
  ```

- Utilisez cette commande pour lister toutes les réparations :

  ```
  repair-data show-ec-repair-status
  ```

Les informations de sortie sont affichées, notamment `repair ID`, pour toutes les réparations précédentes et en cours.

2. Si le résultat indique que l'opération de réparation a échoué, utilisez le `--repair-id` option permettant de réessayer la réparation.

   Cette commande relance une réparation de nœud ayant échoué à l'aide de l'ID de réparation 6949309319275667690 :

   ```
   repair-data start-ec-node-repair --repair-id 6949309319275667690
   ```

   Cette commande relance une réparation de volume en échec à l'aide de l'ID de réparation 6949309319275667690 :

   ```
   repair-data start-ec-volume-repair --repair-id 6949309319275667690
   ```

Une fois que vous avez terminé

Dès que les nœuds déconnectés ont été désaffectés et que toutes les tâches de réparation de données ont été effectuées, vous pouvez désaffecter tous les nœuds de la grille connectés si nécessaire.

Ensuite, procédez comme suit après avoir effectué la procédure de mise hors service :

- Assurez-vous que les disques du nœud de la grille mis hors service sont nettoyés. Utilisez un outil ou un service d'effacement de données disponible dans le commerce pour supprimer définitivement et de manière sécurisée les données des lecteurs.
- Si vous désaffecté un nœud d'appliance et que les données de l'appliance étaient protégées à l'aide du chiffrement des nœuds, utilisez le programme d'installation de l'appliance StorageGRID pour effacer la configuration du serveur de gestion des clés (KMS transparent). Vous devez effacer la configuration KMS si vous souhaitez ajouter l'appliance à une autre grille. Pour obtenir des instructions, reportez-vous à la section "Surveillez le chiffrement des nœuds en mode de maintenance".

Informations associées

"Procédures de restauration des nœuds de la grille"

Désaffectation des nœuds connectés

Vous pouvez mettre hors service et supprimer définitivement les nœuds connectés à la grille.

Avant de commencer

- Vous comprenez les exigences et "facteurs à prendre en compte lors de la mise hors service des nœuds".
- Vous avez réuni tous les documents requis.

- Vous avez vérifié qu'aucun travail de réparation de données n'est actif.
- Vous avez confirmé que la restauration du nœud de stockage n'est pas en cours dans la grille. Si c'est le cas, attendez que toute reconstruction Cassandra effectuée dans le cadre de la restauration soit terminée. Vous pouvez ensuite procéder au déclassement.
- Vous avez vérifié que d'autres procédures de maintenance ne seront pas exécutées alors que la procédure de mise hors service du nœud est en cours d'exécution, à moins que la procédure de mise hors service du nœud soit interrompue.
- Vous avez la phrase secrète pour le provisionnement.
- Les nœuds de la grille sont connectés.
- La colonne **décomposition possible** du ou des nœuds que vous souhaitez désaffecter comporte une coche verte.

> La mise hors service ne démarre pas si un ou plusieurs volumes sont hors ligne (démontés) ou s'ils sont en ligne (montés) mais en état d'erreur.

> Si un ou plusieurs volumes sont déconnectés alors qu'une mise hors service est en cours, le processus de mise hors service se termine une fois ces volumes remis en ligne.

- Tous les nœuds de la grille ont une état normal (vert) . Si l'une de ces icônes apparaît dans la colonne **Santé**, vous devez essayer de résoudre le problème :

Icône	Couleur	Gravité
	Jaune	Avertissement
	Orange clair	Mineur
	Orange foncé	Majeur
	Rouge	Primordial

- Si vous avez précédemment mis hors service un nœud de stockage déconnecté, les tâches de réparation des données ont toutes été effectuées avec succès. Voir "Vérifier les travaux de réparation des données".

> Ne supprimez pas la machine virtuelle ou d'autres ressources d'un nœud de grille avant d'y être invité dans cette procédure.

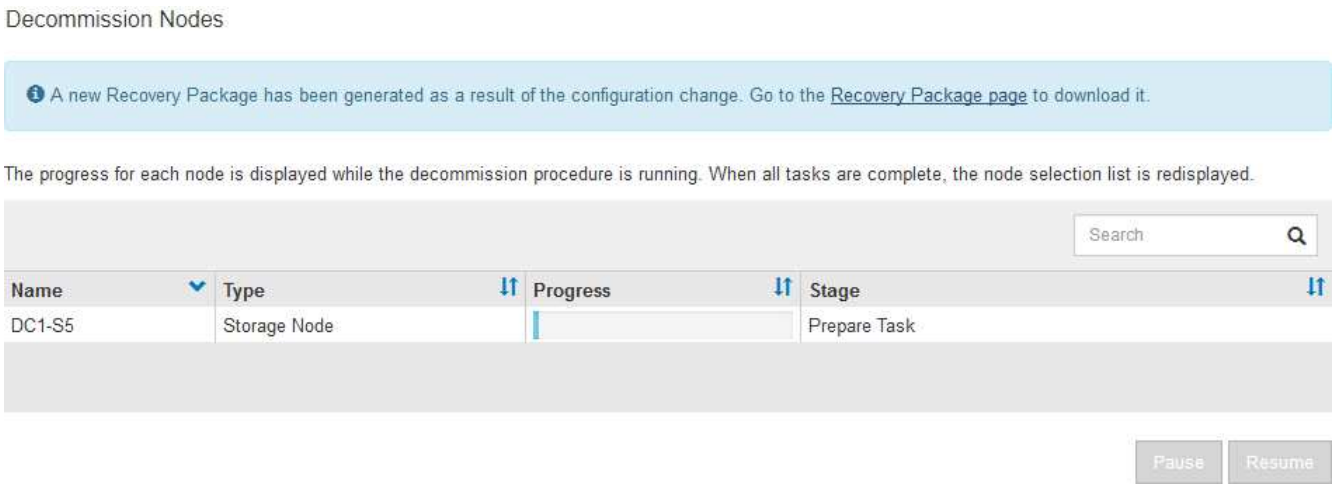
Étapes

1. Dans la page nœuds de décomposition, cochez la case correspondant à chaque nœud de grille que vous souhaitez désaffecter.
2. Saisissez la phrase secrète pour le provisionnement.

   Le bouton **Start Decommission** est activé.

3. Cliquez sur **Start Decommission**.
4. Vérifiez la liste des nœuds dans la boîte de dialogue de confirmation, puis cliquez sur **OK**.

   La procédure de mise hors service du nœud démarre et la progression est affichée pour chaque nœud. Au cours de la procédure, un nouveau progiciel de récupération est généré pour afficher le changement de configuration de la grille.



> Ne mettez pas un nœud de stockage hors ligne après le démarrage de la procédure de mise hors service. La modification de l'état peut entraîner l'absence de copie de contenu vers d'autres emplacements.

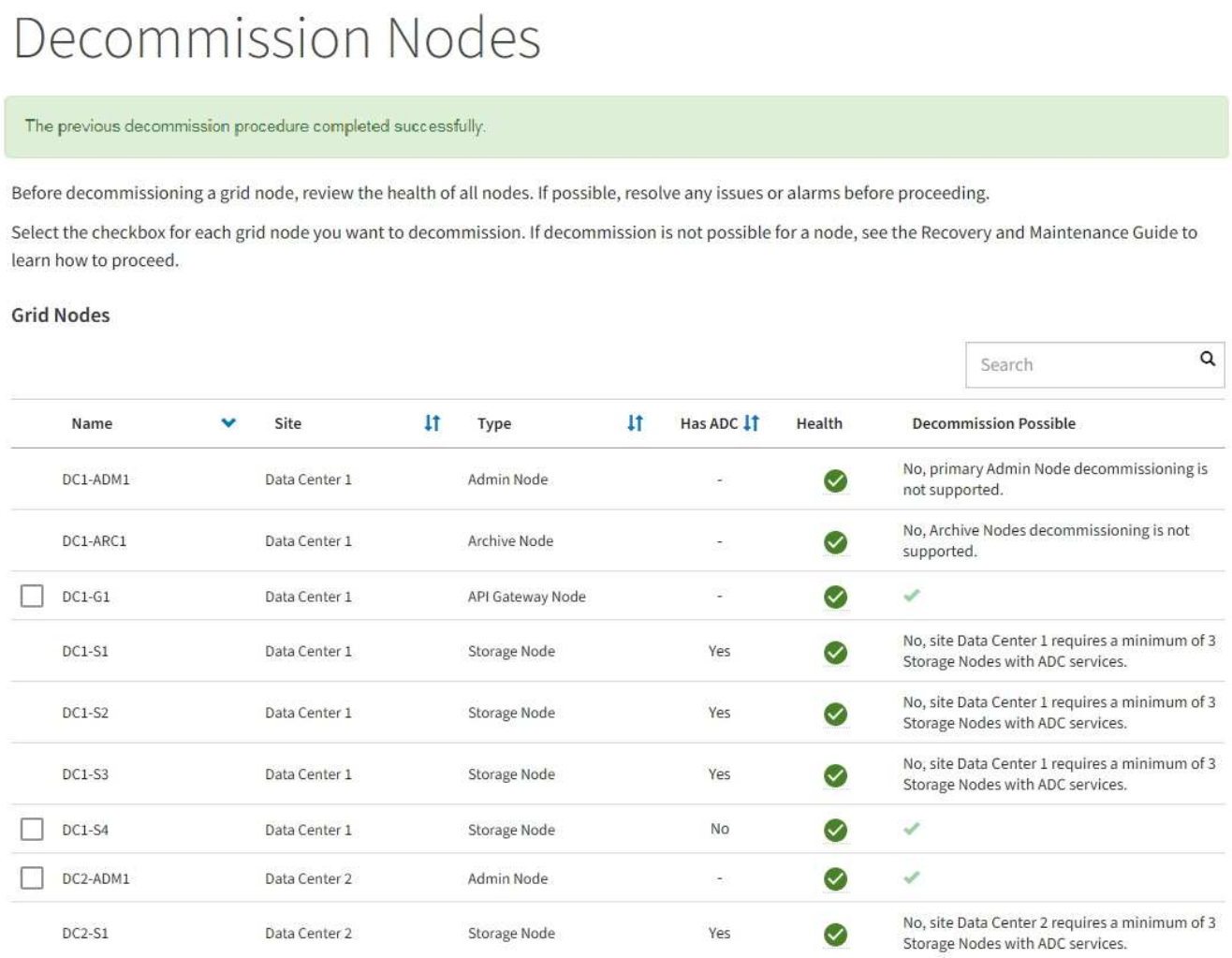
5. Dès que le nouveau progiciel de récupération est disponible, cliquez sur le lien ou sélectionnez **MAINTENANCE** > **système** > **paquet de récupération** pour accéder à la page du progiciel de récupération. Ensuite, téléchargez le `.zip` fichier.

   Reportez-vous aux instructions pour "Téléchargement du progiciel de restauration".

> Téléchargez le progiciel de récupération dès que possible pour vous assurer que vous pouvez récupérer votre grille si un problème survient pendant la procédure de mise hors service.

6. Surveillez régulièrement la page nœuds de mise hors service pour vous assurer que tous les nœuds sélectionnés sont correctement mis hors service.

   La désaffectation des nœuds de stockage peut prendre plusieurs jours ou semaines. Lorsque toutes les tâches sont terminées, la liste de sélection de nœud apparaît à nouveau avec un message de réussite.



7. Suivez l'étape appropriée pour votre plate-forme. Par exemple :
   - **Linux** : vous pouvez détacher les volumes et supprimer les fichiers de configuration de nœud que vous avez créés lors de l'installation.
   - **VMware**: Vous pouvez utiliser l'option vCenter "Supprimer du disque" pour supprimer la machine virtuelle. Il se peut également que vous deviez supprimer tous les disques de données qui sont indépendants de la machine virtuelle.
   - **Appliance StorageGRID** : le nœud de l'appliance revient automatiquement à un état non déployé où vous pouvez accéder au programme d'installation de l'appliance StorageGRID. Vous pouvez mettre l'appareil hors tension ou l'ajouter à un autre système StorageGRID.

Suivez cette procédure une fois la procédure de mise hors service du nœud terminée :

- Assurez-vous que les disques du nœud de la grille mis hors service sont nettoyés. Utilisez un outil ou un service d'effacement de données disponible dans le commerce pour supprimer définitivement et de manière sécurisée les données des lecteurs.
- Si vous avez désaffecté un nœud de l'appliance et que les données de l'appliance ont été protégées par chiffrement des nœuds, utilisez le programme d'installation de l'appliance StorageGRID pour effacer la configuration du serveur de gestion des clés (effacer KMS). Si vous souhaitez ajouter l'appliance à une autre grille, vous devez effacer la configuration KMS. Pour obtenir des instructions, reportez-vous à la section "Surveillez le chiffrement des nœuds en mode de maintenance".

Informations associées

"Installez Red Hat Enterprise Linux ou CentOS"

Interrompre et reprendre le processus de mise hors service des nœuds de stockage

Si vous devez effectuer une deuxième procédure de maintenance, vous pouvez interrompre la procédure de mise hors service d'un nœud de stockage pendant certaines étapes. Une fois l'autre procédure terminée, vous pouvez reprendre la mise hors service.

> Le bouton **Pause** n'est activé que lorsque les étapes d'évaluation ILM ou de déclassement des données avec code d'effacement sont atteintes. Cependant, l'évaluation ILM (migration des données) continue à s'exécuter en arrière-plan.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous disposez de l'autorisation Maintenance ou accès racine.

Étapes

1. Sélectionnez **MAINTENANCE** > **tâches** > **désaffectation**.

   La page mise hors service s'affiche.

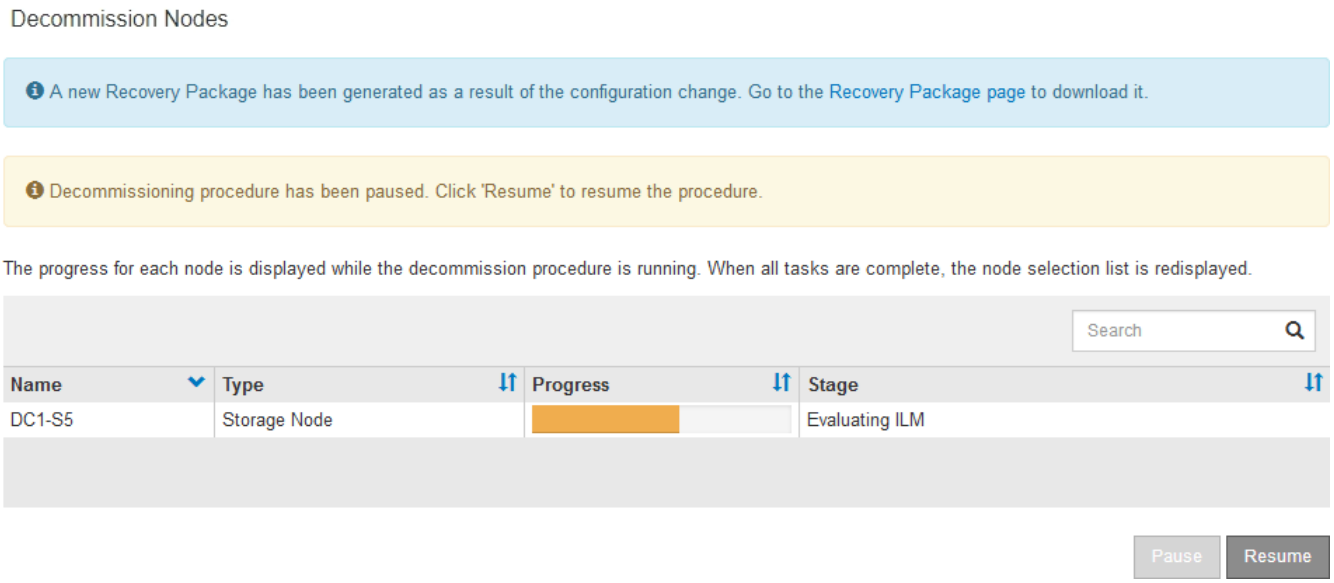
2. Sélectionnez **nœuds de mise hors service**.

   La page nœuds de mise hors service s'affiche. Lorsque la procédure de mise hors service atteint l'une des étapes suivantes, le bouton **Pause** est activé.

   - Évaluation des règles ILM
   - Déclassement des données avec code d'effacement

3. Sélectionnez **Pause** pour suspendre la procédure.

   L'étape en cours est mise en pause et le bouton **reprendre** est activé.



4. Une fois l'autre procédure de maintenance terminée, sélectionnez **reprendre** pour poursuivre la mise hors service.

Dépanner le déclassement des nœuds

Si la procédure de mise hors service du nœud s'arrête à cause d'une erreur, vous pouvez prendre des étapes spécifiques pour résoudre le problème.

Avant de commencer

Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".

Description de la tâche

Si vous arrêtez le nœud de la grille en cours de mise hors service, la tâche s'arrête jusqu'au redémarrage du nœud de la grille. Le nœud grid doit être en ligne.

Étapes

1. Sélectionnez **SUPPORT** > **Outils** > **topologie de grille**.
2. Dans l'arborescence de la topologie grille, développez chaque entrée de noeud de stockage et vérifiez que les services DDS et LDR sont tous deux en ligne.

   Pour désaffecter les nœuds de stockage, tous les nœuds et tous les services doivent être sains au début du déclassement d'un nœud/site en ligne.

3. Pour afficher les tâches de grille actives, sélectionnez **Primary Admin Node** > **CMN** > **Grid Tasks** > **Overview**.
4. Vérifiez l'état de la tâche de grille de mise hors service.

   a. Si l'état de la tâche de grille de déclassement indique un problème lors de l'enregistrement des ensembles de tâches de grille, sélectionnez **Primary Admin Node** > **CMN** > **Events** > **Overview**

   b. Vérifier le nombre de relais d'audit disponibles.

      Si l'attribut Relais d'audit disponible est un ou plusieurs, le service CMN est connecté à au moins un service ADC. Les services ADC font office de relais d'audit.

   Le service CMN doit être connecté à au moins un service ADC et une majorité (50 % plus un) des services ADC du système StorageGRID doit être disponible pour qu'une tâche de grille passe d'une étape de déclassement à une autre et se termine.

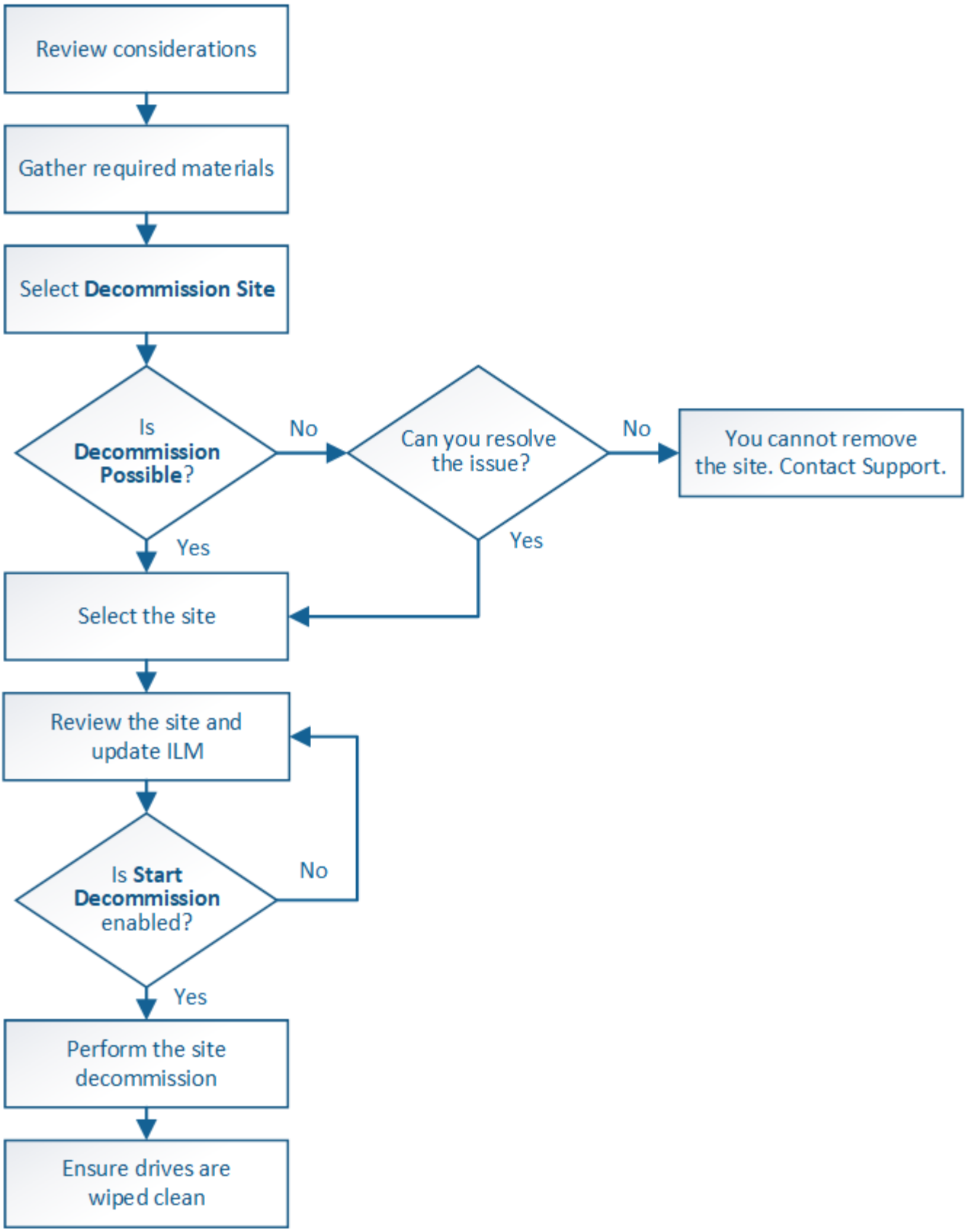
   a. Si le service CMN n'est pas connecté à suffisamment de services ADC, assurez-vous que les nœuds de stockage sont en ligne et vérifiez la connectivité réseau entre le nœud d'administration principal et les nœuds de stockage.

Mise hors service du site

Désaffectation du site : présentation

Il se peut que vous deviez supprimer un site de data Center du système StorageGRID. Pour supprimer un site, vous devez le mettre hors service.

L'organigramme présente les étapes générales de la mise hors service d'un site.



Considérations relatives à la suppression d'un site

Avant d'utiliser la procédure de mise hors service du site pour supprimer un site, vous devez prendre en compte les considérations.

Que se passe-t-il lorsque vous désaffectez un site

Lorsque vous désaffectez un site, StorageGRID supprime définitivement tous les nœuds du site et le site lui-même du système StorageGRID.

Lorsque la procédure de mise hors service du site est terminée :

- Vous ne pouvez plus utiliser StorageGRID pour afficher ou accéder au site ou à l'un des nœuds du site.
- Vous ne pouvez plus utiliser de pools de stockage ou de profils de code d'effacement faisant référence au site. Lorsque StorageGRID décompresse un site, il supprime automatiquement ces pools de stockage et désactive ces profils de code d'effacement.

Différences entre les procédures de mise hors service du site connecté et du site déconnecté

Vous pouvez utiliser la procédure de mise hors service du site pour supprimer un site dans lequel tous les nœuds sont connectés à StorageGRID (appelé mise hors service du site connecté) ou pour supprimer un site dans lequel tous les nœuds sont déconnectés de StorageGRID (appelé mise hors service hors site déconnectée). Avant de commencer, vous devez comprendre les différences entre ces procédures.

> Si un site contient un mélange de connecté ( ) et noeuds déconnectés (ou), vous devez remettre tous les nœuds hors ligne en ligne.

- Une désaffectation de site connecté vous permet de supprimer un site opérationnel du système StorageGRID. Par exemple, vous pouvez effectuer une mise hors service du site connecté pour supprimer un site qui fonctionne mais qui n'est plus nécessaire.
- Lorsque StorageGRID supprime un site connecté, il gère les données d'objet du site à l'aide de ILM. Avant de pouvoir lancer la désaffectation d'un site connecté, vous devez supprimer ce site de toutes les règles ILM et activer une nouvelle règle ILM. Les processus ILM pour migrer les données d'objet et les processus internes pour supprimer un site peuvent se produire au même moment, mais la meilleure pratique consiste à exécuter la procédure ILM avant de démarrer la procédure de déclassement.
- Une désaffectation du site vous permet de supprimer un site défectueux du système StorageGRID. Par exemple, vous pouvez effectuer une mise hors service du site déconnecté pour retirer un site qui a été détruit par un incendie ou une inondation.

  Lorsque StorageGRID supprime un site déconnecté, il considère que tous les nœuds sont irrécupérables et ne tentent pas de préserver les données. Toutefois, avant de pouvoir démarrer une mise hors service de site déconnecté, vous devez supprimer le site de toutes les règles ILM et activer une nouvelle règle ILM.

  > Avant d'effectuer une procédure de mise hors service hors site déconnectée, vous devez contacter votre ingénieur commercial NetApp. NetApp évaluera vos besoins avant d'activer toutes les étapes de l'assistant Decommission site. N'essayez pas de désaffecter le site si vous pensez qu'il est possible de récupérer le site ou de récupérer les données d'objet à partir du site.

Conditions générales requises pour supprimer un site connecté ou déconnecté

Avant de supprimer un site connecté ou déconnecté, vous devez connaître les exigences suivantes :

- Vous ne pouvez pas désaffecter un site qui inclut le nœud d'administration principal.
- Vous ne pouvez pas désaffecter un site qui inclut un nœud d'archivage.

- Vous ne pouvez pas désaffecter un site si l'un des nœuds dispose d'une interface appartenant à un groupe haute disponibilité (HA). Vous devez modifier le groupe haute disponibilité pour supprimer l'interface du nœud ou supprimer l'ensemble du groupe haute disponibilité.
- Vous ne pouvez pas désaffecter un site s'il contient un mélange de connecté ( ) et déconnecté (ou) nœuds.
- Vous ne pouvez pas désaffecter un site si un nœud d'un autre site est déconnecté (ou).
- Vous ne pouvez pas démarrer la procédure de mise hors service du site si une opération de réparation de nœud ec est en cours. Voir "Vérifier les travaux de réparation des données" pour suivre les réparations de données codées par effacement.
- Pendant que la procédure de mise hors service du site est en cours d'exécution :
  - Vous ne pouvez pas créer de règles ILM faisant référence au site en cours de désaffectation. Vous ne pouvez pas non plus modifier une règle ILM existante pour faire référence au site.
  - Vous ne pouvez pas effectuer d'autres procédures de maintenance, telles que l'extension ou la mise à niveau.

    Si vous devez effectuer une autre procédure de maintenance pendant la mise hors service d'un site connecté, vous pouvez "Interrompez la procédure pendant le retrait des nœuds de stockage". Le bouton **Pause** n'est activé que lorsque les étapes d'évaluation ILM ou de déclassement des données avec code d'effacement sont atteintes. Cependant, l'évaluation ILM (migration des données) continue à s'exécuter en arrière-plan. Une fois la deuxième procédure d'entretien terminée, vous pouvez reprendre la mise hors service.

  - Si vous devez récupérer un nœud après avoir lancé la procédure de mise hors service du site, vous devez contacter le service de support.
- Vous ne pouvez pas désaffecter plusieurs sites à la fois.
- Si le site inclut un ou plusieurs nœuds d'administration et que l'authentification unique (SSO) est activée pour votre système StorageGRID, vous devez supprimer toutes les approbations tierces pour le site de Active Directory Federation Services (AD FS).

Exigences relatives à la gestion du cycle de vie des informations (ILM)

Dans le cadre de la suppression d'un site, vous devez mettre à jour votre configuration ILM. L'assistant dédié au site de désaffection vous guide à travers un certain nombre d'étapes préalables pour vous assurer que :

- Le site n'est pas référencé à la politique ILM active. Le cas échéant, vous devez créer et activer une nouvelle règle ILM avec de nouvelles règles ILM.
- Aucune règle ILM proposée n'existe. Si vous avez une stratégie proposée, vous devez la supprimer.
- Aucune règle ILM ne renvoie au site, même si ces règles ne sont pas utilisées dans la politique active ou proposée. Vous devez supprimer ou modifier toutes les règles qui font référence au site.

Lorsque StorageGRID décompresse le site, il désactive automatiquement tous les profils de code d'effacement inutilisés qui font référence au site et supprime automatiquement les pools de stockage inutilisés qui font référence au site. Si le pool de stockage tous les nœuds existe (StorageGRID 11.6 et versions antérieures), il est supprimé car il utilise tous les sites.

Avant de pouvoir supprimer un site, vous devrez peut-être créer de nouvelles règles ILM et activer une nouvelle politique ILM. Ces instructions supposent que vous connaissez bien le fonctionnement d'ILM et que vous connaissez déjà la création de pools de stockage, les profils de code d'effacement, les règles ILM ainsi que la simulation et l'activation d'une stratégie ILM. Voir "Gestion des objets avec ILM".

Considérations relatives aux données d'objet sur un site connecté

Si vous effectuez la mise hors service d'un site connecté, vous devez décider ce que vous devez faire avec les données d'objet existantes sur le site lorsque vous créez de nouvelles règles ILM et une nouvelle règle ILM. Vous pouvez effectuer l'une des opérations suivantes ou les deux :

- Déplacez les données d'objet du site sélectionné vers un ou plusieurs autres sites de votre grille.

  Exemple de déplacement de données : supposons que vous souhaitiez désaffecter un site à Raleigh parce que vous avez ajouté un nouveau site à Sunnyvale. Dans cet exemple, vous voulez déplacer toutes les données d'objet de l'ancien site vers le nouveau site. Avant de mettre à jour vos règles ILM et notre politique ILM, vous devez étudier la capacité des deux sites. Vous devez vous assurer que la capacité du site de Sunnyvale est suffisante pour prendre en charge les données objet depuis le site Raleigh, et que la capacité nécessaire à sa croissance future restera celle de Sunnyvale.

  Pour assurer la disponibilité d'une capacité adéquate, vous devrez peut-être le faire "développez votre grille" En ajoutant des volumes de stockage ou des nœuds de stockage à un site existant ou en ajoutant un nouveau site avant d'effectuer cette procédure.

- Supprimer les copies d'objet du site sélectionné.

  Exemple de suppression de données : supposons que vous utilisez actuellement une règle ILM de 3 copies pour répliquer des données d'objet sur trois sites. Avant de désaffecter un site, vous pouvez créer une règle ILM à 2 copies pour stocker les données sur seulement deux sites. Lorsque vous activez une nouvelle règle ILM utilisant la règle à 2 copies, StorageGRID supprime les copies du troisième site car elles ne satisfont plus aux exigences ILM. Cependant, les données d'objet seront toujours protégées et la capacité des deux sites restants restera identique.

  Ne créez jamais de règle ILM à copie unique pour la suppression d'un site. La règle ILM de création d'une seule copie répliquée pendant toute période met les données à risque de perte permanente. Si une seule copie répliquée d'un objet existe, cet objet est perdu en cas de défaillance ou d'erreur importante d'un noeud de stockage. De plus, lors des procédures de maintenance telles que les mises à niveau, l'accès à l'objet est temporairement perdu.

Exigences supplémentaires relatives à la mise hors service d'un site connecté

Avant que StorageGRID puisse supprimer un site connecté, vous devez vous assurer que :

- Tous les nœuds de votre système StorageGRID doivent avoir un état de connexion * connecté* ( ), cependant, les nœuds peuvent avoir des alertes actives.

  Vous pouvez exécuter les étapes 1-4 de l'assistant Decommission site si un ou plusieurs nœuds sont déconnectés. Toutefois, vous ne pouvez pas effectuer l'étape 5 de l'assistant, qui démarre le processus de mise hors service, sauf si tous les nœuds sont connectés.

- Si le site que vous souhaitez supprimer contient un nœud de passerelle ou un nœud d'administration utilisé pour l'équilibrage de charge, vous devrez peut-être le faire"développez votre grille" pour ajouter un nouveau nœud équivalent sur un autre site. Assurez-vous que les clients peuvent vous connecter au nœud de remplacement avant de lancer la procédure de mise hors service du site.
- Si le site que vous prévoyez de supprimer contient un nœud de passerelle ou des nœuds d'administration qui se trouvent dans un groupe haute disponibilité, vous pouvez effectuer les étapes 1-4 de l'assistant dédié au site de mise hors service. Toutefois, vous ne pouvez pas effectuer l'étape 5 de l'assistant, qui démarre le processus de mise hors service, tant que vous n'avez pas supprimé ces nœuds de tous les groupes haute disponibilité. Si des clients existants se connectent à un groupe haute disponibilité incluant des nœuds du site, assurez-vous qu'ils peuvent continuer à se connecter à StorageGRID une fois le site supprimé.
- Si les clients se connectent directement aux nœuds de stockage du site que vous prévoyez de supprimer, assurez-vous qu'ils peuvent se connecter aux nœuds de stockage sur d'autres sites avant de lancer la procédure de mise hors service du site.
- Vous devez fournir un espace suffisant sur les sites restants pour prendre en charge les données d'objet qui seront déplacées en raison des modifications apportées à la politique ILM active. Dans certains cas, vous devrez peut-être le faire "développez votre grille" En ajoutant des nœuds de stockage, des volumes de stockage ou de nouveaux sites avant de pouvoir désaffecter un site connecté.
- Vous devez prévoir suffisamment de temps pour que la procédure de mise hors service soit terminée. Les processus ILM d'StorageGRID peuvent prendre plusieurs jours, semaines, voire plusieurs mois pour déplacer ou supprimer les données d'objet depuis le site avant la mise hors service du site.

> Le déplacement ou la suppression de données d'objet depuis un site peut prendre plusieurs jours, semaines, voire mois, en fonction de la quantité de données sur le site, de la charge sur votre système, des latences réseau et de la nature des modifications ILM requises.

- Dans la mesure du possible, vous devez exécuter les étapes 1-4 de l'assistant Decommission site dès que possible. La procédure de mise hors service se termine plus rapidement et avec moins d'interruptions et d'impacts sur les performances si vous permettez le déplacement des données depuis le site avant de démarrer la procédure de mise hors service réelle (en sélectionnant **Démarrer la mise hors service** à l'étape 5 de l'assistant).

Exigences supplémentaires relatives à la mise hors service d'un site déconnecté

Avant que StorageGRID puisse supprimer un site déconnecté, vous devez vérifier ce qui suit :

- Vous avez contacté votre ingénieur commercial NetApp. NetApp évaluera vos besoins avant d'activer toutes les étapes de l'assistant Decommission site.

> N'essayez pas de désaffecter le site si vous pensez qu'il est possible de récupérer le site ou de récupérer des données objet à partir du site. Voir"Comment la reprise sur site est effectuée par le support technique".

- Tous les nœuds du site doivent avoir un état de connexion de l'un des éléments suivants :
  - **Inconnu** ( ) : Pour une raison inconnue, un nœud est déconnecté ou les services du nœud sont arrêtés de manière inattendue. Par exemple, un service du nœud peut être arrêté, ou le nœud a perdu sa connexion réseau en raison d'une panne de courant ou d'une panne imprévue.
  - * Arrêt administratif* ( ) : Le nœud n'est pas connecté à la grille pour une raison attendue. Par exemple, le ou les services du nœud ont été normalement arrêtés.

- Tous les nœuds de tous les autres sites doivent avoir un état de connexion * connecté* ( ), cependant, ces autres nœuds peuvent avoir des alertes actives.
- Vous devez comprendre que vous ne pourrez plus utiliser StorageGRID pour consulter ou récupérer toutes les données d'objet qui ont été stockées sur le site. Lorsque StorageGRID exécute cette procédure, il ne tente pas de préserver les données du site déconnecté.

> Si vos règles et règles ILM ont été conçues pour protéger contre la perte d'un seul site, des copies de vos objets existent toujours sur les sites restants.

- Vous devez comprendre que si le site contenait la seule copie d'un objet, l'objet est perdu et ne peut pas être récupéré.

Considérations relatives aux contrôles de cohérence lorsque vous supprimez un site

Le niveau de cohérence d'un compartiment S3 ou d'un conteneur Swift détermine si StorageGRID réplique entièrement les métadonnées d'objet vers tous les nœuds et sites avant de transmettre le bon déroulement de l'ingestion de l'objet à un client. Les contrôles de cohérence assurent un équilibre entre la disponibilité des objets et la cohérence de ces objets entre plusieurs nœuds de stockage et sites.

Lorsque StorageGRID supprime un site, il doit s'assurer qu'aucune donnée n'est écrite sur le site supprimé. Par conséquent, il remplace temporairement le niveau de cohérence pour chaque compartiment ou conteneur. Une fois le processus de mise hors service du site démarré, StorageGRID utilise temporairement une cohérence forte entre les sites pour empêcher l'écriture des métadonnées d'objet sur le site.

Par conséquent, sachez que toute opération d'écriture, de mise à jour et de suppression du client qui se produit lors de la désaffectation d'un site peut échouer si plusieurs nœuds ne sont plus disponibles sur les sites restants.

Rassembler les matériaux nécessaires

Avant de mettre un site hors service, vous devez obtenir les documents suivants.

Élément	Remarques
Package de restauration `.zip` fichier	Vous devez télécharger le dernier progiciel de récupération `.zip` fichier (`sgws-recovery-package-id-revision.zip`). Vous pouvez utiliser le fichier du progiciel de récupération pour restaurer le système en cas de défaillance. "Téléchargez le progiciel de restauration"
`Passwords.txt` fichier	Ce fichier contient les mots de passe requis pour accéder aux nœuds de la grille sur la ligne de commande et est inclus dans le progiciel de récupération.
Phrase secrète pour le provisionnement	La phrase de passe est créée et documentée lors de l'installation initiale du système StorageGRID. La phrase de passe de provisionnement n'est pas dans le `Passwords.txt` fichier.

Élément	Remarques
Description de la topologie du système StorageGRID avant la mise hors service	Le cas échéant, procurez-vous toute documentation décrivant la topologie actuelle du système.

Informations associées

"Navigateurs Web pris en charge"

Étape 1 : sélectionnez site

Pour déterminer si un site peut être déclassé, commencez par accéder à l'assistant Decommission site.

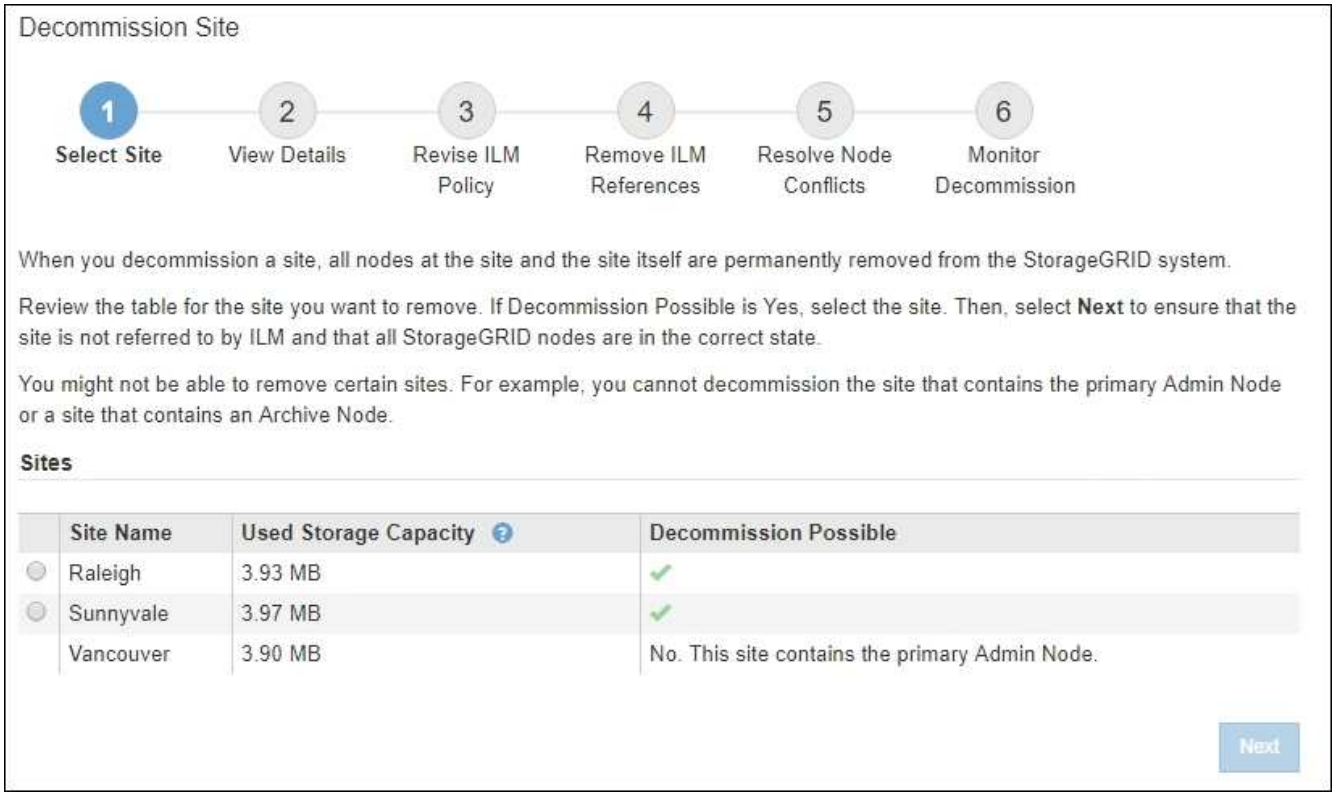
Avant de commencer

- Vous avez obtenu tous les matériaux requis.
- Vous avez examiné les considérations relatives à la suppression d'un site.
- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous disposez de l'autorisation d'accès racine ou des autorisations Maintenance et ILM.

Étapes

1. Sélectionnez **MAINTENANCE** > **tâches** > **désaffectation**.
2. Sélectionnez **site de désaffection**.

   L'étape 1 (Sélectionner le site) de l'assistant de site de désaffection s'affiche. Cette étape contient une liste alphabétique des sites de votre système StorageGRID.



3. Affichez les valeurs de la colonne capacité de stockage * utilisée pour déterminer la quantité de stockage actuellement utilisée pour les données d'objet de chaque site.

   La capacité de stockage utilisée est une estimation. Si les nœuds sont hors ligne, la capacité de stockage utilisée est la dernière valeur connue du site.

   - Dans le cas d'une désaffectation d'un site connecté, cette valeur représente la quantité de données d'objet à déplacer vers d'autres sites ou à supprimer via ILM avant de désaffecter ce site en toute sécurité.
   - Dans le cas d'une désaffectation de site déconnectée, cette valeur représente la proportion de stockage de données de votre système qui deviendra inaccessible lorsque vous désaffectez ce site.

   > ⓘ Si votre politique ILM a été conçue pour vous protéger contre la perte d'un seul site, des copies de vos données d'objet doivent toujours exister sur les sites restants.

4. Consultez les raisons de la colonne **Decommission possible** pour déterminer quels sites peuvent être désaffectés actuellement.

   > ⓘ S'il y a plusieurs raisons pour lesquelles un site ne peut pas être désaffecté, la raison la plus critique est indiquée.

Motif de mise hors service possible	Description	Étape suivante
Coche verte (✔)	Vous pouvez désaffecter ce site.	Accédez à l'étape suivante.
Non Ce site contient le nœud d'administration principal.	Vous ne pouvez pas désaffecter un site contenant le nœud d'administration principal.	Aucune. Vous ne pouvez pas effectuer cette procédure.
Non Ce site contient un ou plusieurs nœuds d'archivage.	Vous ne pouvez pas désaffecter un site contenant un nœud d'archivage.	Aucune. Vous ne pouvez pas effectuer cette procédure.
Non Tous les nœuds de ce site sont déconnectés. Contactez votre ingénieur commercial NetApp.	Vous ne pouvez pas désaffecter un site connecté sauf si chaque nœud du site est connecté (✔).	Si vous souhaitez effectuer une mise hors service hors site déconnectée, vous devez contacter votre ingénieur commercial NetApp, qui examinera vos besoins et active le reste de l'assistant de mise hors service. **IMPORTANT**: Ne mettez jamais les noeuds en ligne hors ligne pour que vous puissiez supprimer un site. Vous allez perdre des données.

L'exemple montre un système StorageGRID avec trois sites. La coche verte (✔) Pour les sites Raleigh et

Sunnyvale indique que vous pouvez désaffecter ces sites. Cependant, vous ne pouvez pas désaffecter le site de Vancouver car il contient le nœud d'administration principal.

1. Si une mise hors service est possible, sélectionnez le bouton radio du site.

   Le bouton **Suivant** est activé.

2. Sélectionnez **Suivant**.

   L'étape 2 (Détails de la vue) s'affiche.

Étape 2 : Détails de la vue

À partir de l'étape 2 (Afficher les détails) de l'assistant Decommission site, vous pouvez vérifier quels nœuds sont inclus sur le site, voir combien d'espace a été utilisé sur chaque noeud de stockage et évaluer la quantité d'espace disponible sur les autres sites de votre grille.

Avant de commencer

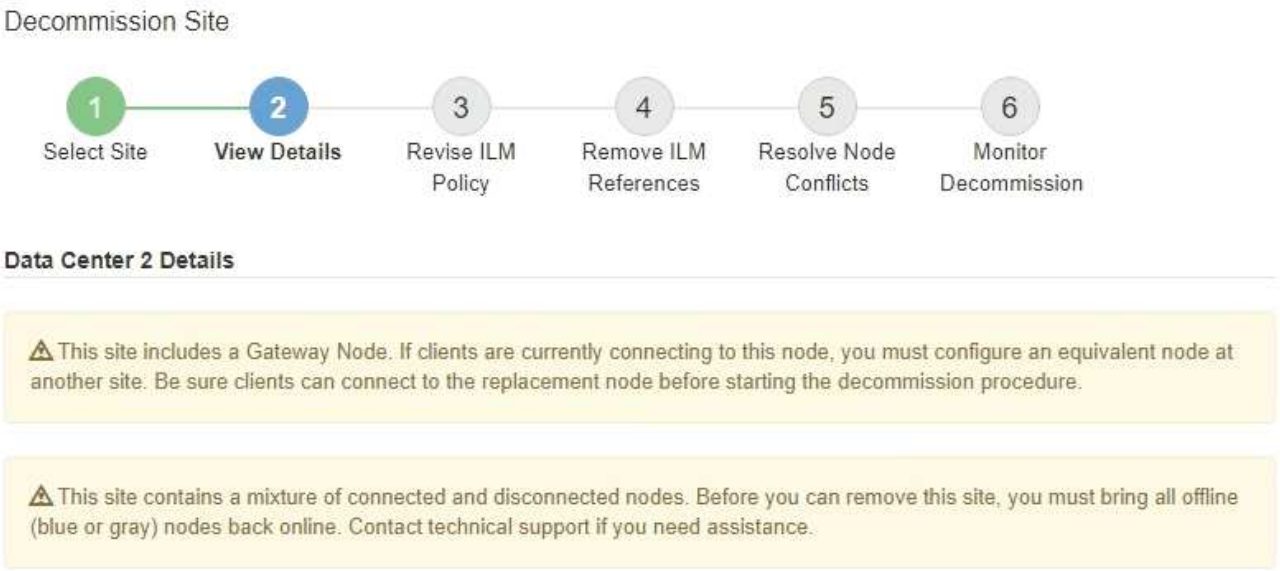
Avant de désaffecter un site, vous devez vérifier la quantité de données d'objet présentes sur le site.

- Si vous effectuez une mise hors service d'un site connecté, vous devez connaître la quantité de données d'objet présentes sur le site avant de mettre à jour le ILM. En fonction des capacités de votre site et de vos besoins en termes de protection des données, vous pouvez créer de nouvelles règles ILM pour déplacer des données vers d'autres sites ou supprimer les données d'objet du site.
- Exécutez les extensions du nœud de stockage requises avant de démarrer la procédure de mise hors service si possible.
- Si vous effectuez une mise hors service de site déconnecté, vous devez comprendre combien de données d'objet deviennent définitivement inaccessibles lorsque vous supprimez le site.

> Si vous désaffectez un site, la règle ILM ne permet pas de déplacer ou de supprimer des données d'objet. Toutes les données conservées sur le site seront perdues. Toutefois, si votre politique ILM a été conçue pour protéger contre la perte d'un seul site, des copies de vos données d'objet existent toujours sur les sites restants. Voir "Activer la protection contre la perte de site".

Étapes

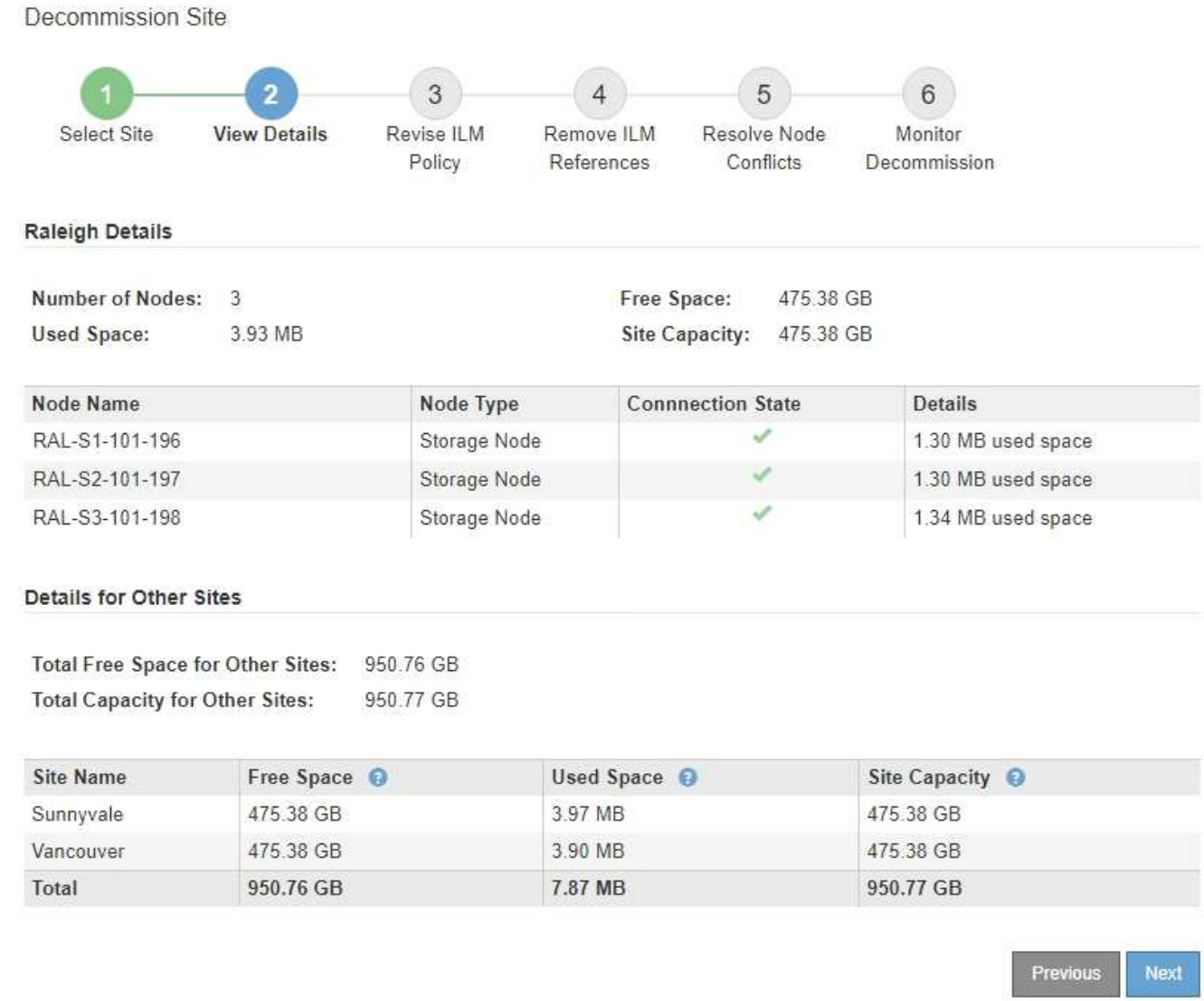
1. À partir de l'étape 2 (Afficher les détails), passez en revue tous les avertissements relatifs au site que vous avez sélectionné pour le supprimer.



Un avertissement apparaît dans ces cas :

- Le site inclut un nœud de passerelle. Si les clients S3 et Swift se connectent actuellement à ce nœud, vous devez configurer un nœud équivalent sur un autre site. Assurez-vous que les clients peuvent se connecter au nœud de remplacement avant de poursuivre la procédure de mise hors service.
- Le site contient un mélange de connecté ( ) et noeuds déconnectés (ou). Avant de pouvoir supprimer ce site, vous devez remettre tous les nœuds hors ligne en ligne.

2. Examinez les détails du site que vous avez sélectionné pour le supprimer.



Les informations suivantes sont incluses pour le site sélectionné :

- Nombre de nœuds
- Espace utilisé total, espace libre et capacité de tous les nœuds de stockage du site.
  - Pour une mise hors service de site connecté, la valeur **espace utilisé** représente la quantité de données d'objet à déplacer vers d'autres sites ou à supprimer avec ILM.
  - Pour une mise hors service du site déconnecté, la valeur **espace utilisé** indique la quantité de données d'objet qui deviennent inaccessibles lorsque vous supprimez le site.
- Noms, types et États de connexion des nœuds :
  - (Connecté)
  - (Arrêt administratif)
  - (Inconnu)
- Détails sur chaque nœud :
  - Pour chaque nœud de stockage, quantité d'espace utilisée pour les données d'objet.

- Pour les nœuds d'administration et les nœuds de passerelle, que le nœud soit actuellement utilisé dans un groupe haute disponibilité (HA). Vous ne pouvez pas désaffecter un nœud d'administration ou un nœud de passerelle utilisé dans un groupe haute disponibilité. Avant de commencer la désaffectation, éditez les groupes haute disponibilité pour supprimer tous les nœuds du site ou supprimez le groupe haute disponibilité si seuls les nœuds sont inclus dans ce site. Pour obtenir des instructions, reportez-vous à la section "Gestion des groupes haute disponibilité".

3. Dans la section Détails des autres sites de la page, évaluez la quantité d'espace disponible sur les autres sites de votre grille.

Details for Other Sites

Total Free Space for Other Sites:	950.76 GB
Total Capacity for Other Sites:	950.77 GB

Site Name	Free Space	Used Space	Site Capacity
Sunnyvale	475.38 GB	3.97 MB	475.38 GB
Vancouver	475.38 GB	3.90 MB	475.38 GB
Total	950.76 GB	7.87 MB	950.77 GB

Si vous désaffectez un site connecté et que vous prévoyez d'utiliser ILM pour déplacer les données d'objet depuis le site sélectionné (au lieu de simplement les supprimer), vous devez vous assurer que les autres sites disposent de la capacité suffisante pour prendre en charge les données déplacées et que la capacité adéquate reste adaptée à la croissance future.

Un avertissement s'affiche si l'espace **utilisé** pour le site que vous souhaitez supprimer est supérieur à **l'espace libre total pour les autres sites**. Pour garantir que la capacité de stockage adéquate est disponible après le retrait du site, vous devrez peut-être procéder à une extension avant d'effectuer cette procédure.

4. Sélectionnez **Suivant**.

L'étape 3 (réviser la politique ILM) s'affiche.

Étape 3 : réviser la politique ILM

À partir de l'étape 3 (réviser la politique ILM) de l'assistant site de désaffection, vous pouvez déterminer si le site est référencé par la politique ILM active.

Avant de commencer

Vous connaissez bien le fonctionnement d'ILM et vous connaissez déjà la création de pools de stockage, de profils de code d'effacement, de règles ILM et la simulation et l'activation d'une stratégie ILM. Voir "Gestion des objets avec ILM".

Description de la tâche

StorageGRID ne peut pas désaffecter un site si ce site est référencé par une règle ILM de la règle ILM active.

Si votre politique ILM actuelle renvoie au site que vous souhaitez supprimer, vous devez activer une nouvelle règle ILM qui répond à certaines exigences. Plus précisément, la nouvelle règle ILM :

- Impossible d'utiliser un pool de stockage faisant référence au site ou utilisant l'option tous les sites.

- Impossible d'utiliser un profil de code d'effacement faisant référence au site.
- Impossible d'utiliser la règle Make 2 copies à partir d'installations StorageGRID 11.6 ou antérieures.
- Doit être conçue pour protéger entièrement toutes les données d'objet.

> Ne créez jamais de règle ILM à copie unique pour la suppression d'un site. La règle ILM de création d'une seule copie répliquée pendant toute période met les données à risque de perte permanente. Si une seule copie répliquée d'un objet existe, cet objet est perdu en cas de défaillance ou d'erreur importante d'un noeud de stockage. De plus, lors des procédures de maintenance telles que les mises à niveau, l'accès à l'objet est temporairement perdu.

Si vous effectuez une *mise hors service du site connecté*, vous devez réfléchir à la manière dont StorageGRID doit gérer les données d'objet actuellement sur le site que vous souhaitez supprimer. Selon les exigences en matière de protection des données, les nouvelles règles peuvent déplacer les données d'objet vers d'autres sites ou supprimer les copies d'objets supplémentaires qui ne sont plus utiles.

Contactez l'assistance technique si vous avez besoin d'aide pour concevoir la nouvelle politique.

Étapes

1. À partir de l'étape 3 (réviser la politique ILM), déterminez si des règles ILM de la politique ILM active font référence au site que vous avez sélectionné pour supprimer.
2. Si aucune règle n'est répertoriée, sélectionnez **Suivant** pour accéder à "Étape 4 : supprimer les références ILM".
3. Si une ou plusieurs règles ILM sont répertoriées dans le tableau, sélectionnez le lien en regard de **Active Policy Name**.

   La page des règles ILM s'affiche dans un nouvel onglet de navigateur. Cet onglet permet de mettre à jour la gestion du cycle de vie des informations La page site de désaffection reste ouverte dans l'onglet autre.

   a. Si nécessaire, sélectionnez **ILM** > **Storage pools** pour créer un ou plusieurs pools de stockage qui ne font pas référence au site.

      > Pour plus de détails, reportez-vous aux instructions relatives à la gestion des objets avec la gestion du cycle de vie des informations.

   b. Si vous prévoyez d'utiliser le code d'effacement, sélectionnez **ILM** > **code d'effacement** pour créer un ou plusieurs profils de code d'effacement.

      Vous devez sélectionner des pools de stockage qui ne font pas référence au site.

      > N'utilisez pas le pool de stockage **tous les nœuds de stockage** (StorageGRID 11.6 et versions antérieures) dans les profils de code d'effacement.

4. Sélectionnez **ILM** > **Rules** et clonez chacune des règles répertoriées dans le tableau pour l'étape 3 (réviser la politique ILM).

   > Pour plus de détails, reportez-vous aux instructions relatives à la gestion des objets avec la gestion du cycle de vie des informations.

   a. Utilisez des noms qui facilitent la sélection de ces règles dans une nouvelle stratégie.

b. Mettez à jour les instructions de positionnement.

   Supprimez les pools de stockage ou les profils de code d'effacement qui font référence au site et remplacez-les par de nouveaux pools de stockage ou de nouveaux profils de code d'effacement.

   N'utilisez pas le pool de stockage **tous les nœuds de stockage** dans les nouvelles règles.

5. Sélectionnez **ILM** > **Policies** et créez une nouvelle stratégie qui utilise les nouvelles règles.

   Pour plus de détails, reportez-vous aux instructions relatives à la gestion des objets avec la gestion du cycle de vie des informations.

   a. Sélectionnez la stratégie active et sélectionnez **Clone**.

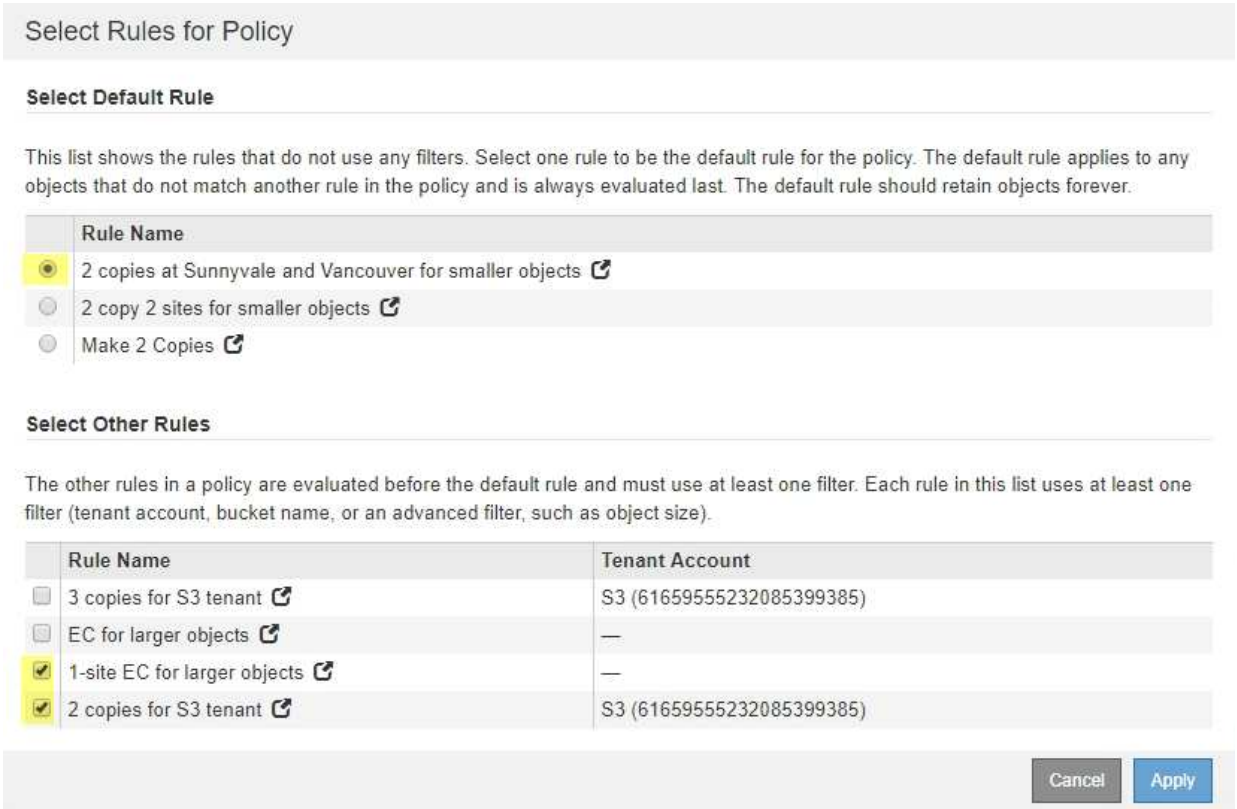
   b. Spécifiez un nom de stratégie et un motif de modification.

   c. Sélectionnez des règles pour la stratégie clonée.

      - Effacez toutes les règles répertoriées pour l'étape 3 (réviser la politique ILM) de la page site de désaffectation.
      - Sélectionnez une règle par défaut qui ne fait pas référence au site.

        Ne sélectionnez pas la règle **make 2 copies** car cette règle utilise le pool de stockage **All Storage Nodes**, qui n'est pas autorisé.

      - Sélectionnez les autres règles de remplacement que vous avez créées. Ces règles ne doivent pas faire référence au site.



   d. Sélectionnez **appliquer**.

e. Faites glisser les lignes pour réorganiser les règles de la stratégie.

   Vous ne pouvez pas déplacer la règle par défaut.

   Vous devez confirmer que les règles ILM sont dans l'ordre correct. Lorsque la stratégie est activée, les objets nouveaux et existants sont évalués par les règles dans l'ordre indiqué, à partir du haut.

a. Enregistrez la stratégie proposée.

6. Les objets de test d'ingestion et simulent la règle proposée pour s'assurer que les règles appropriées sont appliquées.

   Les erreurs de la règle ILM peuvent entraîner des pertes de données irrécupérables. Examinez attentivement et simulez la stratégie avant de l'activer pour confirmer qu'elle fonctionnera comme prévu.

   Lorsque vous activez une nouvelle règle ILM, StorageGRID l'utilise pour gérer tous les objets, y compris les objets existants et les objets récemment ingérées. Avant d'activer une nouvelle règle ILM, vérifiez toutes les modifications du placement des objets répliqués et soumis au code d'effacement. La modification de l'emplacement d'un objet existant peut entraîner des problèmes de ressources temporaires lorsque les nouveaux placements sont évalués et implémentés.

7. Activer la nouvelle règle.

   Si vous effectuez une mise hors service du site connecté, StorageGRID commence à supprimer les données d'objet du site sélectionné dès que vous activez la nouvelle règle ILM. Le déplacement ou la suppression de toutes les copies d'objet peut prendre plusieurs semaines. Vous pouvez démarrer en toute sécurité une mise hors service d'un site alors que les données d'objet existent toujours sur le site. Toutefois, la procédure de mise hors service est plus rapide et avec moins de perturbations et d'impacts sur les performances si vous permet de déplacer les données depuis le site avant de démarrer la procédure de mise hors service (En sélectionnant **Start Decommission** à l'étape 5 de l'assistant).

8. Revenir à **étape 3 (réviser la politique ILM)** pour s'assurer qu'aucune règle ILM de la nouvelle politique active ne fait référence au site et que le bouton **Suivant** est activé.

   Si des règles sont répertoriées, vous devez créer et activer une nouvelle règle ILM avant de continuer.

9. Si aucune règle n’est répertoriée, sélectionnez **Suivant**.

   L’étape 4 (Supprimer les références ILM) s’affiche.

Étape 4 : supprimer les références ILM

À partir de l’étape 4 (Supprimer les références ILM) de l’assistant site de désaffection, vous pouvez supprimer la stratégie proposée s’il en existe une et supprimer ou modifier toute règle ILM inutilisée qui fait toujours référence au site.

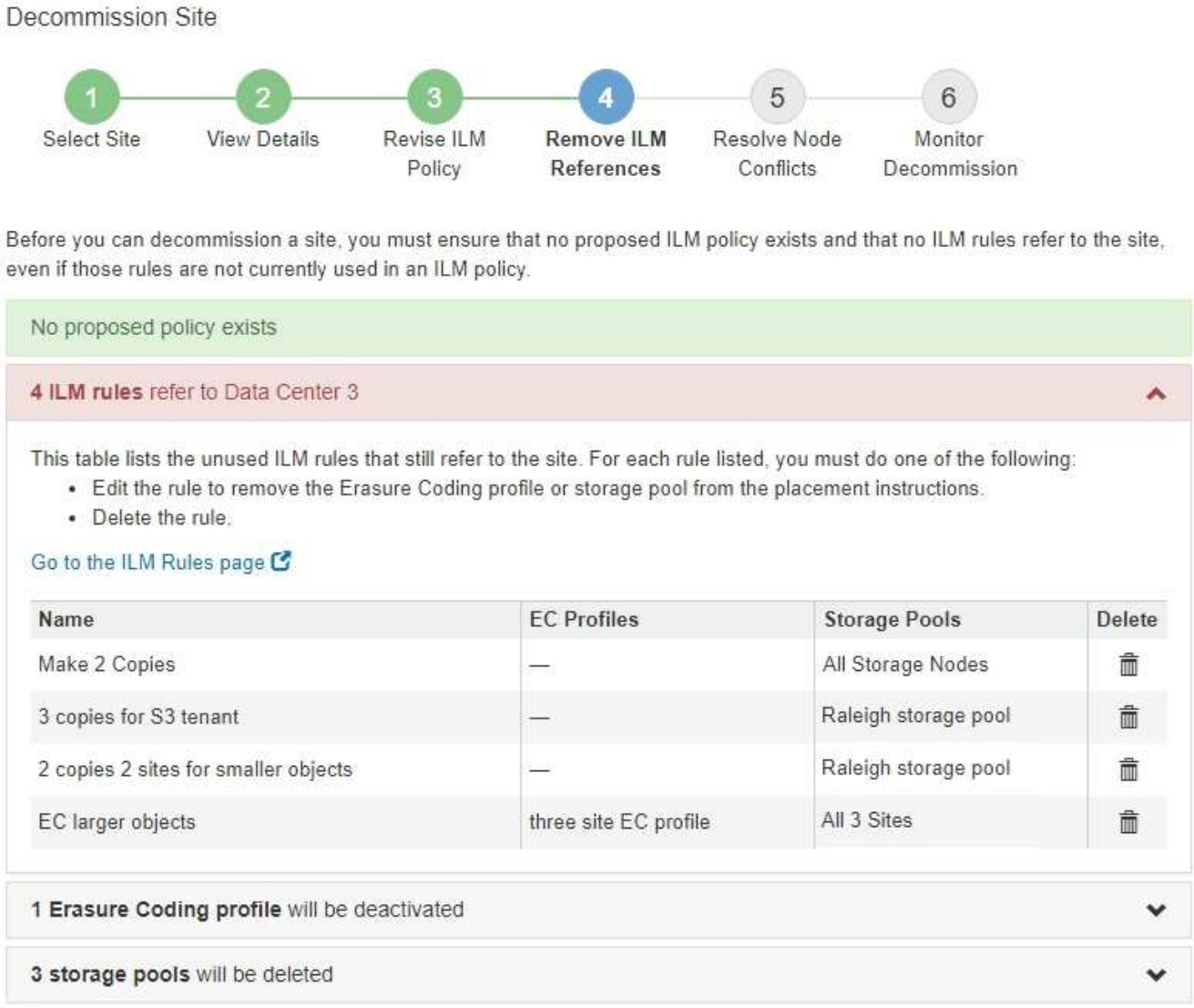
Description de la tâche

Dans ces cas, vous ne pouvez pas démarrer la procédure de mise hors service du site :

- Une politique ILM proposée existe. Si vous avez une stratégie proposée, vous devez la supprimer.
- Une règle ILM fait référence au site, même si cette règle n’est utilisée dans aucune politique ILM. Vous devez supprimer ou modifier toutes les règles qui font référence au site.

Étapes

1. Si une stratégie proposée est répertoriée, supprimez-la.
   a. Sélectionnez **Supprimer la stratégie proposée**.
   b. Sélectionnez **OK** dans la boîte de dialogue de confirmation.
2. Déterminez si des règles ILM inutilisées font référence au site.



Toutes les règles ILM répertoriées font toujours référence au site, mais ne sont utilisées dans aucune règle. Dans l'exemple :

- La règle **make 2 copies** utilise le pool de stockage **All Storage Nodes** (StorageGRID 11.6 et versions antérieures), qui utilise le site **All sites**.
- La règle **3 copies non utilisées pour le locataire S3** fait référence au pool de stockage **Raleigh**.
- La règle **2 copie 2 non utilisée pour les objets plus petits** fait référence au pool de stockage **Raleigh**.
- Les règles **EC grosses objets** inutilisées utilisent le site Raleigh dans le profil de code d'effacement **All 3 sites**.
- Si aucune règle ILM n'est répertoriée, sélectionnez **Suivant** pour accéder à "Étape 5 : résoudre les conflits de nœuds (et démarrer la mise hors service)".

> Lorsque StorageGRID décompresse le site, il désactive automatiquement tous les profils de code d'effacement inutilisés qui font référence au site et supprime automatiquement les pools de stockage inutilisés qui font référence au site. Le pool de stockage tous les nœuds de stockage (StorageGRID 11.6 et versions antérieures) est supprimé car il utilise le site tous les sites.

- Si une ou plusieurs règles ILM sont répertoriées, passez à l'étape suivante.

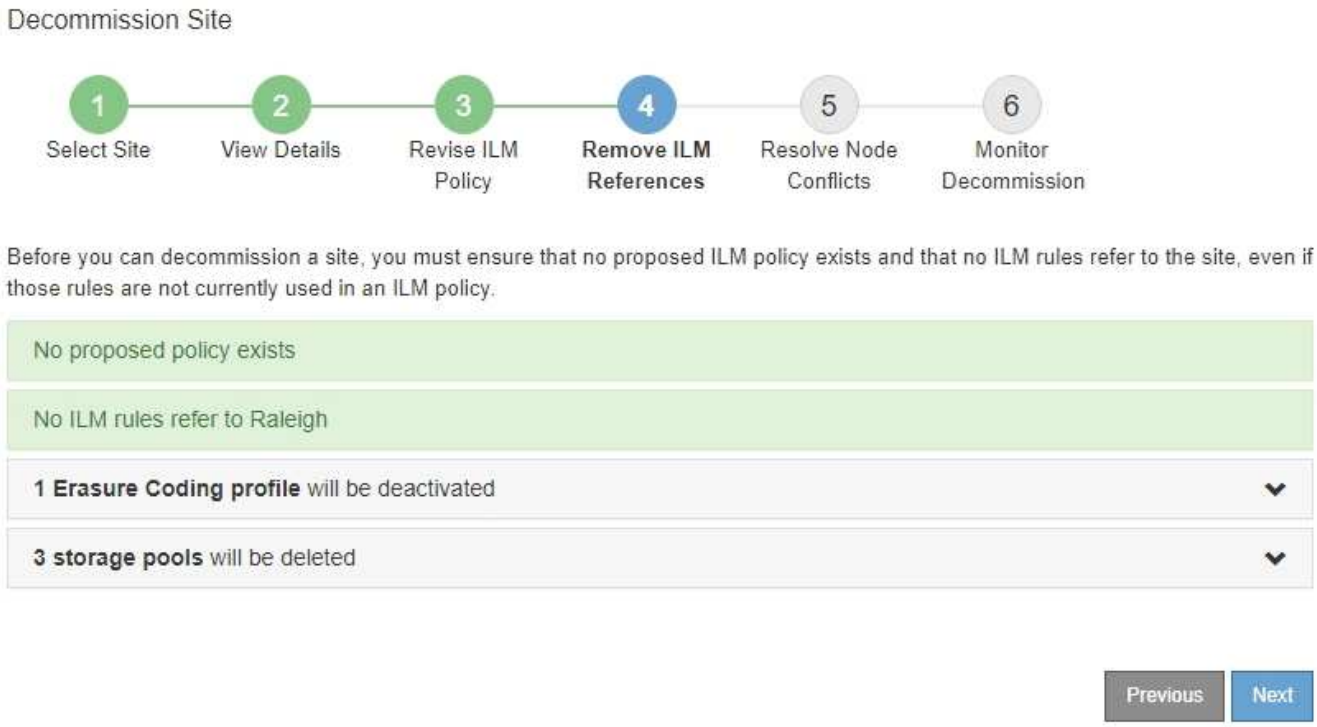
3. Modifier ou supprimer chaque règle inutilisée :
   - Pour modifier une règle, accédez à la page de règles ILM et mettez à jour tous les placements qui utilisent un profil de code d'effacement ou un pool de stockage faisant référence au site. Ensuite, revenez à **étape 4 (Supprimer les références ILM)**.

     Pour plus de détails, reportez-vous aux instructions relatives à la gestion des objets avec la gestion du cycle de vie des informations.

   - Pour supprimer une règle, sélectionnez l'icône de corbeille Et sélectionnez **OK**.

     Vous devez supprimer la règle **make 2 copies** avant de pouvoir désaffecter un site.

4. Vérifiez qu'aucune politique ILM proposée n'existe, qu'aucune règle ILM non utilisée ne fait référence au site et que le bouton **Suivant** est activé.



5. Sélectionnez **Suivant**.

   Les pools de stockage et les profils de code d'effacement qui font référence au site ne seront plus valides après la suppression du site. Lorsque StorageGRID décompresse le site, il désactive automatiquement tous les profils de code d'effacement inutilisés qui font référence au site et supprime automatiquement les pools de stockage inutilisés qui font référence au site. Le pool de stockage tous les nœuds de stockage (StorageGRID 11.6 et versions antérieures) est supprimé car il utilise le site tous les sites.

   L'étape 5 (résoudre les conflits de nœuds) s'affiche.

Étape 5 : résoudre les conflits de nœuds (et démarrer la mise hors service)

À partir de l'étape 5 (résoudre les conflits de nœuds) de l'assistant site de mise hors service, vous pouvez déterminer si des nœuds de votre système StorageGRID sont déconnectés ou si des nœuds du site sélectionné appartiennent à un groupe haute disponibilité (HA). Après la résolution d'un conflit de nœud, vous démarrez la procédure de mise hors service à partir de cette page.

Avant de commencer

Vous devez vous assurer que tous les nœuds de votre système StorageGRID sont dans l'état approprié, comme suit :

- Tous les nœuds de votre système StorageGRID doivent être connectés ( ).

> Si vous effectuez une mise hors service du site déconnecté, tous les nœuds du site que vous supprimez doivent être déconnectés et tous les nœuds de tous les autres sites doivent être connectés.

> La mise hors service ne démarre pas si un ou plusieurs volumes sont hors ligne (démontés) ou s'ils sont en ligne (montés) mais en état d'erreur.

> Si un ou plusieurs volumes sont déconnectés alors qu'une mise hors service est en cours, le processus de mise hors service se termine une fois ces volumes remis en ligne.

- Aucun nœud sur le site que vous supprimez peut avoir une interface appartenant à un groupe haute disponibilité.

Description de la tâche

Si un nœud est répertorié pour l'étape 5 (résoudre les conflits de nœud), vous devez corriger le problème avant de pouvoir démarrer la mise hors service.

Avant de commencer la procédure de mise hors service du site à partir de cette page, prenez en compte les considérations suivantes :

- Vous devez prévoir suffisamment de temps pour que la procédure de mise hors service soit terminée.

> Le déplacement ou la suppression de données d'objet depuis un site peut prendre plusieurs jours, semaines, voire mois, en fonction de la quantité de données sur le site, de la charge sur votre système, des latences réseau et de la nature des modifications ILM requises.

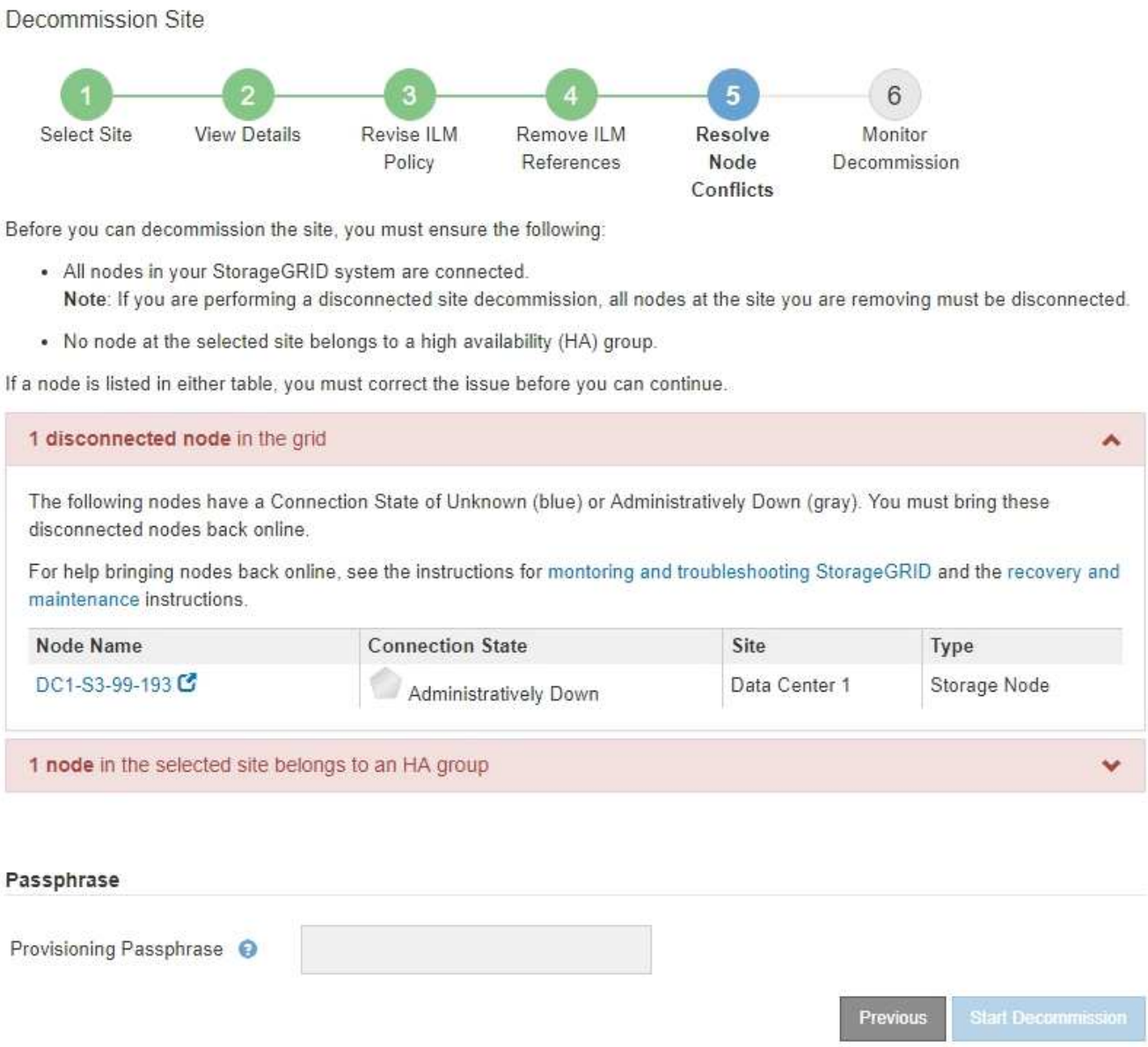
- Pendant que la procédure de mise hors service du site est en cours d'exécution :
  - Vous ne pouvez pas créer de règles ILM faisant référence au site en cours de désaffectation. Vous ne pouvez pas non plus modifier une règle ILM existante pour faire référence au site.
  - Vous ne pouvez pas effectuer d'autres procédures de maintenance, telles que l'extension ou la mise à niveau.

Si vous devez effectuer une autre procédure de maintenance lors de la mise hors service d'un site connecté, vous pouvez interrompre la procédure pendant que les nœuds de stockage sont supprimés. Le bouton **Pause** est activé au cours de l'étape "données répliquées et codées d'effacement".

- Si vous devez récupérer un nœud après avoir lancé la procédure de mise hors service du site, vous devez contacter le service de support.

Étapes

1. Passez en revue la section noeuds déconnectés de l'étape 5 (résoudre les conflits de nœuds) pour déterminer si les nœuds de votre système StorageGRID ont un état de connexion inconnu ( ) Ou administratif ( ).

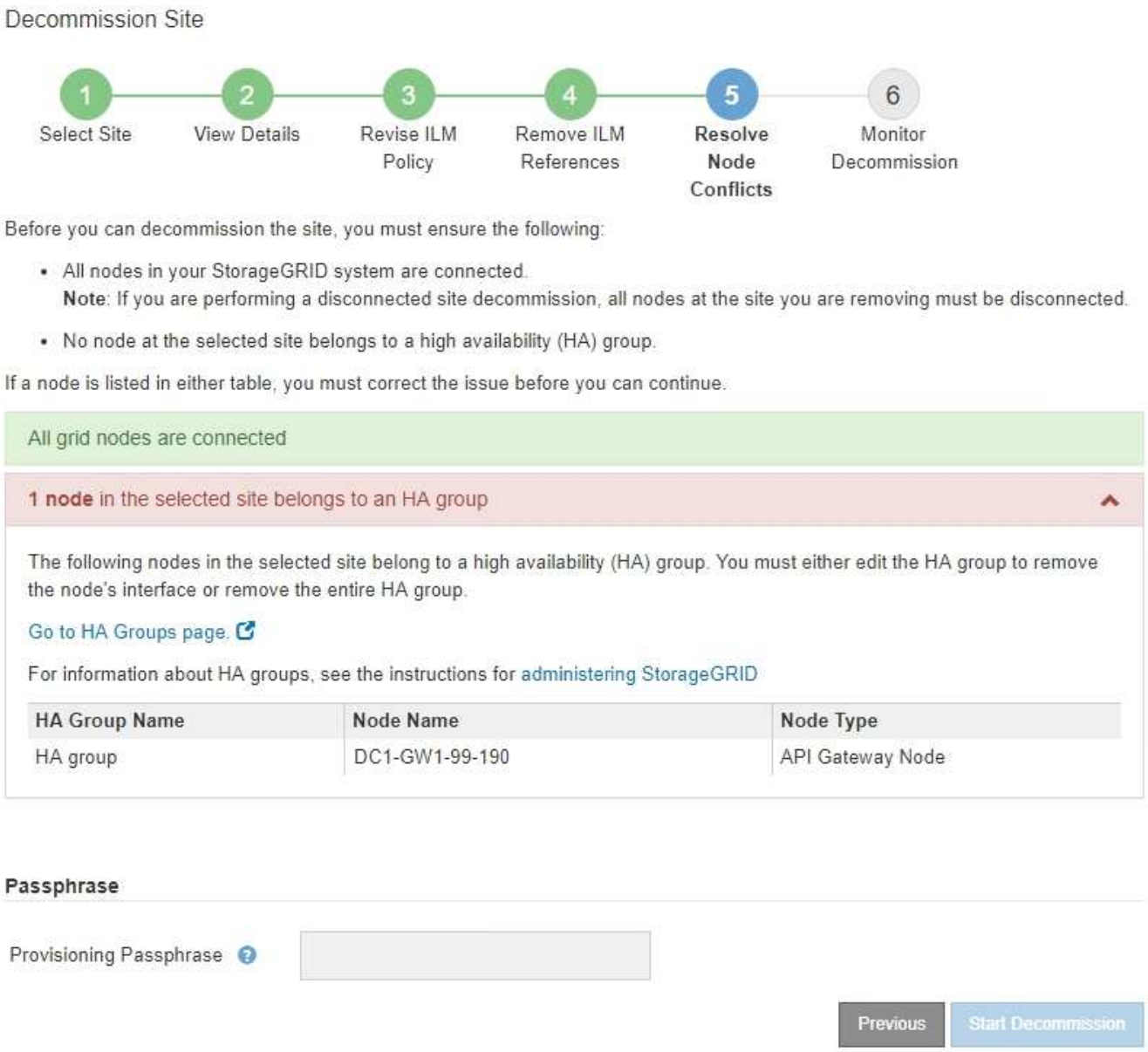


2. Si un nœud est déconnecté, remettre en ligne.

   Voir la "Procédures des nœuds de la grille". Contactez le support technique si vous avez besoin d'aide.

3. Lorsque tous les nœuds déconnectés ont été remis en ligne, passez en revue la section HA Groups de l'étape 5 (résoudre les conflits de nœuds).

   Ce tableau répertorie tous les nœuds du site sélectionné qui appartiennent à un groupe haute disponibilité (HA).



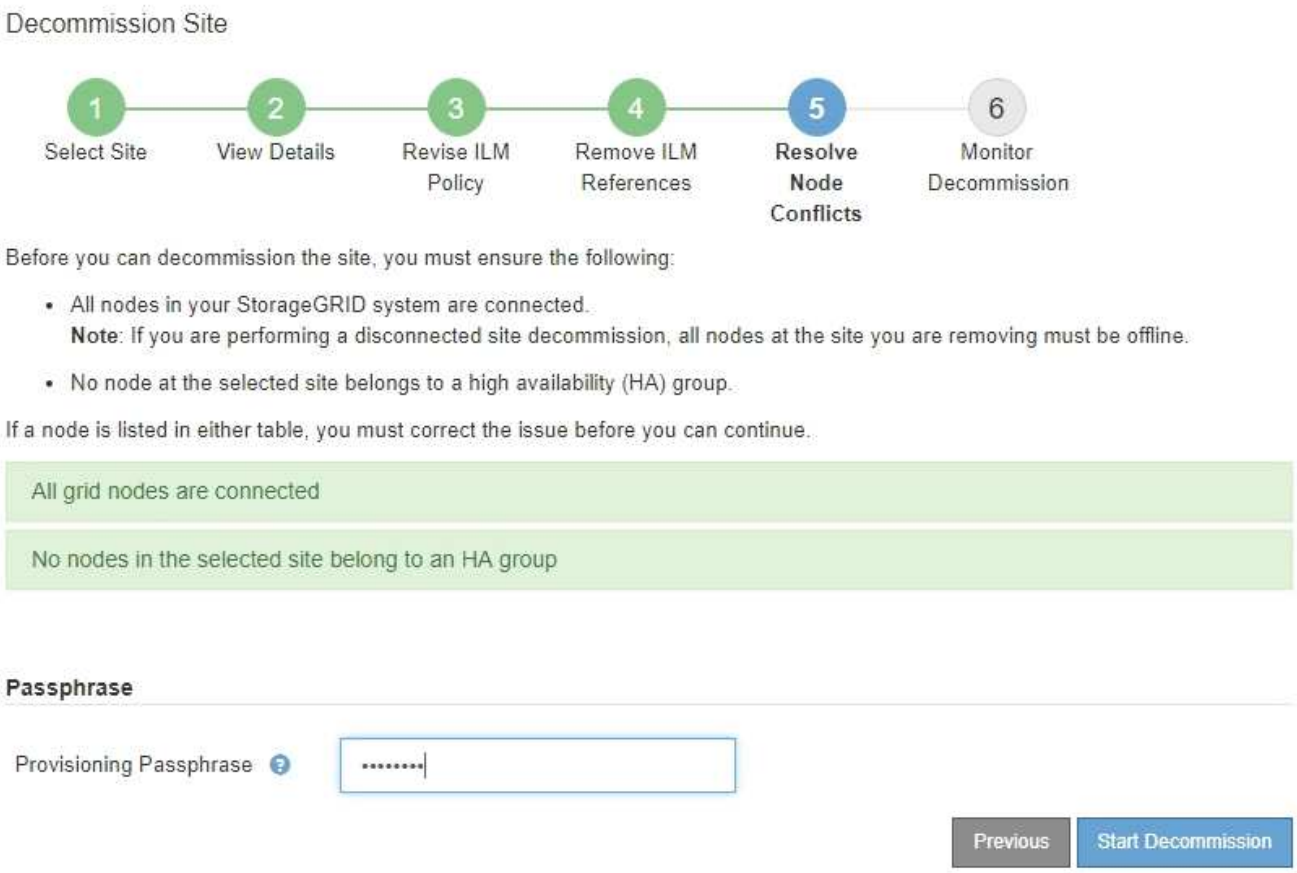
4. Si des nœuds sont répertoriés, effectuez l'une des opérations suivantes :

   - Modifiez chaque groupe haute disponibilité affecté afin de supprimer l'interface de nœud.
   - Supprimez un groupe haute disponibilité qui inclut uniquement les nœuds de ce site. Voir les instructions d'administration de StorageGRID.

   Si tous les nœuds sont connectés et qu'aucun nœud du site sélectionné n'est utilisé dans un groupe HA, le champ **phrase de passe d'approvisionnement** est activé.

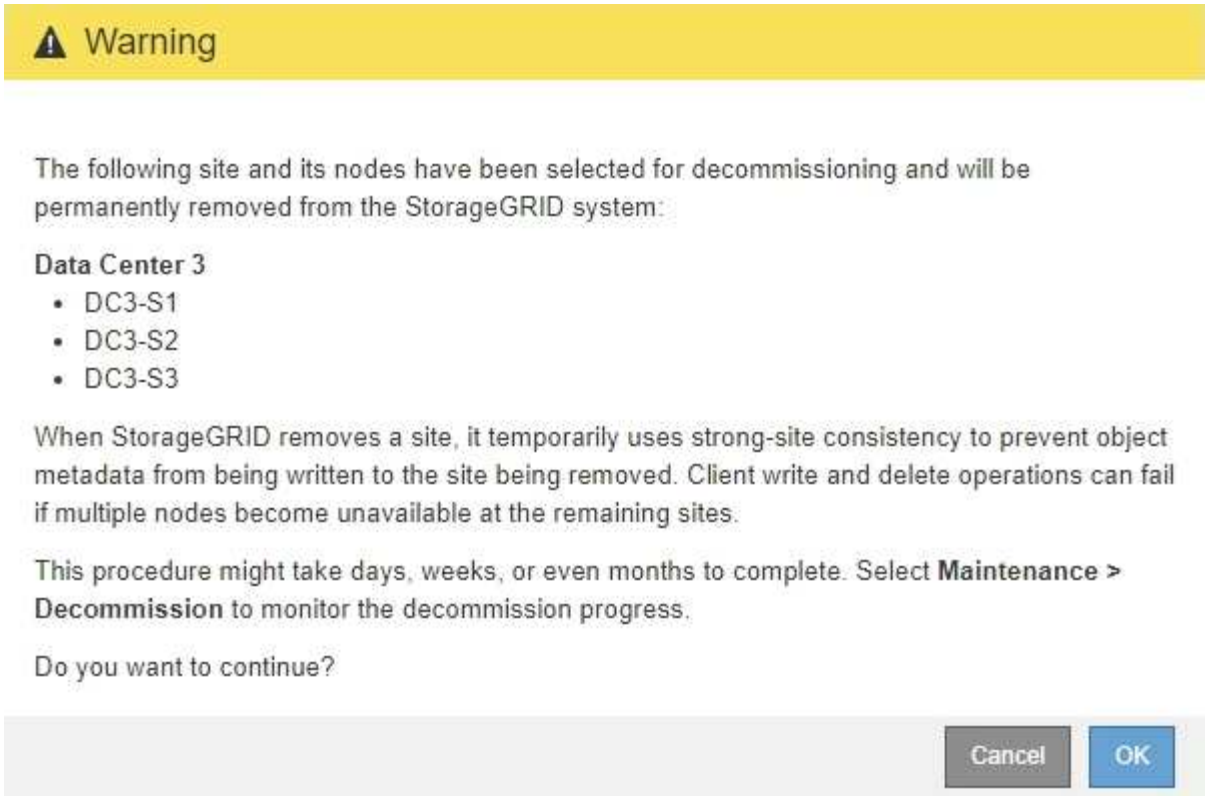
5. Saisissez la phrase secrète pour le provisionnement.

   Le bouton **Start Decommission** devient activé.



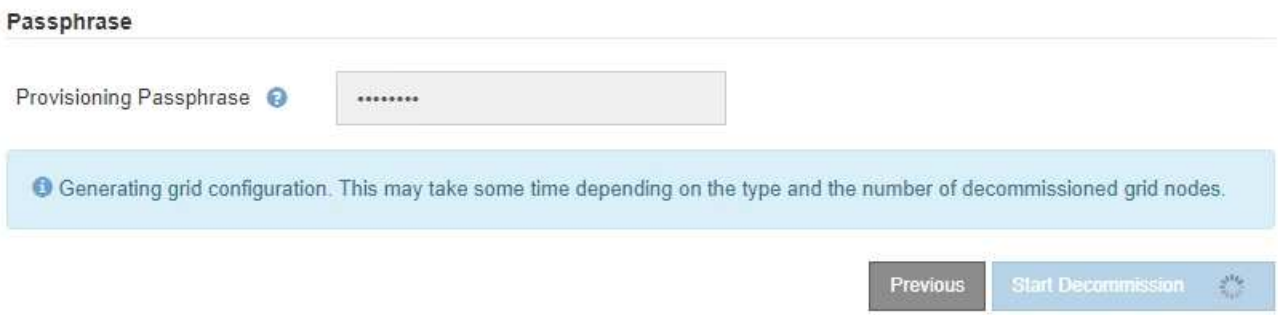
6. Si vous êtes prêt à démarrer la procédure de mise hors service du site, sélectionnez **Start Decommission**.

   Un avertissement répertorie le site et les nœuds qui seront supprimés. Nous vous rappelons qu'il peut prendre des jours, des semaines, voire des mois pour supprimer complètement le site.



7. Vérifiez l'avertissement. Si vous êtes prêt à commencer, sélectionnez **OK**.

   Un message apparaît au fur et à mesure que la nouvelle configuration de grille est générée. Ce processus peut prendre un certain temps, selon le type et le nombre de nœuds de la grille désaffectés.



   Lorsque la nouvelle configuration de grille a été générée, l'étape 6 (Monitor Decommission) s'affiche.

   > Le bouton **Previous** reste désactivé jusqu'à ce que la mise hors service soit terminée.

Étape 6 : surveiller la mise hors service

À partir de l'étape 6 (Monitor Decommission) de l'assistant de page site de désaffection, vous pouvez surveiller la progression du site à mesure que celui-ci est supprimé.

Description de la tâche

Lorsque StorageGRID supprime un site connecté, il supprime des nœuds dans l'ordre suivant :

1. Nœuds de passerelle

2. Nœuds d'administration
3. Nœuds de stockage

Lorsque StorageGRID supprime un site déconnecté, il supprime des nœuds dans l'ordre suivant :

1. Nœuds de passerelle
2. Nœuds de stockage
3. Nœuds d'administration

La suppression de chaque nœud de passerelle ou d'un nœud d'administration peut prendre quelques minutes ou une heure. En revanche, les nœuds de stockage peuvent prendre des jours ou des semaines.

Étapes

1. Dès qu'un nouveau progiciel de récupération a été généré, téléchargez le fichier.

> Téléchargez le progiciel de récupération dès que possible pour vous assurer que vous pouvez récupérer votre grille si un problème survient pendant la procédure de mise hors service.

   a. Sélectionnez le lien dans le message ou sélectionnez **MAINTENANCE** > **système** > **paquet de récupération**.

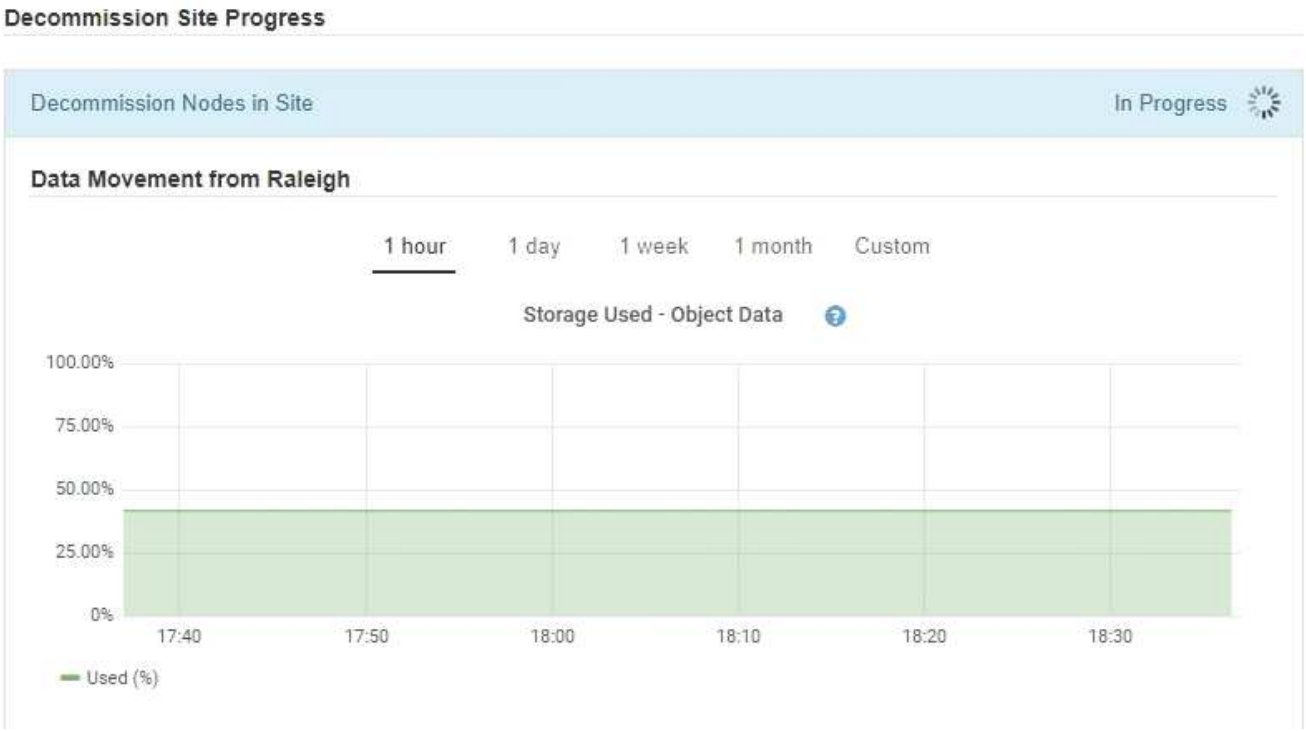
   b. Téléchargez le `.zip` fichier.

      Reportez-vous aux instructions pour "Téléchargement du progiciel de restauration".

> Le fichier du progiciel de récupération doit être sécurisé car il contient des clés de cryptage et des mots de passe qui peuvent être utilisés pour obtenir des données du système StorageGRID.

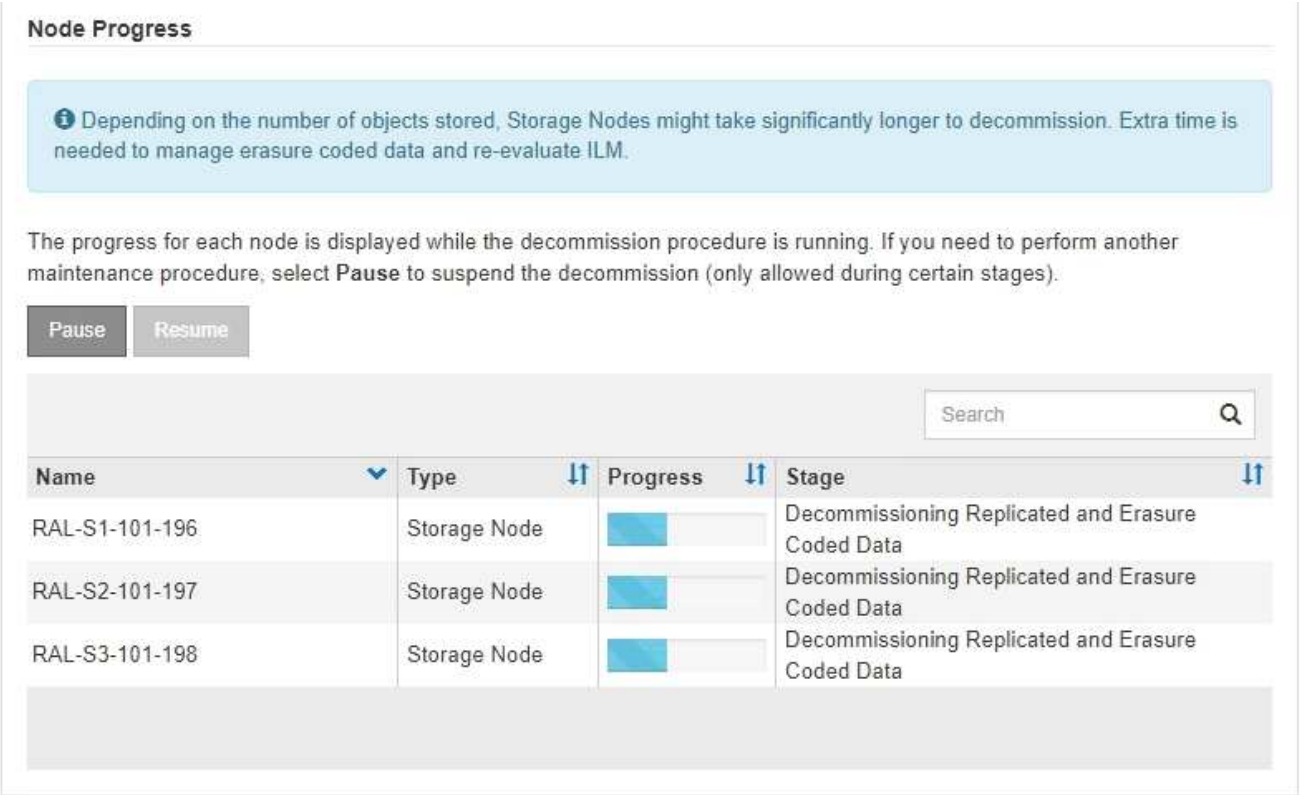
2. À l'aide du diagramme de déplacement des données, surveillez le déplacement des données d'objet de ce site vers d'autres sites.

   Le déplacement des données a commencé lorsque vous avez activé la nouvelle règle ILM à l'étape 3 (réviser la politique ILM). Un déplacement des données sera effectué tout au long de la procédure de mise hors service.



3. Dans la section progression du nœud de la page, surveillez la progression de la procédure de mise hors service lorsque les nœuds sont supprimés.

   Lorsqu'un nœud de stockage est supprimé, chaque nœud passe par une série d'étapes. Si la plupart de ces étapes se produisent rapidement, voire de façon imperceptible, vous devrez peut-être attendre des jours, voire des semaines, pour les autres étapes, et déterminer le volume de données à déplacer. Du temps supplémentaire est nécessaire pour gérer les données codées et réévaluer les règles ILM.



Si vous surveillez la progression de la désaffectation d'un site connecté, consultez ce tableau pour comprendre les étapes de mise hors service d'un nœud de stockage :

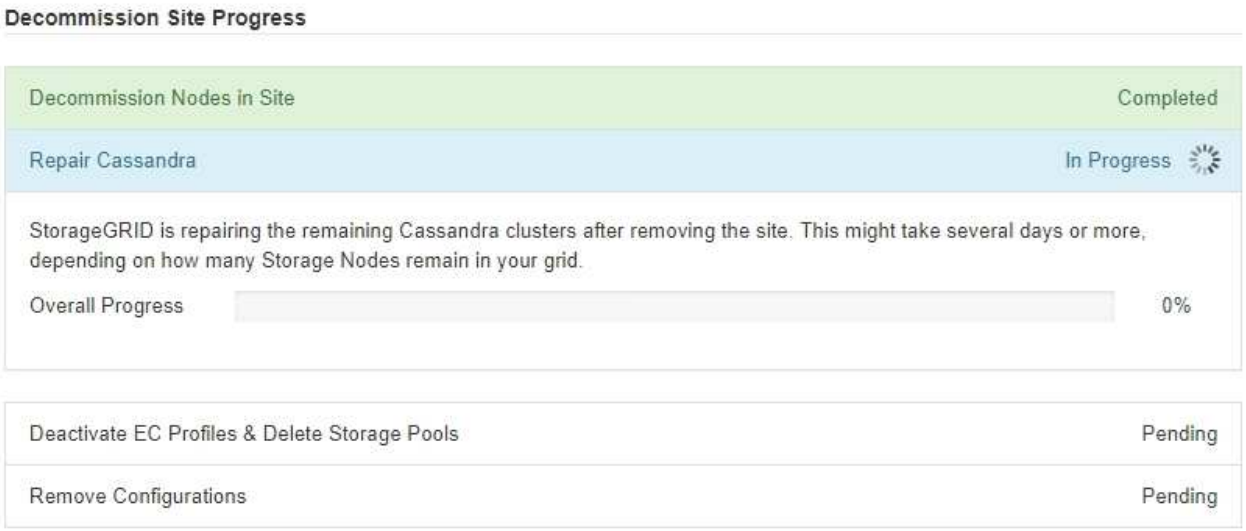
Étape	Durée estimée
En attente	Minute ou moins
Attendez les verrous	Quelques minutes
Préparer la tâche	Minute ou moins
Marquage LDR déclassé	Quelques minutes
Désaffectation des données répliquées et code d'effacement	Heures, jours ou semaines en fonction de la quantité de données **Remarque** : si vous devez effectuer d'autres activités de maintenance, vous pouvez mettre le site hors service pendant cette étape.
Etat défini LDR	Quelques minutes
Vider les files d'attente d'audit	Quelques minutes à plusieurs heures, selon le nombre de messages et la latence du réseau.
Terminé	Quelques minutes

Si vous surveillez la progression d'une mise hors service d'un site déconnecté, consultez ce tableau pour connaître les étapes de mise hors service d'un nœud de stockage :

Étape	Durée estimée
En attente	Minute ou moins
Attendez les verrous	Quelques minutes
Préparer la tâche	Minute ou moins
Désactiver les services externes	Quelques minutes
Révocation de certificat	Quelques minutes
Annulation de l'enregistrement du nœud	Quelques minutes
Annulation du registre de notes de stockage	Quelques minutes
Retrait du groupe de stockage	Quelques minutes

Étape	Durée estimée
Suppression d'entité	Quelques minutes
Terminé	Quelques minutes

4. Une fois que tous les nœuds ont atteint l'étape terminée, attendez la fin des opérations de désaffectation du site restantes.
   - Pendant l'étape **réparer Cassandra**, StorageGRID effectue les réparations nécessaires aux clusters Cassandra qui restent dans votre réseau. Ces réparations peuvent prendre plusieurs jours ou plus, selon le nombre de nœuds de stockage restants dans votre grid.

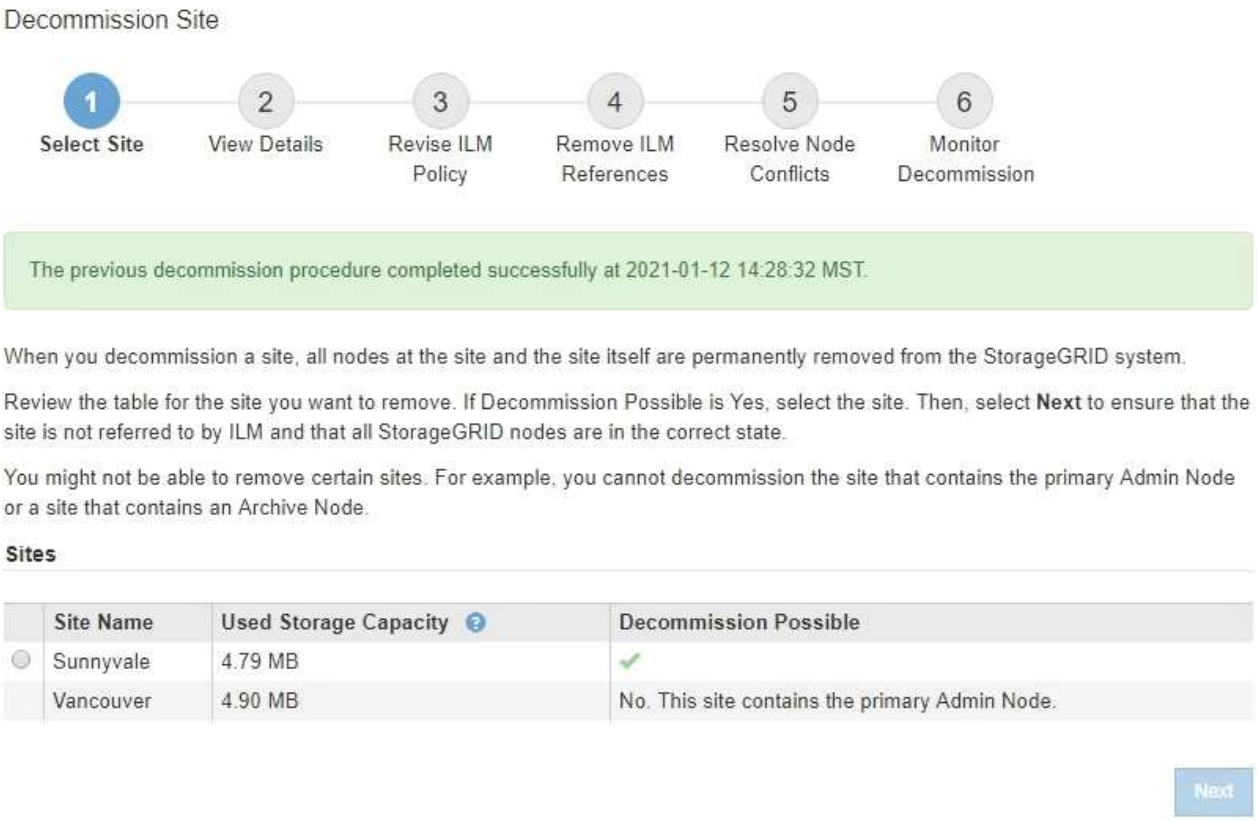


   - Au cours de l'étape **Désactiver les profils EC et Supprimer les pools de stockage**, les modifications ILM suivantes sont apportées :
     - Tous les profils de code d'effacement faisant référence au site sont désactivés.
     - Tous les pools de stockage auxquels le site fait référence sont supprimés.

> Le pool de stockage tous les nœuds (StorageGRID 11.6 et versions antérieures) est également supprimé car il utilise le site tous les sites.

   - Enfin, lors de l'étape **Remove Configuration**, toutes les références restantes au site et à ses nœuds sont supprimées du reste de la grille.

5. Une fois la procédure de mise hors service terminée, la page site de mise hors service affiche un message de réussite et le site supprimé n'est plus affiché.



Une fois que vous avez terminé

Effectuez les tâches suivantes une fois la procédure de mise hors service du site terminée :

- Assurez-vous que les disques de tous les nœuds de stockage du site mis hors service sont nettoyés. Utilisez un outil ou un service d'effacement de données disponible dans le commerce pour supprimer définitivement et de manière sécurisée les données des lecteurs.
- Si le site inclut un ou plusieurs nœuds d'administration et que l'authentification unique (SSO) est activée pour votre système StorageGRID, supprimez toutes les approbations de tiers de confiance pour le site de Active Directory Federation Services (AD FS).
- Une fois que les nœuds ont été mis hors tension automatiquement dans le cadre de la procédure de mise

hors service du site connecté, supprimez les machines virtuelles associées.

Renommez la grille, les sites et les nœuds

Renommer la grille, les sites et les nœuds : présentation

Si nécessaire, vous pouvez modifier les noms d'affichage affichés dans le Gestionnaire de grille pour l'ensemble de la grille, chaque site et chaque nœud. Vous pouvez mettre à jour les noms d'affichage en toute sécurité et à tout moment.

Qu'est-ce que la procédure de renommage ?

Lorsque vous installez StorageGRID au départ, vous spécifiez un nom pour la grille, chaque site et chaque nœud. Ces noms initiaux sont connus sous le nom de *System Names*, et ils sont les noms initialement affichés dans StorageGRID.

Les noms de système sont requis pour les opérations StorageGRID internes et ne peuvent pas être modifiés. Toutefois, vous pouvez utiliser la procédure rename pour définir de nouveaux *noms d'affichage* pour la grille, chaque site et chaque nœud. Ces noms d'affichage apparaissent dans divers emplacements StorageGRID au lieu (ou dans certains cas, en plus de) des noms de système sous-jacents.

Utilisez la procédure de renommage pour corriger les fautes de frappe, mettre en œuvre une convention de nommage différente ou indiquer qu'un site et tous ses nœuds ont été déplacés. Contrairement aux noms des systèmes, les noms d'affichage peuvent être mis à jour en fonction des besoins et sans incidence sur les opérations StorageGRID.

Où les noms du système et de l'affichage apparaissent-ils ?

Le tableau suivant récapitule les emplacements où les noms des systèmes et les noms d'affichage sont affichés dans l'interface utilisateur de StorageGRID et dans les fichiers StorageGRID.

Emplacement	Nom du système	Nom d'affichage
Pages Grid Manager	Affiché sauf si l'élément est renommé	Si un élément est renommé, affiché à la place du nom du système dans les emplacements suivants : • Tableau de bord • Page nœuds • Pages de configuration pour les groupes haute disponibilité, les terminaux d'équilibrage de charge, les interfaces VLAN, les serveurs de gestion des clés, les mots de passe grid, et le contrôle du pare-feu • Alertes • Définitions de pool de stockage • Page de recherche de métadonnées d'objet • Pages relatives aux procédures de maintenance, y compris la mise à niveau, le correctif, la mise à niveau du système d'exploitation SANtricity, la mise hors service, expansion, récupération et vérification de l'existence de l'objet • Pages de support (journaux et diagnostics) • Page d'ouverture de session unique, en regard du nom d'hôte du nœud d'administration dans le tableau pour les détails du nœud d'administration
NOEUDS > **vue d'ensemble** pour un noeud	Toujours affiché	S'affiche uniquement si l'élément est renommé
Pages héritées dans le gestionnaire de grille (par exemple, **SUPPORT** > **topologie de grille**)	Illustré	Non illustré
API Node-Health	Toujours renvoyé	Renvoyé uniquement si l'élément est renommé

Emplacement	Nom du système	Nom d'affichage

Lors de l'utilisation de SSH pour accéder à un nœud	Affiché comme nom principal, sauf si l'élément a été renommé :
	
	`admin@SYSTEM-NAME: ~ $`
	
	Inclus entre parenthèses lorsque l'élément est renommé :
	
	`admin@DISPLAY-NAME(SYSTEM-NAME):~ $`
		Affiché comme nom principal lorsque l'élément est renommé :
		
		`admin@DISPLAY-NAME(SYSTEM-NAME):~ $`

`Passwords.txt` Dans le progiciel de récupération	Comme illustré `Server Name`	Comme illustré `Display Name`
`/etc/hosts` sur tous les nœuds Par exemple : `10.96.99.128 SYSTEM-NAME 28989c59-a2c3-4d30-bb09-6879adf2437f DISPLAY-NAME localhost-grid # storagegrid-gen-host`	Toujours affiché dans la deuxième colonne	Lorsque l'élément est renommé, il apparaît dans la quatrième colonne
`topology-display-names.json`, Inclus avec les données AutoSupport	Non inclus	Vide, sauf si les éléments ont été renommés ; sinon, mappe les ID de grille, de site et de nœud sur leurs noms d'affichage.

Afficher les exigences relatives au nom

Avant d'utiliser cette procédure, vérifiez les exigences relatives aux noms d'affichage.

Afficher les noms des nœuds

Les noms d'affichage des nœuds doivent respecter les règles suivantes :

- Doit être unique sur l'ensemble de votre système StorageGRID.
- Ne peut pas être identique au nom système d'un autre élément de votre système StorageGRID.
- Doit contenir au moins 1 et 32 caractères.
- Peut contenir des chiffres, des tirets (-) et des lettres majuscules et minuscules.
- Peut commencer ou se terminer par une lettre ou un chiffre, mais ne peut pas commencer ou se terminer par un tiret.
- Ne peut pas être tous des nombres.

- Ne sont pas sensibles à la casse. Par exemple : `DC1-ADM` et `dc1-adm` sont considérés comme des doublons.

Vous pouvez renommer un nœud avec un nom d'affichage précédemment utilisé par un autre nœud, à condition que le renommage ne crée pas de nom d'affichage ni de nom de système en double.

Afficher les noms de la grille et des sites

Les noms d'affichage de la grille et des sites suivent les mêmes règles avec les exceptions suivantes :

- Peut inclure des espaces.
- Les caractères spéciaux suivants peuvent être inclus : `= - _ : , . @ !`
- Vous pouvez commencer et terminer par les caractères spéciaux, y compris les tirets.
- Il peut s'agir de tous les chiffres ou de caractères spéciaux.

Meilleures pratiques relatives aux noms d'affichage

Si vous prévoyez de renommer plusieurs éléments, documentez votre schéma de dénomination général avant d'utiliser cette procédure. Trouvez un système qui garantit que les noms sont uniques, cohérents et faciles à comprendre d'un seul coup d'œil.

Vous pouvez utiliser n'importe quelle convention de dénomination adaptée aux besoins de votre entreprise. Prenez en compte les suggestions de base suivantes concernant les éléments à inclure :

- **Indicateur de site** : si vous avez plusieurs sites, ajoutez un code de site à chaque nom de nœud.
- **Type de noeud** : les noms de noeud indiquent généralement le type de noeud. Vous pouvez utiliser des abréviations telles que `s`, `adm`, `gw`, et `arc` (Nœud de stockage, nœud d'administration, nœud de passerelle et nœud d'archivage).
- **Numéro de nœud** : si un site contient plusieurs nœuds d'un type particulier, ajoutez un numéro unique au nom de chaque nœud.

Réfléchissez deux fois avant d'ajouter des détails spécifiques aux noms susceptibles de changer au fil du temps. Par exemple, n'incluez pas d'adresses IP dans les noms de nœuds car ces adresses peuvent être modifiées. De même, l'emplacement des racks ou les numéros de modèle des appliances peuvent changer si vous déplacez des équipements ou mettez à niveau le matériel.

Exemples de noms d'affichage

Supposons que votre système StorageGRID dispose de trois data centers et que chaque data Center dispose de nœuds de différents types. Vos noms d'affichage peuvent être aussi simples que ceux-ci :

- **Grille** : `StorageGRID Deployment`
- **Premier site** : `Data Center 1`
  - `dc1-adm1`
  - `dc1-s1`
  - `dc1-s2`
  - `dc1-s3`
  - `dc1-gw1`

- **Deuxième site**: `Data Center 2`
  - `dc2-adm2`
  - `dc2-s1`
  - `dc2-s2`
  - `dc2-s3`
- **Troisième site**: `Data Center 3`
  - `dc3-s1`
  - `dc3-s2`
  - `dc3-s3`

Ajouter ou mettre à jour les noms d'affichage

Vous pouvez utiliser cette procédure pour ajouter ou mettre à jour les noms d'affichage utilisés pour votre grille, vos sites et vos nœuds. Vous pouvez renommer un seul élément, plusieurs éléments ou même tous les éléments en même temps. La définition ou la mise à jour d'un nom d'affichage n'affecte en aucune façon les opérations StorageGRID.

Avant de commencer

- À partir du **nœud d'administration principal**, vous êtes connecté au gestionnaire de grille à l'aide d'un "navigateur web pris en charge".

> Vous pouvez ajouter ou mettre à jour des noms d'affichage à partir d'un nœud d'administration non principal, mais vous devez être connecté au nœud d'administration principal pour télécharger un package de récupération.

- Vous disposez de l'autorisation Maintenance ou accès racine.
- Vous avez la phrase secrète pour le provisionnement.
- Vous comprenez les exigences et les meilleures pratiques en matière d'affichage des noms. Voir "Renommer la grille, les sites et les nœuds : présentation".

Comment renommer la grille, les sites ou les nœuds

Vous pouvez renommer votre système StorageGRID, un ou plusieurs sites ou un ou plusieurs nœuds.

Vous pouvez utiliser un nom d'affichage précédemment utilisé par un autre nœud, tant que le changement de nom n'entraîne pas de doublon de nom d'affichage ou de nom de système.

Sélectionnez les éléments à renommer

Pour commencer, sélectionnez les éléments à renommer.

Étapes

1. Sélectionnez **MAINTENANCE** > **tâches** > **Renommer la grille, les sites et les nœuds**.
2. Pour l'étape **Sélectionner les noms**, sélectionnez les éléments que vous souhaitez renommer.

Élément à modifier	Instructions
Noms de tout (ou presque tout) dans votre système	a. Sélectionnez **Sélectionner tout**. b. Vous pouvez également effacer les éléments que vous ne souhaitez pas renommer.
Nom de la grille	Cochez la case de la grille.
Nom d'un site et de certains ou de tous ses nœuds	a. Cochez la case dans l'en-tête du tableau pour le site. b. Si vous le souhaitez, désactivez les nœuds que vous ne souhaitez pas renommer.
Nom d'un site	Cochez la case du site.
Nom d'un nœud	Cochez la case du nœud.

3. Sélectionnez **Continuer**.
4. Passez en revue le tableau, qui inclut les éléments que vous avez sélectionnés.
   - La colonne **Nom d'affichage** indique le nom actuel de chaque élément. Si l'élément n'a jamais été renommé, son nom d'affichage est le même que son nom système.
   - La colonne **Nom du système** indique le nom que vous avez saisi pour chaque élément au cours de l'installation. Les noms de système sont utilisés pour les opérations StorageGRID internes et ne peuvent pas être modifiés. Par exemple, le nom système d'un nœud peut correspondre à son nom d'hôte.
   - La colonne **Type** indique le type de l'élément : grille, site ou le type de nœud spécifique.

Proposer de nouveaux noms

Pour l'étape **proposer de nouveaux noms**, vous pouvez entrer un nom d'affichage pour chaque élément individuellement ou renommer les éléments en bloc.

Renommer les éléments individuellement

Procédez comme suit pour entrer un nom d'affichage pour chaque élément à renommer.

Étapes

1. Dans le champ **Nom d'affichage**, entrez un nom d'affichage proposé pour chaque élément de la liste.

   Voir "Renommer la grille, les sites et les nœuds : présentation" pour en savoir plus sur les exigences de nommage.

2. Pour supprimer les éléments que vous ne souhaitez pas renommer, sélectionnez ✕ Dans la colonne **Supprimer de la liste**.

   Si vous ne proposez pas de nouveau nom pour un élément, vous devez le supprimer de la table.

3. Lorsque vous avez proposé de nouveaux noms pour tous les éléments de la table, sélectionnez **Renommer**.

   Un message de réussite s'affiche. Les nouveaux noms d'affichage sont maintenant utilisés dans le Gestionnaire de grille.

Renommer les éléments en bloc

Utilisez l'outil de renommage en bloc si les noms d'élément partagent une chaîne commune que vous souhaitez remplacer par une autre chaîne.

Étapes

1. Pour l'étape **proposer de nouveaux noms**, sélectionnez **utiliser l'outil de renommage en bloc**.

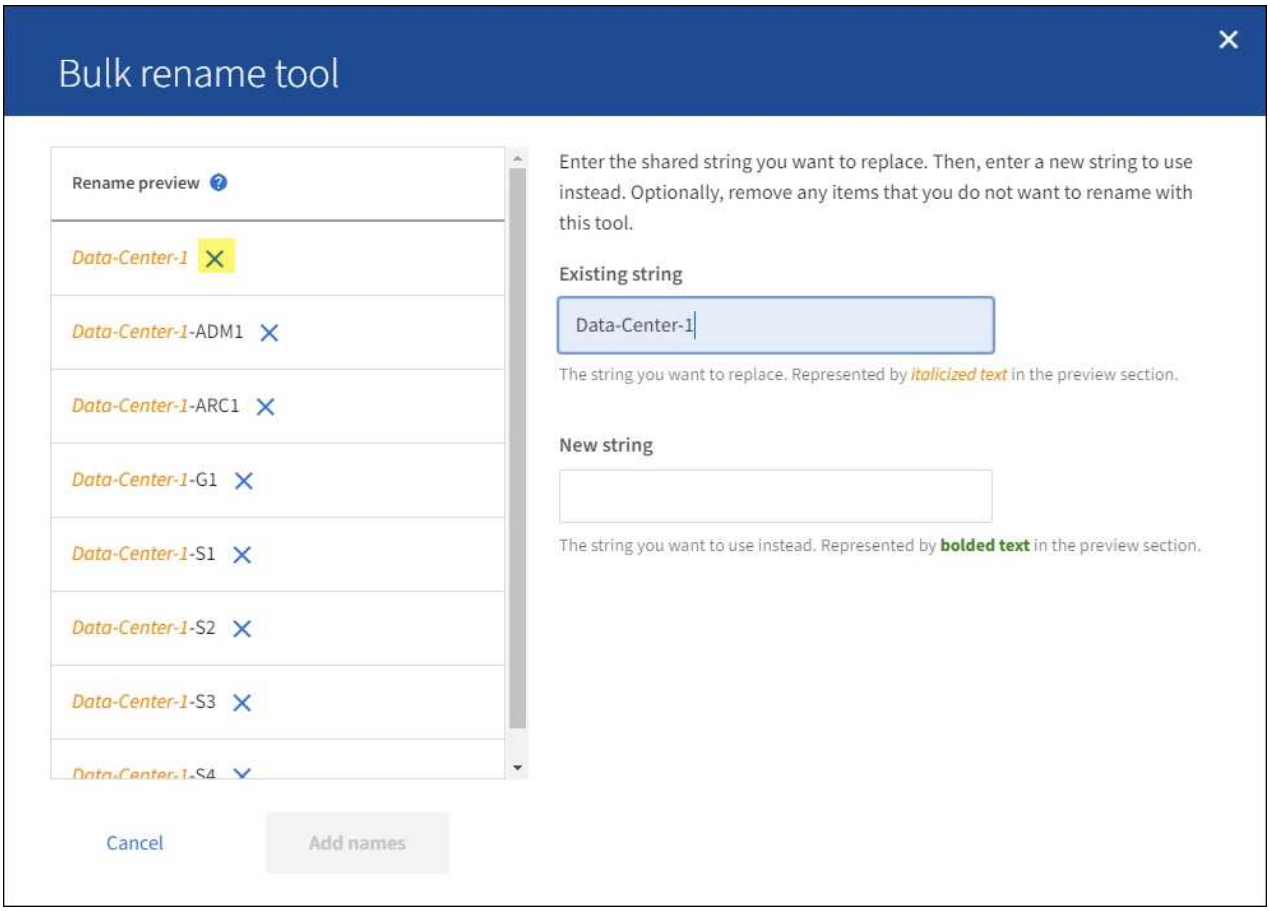
   L'aperçu **Renommer** inclut tous les éléments affichés pour l'étape **proposer de nouveaux noms**. Vous pouvez utiliser l'aperçu pour voir comment les noms d'affichage seront pris en compte après le remplacement d'une chaîne partagée.

2. Dans le champ **existing string**, entrez la chaîne partagée que vous souhaitez remplacer. Par exemple, si la chaîne que vous souhaitez remplacer est `Data-Center-1`, Entrez **Data-Center-1**.

   Au fur et à mesure que vous tapez, votre texte est mis en surbrillance à l'endroit où il se trouve dans les noms à gauche.

3. Sélectionnez ✕ pour supprimer les éléments que vous ne souhaitez pas renommer avec cet outil.

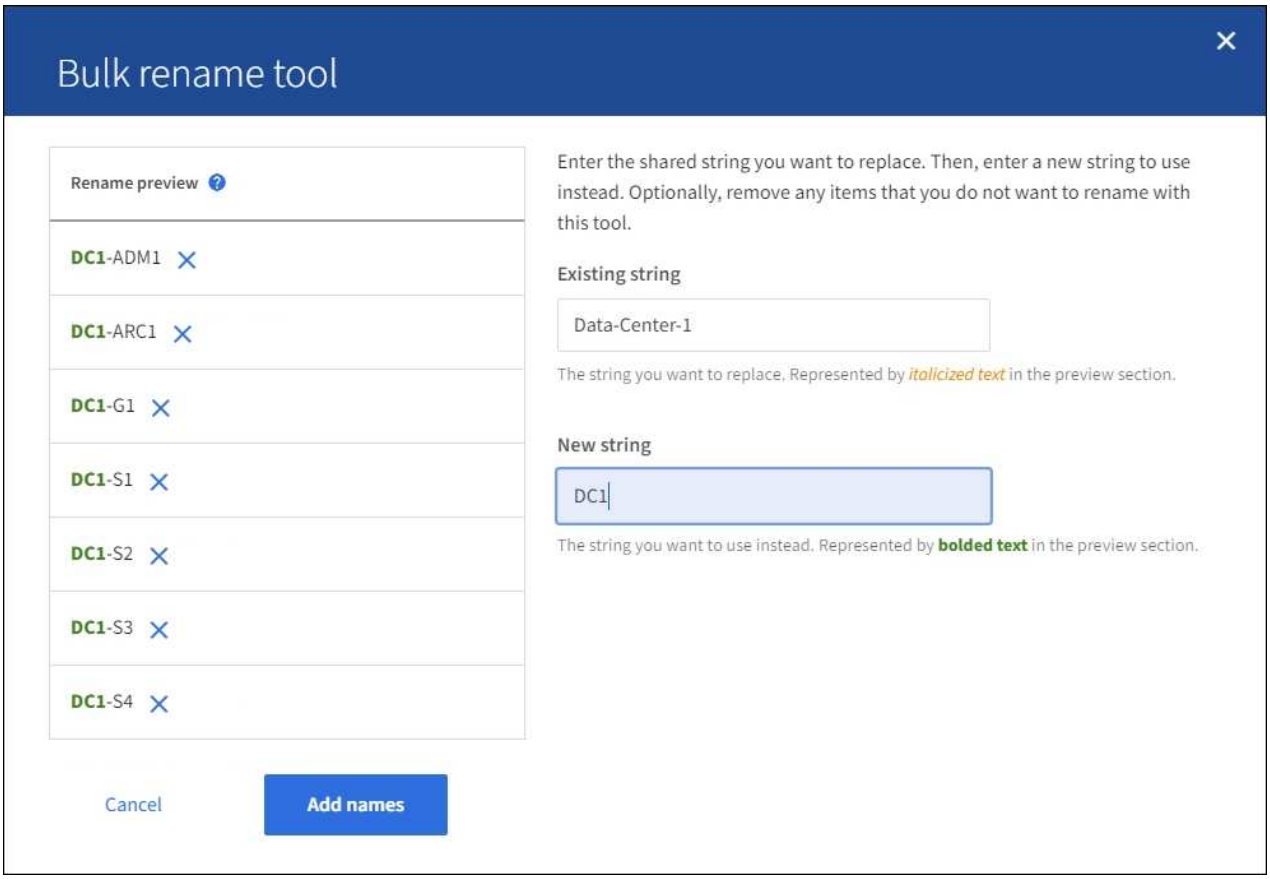
   Par exemple, supposons que vous souhaitiez renommer tous les nœuds qui contiennent la chaîne `Data-Center-1`, mais vous ne voulez pas renommer le `Data-Center-1` site lui-même. Sélectionnez ✕ pour supprimer le site de l'aperçu de changement de nom.



4. Dans le champ **Nouvelle chaîne**, entrez la chaîne de remplacement que vous souhaitez utiliser. Par exemple, entrez **DC1**.

   Voir "Renommer la grille, les sites et les nœuds : présentation" pour en savoir plus sur les exigences de nommage.

   Lorsque vous entrez la chaîne de remplacement, les noms à gauche sont mis à jour, ce qui vous permet de vérifier que les nouveaux noms seront corrects.



5. Lorsque vous êtes satisfait des noms affichés dans l'aperçu, sélectionnez **Ajouter des noms** pour ajouter les noms à la table pour l'étape **proposer de nouveaux noms**.
6. Apportez les modifications supplémentaires requises ou sélectionnez ✕ pour supprimer les éléments que vous ne souhaitez pas renommer.
7. Lorsque vous êtes prêt à renommer tous les éléments de la table, sélectionnez **Renommer**.

   Un message de réussite s'affiche. Les nouveaux noms d'affichage sont maintenant utilisés dans le Gestionnaire de grille.

Téléchargez le package de récupération

Lorsque vous avez terminé de renommer des éléments, téléchargez et enregistrez un nouveau package de récupération. Les nouveaux noms d'affichage des éléments que vous avez renommés sont inclus dans le `Passwords.txt` fichier.

Étapes

1. Saisissez la phrase secrète pour le provisionnement.
2. Sélectionnez **Télécharger le paquet de récupération**.

   Le téléchargement commence immédiatement.

3. Une fois le téléchargement terminé, ouvrez le `Passwords.txt` fichier pour afficher le nom du serveur pour tous les nœuds et les noms d'affichage des nœuds renommés.
4. Copiez le `sgws-recovery-package-`*`id-revision`*`.zip` classez-les dans deux emplacements sûrs, sécurisés et séparés.

Le fichier du progiciel de récupération doit être sécurisé car il contient des clés de cryptage et des mots de passe qui peuvent être utilisés pour obtenir des données du système StorageGRID.

5. Sélectionnez **Terminer** pour revenir à la première étape.

Rétablit les noms d'affichage des noms système

Vous pouvez rétablir le nom d'origine d'une grille, d'un site ou d'un nœud renommé. Lorsque vous rétablissez le nom système d'un élément, les pages du Gestionnaire de grille et les autres emplacements StorageGRID n'affichent plus de **Nom d'affichage** pour cet élément. Seul le nom système de l'élément est affiché.

Étapes

1. Sélectionnez **MAINTENANCE** > **tâches** > **Renommer la grille, les sites et les nœuds**.
2. Pour l'étape **Sélectionner les noms**, sélectionnez les éléments que vous souhaitez restaurer aux noms système.
3. Sélectionnez **Continuer**.
4. Pour l'étape **proposer de nouveaux noms**, restaurez les noms d'affichage individuellement ou en bloc.

Revenir aux noms de système individuellement

a. Copiez le nom système d'origine de chaque élément et collez-le dans le champ **Nom d'affichage** ou sélectionnez ✕ pour supprimer les éléments que vous ne souhaitez pas rétablir.

   Pour rétablir un nom d'affichage, le nom du système doit apparaître dans le champ **Nom d'affichage**, mais le nom n'est pas sensible à la casse.

b. Sélectionnez **Renommer**.

   Un message de réussite s'affiche. Les noms d'affichage de ces éléments ne sont plus utilisés.

Revenir aux noms de système en bloc

a. Pour l'étape **proposer de nouveaux noms**, sélectionnez **utiliser l'outil de renommage en bloc**.
b. Dans le champ **existing string**, entrez la chaîne de nom d'affichage que vous souhaitez remplacer.
c. Dans le champ **Nouvelle chaîne**, entrez la chaîne de nom système que vous souhaitez utiliser.
d. Sélectionnez **Ajouter des noms** pour ajouter les noms à la table pour l'étape **proposer de nouveaux noms**.
e. Vérifiez que chaque entrée du champ **Nom d'affichage** correspond au nom du champ **Nom du système**. Effectuez les modifications ou sélectionnez ✕ pour supprimer tous les éléments que vous ne souhaitez pas rétablir.

   Pour rétablir un nom d'affichage, le nom du système doit apparaître dans le champ **Nom d'affichage**, mais le nom n'est pas sensible à la casse.

f. Sélectionnez **Renommer**.

   Un message de réussite s'affiche. Les noms d'affichage de ces éléments ne sont plus utilisés.

5. Téléchargez et enregistrez un nouveau package de récupération.

   Les noms d'affichage des éléments que vous avez restaurés ne sont plus inclus dans le `Passwords.txt` fichier.

Procédures de maintenance du réseau

Mise à jour des sous-réseaux pour le réseau Grid

StorageGRID conserve une liste des sous-réseaux réseau utilisés pour communiquer entre les nœuds de la grille sur le réseau Grid (eth0). Ces entrées incluent les sous-réseaux utilisés pour le réseau Grid par chaque site du système StorageGRID, ainsi que tous les sous-réseaux utilisés pour les serveurs NTP, DNS, LDAP ou autres serveurs externes accessibles via la passerelle réseau Grid. Lorsque vous ajoutez des nœuds de grille ou un nouveau site dans une extension, vous devrez peut-être mettre à jour ou ajouter des sous-réseaux au réseau Grid.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous avez le "Maintenance ou autorisation d'accès racine".
- Vous avez la phrase secrète pour le provisionnement.
- Les adresses réseau des sous-réseaux que vous souhaitez configurer sont définies, en notation CIDR.

Description de la tâche

Si vous effectuez une activité d'extension incluant l'ajout d'un nouveau sous-réseau, vous devez ajouter un nouveau sous-réseau à la liste de sous-réseaux réseau de la grille avant de démarrer la procédure d'extension. Sinon, vous devrez annuler l'extension, ajouter le nouveau sous-réseau et relancer l'extension.

Ajoutez un sous-réseau

Étapes

1. Sélectionnez **MAINTENANCE** > **réseau** > **réseau Grid**.
2. Sélectionnez **Ajouter un autre sous-réseau** pour ajouter un nouveau sous-réseau en notation CIDR.

   Par exemple, entrez `10.96.104.0/22`.

3. Saisissez le mot de passe de provisionnement et sélectionnez **Enregistrer**.
4. Attendez que les modifications soient appliquées, puis téléchargez un nouveau progiciel de récupération.
   a. Sélectionnez **MAINTENANCE** > **système** > **progiciel de récupération**.
   b. Saisissez la phrase de passe de provisionnement *.

> Le fichier du progiciel de récupération doit être sécurisé car il contient des clés de cryptage et des mots de passe qui peuvent être utilisés pour obtenir des données du système StorageGRID. Elle permet également de restaurer le nœud d'administration principal.

Les sous-réseaux que vous avez spécifiés sont automatiquement configurés pour votre système

StorageGRID.

Modifier un sous-réseau

Étapes

1. Sélectionnez **MAINTENANCE** > **réseau** > **réseau Grid**.
2. Sélectionnez le sous-réseau à modifier et apportez les modifications nécessaires.
3. Entrez la phrase de passe de provisionnement et sélectionnez **Enregistrer**.
4. Sélectionnez **Oui** dans la boîte de dialogue de confirmation.
5. Attendez que les modifications soient appliquées, puis téléchargez un nouveau progiciel de récupération.
   a. Sélectionnez **MAINTENANCE** > **système** > **progiciel de récupération**.
   b. Saisissez la phrase de passe de provisionnement *.

Supprimez un sous-réseau

Étapes

1. Sélectionnez **MAINTENANCE** > **réseau** > **réseau Grid**.
2. Sélectionnez l'icône de suppression ✕ en regard du sous-réseau.
3. Entrez la phrase de passe de provisionnement et sélectionnez **Enregistrer**.
4. Sélectionnez **Oui** dans la boîte de dialogue de confirmation.
5. Attendez que les modifications soient appliquées, puis téléchargez un nouveau progiciel de récupération.
   a. Sélectionnez **MAINTENANCE** > **système** > **progiciel de récupération**.
   b. Saisissez la phrase de passe de provisionnement *.

Configurez les adresses IP

Configurez les adresses IP

Vous pouvez configurer le réseau en configurant des adresses IP pour les noeuds de la grille à l'aide de l'outil Modifier les adresses IP.

Vous devez utiliser l'outil Modifier l'IP pour apporter la plupart des modifications à la configuration réseau qui ont été initialement définies lors du déploiement de la grille. Les modifications manuelles effectuées à l'aide de commandes et de fichiers de mise en réseau Linux standard peuvent ne pas se propager à tous les services StorageGRID et ne pas persister entre les mises à niveau, redémarrages ou les procédures de restauration des nœuds.

ⓘ La procédure de modification IP peut être une procédure perturbateur. Des parties de la grille peuvent être indisponibles jusqu'à l'application de la nouvelle configuration.

ⓘ Si vous apportez uniquement des modifications à la liste de sous-réseaux du réseau Grid, utilisez le gestionnaire de grille pour ajouter ou modifier la configuration du réseau. Dans le cas contraire, utilisez l'outil Modifier IP si le gestionnaire de grille est inaccessible en raison d'un problème de configuration du réseau ou si vous effectuez une modification du routage du réseau Grid et d'autres modifications du réseau simultanément.

Si vous souhaitez modifier l'adresse IP du réseau Grid pour tous les nœuds de la grille, utilisez le "procédure spéciale pour les changements à l'échelle de la grille".

Interfaces Ethernet

L'adresse IP attribuée à eth0 est toujours l'adresse IP réseau du nœud de la grille. L'adresse IP attribuée à eth1 est toujours l'adresse IP du réseau Admin du nœud de la grille. L'adresse IP attribuée à eth2 est toujours l'adresse IP du réseau client du nœud de la grille.

Notez que, sur certaines plateformes, comme les appliances StorageGRID, eth0, eth1 et eth2 peuvent être des interfaces agrégées composées de ponts subordonnés ou de liaisons d'interfaces physiques ou VLAN. Sur ces plates-formes, l'onglet **SSM** > **Resources** peut afficher l'adresse IP de la grille, de l'administrateur et du réseau client attribuée à d'autres interfaces en plus de eth0, eth1 ou eth2.

DHCP

Vous ne pouvez configurer DHCP que pendant la phase de déploiement. Vous ne pouvez pas configurer DHCP pendant la configuration. Vous devez utiliser les procédures de modification d'adresse IP pour modifier les adresses IP, les masques de sous-réseau et les passerelles par défaut pour un nœud de grille. L'utilisation de l'outil Modifier les adresses IP va rendre les adresses DHCP statiques.

Groupes haute disponibilité (HA)

- Si une interface client Network se trouve dans un groupe haute disponibilité, vous ne pouvez pas modifier l'adresse IP client Network de cette interface en une adresse qui se trouve en dehors du sous-réseau configuré pour le groupe haute disponibilité.
- Vous ne pouvez pas modifier l'adresse IP du réseau client en fonction de la valeur d'une adresse IP virtuelle existante attribuée à un groupe haute disponibilité configuré sur l'interface réseau client.
- Si une interface réseau Grid est contenue dans un groupe haute disponibilité, vous ne pouvez pas modifier l'adresse IP réseau Grid de cette interface pour la remplacer par une adresse située en dehors du sous-réseau configuré pour le groupe haute disponibilité.
- Vous ne pouvez pas modifier l'adresse IP du réseau Grid sur la valeur d'une adresse IP virtuelle existante attribuée à un groupe HA configuré sur l'interface réseau Grid.

Modifier la configuration réseau du nœud

Vous pouvez modifier la configuration réseau d'un ou plusieurs nœuds à l'aide de l'outil Modifier IP. Vous pouvez modifier la configuration du réseau Grid ou ajouter, modifier ou supprimer les réseaux d'administration ou de client.

Avant de commencer

Vous avez le `Passwords.txt` fichier.

Description de la tâche

Linux: si vous ajoutez un noeud de grille au réseau Admin ou au réseau client pour la première fois, et que vous n'avez pas configuré précédemment ADMIN_NETWORK_TARGET ni CLIENT_NETWORK_TARGET dans le fichier de configuration de noeud, vous devez le faire maintenant.

Consultez les instructions d'installation de StorageGRID pour votre système d'exploitation Linux :

- "Installez Red Hat Enterprise Linux ou CentOS"

- "Installez Ubuntu ou Debian"

Appareils : sur les appareils StorageGRID, si le réseau client ou administrateur n'a pas été configuré dans le programme d'installation de l'appliance StorageGRID pendant l'installation initiale, le réseau ne peut pas être ajouté en utilisant uniquement l'outil Modifier IP. Tout d'abord, vous devez "mettez l'appareil en mode de maintenance", Configurez les liaisons, ramenez le serveur en mode de fonctionnement normal, puis utilisez l'outil Modifier IP pour modifier la configuration du réseau. Voir la "procédure de configuration des liens réseau".

Vous pouvez modifier l'adresse IP, le masque de sous-réseau, la passerelle ou la valeur MTU d'un ou plusieurs nœuds sur n'importe quel réseau.

Vous pouvez également ajouter ou supprimer un nœud d'un réseau client ou d'un réseau d'administration :

- Vous pouvez ajouter un nœud à un réseau client ou à un réseau d'administration en ajoutant une adresse IP/un masque de sous-réseau sur ce réseau au nœud.
- Vous pouvez supprimer un nœud d'un réseau client ou d'un réseau d'administration en supprimant l'adresse IP/le masque de sous-réseau du nœud sur ce réseau.

  Impossible de supprimer des nœuds du réseau Grid.

> Les échanges d'adresses IP ne sont pas autorisés. Si vous devez échanger des adresses IP entre des noeuds de grille, vous devez utiliser une adresse IP intermédiaire temporaire.

> Si l'authentification unique (SSO) est activée pour votre système StorageGRID et que vous modifiez l'adresse IP d'un nœud d'administration, sachez que toute confiance de tiers qui a été configurée à l'aide de l'adresse IP du nœud d'administration (au lieu de son nom de domaine complet, comme recommandé) deviendra non valide. Vous ne pourrez plus vous connecter au nœud. Immédiatement après avoir modifié l'adresse IP, vous devez mettre à jour ou reconfigurer la confiance de l'organisme de confiance du nœud dans Active Directory Federation Services (AD FS) avec la nouvelle adresse IP. Reportez-vous aux instructions pour "Configuration de SSO".

> Toutes les modifications que vous apportez au réseau à l'aide de l'outil Modifier IP sont propagées au micrologiciel du programme d'installation des appliances StorageGRID. Ainsi, si le logiciel StorageGRID est réinstallé sur une appliance ou si une appliance est placée en mode de maintenance, la configuration réseau est correcte.

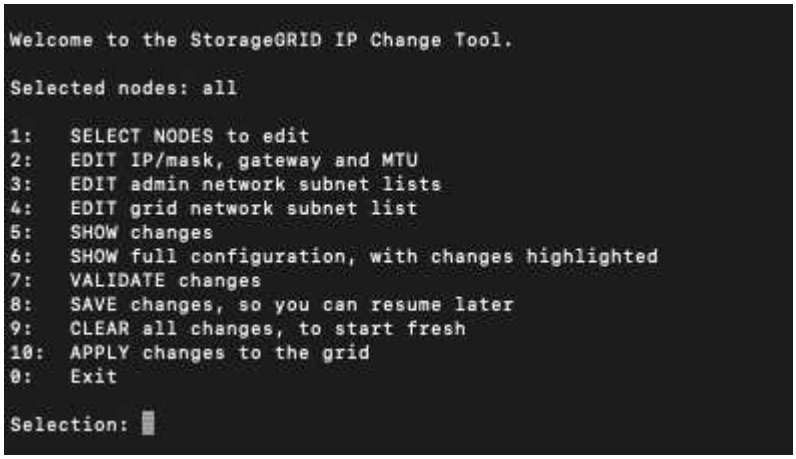
Étapes

1. Connectez-vous au nœud d'administration principal :
   a. Saisissez la commande suivante : `ssh admin@primary_Admin_Node_IP`
   b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
   c. Entrez la commande suivante pour passer à la racine : `su -`
   d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

      Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

2. Lancez l'outil Modifier IP en entrant la commande suivante : `change-ip`
3. Saisissez la phrase de passe de provisionnement à l'invite.

Le menu principal s'affiche.



4. Vous pouvez également sélectionner **1** pour choisir les nœuds à mettre à jour. Sélectionnez ensuite l'une des options suivantes :

   - **1** : nœud unique — sélectionnez par nom
   - **2** : nœud unique — sélectionnez par site, puis par nom
   - **3** : nœud unique — sélectionnez par adresse IP actuelle
   - **4**: Tous les nœuds d'un site
   - **5** : tous les nœuds de la grille

   Remarque : si vous souhaitez mettre à jour tous les nœuds, laissez "tous" rester sélectionnés.

   Une fois votre sélection effectuée, le menu principal s'affiche, le champ **noeuds sélectionnés** étant mis à jour pour refléter votre choix. Toutes les actions suivantes sont uniquement réalisées sur les nœuds affichés.

5. Dans le menu principal, sélectionnez l'option **2** pour modifier les informations IP/masque, passerelle et MTU pour les nœuds sélectionnés.
   a. Sélectionnez le réseau sur lequel vous souhaitez apporter des modifications :

      - **1** : réseau de grille
      - **2**: Réseau d'administration
      - **3**: Réseau client
      - **4** : tous les réseaux après votre sélection, l'invite affiche le nom du nœud, le nom du réseau (grille, Admin ou client), le type de données (IP/masque, Passerelle ou MTU) et valeur actuelle.

        La modification de l'adresse IP, de la longueur du préfixe, de la passerelle ou de la MTU d'une interface configurée par DHCP changera l'interface en mode statique. Lorsque vous sélectionnez pour modifier une interface configurée par DHCP, un avertissement s'affiche pour vous informer que l'interface passe en mode statique.

      Interfaces configurées en tant que `fixed` ne peut pas être modifié.

   b. Pour définir une nouvelle valeur, saisissez-la dans le format indiqué pour la valeur actuelle.
   c. Pour laisser la valeur actuelle inchangée, appuyez sur **entrée**.

d. Si le type de données est `IP/mask`, Vous pouvez supprimer le réseau Admin ou client du nœud en entrant **d** ou **0.0.0.0/0**.

e. Après avoir modifié tous les noeuds que vous souhaitez modifier, entrez **q** pour revenir au menu principal.

   Vos modifications sont conservées jusqu'à ce qu'elles soient supprimées ou appliquées.

6. Vérifiez vos modifications en sélectionnant l'une des options suivantes :

   - **5** : affiche les modifications dans la sortie isolées pour afficher uniquement l'élément modifié. Les modifications sont mises en évidence en vert (ajouts) ou en rouge (suppressions), comme indiqué dans l'exemple de sortie :

```
================================================================================
Site: RTP
================================================================================
username-x Grid    IP      [    172.16.0.239/21 ]: 172.16.0.240/21
username-x Grid    MTU     [              1400 ]: 9000
username-x Grid    MTU     [              1400 ]: 9000
username-x Grid    MTU     [              1400 ]: 9000
username-x Grid    MTU     [              1400 ]: 9000
username-x Grid    MTU     [              1400 ]: 9000
username-x Grid    MTU     [              1400 ]: 9000
username-x Grid    MTU     [              1400 ]: 9000
username-x Admin   IP      [    10.224.0.244/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.245/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.240/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.241/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.242/21 ]: 0.0.0.0/0
username-x Admin   IP      [    10.224.0.243/21 ]: 0.0.0.0/0
username-x Admin   Gateway [         10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [         10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [         10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [         10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [         10.224.0.1 ]: 0.0.0.0
username-x Admin   Gateway [         10.224.0.1 ]: 0.0.0.0
username-x Admin   MTU     [              1400 ]: 0
username-x Admin   MTU     [              1400 ]: 0
username-x Admin   MTU     [              1400 ]: 0
username-x Admin   MTU     [              1400 ]: 0
username-x Admin   MTU     [              1400 ]: 0
username-x Admin   MTU     [              1400 ]: 0
Press Enter to continue
```

   - **6** : affiche les modifications en sortie qui affichent la configuration complète. Les modifications sont mises en surbrillance en vert (ajouts) ou en rouge (suppressions).

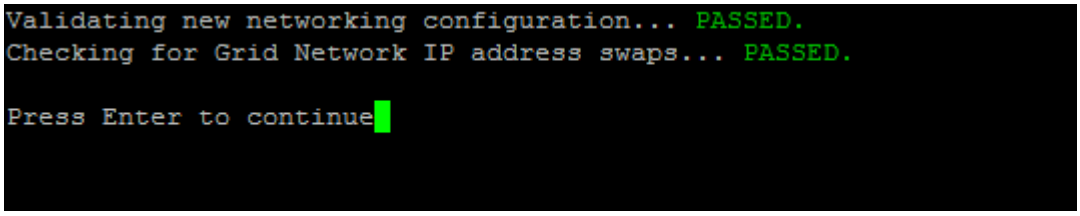
> Certaines interfaces de ligne de commande peuvent afficher des ajouts et des suppressions en utilisant le formatage barré. L'affichage correct dépend de votre client terminal prenant en charge les séquences d'échappement VT100 nécessaires.

7. Sélectionnez l'option **7** pour valider toutes les modifications.

   Cette validation garantit que les règles pour les réseaux Grid, Admin et client, telles que l'absence de sous-réseaux superposés, ne sont pas violées.

   Dans cet exemple, la validation a renvoyé des erreurs.

Dans cet exemple, la validation a réussi.



8. Une fois la validation terminée, choisissez l'une des options suivantes :
   - **8**: Enregistrer les modifications non appliquées.

     Cette option vous permet de quitter l'outil Modifier l'IP et de le redémarrer ultérieurement, sans perdre les modifications non appliquées.

   - **10** : appliquer la nouvelle configuration réseau.
9. Si vous avez sélectionné l'option **10**, choisissez l'une des options suivantes :
   - **Appliquer** : appliquez les modifications immédiatement et redémarrez automatiquement chaque nœud si nécessaire.

     Si la nouvelle configuration réseau ne nécessite aucune modification de réseau physique, vous pouvez sélectionner **appliquer** pour appliquer les modifications immédiatement. Les nœuds seront redémarrés automatiquement, si nécessaire. Les nœuds qui doivent être redémarrés s'affichent.

   - **Etape** : appliquez les modifications lors du prochain redémarrage manuel des nœuds.

     Si vous devez apporter des modifications de configuration de réseau physique ou virtuel pour que la nouvelle configuration de réseau fonctionne, vous devez utiliser l'option **stage**, arrêter les nœuds affectés, effectuer les modifications de réseau physique nécessaires et redémarrer les nœuds affectés. Si vous sélectionnez **appliquer** sans effectuer au préalable ces modifications de mise en réseau, les modifications échoueront généralement.

     > ⓘ Si vous utilisez l'option **stage**, vous devez redémarrer le nœud le plus rapidement possible après le staging pour minimiser les interruptions.

   - **Annuler**: Ne faites pas de modifications de réseau pour le moment.

     Si vous n'étiez pas conscient que les modifications proposées nécessitent de redémarrer les nœuds, vous pouvez reporter les modifications pour minimiser l'impact sur les utilisateurs. Si vous sélectionnez **annuler**, vous revenez au menu principal et les modifications sont préservés pour pouvoir les appliquer ultérieurement.

     Lorsque vous sélectionnez **appliquer** ou **stage**, un nouveau fichier de configuration réseau est généré, le provisionnement est effectué et les nœuds sont mis à jour avec de nouvelles informations de travail.

Pendant l'approvisionnement, la sortie affiche l'état au fur et à mesure de l'application des mises à jour.

```
Generating new grid networking description file...

Running provisioning...

Updating grid network configuration on Name
```

Après application ou transfert des modifications, un nouveau progiciel de récupération est généré à la suite de la modification de la configuration de la grille.

10. Si vous avez sélectionné **stage**, suivez ces étapes une fois le provisionnement terminé :

    a. Apportez les modifications nécessaires au réseau physique ou virtuel.

    Modifications de mise en réseau physique : apportez les modifications nécessaires à la mise en réseau physique, en arrêtant le nœud en toute sécurité si nécessaire.

    Linux : si vous ajoutez le nœud à un réseau Admin ou client pour la première fois, assurez-vous d'avoir ajouté l'interface comme décrit dans "Linux : ajoutez des interfaces au nœud existant".

    a. Redémarrez les nœuds concernés.

11. Sélectionnez **0** pour quitter l'outil Modifier l'IP une fois les modifications effectuées.
12. Téléchargez un nouveau package de récupération depuis Grid Manager.
    a. Sélectionnez **MAINTENANCE** > **système** > **progiciel de récupération**.
    b. Saisissez la phrase secrète pour le provisionnement.

Informations associées

"Appliances de stockage SGF6112"

"Dispositifs de stockage SG6000"

"Appliances de stockage SG5700"

"Appareils de services SG100 et SG1000"

Ajouter ou modifier des listes de sous-réseaux sur le réseau d'administration

Vous pouvez ajouter, supprimer ou modifier les sous-réseaux dans la liste de sous-réseaux réseau réseau Admin d'un ou plusieurs nœuds.

Avant de commencer

- Vous avez le `Passwords.txt` fichier.

Vous pouvez ajouter, supprimer ou modifier des sous-réseaux à tous les nœuds de la liste des sous-réseaux du réseau d'administration.

Étapes

1. Connectez-vous au nœud d'administration principal :

a. Saisissez la commande suivante : `ssh admin@primary_Admin_Node_IP`

b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

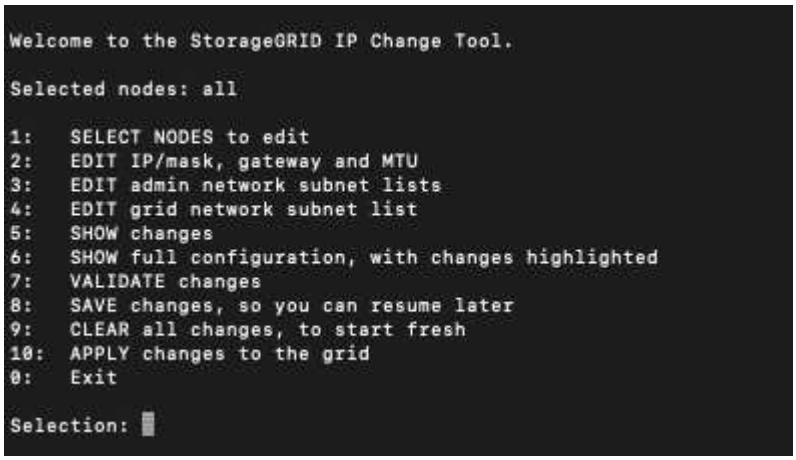
c. Entrez la commande suivante pour passer à la racine : `su -`

d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

2. Lancez l'outil Modifier IP en entrant la commande suivante : `change-ip`
3. Saisissez la phrase de passe de provisionnement à l'invite.

Le menu principal s'affiche.



4. Limitez éventuellement les réseaux/nœuds sur lesquels les opérations sont effectuées. Options au choix :
   - Sélectionnez les nœuds à modifier en choisissant **1**, si vous souhaitez filtrer sur des nœuds spécifiques sur lesquels effectuer l'opération. Sélectionnez l'une des options suivantes :
     - **1** : nœud unique (sélectionner par nom)
     - **2** : nœud unique (sélectionnez par site, puis par nom)
     - **3** : nœud unique (sélection par IP actuel)
     - **4**: Tous les nœuds d'un site
     - **5** : tous les nœuds de la grille
     - **0**: Retour
   - Autoriser « tous » à rester sélectionné. Une fois la sélection effectuée, l'écran du menu principal s'affiche. Le champ noeuds sélectionnés reflète votre nouvelle sélection, et maintenant toutes les opérations sélectionnées ne seront effectuées que sur cet élément.
5. Dans le menu principal, sélectionnez l'option permettant de modifier les sous-réseaux du réseau Admin (option **3**).
6. Options au choix :
   - Ajoutez un sous-réseau en entrant la commande suivante : `add CIDR`
   - Supprimez un sous-réseau en entrant la commande suivante : `del CIDR`
   - Définissez la liste des sous-réseaux en entrant la commande suivante : `set CIDR`

Pour toutes les commandes, vous pouvez entrer plusieurs adresses sous ce format : `add CIDR, CIDR`

Exemple : `add 172.14.0.0/16, 172.15.0.0/16, 172.16.0.0/16`

Vous pouvez réduire la quantité de saisie requise à l'aide de la « flèche vers le haut » pour rappeler les valeurs saisies précédemment dans l'invite de saisie actuelle, puis les modifier si nécessaire.

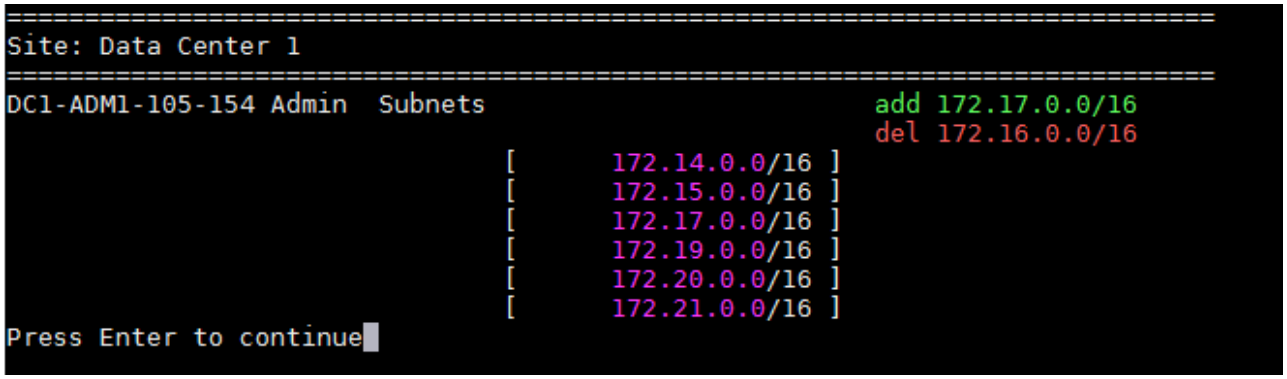
L'exemple ci-dessous illustre l'ajout de sous-réseaux à la liste de sous-réseaux du réseau Admin :

7. Lorsque vous êtes prêt, saisissez **q** pour revenir à l'écran du menu principal. Vos modifications sont conservées jusqu'à ce qu'elles soient supprimées ou appliquées.

   Si vous avez sélectionné l'un des modes de sélection de nœud "tous" à l'étape 2, appuyez sur **entrée** (sans **q**) pour passer au nœud suivant de la liste.

8. Options au choix :

   - Sélectionnez l'option **5** pour afficher les modifications dans la sortie qui sont isolées pour afficher uniquement l'élément modifié. Les modifications sont mises en surbrillance en vert (ajouts) ou en rouge (suppressions), comme indiqué dans l'exemple ci-dessous :



   - Sélectionnez l'option **6** pour afficher les modifications en sortie qui affichent la configuration complète. Les modifications sont mises en surbrillance en vert (ajouts) ou en rouge (suppressions). **Note:** certains émulateurs de terminaux peuvent montrer des ajouts et des suppressions en utilisant le formatage barré.

     Lorsque vous tentez de modifier la liste des sous-réseaux, le message suivant s'affiche :

```
CAUTION: The Admin Network subnet list on the node might contain /32
subnets derived from automatically applied routes that aren't
persistent. Host routes (/32 subnets) are applied automatically if
the IP addresses provided for external services such as NTP or DNS
aren't reachable using default StorageGRID routing, but are reachable
using a different interface and gateway. Making and applying changes
to the subnet list will make all automatically applied subnets
persistent. If you don't want that to happen, delete the unwanted
subnets before applying changes. If you know that all /32 subnets in
the list were added intentionally, you can ignore this caution.
```

Si vous n'avez pas spécifiquement affecté les sous-réseaux de serveurs NTP et DNS à un réseau, StorageGRID crée automatiquement une route hôte (/32) pour la connexion. Si, par exemple, vous préférez avoir une route /16 ou /24 pour la connexion sortante à un serveur DNS ou NTP, vous devez supprimer la route /32 créée automatiquement et ajouter les routes souhaitées. Si vous ne supprimez pas la route hôte créée automatiquement, elle sera conservée après que vous avez appliqué les modifications à la liste de sous-réseaux.

Bien que vous puissiez utiliser ces routes hôtes automatiquement découvertes, vous devez en général configurer manuellement les routes DNS et NTP pour assurer la connectivité.

9. Sélectionnez l'option **7** pour valider toutes les modifications échelonnée.

   Cette validation garantit que les règles des réseaux Grid, Admin et client sont respectées, telles que l'utilisation de sous-réseaux redondants.

10. Vous pouvez également sélectionner l'option **8** pour enregistrer toutes les modifications échelonnée et revenir ultérieurement pour continuer à effectuer les modifications.

    Cette option vous permet de quitter l'outil Modifier l'IP et de le redémarrer ultérieurement, sans perdre les modifications non appliquées.

11. Effectuez l'une des opérations suivantes :
    - Sélectionnez l'option **9** si vous souhaitez effacer toutes les modifications sans enregistrer ni appliquer la nouvelle configuration réseau.
    - Sélectionnez l'option **10** si vous êtes prêt à appliquer des modifications et à provisionner la nouvelle configuration réseau. Pendant le provisionnement, la sortie affiche l'état des mises à jour, comme indiqué dans l'exemple de sortie suivant :

      ```
      Generating new grid networking description file...

      Running provisioning...

      Updating grid network configuration on Name
      ```

12. Téléchargez un nouveau package de récupération depuis Grid Manager.
    a. Sélectionnez **MAINTENANCE** > **système** > **progiciel de récupération**.

b. Saisissez la phrase secrète pour le provisionnement.

Ajouter ou modifier des listes de sous-réseaux sur le réseau Grid

Vous pouvez utiliser l'outil Modifier IP pour ajouter ou modifier des sous-réseaux sur le réseau de grille.

Avant de commencer

- Vous avez le `Passwords.txt` fichier.

Vous pouvez ajouter, supprimer ou modifier des sous-réseaux dans la liste de sous-réseaux du réseau de la grille. Les modifications affectent le routage sur tous les nœuds de la grille.

> Si vous apportez uniquement des modifications à la liste de sous-réseaux du réseau Grid, utilisez le gestionnaire de grille pour ajouter ou modifier la configuration du réseau. Dans le cas contraire, utilisez l'outil Modifier IP si le gestionnaire de grille est inaccessible en raison d'un problème de configuration du réseau ou si vous effectuez une modification du routage du réseau Grid et d'autres modifications du réseau simultanément.

Étapes

1. Connectez-vous au nœud d'administration principal :
   a. Saisissez la commande suivante : `ssh admin@primary_Admin_Node_IP`
   b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
   c. Entrez la commande suivante pour passer à la racine : `su -`
   d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

      Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

2. Lancez l'outil Modifier IP en entrant la commande suivante : `change-ip`
3. Saisissez la phrase de passe de provisionnement à l'invite.

   Le menu principal s'affiche.

```
Welcome to the StorageGRID IP Change Tool.

Selected nodes: all

1:   SELECT NODES to edit
2:   EDIT IP/mask, gateway and MTU
3:   EDIT admin network subnet lists
4:   EDIT grid network subnet list
5:   SHOW changes
6:   SHOW full configuration, with changes highlighted
7:   VALIDATE changes
8:   SAVE changes, so you can resume later
9:   CLEAR all changes, to start fresh
10:  APPLY changes to the grid
0:   Exit

Selection:
```

4. Dans le menu principal, sélectionnez l'option permettant de modifier les sous-réseaux du réseau Grid (option **4**).

Les modifications apportées à la liste des sous-réseaux du réseau de la grille sont effectuées dans toute la grille.

5. Options au choix :
   - Ajoutez un sous-réseau en entrant la commande suivante : `add CIDR`
   - Supprimez un sous-réseau en entrant la commande suivante : `del CIDR`
   - Définissez la liste des sous-réseaux en entrant la commande suivante : `set CIDR`

   Pour toutes les commandes, vous pouvez entrer plusieurs adresses sous ce format : `add CIDR, CIDR`

   Exemple : `add 172.14.0.0/16, 172.15.0.0/16, 172.16.0.0/16`

   Vous pouvez réduire la quantité de saisie requise à l'aide de la « flèche vers le haut » pour rappeler les valeurs saisies précédemment dans l'invite de saisie actuelle, puis les modifier si nécessaire.

   L'exemple ci-dessous montre le paramétrage des sous-réseaux pour la liste de sous-réseaux du réseau Grid :

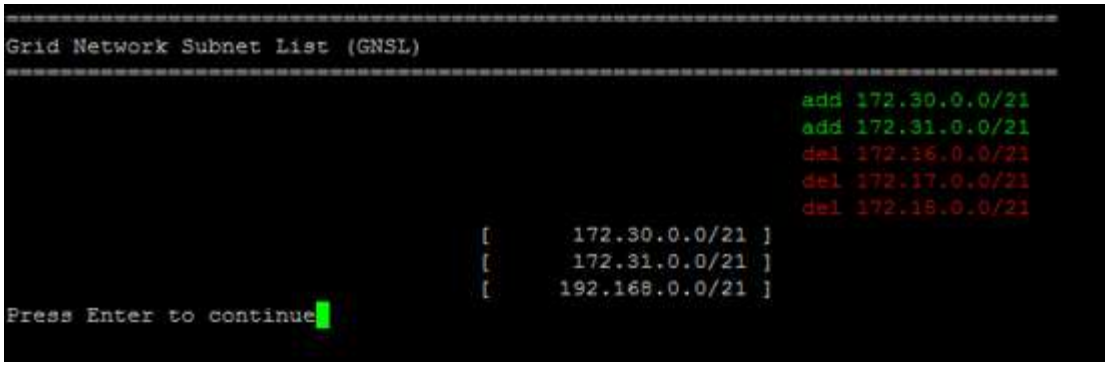
```
Editing: Grid Network Subnet List

Press <enter> to use the list as shown
Use up arrow to recall a previously typed value, which you can then edit
Use 'add <CIDR> [, <CIDR>]' to add subnets <CIDR> [, <CIDR>] to the list
Use 'del <CIDR> [, <CIDR>]' to delete subnets <CIDR> [, <CIDR>] from the list
Use 'set <CIDR> [, <CIDR>]' to set the list to the given list
Use q to complete the editing session early and return to the previous menu

Grid Network Subnet List
  172.16.0.0/21
  172.17.0.0/21
  172.18.0.0/21
  192.168.0.0/21

[add/del/set/quit <CIDR>, ...]: set 172.30.0.0/21, 172.31.0.0/21, 192.168.0.0/21
```

6. Lorsque vous êtes prêt, saisissez **q** pour revenir à l'écran du menu principal. Vos modifications sont conservées jusqu'à ce qu'elles soient supprimées ou appliquées.
7. Options au choix :
   - Sélectionnez l'option **5** pour afficher les modifications dans la sortie qui sont isolées pour afficher uniquement l'élément modifié. Les modifications sont mises en surbrillance en vert (ajouts) ou en rouge (suppressions), comme indiqué dans l'exemple ci-dessous :



- Sélectionnez l'option **6** pour afficher les modifications en sortie qui affichent la configuration complète. Les modifications sont mises en surbrillance en vert (ajouts) ou en rouge (suppressions).

> Certaines interfaces de ligne de commande peuvent afficher des ajouts et des suppressions en utilisant le formatage barré.

8. Sélectionnez l'option **7** pour valider toutes les modifications échelonnée.

   Cette validation garantit que les règles des réseaux Grid, Admin et client sont respectées, telles que l'utilisation de sous-réseaux redondants.

9. Vous pouvez également sélectionner l'option **8** pour enregistrer toutes les modifications échelonnée et revenir ultérieurement pour continuer à effectuer les modifications.

   Cette option vous permet de quitter l'outil Modifier l'IP et de le redémarrer ultérieurement, sans perdre les modifications non appliquées.

10. Effectuez l'une des opérations suivantes :
    - Sélectionnez l'option **9** si vous souhaitez effacer toutes les modifications sans enregistrer ni appliquer la nouvelle configuration réseau.
    - Sélectionnez l'option **10** si vous êtes prêt à appliquer des modifications et à provisionner la nouvelle configuration réseau. Pendant le provisionnement, la sortie affiche l'état des mises à jour, comme indiqué dans l'exemple de sortie suivant :

```
Generating new grid networking description file...

Running provisioning...

Updating grid network configuration on Name
```

11. Si vous avez sélectionné l'option **10** lors de la modification du réseau grille, sélectionnez l'une des options suivantes :
    - **Appliquer** : appliquez les modifications immédiatement et redémarrez automatiquement chaque nœud si nécessaire.

      Si la nouvelle configuration réseau fonctionnera simultanément avec l'ancienne configuration réseau sans aucune modification externe, vous pouvez utiliser l'option **appliquer** pour une modification de configuration entièrement automatisée.

- **Etape** : appliquez les modifications lors du prochain redémarrage des nœuds.

  Si vous devez apporter des modifications de configuration de réseau physique ou virtuel pour que la nouvelle configuration de réseau fonctionne, vous devez utiliser l'option **stage**, arrêter les nœuds affectés, effectuer les modifications de réseau physique nécessaires et redémarrer les nœuds affectés.

  > Si vous utilisez l'option **stage**, redémarrez le nœud dès que possible après l'activation afin de minimiser les interruptions.

- **Annuler**: Ne faites pas de modifications de réseau pour le moment.

  Si vous n'étiez pas conscient que les modifications proposées nécessitent de redémarrer les nœuds, vous pouvez reporter les modifications pour minimiser l'impact sur les utilisateurs. Si vous sélectionnez **annuler**, vous revenez au menu principal et les modifications sont préservés pour pouvoir les appliquer ultérieurement.

Après application ou transfert des modifications, un nouveau progiciel de récupération est généré à la suite de la modification de la configuration de la grille.

12. Si la configuration est interrompue en raison d'erreurs, les options suivantes sont disponibles :
    - Pour mettre fin à la procédure de modification IP et revenir au menu principal, entrez **a**.
    - Pour réessayer l'opération qui a échoué, entrez **r**.
    - Pour passer à l'opération suivante, saisissez **c**.

      L'opération échouée peut être relancée ultérieurement en sélectionnant l'option **10** (appliquer les modifications) dans le menu principal. La procédure de modification IP ne sera pas terminée tant que toutes les opérations n'auront pas été effectuées avec succès.

    - Si vous avez dû intervenir manuellement (pour redémarrer un nœud, par exemple) et que l'action que l'outil pense avoir échoué a été réellement terminée, entrez **f** pour la marquer comme réussie et passer à l'opération suivante.
13. Téléchargez un nouveau package de récupération depuis Grid Manager.
    a. Sélectionnez **MAINTENANCE** > **système** > **progiciel de récupération**.
    b. Saisissez la phrase secrète pour le provisionnement.

    > Le fichier du progiciel de récupération doit être sécurisé car il contient des clés de cryptage et des mots de passe qui peuvent être utilisés pour obtenir des données du système StorageGRID.

Modifiez les adresses IP de tous les nœuds de la grille

Si vous devez modifier l'adresse IP du réseau Grid pour tous les nœuds de la grille, vous devez suivre cette procédure spéciale. Vous ne pouvez pas modifier l'adresse IP d'un réseau Grid Network à l'échelle de la grille en utilisant la procédure de modification de nœuds individuels.

Avant de commencer

- Vous avez le `Passwords.txt` fichier.

Pour vous assurer que la grille démarre correctement, vous devez effectuer toutes les modifications en même temps.

> Cette procédure s'applique uniquement au réseau Grid. Vous ne pouvez pas utiliser cette procédure pour modifier les adresses IP sur les réseaux Admin ou client.

Si vous souhaitez modifier les adresses IP et MTU des nœuds sur un seul site, suivez la "Modifier la configuration réseau du nœud" instructions.

Étapes

1. Planifiez les modifications que vous devez apporter en dehors de l'outil Modifier l'IP, telles que les modifications apportées à DNS ou NTP, et les modifications apportées à la configuration SSO (Single Sign-On), si utilisée.

   > Si les serveurs NTP existants ne sont pas accessibles à la grille sur les nouvelles adresses IP, ajoutez les nouveaux serveurs NTP avant d'effectuer la procédure de modification ip.

   > Si les serveurs DNS existants ne seront pas accessibles à la grille sur les nouvelles adresses IP, ajoutez les nouveaux serveurs DNS avant d'effectuer la procédure de modification ip.

   > Si l'authentification SSO est activée pour votre système StorageGRID et que les approbations des parties utilisatrices ont été configurées à l'aide d'adresses IP de nœud d'administration (au lieu de noms de domaine entièrement qualifiés, selon les recommandations), soyez prêt à mettre à jour ou à reconfigurer ces approbations des parties utilisatrices dans Active Directory Federation Services (AD FS). Immédiatement après la modification des adresses IP. Voir "Configurer l'authentification unique".

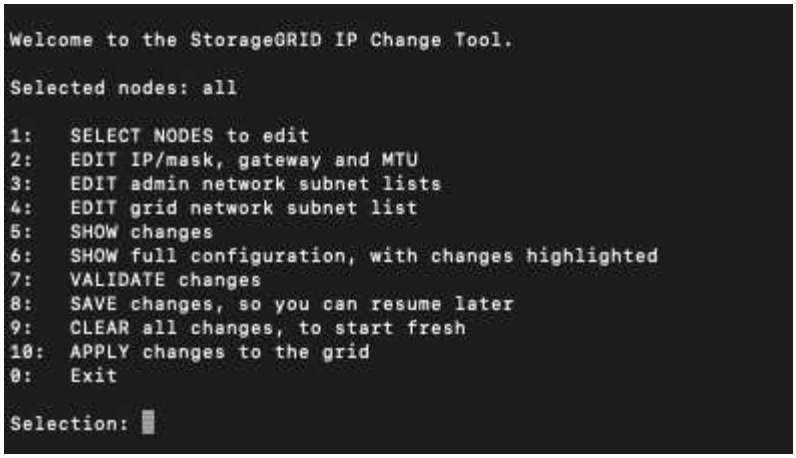
   > Si nécessaire, ajoutez le nouveau sous-réseau pour les nouvelles adresses IP.

2. Connectez-vous au nœud d'administration principal :
   a. Saisissez la commande suivante : `ssh admin@primary_Admin_Node_IP`
   b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
   c. Entrez la commande suivante pour passer à la racine : `su -`
   d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

   Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

3. Lancez l'outil Modifier IP en entrant la commande suivante : `change-ip`
4. Saisissez la phrase de passe de provisionnement à l'invite.

   Le menu principal s'affiche. Par défaut, le `Selected nodes` le champ est défini sur `all`.



5. Dans le menu principal, sélectionnez **2** pour modifier les informations IP/masque de sous-réseau, passerelle et MTU pour tous les nœuds.

   a. Sélectionnez **1** pour modifier le réseau de grille.

      Une fois votre sélection effectuée, l'invite affiche les noms des nœuds, le nom du réseau Grid, le type de données (IP/masque, passerelle ou MTU), et valeurs actuelles.

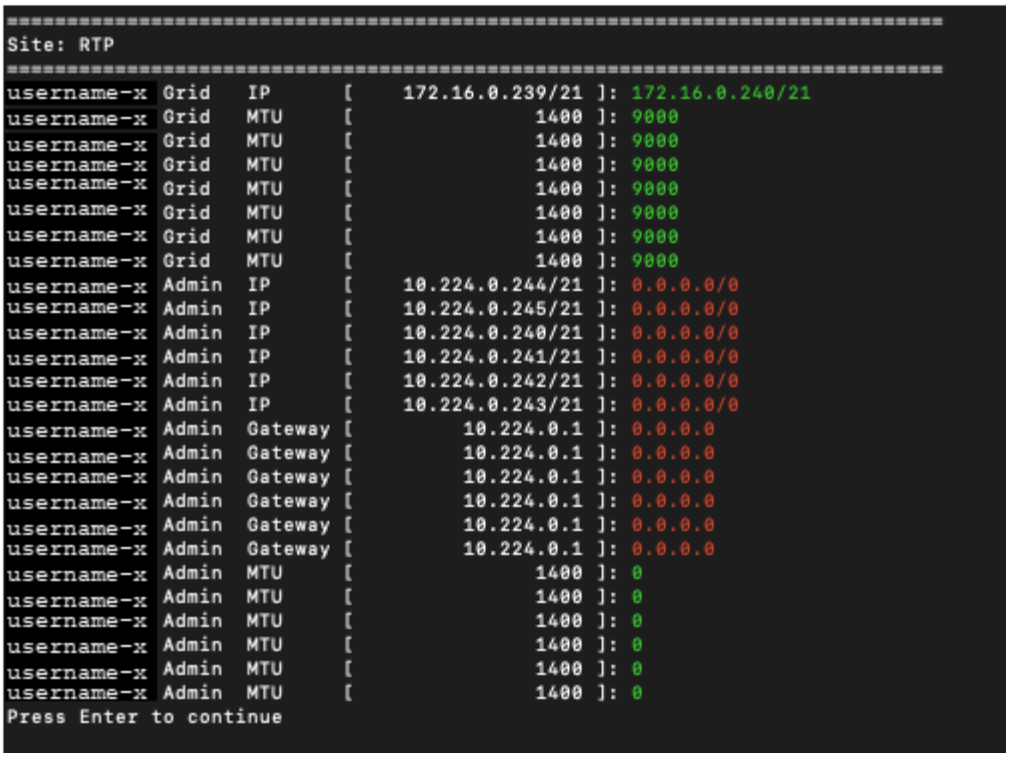
      La modification de l'adresse IP, de la longueur du préfixe, de la passerelle ou de la MTU d'une interface configurée par DHCP changera l'interface en mode statique. Un avertissement s'affiche avant chaque interface configurée par DHCP.

   Interfaces configurées en tant que `fixed` ne peut pas être modifié.

   a. Pour définir une nouvelle valeur, saisissez-la dans le format indiqué pour la valeur actuelle.
   b. Après avoir modifié tous les noeuds que vous souhaitez modifier, entrez **q** pour revenir au menu principal.

      Vos modifications sont conservées jusqu'à ce qu'elles soient supprimées ou appliquées.

6. Vérifiez vos modifications en sélectionnant l'une des options suivantes :
   - **5** : affiche les modifications dans la sortie isolées pour afficher uniquement l'élément modifié. Les modifications sont mises en évidence en vert (ajouts) ou en rouge (suppressions), comme indiqué dans l'exemple de sortie :



- **6** : affiche les modifications en sortie qui affichent la configuration complète. Les modifications sont mises en surbrillance en vert (ajouts) ou en rouge (suppressions).

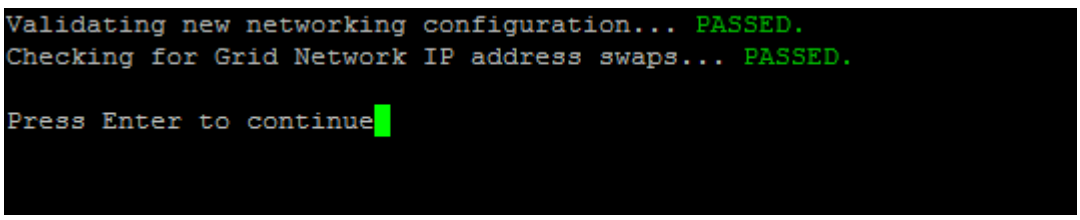
> Certaines interfaces de ligne de commande peuvent afficher des ajouts et des suppressions en utilisant le formatage barré. L'affichage correct dépend de votre client terminal prenant en charge les séquences d'échappement VT100 nécessaires.

7. Sélectionnez l'option **7** pour valider toutes les modifications.

   Cette validation garantit que les règles du réseau Grid, telles que l'absence de sous-réseaux se chevauchant, ne sont pas violées.

   Dans cet exemple, la validation a renvoyé des erreurs.

   Dans cet exemple, la validation a réussi.



8. Une fois la validation terminée, sélectionnez **10** pour appliquer la nouvelle configuration réseau.
9. Sélectionnez **stage** pour appliquer les modifications lors du prochain redémarrage des nœuds.

> Vous devez sélectionner **étape**. N'effectuez pas de redémarrage en roulant, soit manuellement, soit en sélectionnant **Apply** au lieu de **stage** ; la grille ne démarrera pas correctement.

10. Une fois vos modifications terminées, sélectionnez **0** pour quitter l'outil Modifier IP.
11. Arrêtez tous les nœuds simultanément.

> L'ensemble de la grille doit être arrêté en une seule fois, de sorte que tous les nœuds soient arrêtés en même temps.

12. Apportez les modifications nécessaires au réseau physique ou virtuel.
13. Vérifiez que tous les nœuds de la grille ne fonctionnent pas.
14. Mettez tous les nœuds sous tension.
15. Une fois le démarrage de la grille réussi :
    a. Si vous avez ajouté des nouveaux serveurs NTP, supprimez les anciennes valeurs de serveur NTP.
    b. Si vous avez ajouté des serveurs DNS, supprimez les anciennes valeurs du serveur DNS.
16. Téléchargez le nouveau package de récupération depuis Grid Manager.
    a. Sélectionnez **MAINTENANCE** > **système** > **progiciel de récupération**.
    b. Saisissez la phrase secrète pour le provisionnement.

Informations associées

- "Ajouter ou modifier des listes de sous-réseaux sur le réseau Grid"
- "Arrêter le nœud de la grille"

Ajoute des interfaces au nœud existant

Linux : ajoutez des interfaces Admin ou client à un nœud existant

Procédez comme suit pour ajouter une interface sur le réseau Admin ou le réseau client à un nœud Linux après l'avoir installé.

Si vous n'avez pas configuré ADMIN_NETWORK_TARGET ni CLIENT_NETWORK_TARGET dans le fichier de configuration du nœud sur l'hôte Linux au cours de l'installation, utilisez cette procédure pour ajouter l'interface. Pour plus d'informations sur le fichier de configuration des nœuds, reportez-vous aux instructions de votre système d'exploitation Linux :

- "Installez Red Hat Enterprise Linux ou CentOS"
- "Installez Ubuntu ou Debian"

Cette procédure est effectuée sur le serveur Linux hébergeant le nœud nécessitant la nouvelle affectation de réseau, et non à l'intérieur du nœud. Cette procédure ajoute uniquement l'interface au nœud. Une erreur de validation se produit si vous tentez de spécifier d'autres paramètres réseau.

Pour fournir des informations d'adressage, vous devez utiliser l'outil Modifier IP. Voir "Modifier la configuration

réseau du nœud".

Étapes

1. Connectez-vous au serveur Linux hébergeant le nœud.
2. Modifiez le fichier de configuration de nœud : `/etc/storagegrid/nodes/node-name.conf`.

   Ne spécifiez aucun autre paramètre réseau, sinon une erreur de validation se produit.

   a. Ajouter une entrée pour la nouvelle cible réseau. Par exemple :

      ```
      CLIENT_NETWORK_TARGET = bond0.3206
      ```

   b. Facultatif : ajoutez une entrée pour l'adresse MAC. Par exemple :

      ```
      CLIENT_NETWORK_MAC = aa:57:61:07:ea:5c
      ```

3. Lancer la commande node validate :

   ```
   sudo storagegrid node validate node-name
   ```

4. Résoudre toutes les erreurs de validation.
5. Lancer la commande node reload :

   ```
   sudo storagegrid node reload node-name
   ```

Linux : ajoutez une jonction ou des interfaces d'accès à un nœud

Vous pouvez ajouter une jonction ou des interfaces d'accès supplémentaires à un nœud Linux après l'avoir installé. Les interfaces que vous ajoutez s'affichent sur la page des interfaces VLAN et sur la page des groupes haute disponibilité.

Avant de commencer

- Vous avez accès aux instructions d'installation de StorageGRID sur votre plate-forme Linux.
  - "Installez Red Hat Enterprise Linux ou CentOS"
  - "Installez Ubuntu ou Debian"
- Vous avez le `Passwords.txt` fichier.
- Vous disposez d'autorisations d'accès spécifiques.

N'essayez pas d'ajouter des interfaces à un nœud pendant qu'une mise à niveau logicielle, une procédure de restauration ou une procédure d'extension est active.

Description de la tâche

Procédez comme suit pour ajouter une ou plusieurs interfaces supplémentaires à un nœud Linux après l'installation du nœud. Par exemple, vous pouvez ajouter une interface de jonction à un noeud d'administration ou de passerelle, de sorte que vous pouvez utiliser des interfaces VLAN pour isoler le trafic appartenant à différentes applications ou locataires. Vous pouvez également ajouter une interface d'accès à utiliser au sein d'un groupe de haute disponibilité (HA).

Si vous ajoutez une interface de jonction, vous devez configurer une interface VLAN dans StorageGRID. Si

vous ajoutez une interface d'accès, vous pouvez l'ajouter directement à un groupe haute disponibilité ; il n'est pas nécessaire de configurer une interface VLAN.

Le nœud est indisponible durant une brève ajout d'interfaces. Vous devez effectuer cette procédure sur un nœud à la fois.

Étapes

1. Connectez-vous au serveur Linux hébergeant le nœud.
2. À l'aide d'un éditeur de texte tel que vim ou pico, modifiez le fichier de configuration du nœud :

   `/etc/storagegrid/nodes/node-name.conf`

3. Ajoutez une entrée au fichier pour spécifier le nom et, éventuellement, la description de chaque interface supplémentaire que vous souhaitez ajouter au nœud. Utilisez ce format.

   `INTERFACE_TARGET_nnnn=value`

   Pour *nnnn*, spécifiez un numéro unique pour chaque `INTERFACE_TARGET` entrée que vous ajoutez.

   Pour *value*, spécifiez le nom de l'interface physique sur l'hôte bare-Metal. Ensuite, si vous le souhaitez, ajoutez une virgule et fournissez une description de l'interface, qui s'affiche sur la page des interfaces VLAN et sur la page des groupes haute disponibilité.

   Par exemple :

   `INTERFACE_TARGET_0001=ens256, Trunk`

   > Ne spécifiez aucun autre paramètre réseau, sinon une erreur de validation se produit.

4. Exécutez la commande suivante pour valider vos modifications dans le fichier de configuration du nœud :

   `sudo storagegrid node validate node-name`

   Traitez les erreurs ou les avertissements avant de passer à l'étape suivante.

5. Exécutez la commande suivante pour mettre à jour la configuration du nœud :

   `sudo storagegrid node reload node-name`

Une fois que vous avez terminé

- Si vous avez ajouté une ou plusieurs interfaces de jonction, accédez à "Configurez les interfaces VLAN" Pour configurer une ou plusieurs interfaces VLAN pour chaque nouvelle interface parent.
- Si vous avez ajouté une ou plusieurs interfaces d'accès, rendez-vous sur "configurez les groupes haute disponibilité" Pour ajouter les nouvelles interfaces directement aux groupes haute disponibilité.

VMware : ajoutez du jonction ou des interfaces d'accès à un nœud

Une fois le nœud installé, vous pouvez ajouter une jonction ou une interface d'accès à un nœud de machine virtuelle. Les interfaces que vous ajoutez s'affichent sur la page des interfaces VLAN et sur la page des groupes haute disponibilité.

Avant de commencer

- Vous avez accès aux instructions pour "Installation de StorageGRID sur votre plate-forme VMware".
- Vous disposez des machines virtuelles VMware des nœuds d'administration et des nœuds de passerelle.
- Vous disposez d'un sous-réseau réseau qui n'est pas utilisé comme réseau, administrateur ou réseau client.
- Vous avez le `Passwords.txt` fichier.
- Vous disposez d'autorisations d'accès spécifiques.

> N'essayez pas d'ajouter des interfaces à un nœud pendant qu'une mise à niveau logicielle, une procédure de restauration ou une procédure d'extension est active.

Description de la tâche

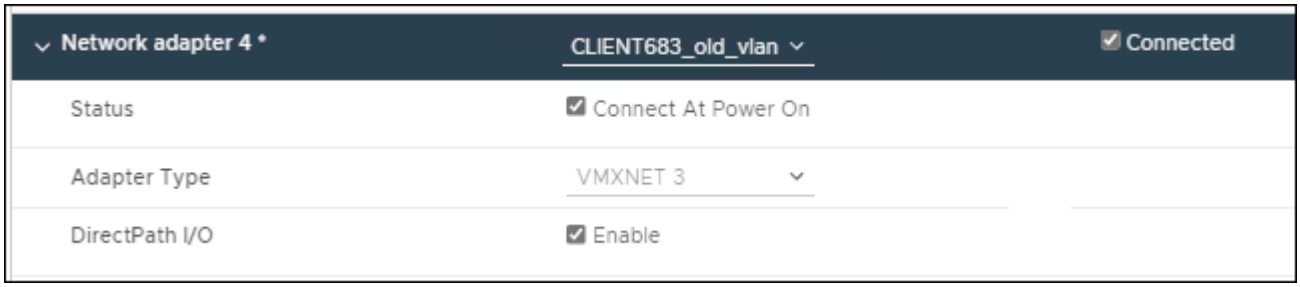
Procédez comme suit pour ajouter une ou plusieurs interfaces supplémentaires à un nœud VMware après l'installation du nœud. Par exemple, vous pouvez ajouter une interface de jonction à un noeud d'administration ou de passerelle, de sorte que vous pouvez utiliser des interfaces VLAN pour isoler le trafic appartenant à différentes applications ou locataires. Vous pouvez également ajouter une interface d'accès à utiliser au sein d'un groupe de haute disponibilité (HA).

Si vous ajoutez une interface de jonction, vous devez configurer une interface VLAN dans StorageGRID. Si vous ajoutez une interface d'accès, vous pouvez l'ajouter directement à un groupe haute disponibilité ; il n'est pas nécessaire de configurer une interface VLAN.

Le nœud peut être indisponible durant une courte période lors de l'ajout d'interfaces.

Étapes

1. Dans vCenter, ajoutez une nouvelle carte réseau (de type VMXNET3) à un nœud d'administration et à une machine virtuelle de nœud de passerelle. Cochez les cases **connecté** et **se connecter à la mise sous tension**.



2. Utilisez SSH pour vous connecter au nœud d'administration ou au nœud de passerelle.
3. Utiliser `ip link show` pour confirmer la détection de la nouvelle interface réseau en256.

```
ip link show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode
DEFAULT group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1400 qdisc mq state UP mode
DEFAULT group default qlen 1000
    link/ether 00:50:56:a0:4e:5b brd ff:ff:ff:ff:ff:ff
3: eth1: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN mode DEFAULT
group default qlen 1000
    link/ether 00:50:56:a0:fa:ce brd ff:ff:ff:ff:ff:ff
4: eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1400 qdisc mq state UP mode
DEFAULT group default qlen 1000
    link/ether 00:50:56:a0:d6:87 brd ff:ff:ff:ff:ff:ff
5: ens256: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq master
ens256vrf state UP mode DEFAULT group default qlen 1000
    link/ether 00:50:56:a0:ea:88 brd ff:ff:ff:ff:ff:ff
```

Une fois que vous avez terminé

- Si vous avez ajouté une ou plusieurs interfaces de jonction, accédez à "Configurez les interfaces VLAN" Pour configurer une ou plusieurs interfaces VLAN pour chaque nouvelle interface parent.
- Si vous avez ajouté une ou plusieurs interfaces d'accès, rendez-vous sur "configurez les groupes haute disponibilité" Pour ajouter les nouvelles interfaces directement aux groupes haute disponibilité.

Configuration des serveurs DNS

Vous pouvez ajouter, mettre à jour et supprimer des serveurs DNS, de sorte que vous puissiez utiliser des noms d'hôte de nom de domaine complet (FQDN) plutôt que des adresses IP.

Pour utiliser des noms de domaine complets (FQDN) au lieu d'adresses IP lorsque vous spécifiez des noms d'hôte pour des destinations externes, spécifiez l'adresse IP de chaque serveur DNS que vous utiliserez. Ces entrées sont utilisées pour AutoSupport, les e-mails d'alerte, les notifications SNMP, les terminaux des services de plateforme, les pools de stockage cloud, et bien plus encore.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous avez le "Maintenance ou autorisation d'accès racine".
- Vous disposez des adresses IP des serveurs DNS à configurer.

Description de la tâche

Pour garantir un fonctionnement correct, spécifiez deux ou trois serveurs DNS. Si vous spécifiez plus de trois, il est possible que seulement trois soient utilisés en raison des limitations connues du système d'exploitation sur certaines plates-formes. Si vous avez des restrictions de routage dans votre environnement, vous pouvez le faire "Personnaliser la liste des serveurs DNS" Pour les nœuds individuels (généralement tous les nœuds d'un site) d'utiliser un ensemble différent de trois serveurs DNS.

Si possible, utilisez des serveurs DNS auxquels chaque site peut accéder localement pour vous assurer qu'un

site isdébarqué peut résoudre les FQDN pour les destinations externes.

Ajouter un serveur DNS

Procédez comme suit pour ajouter un serveur DNS.

Étapes

1. Sélectionnez **MAINTENANCE** > **réseau** > **serveurs DNS**.
2. Sélectionnez **Ajouter un autre serveur** pour ajouter un serveur DNS.
3. Sélectionnez **Enregistrer**.

Modifier un serveur DNS

Procédez comme suit pour modifier un serveur DNS.

Étapes

1. Sélectionnez **MAINTENANCE** > **réseau** > **serveurs DNS**.
2. Sélectionnez l'adresse IP du nom du serveur que vous souhaitez modifier et apportez les modifications nécessaires.
3. Sélectionnez **Enregistrer**.

Supprimer un serveur DNS

Procédez comme suit pour supprimer une adresse IP d'un serveur DNS.

Étapes

1. Sélectionnez **MAINTENANCE** > **réseau** > **serveurs DNS**.
2. Sélectionnez l'icône de suppression ✕ En regard de l'adresse IP.
3. Sélectionnez **Enregistrer**.

Modifiez la configuration DNS pour un nœud de grid unique

Plutôt que de configurer le DNS globalement pour l'ensemble du déploiement, vous pouvez exécuter un script pour configurer le DNS différemment pour chaque nœud de grille.

En général, vous devez utiliser l'option **MAINTENANCE** > **réseau** > **serveurs DNS** du gestionnaire de grille pour configurer les serveurs DNS. N'utilisez le script suivant que si vous avez besoin d'utiliser différents serveurs DNS pour différents nœuds de grille.

Étapes

1. Connectez-vous au nœud d'administration principal :
   a. Saisissez la commande suivante : `ssh admin@primary_Admin_Node_IP`
   b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
   c. Entrez la commande suivante pour passer à la racine : `su -`
   d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

      Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

e. Ajoutez la clé privée SSH à l'agent SSH. Entrez : `ssh-add`

f. Entrez le mot de passe d'accès SSH répertorié dans le `Passwords.txt` fichier.

2. Connectez-vous au nœud que vous souhaitez mettre à jour avec une configuration DNS personnalisée : `ssh node_IP_address`

3. Exécutez le script de configuration DNS : `setup_resolv.rb.`

Le script répond avec la liste des commandes prises en charge.

```
Tool to modify external name servers

available commands:
  add search <domain>
               add a specified domain to search list
               e.g.> add search netapp.com
  remove search <domain>
               remove a specified domain from list
               e.g.> remove search netapp.com
  add nameserver <ip>
               add a specified IP address to the name server list
               e.g.> add nameserver 192.0.2.65
  remove nameserver <ip>
               remove a specified IP address from list
               e.g.> remove nameserver 192.0.2.65
  remove nameserver all
               remove all nameservers from list
  save         write configuration to disk and quit
  abort        quit without saving changes
  help         display this help message


Current list of name servers:
    192.0.2.64
Name servers inherited from global DNS configuration:
    192.0.2.126
    192.0.2.127
Current list of search entries:
    netapp.com

Enter command [`add search <domain>|remove search <domain>|add
nameserver <ip>`]
              [`remove nameserver <ip>|remove nameserver
all|save|abort|help`]
```

4. Ajoutez l'adresse IPv4 d'un serveur qui fournit un service de nom de domaine pour votre réseau : `add <nameserver IP_address>`

5. Répétez le `add nameserver` commande permettant d'ajouter des serveurs de noms.
6. Suivez les instructions qui vous sont demandées pour d'autres commandes.
7. Enregistrez vos modifications et quittez l'application : `save`
8. Fermez le shell de commande sur le serveur : `exit`
9. Répétez les étapes à partir de pour chaque nœud de la grille connectez-vous au nœud à fermeture du shell de commande.
10. Lorsque vous n'avez plus besoin d'un accès sans mot de passe à d'autres serveurs, supprimez la clé privée de l'agent SSH. Entrez : `ssh-add -D`

Gérer les serveurs NTP

Vous pouvez ajouter, mettre à jour ou supprimer des serveurs NTP (Network Time Protocol) pour vous assurer que les données sont synchronisées avec précision entre les nœuds de grid de votre système StorageGRID.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous avez le "Maintenance ou autorisation d'accès racine".
- Vous avez la phrase secrète pour le provisionnement.
- Vous disposez des adresses IPv4 des serveurs NTP à configurer.

Comment StorageGRID utilise-t-il le protocole NTP

Le système StorageGRID utilise le protocole NTP (Network Time Protocol) pour synchroniser l'heure entre tous les nœuds de la grille.

Le rôle NTP principal est attribué à chaque site au moins deux nœuds du système StorageGRID. Ils se synchronisent avec un minimum suggéré de quatre et un maximum de six sources de temps externes et entre elles. Chaque nœud du système StorageGRID qui n'est pas un nœud NTP principal agit comme un client NTP et se synchronise avec ces nœuds NTP primaires.

Les serveurs NTP externes se connectent aux nœuds auxquels vous avez précédemment attribué des rôles NTP principaux. C'est pourquoi il est recommandé de spécifier au moins deux nœuds avec des rôles NTP principaux.

Instructions relatives au serveur NTP

Suivez ces directives pour vous protéger contre les problèmes de synchronisation :

- Les serveurs NTP externes se connectent aux nœuds auxquels vous avez précédemment attribué des rôles NTP principaux. C'est pourquoi il est recommandé de spécifier au moins deux nœuds avec des rôles NTP principaux.
- Assurez-vous qu'au moins deux nœuds sur chaque site peuvent accéder à au moins quatre sources NTP externes. Si un seul nœud d'un site peut atteindre les sources NTP, des problèmes de synchronisation surviennent en cas de panne de ce nœud. En outre, la désignation de deux nœuds par site en tant que sources NTP principales assure une synchronisation précise si un site est isolé du reste de la grille.
- Les serveurs NTP externes spécifiés doivent utiliser le protocole NTP. Vous devez spécifier les références de serveur NTP de Stratum 3 ou mieux pour éviter les problèmes de dérive du temps.

Lorsque vous spécifiez la source NTP externe pour une installation StorageGRID de niveau production, n'utilisez pas le service heure Windows (W32Time) sur une version de Windows antérieure à Windows Server 2016. Le service de temps sur les versions antérieures de Windows n'est pas suffisamment précis et n'est pas pris en charge par Microsoft pour une utilisation dans des environnements de haute précision, y compris StorageGRID. Pour plus de détails, voir "Limite de prise en charge pour configurer le service de temps Windows pour des environnements de haute précision".

Configurer des serveurs NTP

Procédez comme suit pour ajouter, mettre à jour ou supprimer des serveurs NTP.

Étapes

1. Sélectionnez **MAINTENANCE** > **réseau** > **serveurs NTP**.
2. Dans la section serveurs, ajoutez, mettez à jour ou supprimez des entrées de serveur NTP, si nécessaire.

   Vous devez inclure au moins quatre serveurs NTP et vous pouvez spécifier jusqu'à six serveurs.

3. Entrez la phrase de passe de provisionnement pour votre système StorageGRID, puis sélectionnez **Enregistrer**.

   La page est désactivée jusqu'à ce que les mises à jour de la configuration soient terminées.

   Si tous vos serveurs NTP échouent au test de connexion après l'enregistrement des nouveaux serveurs NTP, ne poursuivez pas. Contactez l'assistance technique.

Résoudre les problèmes de serveur NTP

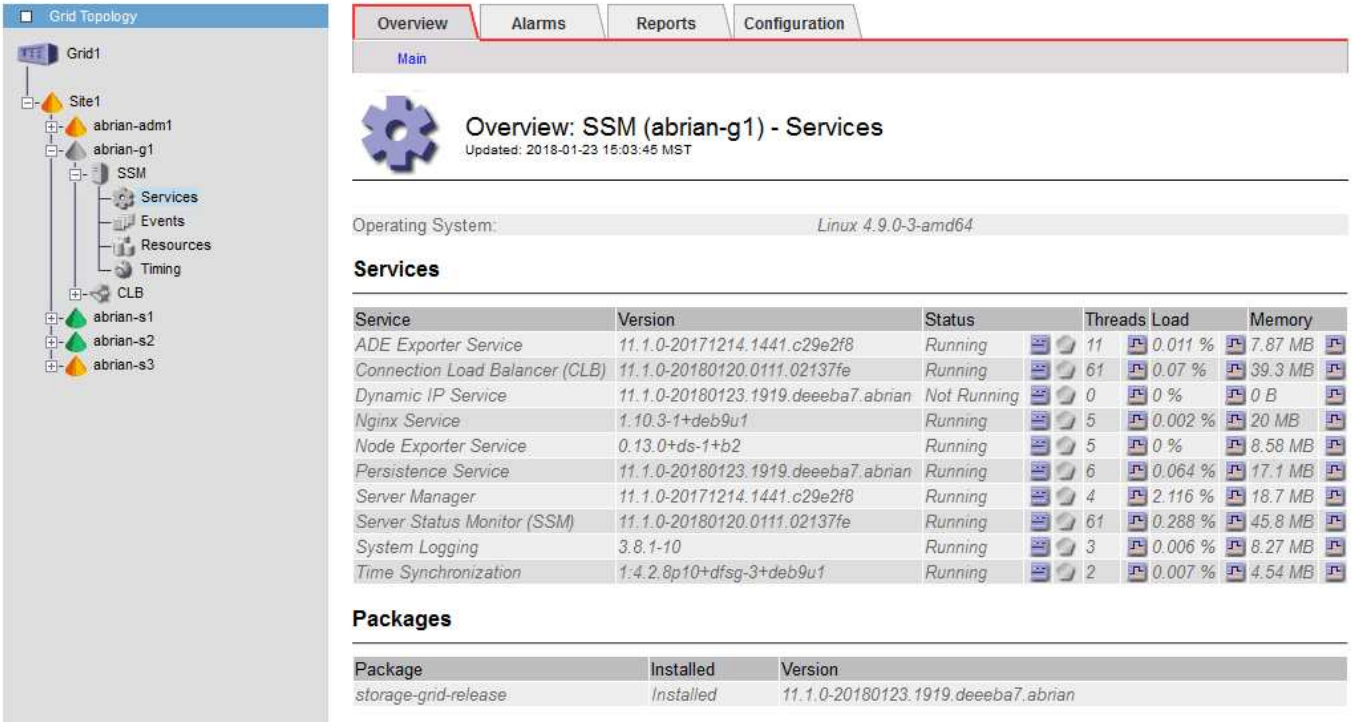
Si vous rencontrez des problèmes de stabilité ou de disponibilité des serveurs NTP initialement spécifiés lors de l'installation, vous pouvez mettre à jour la liste des sources NTP externes que le système StorageGRID utilise en ajoutant des serveurs supplémentaires ou en mettant à jour ou en supprimant des serveurs existants.

Restaurez la connectivité réseau pour les nœuds isolés

Dans certaines circonstances, comme des modifications d'adresse IP à l'échelle du site ou de la grille, il est possible qu'un ou plusieurs groupes de nœuds ne soient pas en mesure de contacter le reste de la grille.

Description de la tâche

Dans le Gestionnaire de grille (**SUPPORT** > **Tools** > **Grid topology**), si un nœud est gris, ou si un nœud est bleu et que plusieurs de ses services affichent un état autre que l'exécution, vous devez vérifier l'isolement du nœud.



L'existence de nœuds isolés entraîne notamment les conséquences suivantes :

- Si plusieurs nœuds sont isolés, il se peut que vous ne puissiez pas vous connecter à ou accéder à Grid Manager.
- Si plusieurs nœuds sont isolés, les valeurs d'utilisation du stockage et de quota affichées sur le tableau de bord pour le gestionnaire de locataires peuvent être obsolètes. Les totaux seront mis à jour lorsque la connectivité réseau sera restaurée.

Pour résoudre le problème d'isolation, vous exécutez un utilitaire de ligne de commande sur chaque nœud isolé ou sur un nœud d'un groupe (tous les nœuds d'un sous-réseau ne contenant pas le noeud d'administration principal) isolé de la grille. L'utilitaire fournit aux nœuds l'adresse IP d'un nœud non isolé dans la grille, ce qui permet au nœud ou au groupe isolé de nœuds de contacter à nouveau toute la grille.

Si le système de noms de domaine multidiffusion (mDNS) est désactivé sur les réseaux, il se peut que l'utilitaire de ligne de commande soit exécuté sur chaque nœud isolé.

Étapes

1. Accéder au nœud et vérifier `/var/local/log/dynip.log` pour les messages d'isolation.

   Par exemple :

   ```
   [2018-01-09T19:11:00.545] UpdateQueue - WARNING -- Possible isolation,
   no contact with other nodes.
   If this warning persists, manual action might be required.
   ```

   Si vous utilisez la console VMware, un message indiquant que le nœud peut être isolé s'affiche.

   Sur les déploiements Linux, des messages d'isolement apparaîtront dans `/var/log/storagegrid/node/<nodename>.log` fichiers.

2. Si les messages d'isolement sont récurrents et persistants, exécutez la commande suivante :

   `add_node_ip.py <address>`

   où `<address>` Est l'adresse IP d'un nœud distant connecté à la grille.

   ```
   # /usr/sbin/add_node_ip.py  10.224.4.210

   Retrieving local host information
   Validating remote node at address 10.224.4.210
   Sending node IP hint for 10.224.4.210 to local node
   Local node found on remote node. Update complete.
   ```

3. Vérifiez les éléments suivants pour chaque nœud précédemment isolé :
   - Les services du nœud ont démarré.
   - Le statut du service IP dynamique est « en cours d'exécution » après l'exécution du `storagegrid-status` commande.
   - Dans l'arborescence de la topologie de grille, le nœud n'apparaît plus déconnecté du reste de la grille.

> Si vous exécutez le `add_node_ip.py` la commande ne résout pas le problème, d'autres problèmes de mise en réseau peuvent être résolus.

Procédures au niveau de l'hôte et du middleware

Linux : migration du nœud grid vers le nouvel hôte

Vous pouvez migrer un ou plusieurs nœuds StorageGRID d'un hôte Linux (l' *hôte source*) vers un autre hôte Linux (l' *hôte cible*) pour effectuer la maintenance de l'hôte sans affecter les fonctionnalités ou la disponibilité de votre grille.

Par exemple, vous pouvez souhaiter migrer un nœud pour effectuer l'application de correctifs et le redémarrage du système d'exploitation.

Avant de commencer

- Vous avez planifié votre déploiement StorageGRID pour inclure une prise en charge de la migration.
  - "Exigences de migration des conteneurs de nœuds pour Red Hat Enterprise Linux ou CentOS"
  - "Configuration requise pour la migration des conteneurs de nœuds pour Ubuntu ou Debian"
- L'hôte cible est déjà prêt pour l'utilisation de StorageGRID.
- Le stockage partagé est utilisé pour tous les volumes de stockage par nœud
- Les interfaces réseau portent des noms cohérents sur tous les hôtes.

Dans un déploiement de production, n'exécutez pas plus d'un nœud de stockage sur un seul hôte. L'utilisation d'un hôte dédié pour chaque nœud de stockage fournit un domaine de défaillance isolé.

D'autres types de nœuds, tels que les nœuds d'administration ou les nœuds de passerelle, peuvent être déployés sur le même hôte. Toutefois, si vous avez plusieurs nœuds du même type (deux nœuds de passerelle, par exemple), n'installez pas toutes les instances sur le même hôte.

Nœud d'exportation à partir de l'hôte source

Dans un premier temps, arrêtez le nœud grid et exportez-le depuis l'hôte Linux source.

Exécutez les commandes suivantes sur l'hôte *source*.

Étapes

1. Obtenez l'état de tous les nœuds en cours d'exécution sur l'hôte source.

   ```
   sudo storagegrid node status all
   ```

   Exemple de résultat :

   ```
   Name Config-State Run-State
   DC1-ADM1 Configured Running
   DC1-ARC1 Configured Running
   DC1-GW1 Configured Running
   DC1-S1 Configured Running
   DC1-S2 Configured Running
   DC1-S3 Configured Running
   ```

2. Identifiez le nom du nœud que vous souhaitez migrer et arrêtez-le si son état d'exécution est en cours d'exécution.

   ```
   sudo storagegrid node stop DC1-S3
   ```

   Exemple de résultat :

   ```
   Stopping node DC1-S3
   Waiting up to 630 seconds for node shutdown
   ```

3. Exportez le nœud depuis l'hôte source.

   ```
   sudo storagegrid node export DC1-S3
   ```

   Exemple de résultat :

```
Finished exporting node DC1-S3 to /dev/mapper/sgws-dc1-s3-var-local.
Use 'storagegrid node import /dev/mapper/sgws-dc1-s3-var-local' if you
want to import it again.
```

4. Notez le `import` commande suggérée dans la sortie.

   Vous allez exécuter cette commande sur l'hôte cible à l'étape suivante.

Importer le nœud sur l'hôte cible

Après avoir exporté le nœud à partir de l'hôte source, vous importez et validez le nœud sur l'hôte cible. La validation confirme que le nœud a accès aux mêmes périphériques d'interface réseau et de stockage bloc que sur l'hôte source.

Exécutez les commandes suivantes sur l'hôte *cible*.

Étapes

1. Importez le nœud sur l'hôte cible.

   ```
   sudo storagegrid node import /dev/mapper/sgws-dc1-s3-var-local
   ```

   Exemple de résultat :

   ```
   Finished importing node DC1-S3 from /dev/mapper/sgws-dc1-s3-var-local.
   You should run 'storagegrid node validate DC1-S3'
   ```

2. Valider la configuration de nœud sur le nouvel hôte.

   ```
   sudo storagegrid node validate DC1-S3
   ```

   Exemple de résultat :

   ```
   Confirming existence of node DC1-S3... PASSED
   Checking configuration file /etc/storagegrid/nodes/DC1-S3.conf for node
   DC1-S3... PASSED
   Checking for duplication of unique values... PASSED
   ```

3. Si des erreurs de validation se produisent, traitez-les avant de démarrer le nœud migré.

   Pour plus d'informations sur le dépannage, reportez-vous aux instructions d'installation de StorageGRID pour votre système d'exploitation Linux.

   - "Installez Red Hat Enterprise Linux ou CentOS"
   - "Installez Ubuntu ou Debian"

Démarrer le nœud migré

Après avoir validé le nœud migré, vous démarrez le nœud en exécutant une commande sur l'hôte *cible*.

Étapes

1. Démarrez le nœud sur le nouvel hôte.

   ```
   sudo storagegrid node start DC1-S3
   ```

2. Connectez-vous au Gestionnaire de grille et vérifiez que l'état du nœud est vert sans alerte.

   > La vérification de l'état du nœud est verte garantit que le nœud migré a redémarré et rejoint la grille. Si l'état n'est pas vert, ne migrez pas les nœuds supplémentaires pour que vous n'ayez plus d'un nœud hors service.

3. Si vous ne parvenez pas à accéder au Grid Manager, attendez 10 minutes, puis exécutez la commande suivante :

   ```
   sudo storagegrid node status _node-name
   ```

   Vérifiez que l'état d'exécution du nœud migré est défini sur en cours d'exécution.

Maintenance du nœud d'archivage pour le middleware TSM

Les nœuds d'archivage peuvent être configurés pour cibler les bandes via un serveur middleware TSM ou le cloud via l'API S3. Une fois configuré, la cible d'un nœud d'archivage ne peut pas être modifiée.

Si le serveur hébergeant le nœud d'archivage échoue, remplacez le serveur et suivez la procédure de récupération appropriée.

Défaut avec les dispositifs de stockage d'archives

Si vous déterminez qu'il y a une erreur au niveau de l'unité de stockage d'archivage à laquelle le nœud d'archivage accède via Tivoli Storage Manager (TSM), mettez le nœud d'archivage hors ligne pour limiter le nombre d'alarmes affichées dans le système StorageGRID. Vous pouvez ensuite utiliser les outils d'administration du serveur TSM ou du périphérique de stockage, ou les deux, pour diagnostiquer et résoudre davantage le problème.

Mettez le composant cible hors ligne

Avant d'entreprendre toute maintenance du serveur middleware TSM pouvant entraîner l'indisponibilité du nœud d'archivage, mettez le composant cible hors ligne pour limiter le nombre d'alarmes déclenchées si le serveur middleware TSM devient indisponible.

Avant de commencer

Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".

Étapes

1. Sélectionnez **SUPPORT** > **Outils** > **topologie de grille**.
2. Sélectionnez **nœud d'archivage** > **ARC** > **cible** > **Configuration** > **principal**.

3. Définissez la valeur de l'état de Tivoli Storage Manager sur **hors ligne**, puis cliquez sur **appliquer les modifications**.
4. Une fois la maintenance terminée, définissez la valeur de l'état de Tivoli Storage Manager sur **Online**, puis cliquez sur **appliquer les modifications**.

Outils d'administration Tivoli Storage Manager

L'outil dsmadmc est la console d'administration du serveur middleware TSM installé sur le nœud d'archivage. Vous pouvez accéder à l'outil en tapant `dsmadmc` sur la ligne de commande du serveur. Connectez-vous à la console d'administration en utilisant le même nom d'utilisateur et mot de passe d'administration que celui configuré pour le service ARC.

Le `tsmquery.rb` le script a été créé pour générer des informations d'état à partir de dsmadmc sous une forme plus lisible. Vous pouvez exécuter ce script en entrant la commande suivante sur la ligne de commande du nœud d'archivage : `/usr/local/arc/tsmquery.rb status`

Pour plus d'informations sur la console d'administration TSM dsmadmc, reportez-vous à la section *Tivoli Storage Manager for Linux: Administrator's Reference*.

Objet définitivement indisponible

Lorsque le nœud d'archivage demande un objet à partir du serveur Tivoli Storage Manager (TSM) et que la récupération échoue, le nœud d'archivage redemande la requête après un intervalle de 10 secondes. Si l'objet est définitivement indisponible (par exemple, parce que l'objet est corrompu sur bande), l'API TSM n'a aucun moyen de l'indiquer au nœud d'archivage, de sorte que le nœud d'archivage continue à réessayer la requête.

Lorsque cette situation se produit, une alarme se déclenche et la valeur continue d'augmenter. Pour voir l'alarme, sélectionnez **SUPPORT** > **Tools** > **Grid topology**. Ensuite, sélectionnez **nœud d'archivage** > **ARC** > **récupérer** > **échecs de la demande**.

Si l'objet est définitivement indisponible, vous devez identifier l'objet et annuler manuellement la demande du nœud d'archivage, comme décrit dans la procédure, Déterminer si les objets sont définitivement indisponibles.

Une récupération peut également échouer si l'objet est temporairement indisponible. Dans ce cas, les demandes de récupération suivantes devraient aboutir.

Si le système StorageGRID est configuré pour utiliser une règle ILM qui crée une copie d'objet unique et que cette copie ne peut pas être récupérée, l'objet est perdu et ne peut pas être restauré. Cependant, vous devez suivre la procédure pour déterminer si l'objet est définitivement indisponible pour « nettoyer » le système StorageGRID, pour annuler la demande du nœud d'archivage et pour purger les métadonnées de l'objet perdu.

Déterminer si les objets sont définitivement indisponibles

Vous pouvez déterminer si des objets sont définitivement indisponibles en effectuant une demande à l'aide de la console administrative TSM.

Avant de commencer

- Vous disposez d'autorisations d'accès spécifiques.
- Vous avez le `Passwords.txt` fichier.
- Vous disposez de l'adresse IP d'un nœud d'administration.

Description de la tâche

Cet exemple est fourni à titre d'information. Cette procédure ne peut pas vous aider à identifier toutes les défaillances susceptibles d'entraîner l'indisponibilité d'objets ou de volumes de bande. Pour plus d'informations sur l'administration TSM, reportez-vous à la documentation du serveur TSM.

Étapes

1. Connectez-vous à un nœud d'administration :
   a. Saisissez la commande suivante : `ssh admin@Admin_Node_IP`
   b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
2. Identifiez le ou les objets qui n'ont pas pu être récupérés par le nœud d'archivage :
   a. Accédez au répertoire contenant les fichiers journaux d'audit : `cd /var/local/audit/export`

      Le fichier journal d'audit actif est nommé audit.log. Une fois par jour, le actif `audit.log` le fichier est enregistré et un nouveau `audit.log` le fichier est démarré. Le nom du fichier enregistré indique quand il a été enregistré, au format `yyyy-mm-dd.txt`. Après un jour, le fichier enregistré est compressé et renommé, au format `yyyy-mm-dd.txt.gz`, qui conserve la date originale.

   b. Recherchez dans le fichier journal d'audit correspondant des messages indiquant qu'un objet archivé n'a pas pu être récupéré. Par exemple, entrez : `grep ARCE audit.log | less -n`

      Lorsqu'un objet ne peut pas être récupéré à partir d'un nœud d'archivage, le message d'audit ARCE (fin de la récupération de l'objet d'archive) affiche ARUN (middleware d'archive indisponible) ou une erreur générale dans le champ résultat. La ligne d'exemple suivante du journal d'audit montre que le message ARCE s'est terminé avec le résultat ARUN pour CBID 498D8A1F681F05B3.

      ```
      [AUDT:[CBID(UI64):0x498D8A1F681F05B3][VLID(UI64):□20091127][RSLT(FC32
      ):ARUN][AVER(UI32):7]
      [ATIM(UI64):1350613602969243][ATYP(FC32):ARCE][ANID(UI32):13959984][A
      MID(FC32):ARCI]
      [ATID(UI64):4560349751312520631]]
      ```

      Pour plus d'informations, reportez-vous aux instructions relatives à la compréhension des messages d'audit.

   c. Enregistrez le CBID de chaque objet ayant subi un échec de demande.

      Vous pouvez également enregistrer les informations supplémentaires suivantes utilisées par TSM pour identifier les objets enregistrés par le nœud d'archivage :

      - **Nom de l'espace fichier** : équivalent à l'ID du nœud d'archivage. Pour trouver l'ID du nœud d'archivage, sélectionnez **SUPPORT** > **Outils** > **topologie de grille**. Ensuite, sélectionnez **nœud d'archivage** > **ARC** > **cible** > **Présentation**.
      - **Nom de niveau élevé** : équivalent à l'ID de volume attribué à l'objet par le noeud d'archivage. L'ID du volume se présente sous la forme d'une date (par exemple, `20091127`), et est enregistré comme VLID de l'objet dans les messages d'audit d'archive.
      - **Nom de niveau bas** : équivalent au CBID attribué à un objet par le système StorageGRID.

   d. Déconnectez-vous du shell de commande : `exit`
3. Vérifiez le serveur TSM pour voir si les objets identifiés à l'étape 2 sont définitivement indisponibles :

a. Connectez-vous à la console d'administration du serveur TSM : `dsmadmc`

   Utilisez le nom d'utilisateur administratif et le mot de passe configurés pour le service ARC. Entrez le nom d'utilisateur et le mot de passe dans Grid Manager. (Pour afficher le nom d'utilisateur, sélectionnez **SUPPORT** > **Tools** > **Grid topology**. Sélectionnez ensuite **nœud d'archivage** > **ARC** > **cible** > **Configuration**.)

b. Déterminez si l'objet est définitivement indisponible.

   Par exemple, vous pouvez rechercher dans le journal d'activités TSM une erreur d'intégrité des données pour cet objet. L'exemple suivant montre une recherche du journal d'activités pour le dernier jour d'un objet avec CBID `498D8A1F681F05B3`.

```
> query actlog begindate=-1 search=276C14E94082CC69
12/21/2008 05:39:15 ANR0548W Retrieve or restore
failed for session 9139359 for node DEV-ARC-20 (Bycast ARC)
processing file space /19130020 4 for file /20081002/
498D8A1F681F05B3 stored as Archive - data
integrity error detected. (SESSION: 9139359)
>
```

   Selon la nature de l'erreur, il se peut que le CBID ne soit pas enregistré dans le journal des activités TSM. Vous devrez peut-être rechercher dans le journal d'autres erreurs TSM au moment de l'échec de la demande.

c. Si une bande entière est définitivement indisponible, identifiez les CBID de tous les objets stockés sur ce volume : `query content TSM_Volume_Name`

   où `TSM_Volume_Name` Est le nom TSM pour la bande indisponible. Voici un exemple de résultat pour cette commande :

```
 > query content TSM-Volume-Name
Node Name     Type Filespace  FSID Client's Name for File Name
------------- ---- ---------- ---- ----------------------------
DEV-ARC-20    Arch /19130020  216  /20081201/ C1D172940E6C7E12
DEV-ARC-20    Arch /19130020  216  /20081201/ F1D7FBC2B4B0779E
```

   Le `Client's Name for File Name` Est identique à l'ID de volume du nœud d'archivage (ou TSM « nom de niveau élevé ») suivi de CBID de l'objet (ou TSM « nom de niveau bas »). C'est, le `Client's Name for File Name` prend la forme `/Archive Node volume ID /CBID`. Sur la première ligne de la sortie d'exemple, le `Client's Name for File Name` est `/20081201/C1D172940E6C7E12`.

   Rappelez-vous également que le `Filespace` Est l'ID de nœud du nœud d'archivage.

Vous aurez besoin du CBID de chaque objet stocké sur le volume et de l'ID de nœud du nœud d'archivage pour annuler la demande de récupération.

4. Pour chaque objet définitivement indisponible, annulez la requête de récupération et émettez une commande pour informer le système StorageGRID de la perte de la copie objet :

> Utilisez la console ADE avec précaution. Si la console n'est pas utilisée correctement, il est possible d'interrompre les opérations du système et de corrompre les données. Saisissez les commandes attentivement et utilisez uniquement les commandes documentées dans cette procédure.

   a. Si vous n'êtes pas déjà connecté au nœud d'archivage, connectez-vous comme suit :
      i. Saisissez la commande suivante : `ssh admin@grid_node_IP`
      ii. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
      iii. Entrez la commande suivante pour passer à la racine : `su -`
      iv. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
   b. Accéder à la console ADE du service ARC : `telnet localhost 1409`
   c. Annuler la demande pour l'objet : `/proc/BRTR/cancel -c CBID`

      où `CBID` Est l'identifiant de l'objet qui ne peut pas être récupéré à partir du TSM.

      Si les seules copies de l'objet sont sur bande, la demande « récupération en bloc » est annulée par un message « 1 requêtes annulées ». Si des copies de l'objet existent ailleurs dans le système, la récupération de l'objet est traitée par un module différent de sorte que la réponse au message est « 0 requêtes annulées ».

   d. Lancer une commande pour informer le système StorageGRID qu'une copie d'objet a été perdue et qu'une copie supplémentaire doit être effectuée : `/proc/CMSI/Object_Lost CBID node_ID`

      où `CBID` Est l'identifiant de l'objet qui ne peut pas être récupéré depuis le serveur TSM, et `node_ID` Est l'ID de nœud du nœud d'archivage où la récupération a échoué.

      Vous devez entrer une commande distincte pour chaque copie d'objet perdue : la saisie d'une plage de CBID n'est pas prise en charge.

      Dans la plupart des cas, le système StorageGRID commence immédiatement à effectuer des copies supplémentaires des données d'objet afin de respecter la règle ILM du système.

      Toutefois, si la règle ILM de l'objet indique qu'une seule copie doit être effectuée et que la copie a été perdue, l'objet ne peut pas être restauré. Dans ce cas, exécutez le `Object_Lost` La commande purge les métadonnées de l'objet perdu du système StorageGRID.

      Lorsque le `Object_Lost` la commande s'exécute correctement, le message suivant est renvoyé :

```
CLOC_LOST_ANS returned result 'SUCS'
```

+

> Le `/proc/CMSI/Object_Lost` La commande n'est valide que pour les objets perdus stockés sur les nœuds d'archivage.

a. Quittez la console ADE : `exit`

b. Déconnectez-vous du nœud d'archivage : `exit`

5. Réinitialisez la valeur des échecs de demande dans le système StorageGRID :

a. Accédez à **Archive Node** > **ARC** > **Retrieve** > **Configuration** et sélectionnez **Reset Request Failure Count**.

b. Cliquez sur **appliquer les modifications**.

Informations associées

"Administrer StorageGRID"

"Examiner les journaux d'audit"

VMware : configurez la machine virtuelle pour un redémarrage automatique

Si la machine virtuelle ne redémarre pas après le redémarrage de l'hyperviseur VMware vSphere, vous devrez peut-être configurer la machine virtuelle pour le redémarrage automatique.

Cette procédure doit être effectuée si vous remarquez qu'une machine virtuelle ne redémarre pas lors de la récupération d'un nœud de la grille ou de l'exécution d'une autre procédure de maintenance.

Étapes

1. Dans l'arborescence du client VMware vSphere, sélectionnez la machine virtuelle qui n'a pas démarré.
2. Cliquez avec le bouton droit de la souris sur la machine virtuelle et sélectionnez **Marche/Arrêt**.
3. Configurez l'hyperviseur VMware vSphere pour redémarrer automatiquement la machine virtuelle à l'avenir.

Procédures des nœuds de la grille

Procédures de nœud de grille : présentation

Vous devrez peut-être effectuer des procédures sur un nœud de grid spécifique. Bien que vous puissiez effectuer quelques-unes de ces procédures à partir de Grid Manager, la plupart des procédures nécessitent d'accéder à Server Manager à partir de la ligne de commande du nœud.

Server Manager s'exécute sur chaque nœud de la grille pour superviser le démarrage et l'arrêt des services et pour s'assurer que les services rejoignent et quittent aisément le système StorageGRID. Server Manager surveille également les services sur chaque nœud de la grille et tente automatiquement de redémarrer les services qui signalent les pannes.

Vous ne devez accéder à Server Manager que si le support technique vous a demandé de le faire.

Vous devez fermer la session de shell de commande en cours et vous déconnecter une fois que vous avez terminé avec Server Manager. Entrez : `exit`

Afficher l'état et la version de Server Manager

Pour chaque nœud de grille, vous pouvez afficher l'état et la version actuels de Server Manager exécuté sur ce nœud de grille. Vous pouvez également obtenir l'état actuel de tous les services exécutés sur ce nœud de grille.

Avant de commencer

Vous avez le `Passwords.txt` fichier.

Étapes

1. Connectez-vous au nœud grid :
   a. Saisissez la commande suivante : `ssh admin@grid_node_IP`
   b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
   c. Entrez la commande suivante pour passer à la racine : `su -`
   d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

   Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

2. Afficher l'état actuel de Server Manager exécuté sur le nœud de la grille : **`service servermanager status`**

   L'état actuel de Server Manager s'exécutant sur le nœud de la grille est signalé (en cours d'exécution ou non). Si l'état de Server Manager est `running`, l'heure à laquelle il a été exécuté depuis son dernier démarrage est indiquée. Par exemple :

   ```
   servermanager running for 1d, 13h, 0m, 30s
   ```

3. Afficher la version actuelle de Server Manager exécutée sur un nœud de grille : **`service servermanager version`**

   La version actuelle est répertoriée. Par exemple :

   ```
   11.1.0-20180425.1905.39c9493
   ```

4. Déconnectez-vous du shell de commande : **`exit`**

Afficher l'état actuel de tous les services

Vous pouvez afficher à tout moment l'état actuel de tous les services s'exécutant sur un nœud de la grille.

Avant de commencer

Vous avez le `Passwords.txt` fichier.

Étapes

1. Connectez-vous au nœud grid :

a. Saisissez la commande suivante : `ssh admin@grid_node_IP`

b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

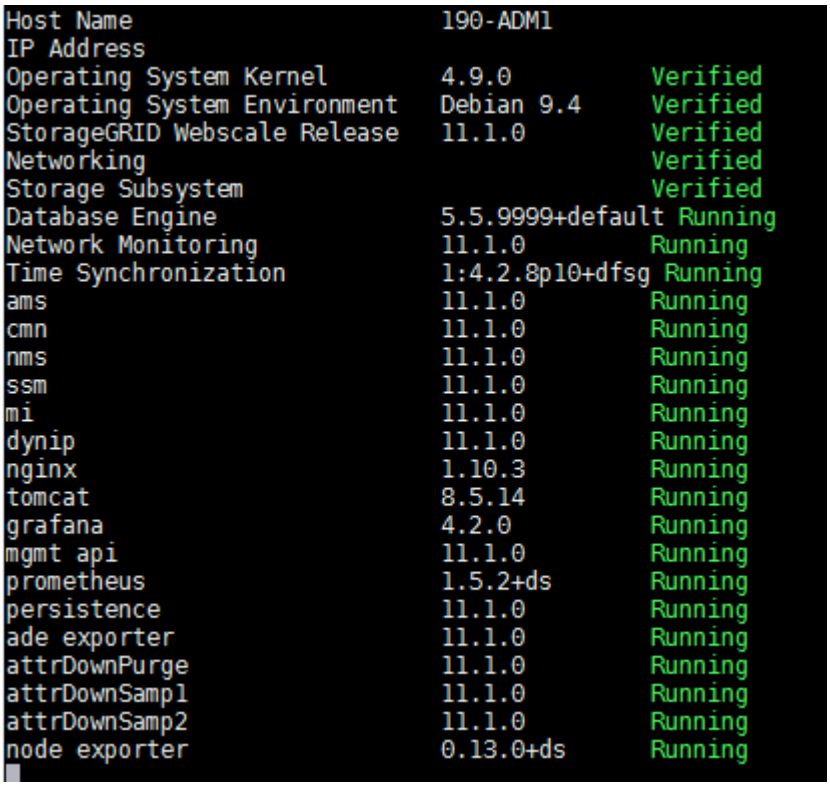
c. Entrez la commande suivante pour passer à la racine : `su -`

d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

2. Afficher l'état de tous les services s'exécutant sur le nœud grid : `storagegrid-status`

   Par exemple, la sortie du nœud d'administration principal indique l'état actuel des services AMS, CMN et NMS en cours d'exécution. Cette sortie est immédiatement mise à jour si l'état d'un service change.



3. Revenez à la ligne de commande, appuyez sur **Ctrl+C**.
4. Vous pouvez également afficher un rapport statique pour tous les services s'exécutant sur le nœud de la grille : `/usr/local/servermanager/reader.rb`

   Ce rapport contient les mêmes informations que le rapport mis à jour en continu, mais il n'est pas mis à jour si l'état d'un service change.

5. Déconnectez-vous du shell de commande : `exit`

Démarrez Server Manager et tous les services

Vous devrez peut-être démarrer Server Manager, qui démarre également tous les services sur le nœud de la grille.

Avant de commencer

Vous avez le `Passwords.txt` fichier.

Description de la tâche

Le démarrage de Server Manager sur un nœud de la grille sur lequel il est déjà en cours d'exécution entraîne le redémarrage de Server Manager et de tous les services sur le nœud de la grille.

Étapes

1. Connectez-vous au nœud grid :
   a. Saisissez la commande suivante : `ssh admin@grid_node_IP`
   b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
   c. Entrez la commande suivante pour passer à la racine : `su -`
   d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

   Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.
2. Démarrez Server Manager : `service servermanager start`
3. Déconnectez-vous du shell de commande : `exit`

Redémarrez Server Manager et tous les services

Vous devrez peut-être redémarrer Server Manager et tous les services s'exécutant sur un nœud de la grille.

Avant de commencer

Vous avez le `Passwords.txt` fichier.

Étapes

1. Connectez-vous au nœud grid :
   a. Saisissez la commande suivante : `ssh admin@grid_node_IP`
   b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
   c. Entrez la commande suivante pour passer à la racine : `su -`
   d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

   Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.
2. Redémarrez Server Manager et tous les services sur le nœud de la grille : `service servermanager restart`

   Server Manager et tous les services du nœud de la grille sont arrêtés, puis redémarrés.

   > ⓘ À l'aide du `restart` la commande est identique à l'utilisation de `stop` suivi de la commande `start` commande.
3. Déconnectez-vous du shell de commande : `exit`

Arrêtez Server Manager et tous les services

Server Manager est conçu pour fonctionner en permanence, mais il peut être nécessaire

d’arrêter Server Manager et tous les services exécutés sur un nœud de grille.

Avant de commencer

Vous avez le `Passwords.txt` fichier.

Étapes

1. Connectez-vous au nœud grid :
   a. Saisissez la commande suivante : `ssh admin@grid_node_IP`
   b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
   c. Entrez la commande suivante pour passer à la racine : `su -`
   d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

   Lorsque vous êtes connecté en tant que root, l’invite passe de `$` à `#`.

2. Arrêter Server Manager et tous les services exécutés sur le noeud grid : `service servermanager stop`

   Server Manager et tous les services exécutés sur le nœud de la grille sont normalement terminés. L’arrêt des services peut prendre jusqu’à 15 minutes.

3. Déconnectez-vous du shell de commande : `exit`

Afficher l’état actuel du service

Vous pouvez afficher à tout moment l’état actuel d’un service exécuté sur un nœud de la grille.

Avant de commencer

Vous avez le `Passwords.txt` fichier.

Étapes

1. Connectez-vous au nœud grid :
   a. Saisissez la commande suivante : `ssh admin@grid_node_IP`
   b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
   c. Entrez la commande suivante pour passer à la racine : `su -`
   d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

   Lorsque vous êtes connecté en tant que root, l’invite passe de `$` à `#`.

2. Afficher l’état actuel d’un service exécuté sur un nœud de grille : `**service *serviceename* status** l’état actuel du service demandé s’exécutant sur le nœud de grille est signalé (en cours d’exécution ou non). Par exemple :

   ```
   cmn running for 1d, 14h, 21m, 2s
   ```

3. Déconnectez-vous du shell de commande : **`exit`**

Arrêtez l'entretien

Certaines procédures de maintenance exigent d'arrêter un seul service tout en maintenant d'autres services sur le nœud de la grille en cours d'exécution. N'arrêtez les services individuels que si vous y êtes invité par une procédure de maintenance.

Avant de commencer

Vous avez le `Passwords.txt` fichier.

Description de la tâche

Lorsque vous utilisez ces étapes pour « arrêter administrativement » un service, Server Manager ne redémarre pas automatiquement le service. Vous devez démarrer le service unique manuellement ou redémarrer Server Manager.

Si vous devez arrêter le service LDR sur un nœud de stockage, veillez à savoir qu'il peut prendre un certain temps pour arrêter le service s'il existe des connexions actives.

Étapes

1. Connectez-vous au nœud grid :
   a. Saisissez la commande suivante : `ssh admin@grid_node_IP`
   b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
   c. Entrez la commande suivante pour passer à la racine : `su -`
   d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

   Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

2. Arrêter un service individuel : `service servicename stop`

   Par exemple :

   ```
   service ldr stop
   ```

   > L'arrêt des services peut prendre jusqu'à 11 minutes.

3. Déconnectez-vous du shell de commande : `exit`

Informations associées

"Forcer la fin du service"

Mettez l'appareil en mode maintenance

Vous devez mettre l'appareil en mode maintenance avant d'effectuer des procédures de maintenance spécifiques.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous disposez de l'autorisation Maintenance ou accès racine. Pour plus de détails, reportez-vous aux

instructions d'administration de StorageGRID.

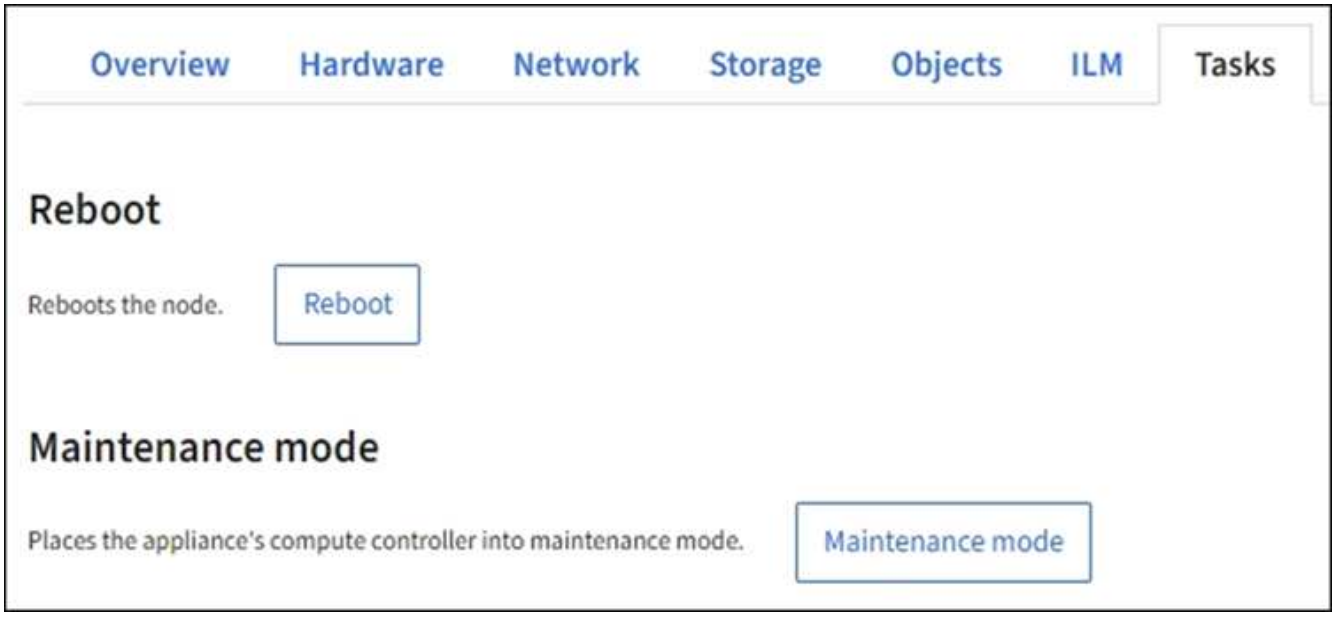
Description de la tâche

Dans de rares cas, le fait de placer une appliance StorageGRID en mode de maintenance peut rendre l'appliance indisponible pour l'accès à distance.

> Le mot de passe du compte admin et les clés d'hôte SSH d'une appliance StorageGRID en mode maintenance restent identiques à ceux de l'appliance lorsqu'elle était en service.

Étapes

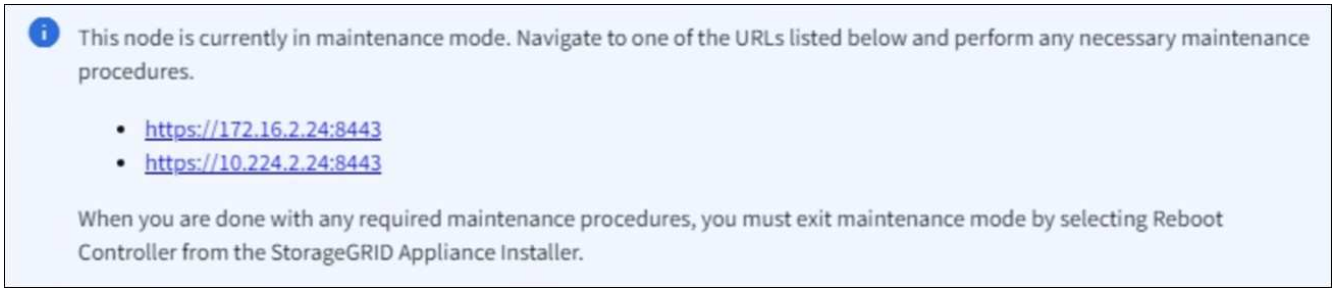
1. Dans Grid Manager, sélectionnez **NODES**.
2. Dans l'arborescence de la page nœuds, sélectionnez le nœud de stockage de l'appliance.
3. Sélectionnez **tâches**.



4. Sélectionnez **Maintenance mode**. Une boîte de dialogue de confirmation s'affiche.
5. Entrez la phrase de passe de provisionnement et sélectionnez **OK**.

   Une barre de progression et une série de messages, notamment « Request sent », « Stopping StorageGRID » et « reboot », indiquent que l'appliance effectue la procédure d'accès au mode de maintenance.

   Lorsque l'appliance est en mode maintenance, un message de confirmation répertorie les URL que vous pouvez utiliser pour accéder au programme d'installation de l'appliance StorageGRID.



6. Pour accéder au programme d'installation de l'appliance StorageGRID, accédez à l'une des URL affichées.

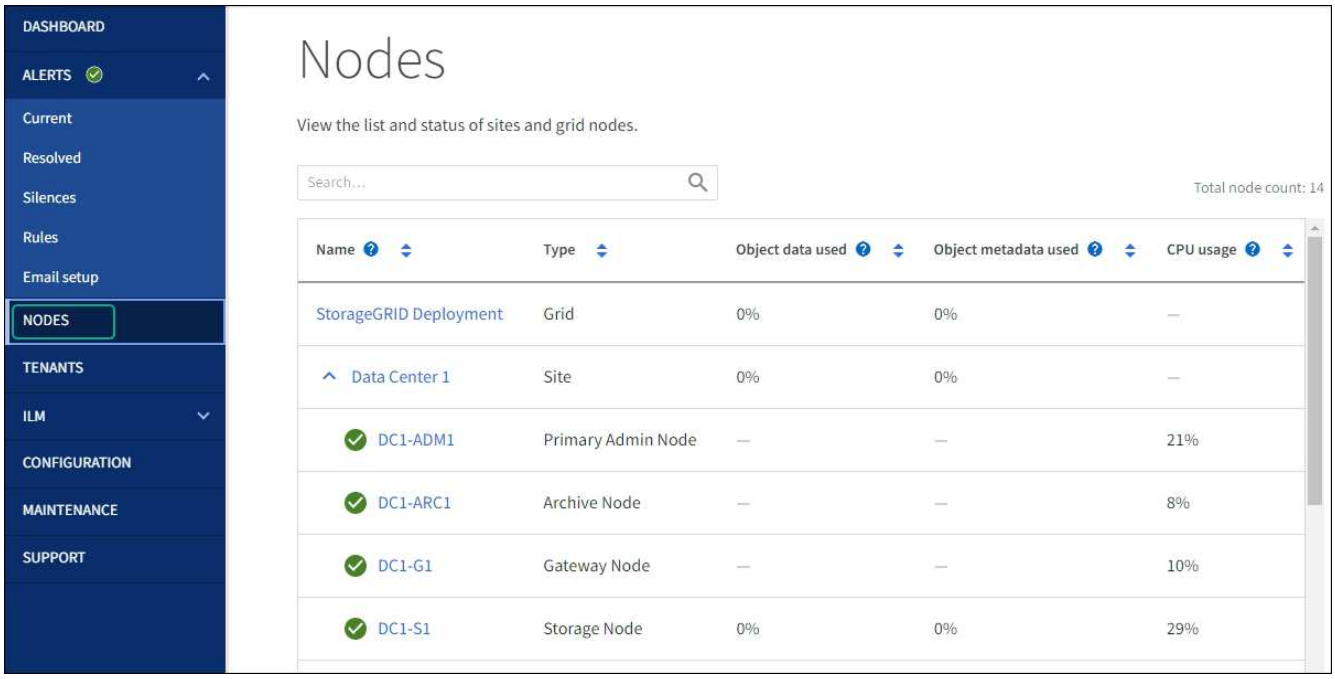
Si possible, utilisez l'URL contenant l'adresse IP du port réseau d'administration de l'appliance.

> Accès à `https://169.254.0.1:8443` nécessite une connexion directe au port de gestion local.

7. Dans le programme d'installation de l'appliance StorageGRID, vérifiez que l'appliance est en mode de maintenance.

8. Effectuez toutes les tâches de maintenance requises.
9. Une fois les tâches de maintenance effectuées, quittez le mode de maintenance et reprenez le fonctionnement normal du nœud. Dans le programme d'installation de l'appliance StorageGRID, sélectionnez **Avancé** > **redémarrer le contrôleur**, puis sélectionnez **redémarrer dans StorageGRID**.

L'appliance peut redémarrer et rejoindre la grille en 20 minutes. Pour confirmer que le redémarrage est terminé et que le nœud a rejoint la grille, retournez à la grille Manager. La page **nœuds** doit afficher un état normal (icône de coche verte) à gauche du nom du nœud) pour le nœud de l'appliance, indiquant qu'aucune alerte n'est active et que le nœud est connecté à la grille.



Forcer la fin du service

Si vous devez arrêter immédiatement un service, vous pouvez utiliser le `force-stop` commande.

Avant de commencer

Vous avez le `Passwords.txt` fichier.

Étapes

1. Connectez-vous au nœud grid :
   a. Saisissez la commande suivante : `ssh admin@grid_node_IP`
   b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
   c. Entrez la commande suivante pour passer à la racine : `su -`
   d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

   Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

2. Forcer manuellement la fin du service : `service servicename force-stop`

   Par exemple :

   ```
   service ldr force-stop
   ```

   Le système attend 30 secondes avant de mettre fin au service.

3. Déconnectez-vous du shell de commande : `exit`

Démarrez ou redémarrez le service

Vous devrez peut-être démarrer un service qui a été arrêté, ou vous devrez peut-être arrêter et redémarrer un service.

Avant de commencer

Vous avez le `Passwords.txt` fichier.

Étapes

1. Connectez-vous au nœud grid :
   a. Saisissez la commande suivante : `ssh admin@grid_node_IP`
   b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
   c. Entrez la commande suivante pour passer à la racine : `su -`
   d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

   Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

2. Choisissez la commande à exécuter, en fonction du type de service en cours d'exécution ou arrêté.
   - Si le service est actuellement arrêté, utilisez le `start` commande pour démarrer le service manuellement : `service servicename start`

     Par exemple :

     ```
     service ldr start
     ```

   - Si le service est en cours d'exécution, utilisez le `restart` commande pour arrêter le service, puis le redémarrer : `service servicename restart`

     Par exemple :

     ```
     service ldr restart
     ```

   +

   > À l'aide du `restart` la commande est identique à l'utilisation de `stop` suivi de la commande `start` commande. Vous pouvez émettre `restart` même si le service est actuellement arrêté.

3. Déconnectez-vous du shell de commande : `exit`

Supprimer les mappages de port

Si vous souhaitez configurer un noeud final pour le service Load Balancer et que vous souhaitez utiliser un port qui a déjà été configuré en tant que port mappé sur d'un remappage de port, vous devez d'abord supprimer le plan de plan de port existant, sinon

le noeud final ne sera pas effectif. Vous devez exécuter un script sur chaque nœud d'administration et nœud de passerelle qui comporte des ports en conflit avec des mappages afin de supprimer tous les mappages de ports du nœud.

Description de la tâche

Cette procédure supprime tous les mappages de ports. Si vous devez conserver certains des plans, contactez le support technique.

Pour plus d'informations sur la configuration des terminaux d'équilibrage de charge, reportez-vous à la section "Configuration des terminaux d'équilibrage de charge".

> Si le remap de port fournit un accès client, reconfigurez le client pour qu'il utilise un autre port comme point final d'équilibrage de charge afin d'éviter toute perte de service. Dans le cas contraire, la suppression du mappage de port entraîne une perte de l'accès client et doit être planifiée de manière appropriée.

> Cette procédure ne fonctionne pas pour un système StorageGRID déployé en tant que conteneur sur les hôtes bare Metal. Reportez-vous aux instructions pour "suppression de mappages de port sur les hôtes bare metal".

Étapes

1. Connectez-vous au nœud.
   a. Saisissez la commande suivante : `ssh -p 8022 admin@node_IP`

      Le port 8022 est le port SSH du système d'exploitation de base, tandis que le port 22 est le port SSH du moteur de mise en conteneurs exécutant StorageGRID.

   b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
   c. Entrez la commande suivante pour passer à la racine : `su -`
   d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

      Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

2. Exécutez le script suivant : `remove-port-remap.sh`
3. Redémarrez le nœud.

   Suivez les instructions de la section "redémarrage d'un nœud de grille".

4. Répétez ces étapes sur chaque nœud d'administration et nœud de passerelle disposant de ports en conflit avec des ports remappés.

Supprimez les mappes de ports sur les hôtes bare Metal

Si vous souhaitez configurer un noeud final pour le service Load Balancer et que vous souhaitez utiliser un port qui a déjà été configuré en tant que port mappé sur d'un remappage de port, vous devez d'abord supprimer le plan de plan de port existant, sinon le noeud final ne sera pas effectif.

Description de la tâche

Si vous exécutez StorageGRID sur des hôtes bare Metal, suivez cette procédure à la place de la procédure générale de suppression des mappages de ports. Vous devez modifier le fichier de configuration de nœud pour chaque nœud d'administration et nœud de passerelle disposant de ports en conflit avec des ports remappés pour supprimer tous les mappages de port du nœud et redémarrer le nœud.

> Cette procédure supprime tous les mappages de ports. Si vous devez conserver certains des plans, contactez le support technique.

Pour plus d'informations sur la configuration des terminaux de l'équilibreur de charge, reportez-vous aux instructions d'administration de StorageGRID.

> Cette procédure peut entraîner une perte temporaire de service au redémarrage des nœuds.

Étapes

1. Connectez-vous à l'hôte supportant le nœud. Connectez-vous en tant que root ou avec un compte disposant de l'autorisation sudo.
2. Exécutez la commande suivante pour désactiver temporairement le nœud : `sudo storagegrid node stop node-name`
3. À l'aide d'un éditeur de texte tel que vim ou pico, modifiez le fichier de configuration de nœud pour le nœud.

   Le fichier de configuration du nœud est disponible à l'adresse `/etc/storagegrid/nodes/node-name.conf`.

4. Recherchez la section du fichier de configuration du nœud qui contient les mappages de port.

   Voir les deux dernières lignes dans l'exemple suivant.

```
ADMIN_NETWORK_CONFIG = STATIC
ADMIN_NETWORK_ESL = 10.0.0.0/8, 172.19.0.0/16, 172.21.0.0/16
ADMIN_NETWORK_GATEWAY = 10.224.0.1
ADMIN_NETWORK_IP = 10.224.5.140
ADMIN_NETWORK_MASK = 255.255.248.0
ADMIN_NETWORK_MTU = 1400
ADMIN_NETWORK_TARGET = eth1
ADMIN_NETWORK_TARGET_TYPE = Interface
BLOCK_DEVICE_VAR_LOCAL = /dev/sda2
CLIENT_NETWORK_CONFIG = STATIC
CLIENT_NETWORK_GATEWAY = 47.47.0.1
CLIENT_NETWORK_IP = 47.47.5.140
CLIENT_NETWORK_MASK = 255.255.248.0
CLIENT_NETWORK_MTU = 1400
CLIENT_NETWORK_TARGET = eth2
CLIENT_NETWORK_TARGET_TYPE = Interface
GRID_NETWORK_CONFIG = STATIC
GRID_NETWORK_GATEWAY = 192.168.0.1
GRID_NETWORK_IP = 192.168.5.140
GRID_NETWORK_MASK = 255.255.248.0
GRID_NETWORK_MTU = 1400
GRID_NETWORK_TARGET = eth0
GRID_NETWORK_TARGET_TYPE = Interface
NODE_TYPE = VM_API_Gateway
PORT_REMAP = client/tcp/8082/443
PORT_REMAP_INBOUND = client/tcp/8082/443
```

5. Modifiez LES entrées PORT_REMAP et PORT_REMAPPAGE_INBOUND pour supprimer les remapes de port.

```
PORT_REMAP =
PORT_REMAP_INBOUND =
```

6. Exécutez la commande suivante pour valider vos modifications dans le fichier de configuration de nœud pour le nœud : `sudo storagegrid node validate node-name`

   Traitez les erreurs ou les avertissements avant de passer à l'étape suivante.

7. Exécutez la commande suivante pour redémarrer le nœud sans mappages de port : `sudo storagegrid node start node-name`
8. Connectez-vous au nœud en tant qu'administrateur à l'aide du mot de passe répertorié dans le `Passwords.txt` fichier.
9. Vérifiez que les services démarrent correctement.
   a. Afficher la liste des États de tous les services sur le serveur :`sudo storagegrid-status`

L'état est mis à jour automatiquement.

b. Attendez que tous les services aient l'état en cours d'exécution ou vérifié.

c. Quitter l'écran d'état :`Ctrl+C`

10. Répétez ces étapes sur chaque nœud d'administration et nœud de passerelle disposant de ports en conflit avec des ports remappés.

Redémarrez le nœud de la grille

Redémarrer le nœud grid : présentation

Vous pouvez redémarrer un nœud grid à partir de Grid Manager ou depuis le shell de commande du nœud.

Lorsque vous redémarrez un nœud de la grille, celui-ci s'arrête et redémarre. Tous les services sont redémarrés automatiquement.

Si vous prévoyez de redémarrer les nœuds de stockage, notez les éléments suivants :

- Si une règle ILM spécifie un comportement d'ingestion de Double allocation ou d'équilibrage et qu'il n'est pas possible de créer immédiatement toutes les copies requises, StorageGRID valide immédiatement tous les objets nouvellement ingérés dans deux nœuds de stockage sur le même site et évalue ce contrôle par la suite. Si vous souhaitez redémarrer deux ou plusieurs nœuds de stockage sur un site donné, il se peut que vous ne puissiez pas accéder à ces objets pendant la durée du redémarrage.
- Pour vous assurer que vous pouvez accéder à tous les objets lors du redémarrage d'un nœud de stockage, arrêtez de les ingérer sur un site pendant environ une heure avant de redémarrer le nœud.

Redémarrez le nœud grid à partir de Grid Manager

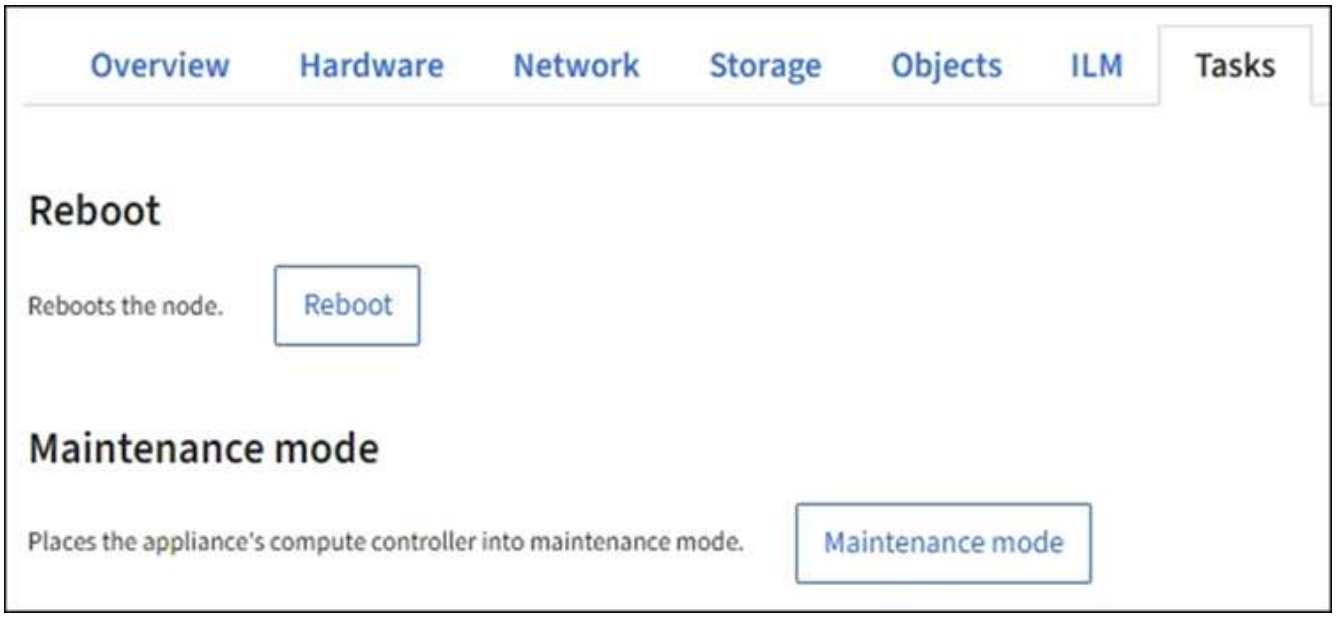
Le redémarrage d'un nœud de grille à partir de Grid Manager émet le `reboot` commande sur le nœud cible.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous disposez de l'autorisation Maintenance ou accès racine.
- Vous avez la phrase secrète pour le provisionnement.

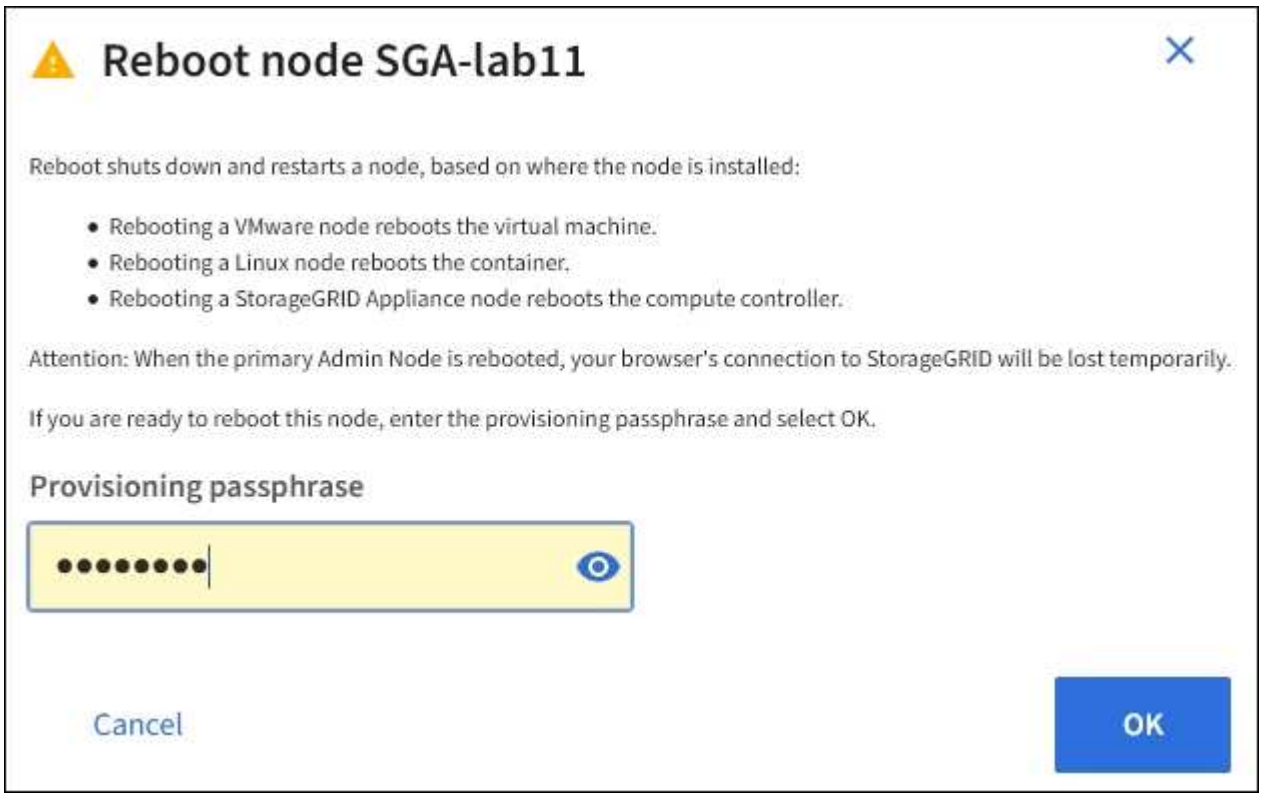
Étapes

1. Sélectionnez **NOEUDS**.
2. Sélectionnez le nœud de grille que vous souhaitez redémarrer.
3. Sélectionnez l'onglet **tâches**.



4. Sélectionnez **Reboot**.

   Une boîte de dialogue de confirmation s'affiche.



> Si vous redémarrez le nœud d'administration principal, la boîte de dialogue de confirmation vous rappelle que la connexion de votre navigateur au Grid Manager sera interrompue temporairement lorsque les services sont arrêtés.

5. Entrez la phrase de passe de provisionnement et sélectionnez **OK**.
6. Attendez que le nœud redémarre.

La fermeture des services peut prendre un certain temps.

Lorsque le nœud est en cours de redémarrage, l'icône grise (administrativement en panne) s'affiche sur le côté gauche de la page **Nodes**. Lorsque tous les services ont redémarré et que le nœud est connecté avec succès à la grille, la page **noeuds** doit afficher un état normal (aucune icône à gauche du nom du nœud), indiquant qu'aucune alerte n'est active et que le nœud est connecté à la grille.

Redémarrez le nœud grid à partir du shell de commande

Si vous devez surveiller de plus près l'opération de redémarrage ou si vous ne parvenez pas à accéder au Gestionnaire de grille, vous pouvez vous connecter au noeud de grille et exécuter la commande de redémarrage de Server Manager à partir du shell de commande.

Avant de commencer

Vous avez le `Passwords.txt` fichier.

Étapes

1. Connectez-vous au nœud grid :

   a. Saisissez la commande suivante : `ssh admin@grid_node_IP`

   b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

   c. Entrez la commande suivante pour passer à la racine : `su -`

   d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

   Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

2. Si vous le souhaitez, arrêtez les services : `service servermanager stop`

   L'arrêt des services est une étape facultative mais recommandée. Les services peuvent prendre jusqu'à 15 minutes pour s'arrêter, et vous pouvez vous connecter au système à distance pour surveiller le processus d'arrêt avant de redémarrer le nœud à l'étape suivante.

3. Redémarrez le nœud grid : `reboot`

4. Déconnectez-vous du shell de commande : `exit`

Arrêter le nœud de la grille

Vous pouvez arrêter un nœud de grille à partir du shell de commande du nœud.

Avant de commencer

- Vous avez le `Passwords.txt` fichier.

Description de la tâche

Avant d'effectuer cette procédure, consultez les considérations suivantes :

- En général, vous ne devez pas arrêter plusieurs nœuds à la fois pour éviter les perturbations.
- N'arrêtez pas un nœud pendant une procédure de maintenance sauf instruction explicite de la documentation ou du support technique.

- Le processus d'arrêt dépend de l'endroit où le nœud est installé, comme suit :
  - L'arrêt d'un nœud VMware arrête la machine virtuelle.
  - L'arrêt d'un nœud Linux arrête le conteneur.
  - L'arrêt d'un nœud d'appliance StorageGRID arrête le contrôleur de calcul.
- Si vous prévoyez d'arrêter plusieurs nœuds de stockage d'un site, arrêtez d'ingérer les objets sur ce site pendant environ une heure avant d'arrêter les nœuds.

  Si une règle ILM utilise l'option d'ingestion **Dual Commit** (ou si une règle utilise l'option **Balanced** et que toutes les copies requises ne peuvent pas être créées immédiatement), StorageGRID valide immédiatement tous les objets nouvellement ingérés sur deux nœuds de stockage sur le même site et évalue ILM ultérieurement. Si plusieurs nœuds de stockage d'un site sont arrêté, il se peut que vous ne puissiez pas accéder aux objets récemment acquis pendant la durée de l'arrêt. Les opérations d'écriture peuvent également échouer si un nombre trop faible de nœuds de stockage restent disponibles sur le site. Voir "Gestion des objets avec ILM".

Étapes

1. Connectez-vous au nœud grid :
   a. Saisissez la commande suivante : `ssh admin@grid_node_IP`
   b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
   c. Entrez la commande suivante pour passer à la racine : `su -`
   d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

   Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

2. Arrêter tous les services : `service servermanager stop`

   L'arrêt des services peut prendre jusqu'à 15 minutes et il est possible que vous souhaitiez vous connecter au système à distance afin de surveiller le processus d'arrêt.

3. Si le nœud s'exécute sur une machine virtuelle VMware ou s'il s'agit d'un nœud d'appliance, exécutez la commande shutdown : `shutdown -h now`

   Effectuer cette étape indépendamment du résultat du `service servermanager stop` commande.

   > Après que vous ayez problématique le `shutdown -h now` commande sur un nœud d'appliance, vous devez mettre l'appliance hors tension puis sous tension afin de redémarrer le nœud.

   Pour l'appliance, cette commande arrête le contrôleur, mais l'appliance est toujours sous tension. Vous devez passer à l'étape suivante.

4. Si vous mettez un nœud d'appliance hors tension, suivez les étapes indiquées pour l'appliance.

SGF6112

a. Mettez l'appareil hors tension.

b. Attendez que le voyant d'alimentation bleu s'éteigne.

SG6000

a. Attendez que la LED verte cache actif située à l'arrière des contrôleurs de stockage s'éteigne.

   Cette LED s'allume lorsque les données en cache doivent être écrites sur les disques. Vous devez attendre que ce voyant s'éteigne avant de mettre le système hors tension.

b. Mettez l'appareil hors tension et attendez que le voyant d'alimentation bleu s'éteigne.

SG5700

a. Attendez que la LED verte cache actif située à l'arrière du contrôleur de stockage s'éteigne.

   Cette LED s'allume lorsque les données en cache doivent être écrites sur les disques. Vous devez attendre que ce voyant s'éteigne avant de mettre le système hors tension.

b. Mettez l'appareil hors tension et attendez que toutes les LED et l'activité d'affichage à sept segments s'arrêtent.

SG100 ou SG1000

a. Mettez l'appareil hors tension.

b. Attendez que le voyant d'alimentation bleu s'éteigne.

Mettez l'hôte hors tension

Avant de mettre un hôte hors tension, vous devez arrêter les services de tous les nœuds du grid sur cet hôte.

Étapes

1. Connectez-vous au nœud grid :

   a. Saisissez la commande suivante : `ssh admin@grid_node_IP`

   b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

   c. Entrez la commande suivante pour passer à la racine : `su -`

   d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

   Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

2. Arrêter tous les services exécutés sur le nœud : `service servermanager stop`

   L'arrêt des services peut prendre jusqu'à 15 minutes et il est possible que vous souhaitiez vous connecter au système à distance afin de surveiller le processus d'arrêt.

3. Répétez les étapes 1 et 2 pour chaque nœud de l'hôte.

4. Si vous disposez d'un hôte Linux :

a. Connectez-vous au système d'exploitation hôte.

b. Arrêter le nœud : `storagegrid node stop`

c. Arrêtez le système d'exploitation hôte.

5. Si le nœud s'exécute sur une machine virtuelle VMware ou s'il s'agit d'un nœud d'appliance, exécutez la commande shutdown : `shutdown -h now`

   Effectuer cette étape indépendamment du résultat du `service servermanager stop` commande.

   > Après que vous ayez problématique le `shutdown -h now` commande sur un nœud d'appliance, vous devez mettre l'appliance hors tension puis sous tension afin de redémarrer le nœud.

   Pour l'appliance, cette commande arrête le contrôleur, mais l'appliance est toujours sous tension. Vous devez passer à l'étape suivante.

6. Si vous mettez un nœud d'appliance hors tension, suivez les étapes indiquées pour l'appliance.

   SGF6112

   a. Mettez l'appareil hors tension.

   b. Attendez que le voyant d'alimentation bleu s'éteigne.

   SG6000

   a. Attendez que la LED verte cache actif située à l'arrière des contrôleurs de stockage s'éteigne.

      Cette LED s'allume lorsque les données en cache doivent être écrites sur les disques. Vous devez attendre que ce voyant s'éteigne avant de mettre le système hors tension.

   b. Mettez l'appareil hors tension et attendez que le voyant d'alimentation bleu s'éteigne.

   SG5700

   a. Attendez que la LED verte cache actif située à l'arrière du contrôleur de stockage s'éteigne.

      Cette LED s'allume lorsque les données en cache doivent être écrites sur les disques. Vous devez attendre que ce voyant s'éteigne avant de mettre le système hors tension.

   b. Mettez l'appareil hors tension et attendez que toutes les LED et l'activité d'affichage à sept segments s'arrêtent.

   SG100 ou SG1000

   a. Mettez l'appareil hors tension.

   b. Attendez que le voyant d'alimentation bleu s'éteigne.

7. Déconnectez-vous du shell de commande : `exit`

Informations associées

"Appliances de stockage SGF6112"

"Dispositifs de stockage SG6000"

"Appliances de stockage SG5700"

"Appareils de services SG100 et SG1000"

Mettez hors tension et sur tous les nœuds du grid

Vous devrez peut-être arrêter l'intégralité de votre système StorageGRID, par exemple si vous déplacez un data Center. Ces étapes fournissent une vue d'ensemble de haut niveau de la séquence recommandée pour effectuer un arrêt et un démarrage contrôlés.

Lorsque vous mettez tous les nœuds hors tension d'un site ou d'un grid, vous ne pourrez pas accéder aux objets ingérés pendant que les nœuds de stockage sont hors ligne.

Arrêtez les services et arrêtez les nœuds de la grille

Avant de mettre un système StorageGRID hors tension, vous devez arrêter tous les services exécutés sur chaque nœud de grid, puis arrêter toutes les machines virtuelles VMware, les moteurs de conteneurs et les appliances StorageGRID.

Description de la tâche

Arrêtez d'abord les services sur les nœuds d'administration et les nœuds de passerelle, puis arrêtez les services sur les nœuds de stockage.

Cette approche vous permet d'utiliser le nœud d'administration principal pour surveiller l'état des autres nœuds de la grille aussi longtemps que possible.

> Si un seul hôte comprend plusieurs nœuds de grille, n'arrêtez pas l'hôte tant que vous n'avez pas arrêté tous les nœuds de cet hôte. Si l'hôte inclut le nœud d'administration principal, arrêtez l'hôte en dernier.

> Si nécessaire, vous pouvez "Migrer des nœuds d'un hôte Linux vers un autre" pour effectuer la maintenance de l'hôte sans affecter les fonctionnalités ou la disponibilité de votre grille.

Étapes

1. Arrêtez toutes les applications client d'accéder à la grille.
2. Connectez-vous à chaque nœud de passerelle :
   a. Saisissez la commande suivante : `ssh admin@grid_node_IP`
   b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
   c. Entrez la commande suivante pour passer à la racine : `su -`
   d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

   Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.
3. Arrêter tous les services exécutés sur le nœud : `service servermanager stop`

   L'arrêt des services peut prendre jusqu'à 15 minutes et il est possible que vous souhaitiez vous connecter au système à distance afin de surveiller le processus d'arrêt.
4. Répétez les deux étapes précédentes pour arrêter les services sur tous les nœuds de stockage, les nœuds d'archivage et les nœuds d'administration non primaires.

Vous pouvez arrêter les services sur ces nœuds dans n'importe quel ordre.

> Si vous émettez le `service servermanager stop` Commande pour arrêter les services d'un nœud de stockage d'appliance, vous devez mettre l'appliance hors tension puis sous tension afin de redémarrer le nœud.

5. Pour le nœud d'administration principal, répétez les étapes à connectez-vous au nœud et arrêt de tous les services du nœud.
6. Pour les nœuds qui s'exécutent sur des hôtes Linux :
   a. Connectez-vous au système d'exploitation hôte.
   b. Arrêter le nœud : `storagegrid node stop`
   c. Arrêtez le système d'exploitation hôte.
7. Pour les nœuds qui s'exécutent sur des machines virtuelles VMware et pour les nœuds de stockage d'appliance, exécutez la commande shutdown : `shutdown -h now`

   Effectuer cette étape indépendamment du résultat du `service servermanager stop` commande.

   Pour l'appliance, cette commande arrête le contrôleur de calcul, mais l'appliance est toujours sous tension. Vous devez passer à l'étape suivante.
8. Si vous disposez de nœuds d'appliance, suivez les étapes correspondant à votre appliance.

   SG100 ou SG1000
   a. Mettez l'appareil hors tension.
   b. Attendez que le voyant d'alimentation bleu s'éteigne.

   SGF6112
   a. Mettez l'appareil hors tension.
   b. Attendez que le voyant d'alimentation bleu s'éteigne.

   SG6000
   a. Attendez que la LED verte cache actif située à l'arrière des contrôleurs de stockage s'éteigne.

      Cette LED s'allume lorsque les données en cache doivent être écrites sur les disques. Vous devez attendre que ce voyant s'éteigne avant de mettre le système hors tension.

   b. Mettez l'appareil hors tension et attendez que le voyant d'alimentation bleu s'éteigne.

   SG5700
   a. Attendez que la LED verte cache actif située à l'arrière du contrôleur de stockage s'éteigne.

      Cette LED s'allume lorsque les données en cache doivent être écrites sur les disques. Vous devez attendre que ce voyant s'éteigne avant de mettre le système hors tension.

   b. Mettez l'appareil hors tension et attendez que toutes les LED et l'activité d'affichage à sept segments s'arrêtent.
9. Si nécessaire, déconnectez-vous du shell de commande : `exit`

La grille StorageGRID est maintenant arrêtée.

Démarrer les nœuds grid

> Si l'ensemble du grid a été arrêté pendant plus de 15 jours, vous devez contacter le support technique avant de démarrer un nœud de grid. Ne tentez pas les procédures de restauration qui reconstruisent les données Cassandra. Cela peut entraîner une perte de données.

Si possible, mettez les nœuds grid sous tension dans l'ordre suivant :

- Mettez d'abord les nœuds d'administration sous tension.
- Appliquer l'alimentation aux nœuds de passerelle en dernier.

> Si un hôte inclut plusieurs nœuds grid, les nœuds sont reconnectés automatiquement lorsque vous mettez l'hôte sous tension.

Étapes

1. Mettez les hôtes sous tension pour le nœud d'administration principal et tous les nœuds d'administration non primaires.

   > Vous ne pourrez pas vous connecter aux nœuds d'administration tant que les nœuds de stockage n'ont pas été redémarrés.

2. Mettez les hôtes sous tension pour tous les nœuds d'archivage et les nœuds de stockage.

   Vous pouvez mettre ces nœuds sous tension dans n'importe quel ordre.

3. Mettez les hôtes sous tension pour tous les nœuds de passerelle.
4. Connectez-vous au Grid Manager.
5. Sélectionnez **NODES** et surveillez l'état des nœuds de la grille. Vérifiez qu'il n'y a pas d'icône d'alerte en regard des noms de nœud.

Informations associées

- "Appareils de services SG100 et SG1000"
- "Dispositifs de stockage SG6000"
- "Appliances de stockage SG5700"

Utilisez un fichier DoNotStart

Si vous effectuez diverses procédures de maintenance ou de configuration sous la direction du support technique, il se peut que vous soyez invité à utiliser un fichier DoNotStart pour empêcher les services de démarrer lorsque Server Manager est démarré ou redémarré.

> Vous ne devez ajouter ou supprimer un fichier DoNotStart que si le support technique vous a demandé de le faire.

Pour empêcher le démarrage d'un service, placez un fichier DoNotStart dans le répertoire du service que vous

souhaitez empêcher de démarrer. Au démarrage, Server Manager recherche le fichier DoNotStart. Si le fichier est présent, le service (et les services qui en dépendent) ne peut pas démarrer. Lorsque le fichier DoNotStart est supprimé, le service précédemment arrêté démarre au prochain démarrage ou redémarrage de Server Manager. Les services ne sont pas automatiquement démarrés lorsque le fichier DoNotStart est supprimé.

Le moyen le plus efficace d'empêcher le redémarrage de tous les services est d'empêcher le démarrage du service NTP. Tous les services dépendent du service NTP et ne peuvent pas s'exécuter si le service NTP n'est pas en cours d'exécution.

Ajouter le fichier DoNotStart pour le service

Vous pouvez empêcher le démarrage d'un service individuel en ajoutant un fichier DoNotStart au répertoire de ce service sur un nœud de grille.

Avant de commencer

Vous avez le `Passwords.txt` fichier.

Étapes

1. Connectez-vous au nœud grid :
   a. Saisissez la commande suivante : `ssh admin@grid_node_IP`
   b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
   c. Entrez la commande suivante pour passer à la racine : `su -`
   d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

   Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

2. Ajouter un fichier DoNotStart: `touch /etc/sv/service/DoNotStart`

   où `service` est le nom du service à empêcher de démarrer. Par exemple :

   ```
   touch /etc/sv/ldr/DoNotStart
   ```

   Un fichier DoNotStart est créé. Aucun contenu de fichier n'est nécessaire.

   Lorsque Server Manager ou le nœud de la grille est redémarré, Server Manager redémarre, mais le service ne le fait pas.

3. Déconnectez-vous du shell de commande : `exit`

Supprimez le fichier DoNotStart pour le service

Lorsque vous supprimez un fichier DoNotStart qui empêche le démarrage d'un service, vous devez démarrer ce service.

Avant de commencer

Vous avez le `Passwords.txt` fichier.

Étapes

1. Connectez-vous au nœud grid :

a. Saisissez la commande suivante : `ssh admin@grid_node_IP`

b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

c. Entrez la commande suivante pour passer à la racine : `su -`

d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

2. Supprimez le fichier DoNotStart du répertoire de services : `rm /etc/sv/service/DoNotStart`

   où `service` est le nom du service. Par exemple :

   ```
   rm /etc/sv/ldr/DoNotStart
   ```

3. Démarrer le service : `service servicename start`

4. Déconnectez-vous du shell de commande : `exit`

Dépanner Server Manager

Si un problème survient lors de l'utilisation de Server Manager, vérifiez son fichier journal.

Les messages d'erreur relatifs à Server Manager sont capturés dans le fichier journal de Server Manager, à l'adresse suivante : `/var/local/log/servermanager.log`

Consultez ce fichier pour voir s'il contient des messages d'erreur relatifs aux échecs. Transmettez le problème au support technique si nécessaire. Il se peut que vous soyez invité à transférer les fichiers journaux au support technique.

Service avec un état d'erreur

Si vous détectez qu'un service a entré un état d'erreur, essayez de redémarrer le service.

Avant de commencer

Vous avez le `Passwords.txt` fichier.

Description de la tâche

Server Manager surveille les services et redémarre tout qui s'est arrêté de façon inattendue. En cas d'échec d'un service, Server Manager tente de le redémarrer. Si trois tentatives de démarrage d'un service ont échoué dans les cinq minutes, le service passe en état d'erreur. Server Manager ne tente pas un redémarrage supplémentaire.

Étapes

1. Connectez-vous au nœud grid :

   a. Saisissez la commande suivante : `ssh admin@grid_node_IP`

   b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

   c. Entrez la commande suivante pour passer à la racine : `su -`

   d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

2. Confirmez l'état d'erreur du service : `service servicename status`

   Par exemple :

   ```
   service ldr status
   ```

   Si le service est en état d'erreur, le message suivant est renvoyé : `servicename in error state`. Par exemple :

   ```
   ldr in error state
   ```

   > Si le statut du service est `disabled`, voir les instructions pour "Suppression d'un fichier DoNotStart pour un service".

3. Essayez de supprimer l'état d'erreur en redémarrant le service : `service servicename restart`

   Si le service ne parvient pas à redémarrer, contactez le support technique.

4. Déconnectez-vous du shell de commande : `exit`

Maintenance de la configuration de l'appliance

Procédures courantes de maintenance des nœuds : présentation

Suivez ces instructions pour entretenir votre système StorageGRID.

À propos de ces instructions

Ces instructions décrivent les procédures communes à tous les nœuds, telles que l'application d'un correctif logiciel, la récupération de nœuds de grille, la restauration d'un site en panne, la désaffectation de nœuds de grille ou d'un site entier, la maintenance du réseau, la réalisation de procédures de maintenance au niveau de l'hôte et du middleware et la réalisation des procédures de nœud de grille.

> Dans ces instructions, « Linux » fait référence à un déploiement Red Hat® Enterprise Linux®, Ubuntu®, CentOS ou Debian®. Utilisez le "Matrice d'interopérabilité NetApp (IMT)" pour obtenir une liste des versions prises en charge.

Avant de commencer

- Vous avez une bonne compréhension du système StorageGRID.
- Vous avez examiné la topologie de votre système StorageGRID et compris la configuration de la grille.
- Vous comprenez que vous devez suivre toutes les instructions exactement et tenir compte de tous les avertissements.
- Vous comprenez que les procédures de maintenance non décrites ne sont pas prises en charge ou requièrent une mission de service.

Procédures de maintenance des appareils

Les procédures de maintenance spécifiques pour chaque type d'appliance StorageGRID se trouvent dans les sections relatives à la maintenance de l'appliance :

- "Maintenance de l'appliance SGF6112"
- "Entretenir l'appareil SG6000"
- "Conservez l'appliance SG5700"
- "Maintenance des appliances SG100 et SG1000"

Mettez l'appareil en mode maintenance

Vous devez mettre l'appareil en mode maintenance avant d'effectuer des procédures de maintenance spécifiques.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous disposez de l'autorisation Maintenance ou accès racine. Pour plus de détails, reportez-vous aux instructions d'administration de StorageGRID.

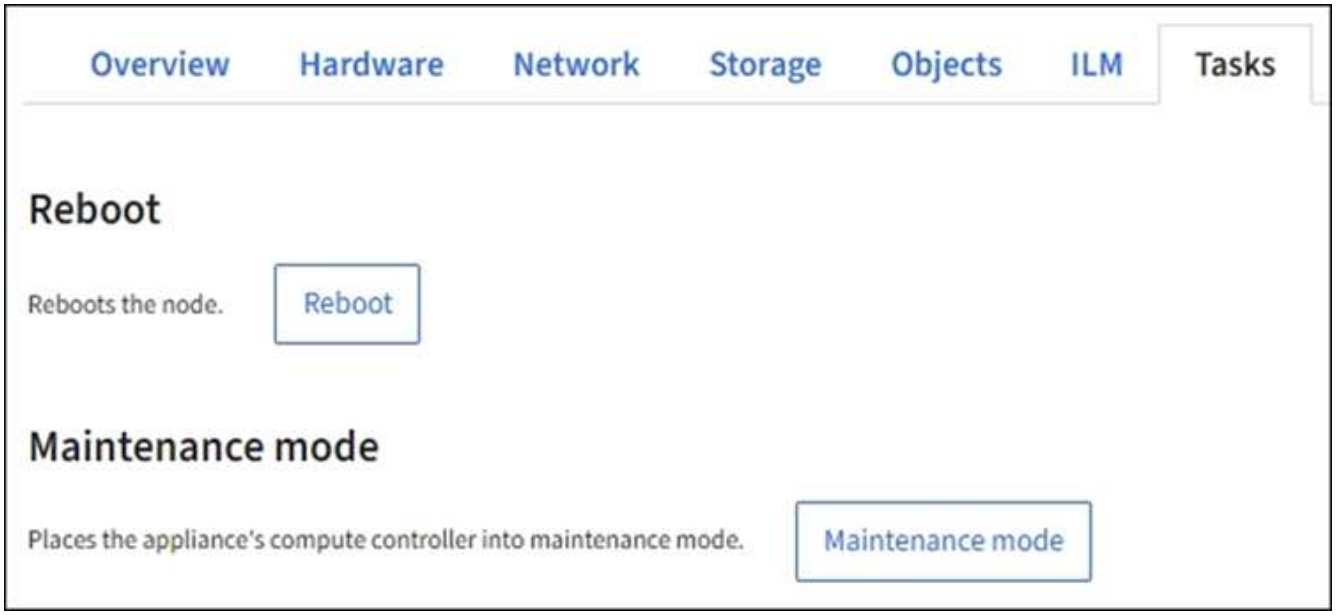
Description de la tâche

Dans de rares cas, le fait de placer une appliance StorageGRID en mode de maintenance peut rendre l'appliance indisponible pour l'accès à distance.

> Le mot de passe du compte admin et les clés d'hôte SSH d'une appliance StorageGRID en mode maintenance restent identiques à ceux de l'appliance lorsqu'elle était en service.

Étapes

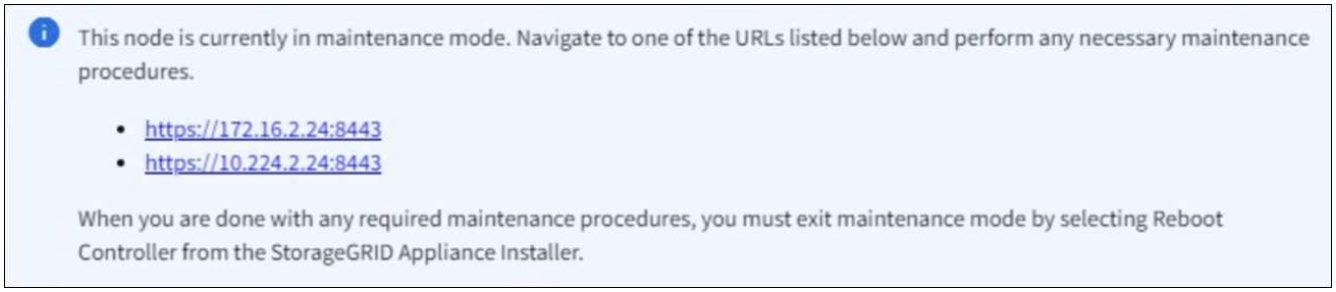
1. Dans Grid Manager, sélectionnez **NODES**.
2. Dans l'arborescence de la page nœuds, sélectionnez le nœud de stockage de l'appliance.
3. Sélectionnez **tâches**.



4. Sélectionnez **Maintenance mode**. Une boîte de dialogue de confirmation s'affiche.
5. Entrez la phrase de passe de provisionnement et sélectionnez **OK**.

   Une barre de progression et une série de messages, notamment « demande envoyée », « arrêt de StorageGRID » et « redémarrage », indiquent que l'appliance effectue les étapes de passage en mode maintenance.

   Lorsque l'appliance est en mode maintenance, un message de confirmation répertorie les URL que vous pouvez utiliser pour accéder au programme d'installation de l'appliance StorageGRID.



6. Pour accéder au programme d'installation de l'appliance StorageGRID, accédez à l'une des URL affichées.

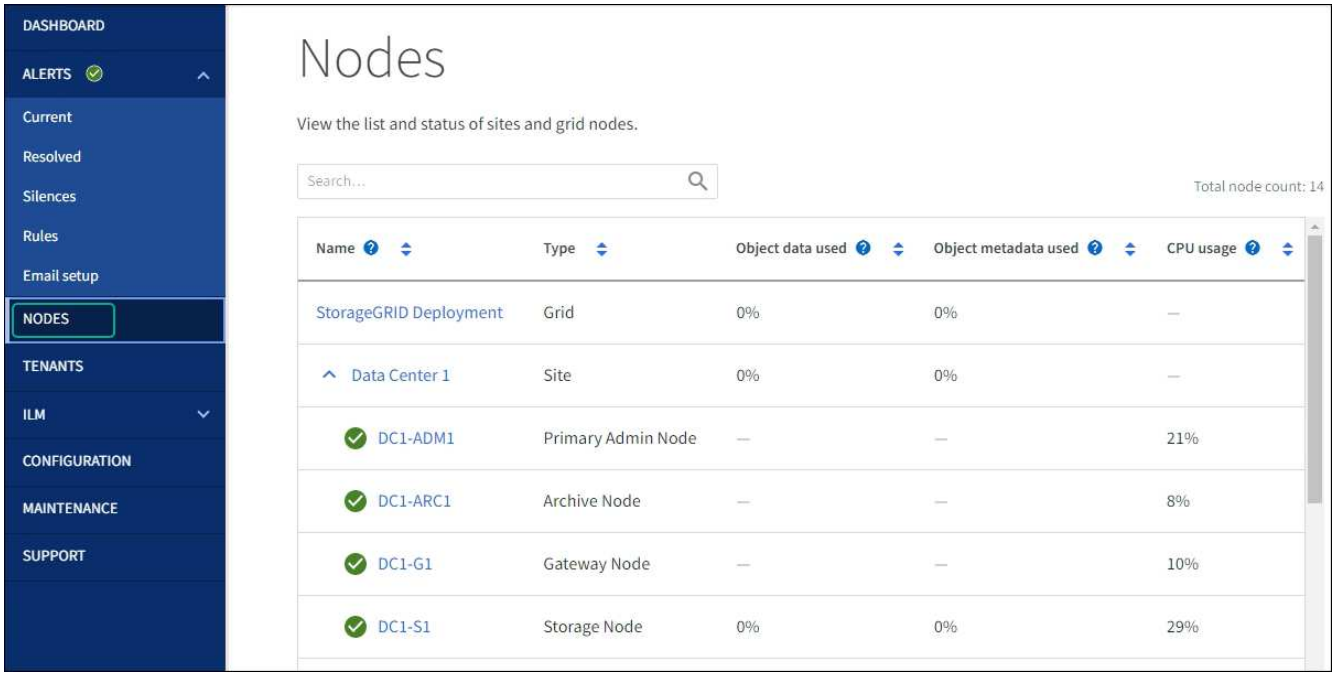
   Si possible, utilisez l'URL contenant l'adresse IP du port réseau d'administration de l'appliance.

   > Si vous disposez d'une connexion directe au port de gestion de l'appliance, utilisez `https://169.254.0.1:8443` Pour accéder à la page du programme d'installation de l'appliance StorageGRID.

7. Dans le programme d'installation de l'appliance StorageGRID, vérifiez que l'appliance est en mode de maintenance.

8. Effectuez toutes les tâches de maintenance requises.
9. Une fois les tâches de maintenance effectuées, quittez le mode de maintenance et reprenez le fonctionnement normal du nœud. Dans le programme d'installation de l'appliance StorageGRID, sélectionnez **Avancé** > **redémarrer le contrôleur**, puis sélectionnez **redémarrer dans StorageGRID**.

L'appliance peut redémarrer et rejoindre la grille en 20 minutes. Pour confirmer que le redémarrage est terminé et que le nœud a rejoint la grille, retournez à la grille Manager. La page **NODES** doit afficher un état normal (icône de coche verte à gauche du nom du nœud) pour le nœud de l'appliance, indiquant qu'aucune alerte n'est active et que le nœud est connecté à la grille.



Modifier le paramètre MTU

Vous pouvez modifier le paramètre MTU que vous avez attribué lorsque vous avez configuré des adresses IP pour le nœud de l'appliance.

Description de la tâche

La valeur MTU du réseau doit correspondre à la valeur configurée sur le port du commutateur auquel le nœud est connecté. Dans le cas contraire, des problèmes de performances réseau ou une perte de paquets peuvent se produire.

Pour des performances réseau optimales, tous les nœuds doivent être configurés avec des valeurs MTU similaires sur leurs interfaces réseau Grid. L'alerte **Grid Network MTU mismatch** est déclenchée en cas de différence importante dans les paramètres MTU pour le réseau Grid sur les nœuds individuels. Les valeurs MTU ne doivent pas nécessairement être identiques pour tous les types de réseau.

Pour modifier le paramètre MTU sans redémarrer le nœud d'appliance, Utilisez l'outil Modifier IP.

Si le réseau client ou administrateur n'a pas été configuré dans le programme d'installation de l'appliance StorageGRID lors de l'installation initiale, Modifiez le paramètre MTU en mode maintenance.

Modifiez le paramètre MTU à l'aide de l'outil Modifier l'IP

Avant de commencer

Vous avez le `Passwords.txt` Fichier pour utiliser l'outil Modifier IP.

Étapes

Accédez à l'outil Modifier IP et mettez à jour les paramètres MTU comme décrit dans "Modifier la configuration réseau du nœud".

Modifiez le paramètre MTU en mode maintenance

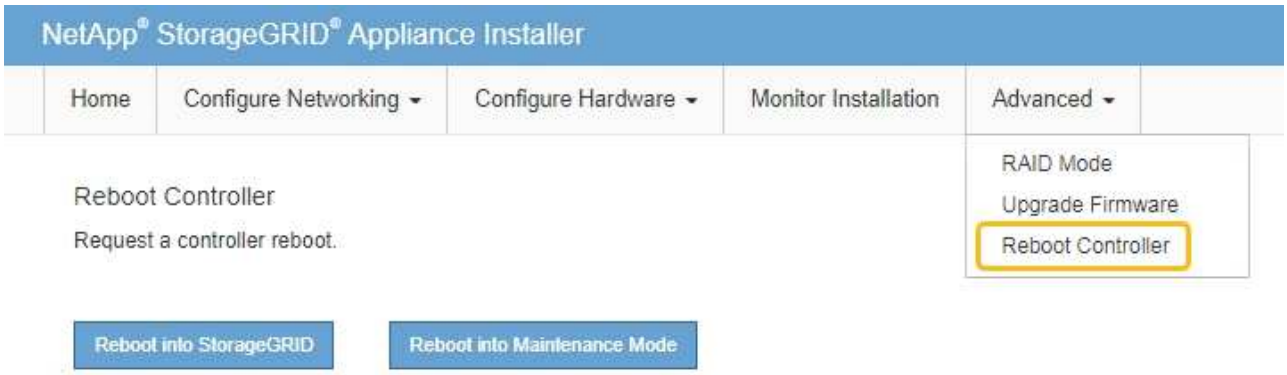
Modifiez le paramètre MTU en mode maintenance si vous ne parvenez pas à accéder à ces paramètres à l'aide de l'outil Modifier IP.

Avant de commencer

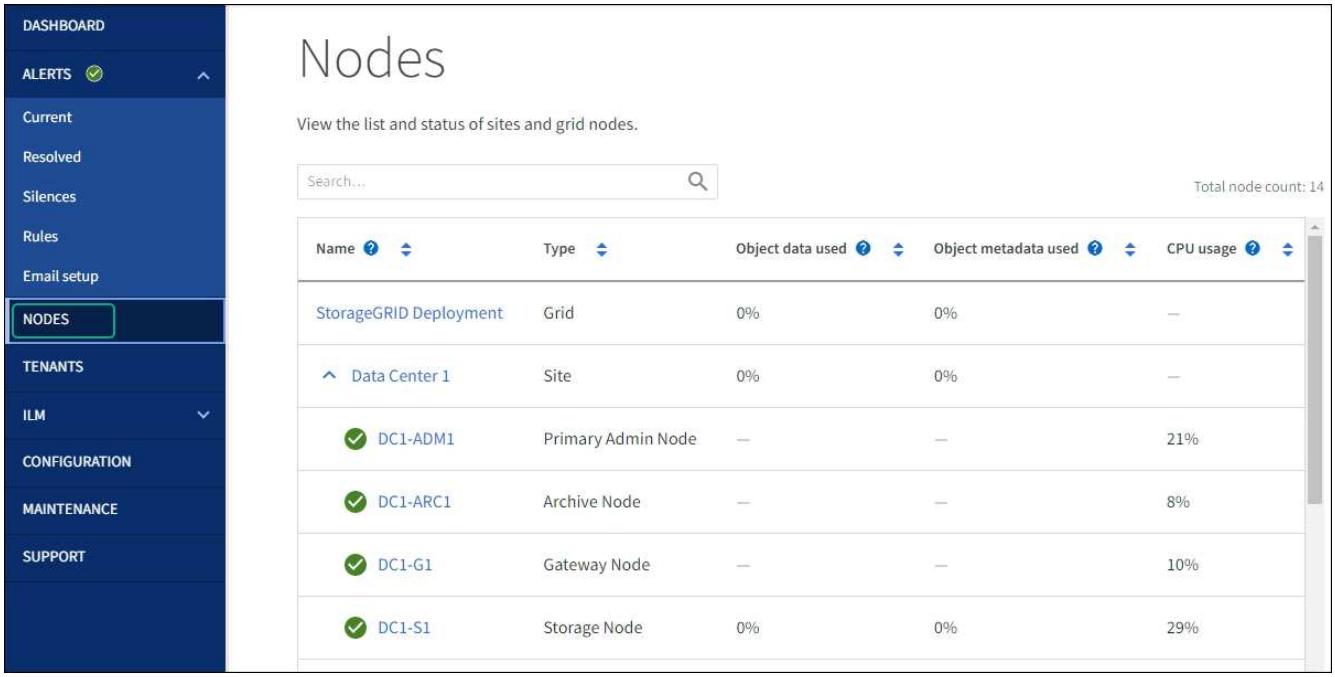
L'appareil a été "passage en mode maintenance".

Étapes

1. Dans le programme d'installation de l'appliance StorageGRID, sélectionnez **configurer le réseau** > **Configuration IP**.
2. Apportez les modifications souhaitées aux paramètres MTU du réseau Grid, du réseau Admin et du réseau client.
3. Lorsque vous êtes satisfait des paramètres, sélectionnez **Enregistrer**.
4. Si cette procédure s'est terminée avec succès et que vous disposez de procédures supplémentaires pour effectuer cette opération pendant que le nœud est en mode de maintenance, effectuez-les maintenant. Lorsque vous avez terminé, ou si vous avez rencontré des échecs et souhaitez recommencer, sélectionnez **Avancé** > **redémarrer le contrôleur**, puis sélectionnez l'une des options suivantes :
    - Sélectionnez **redémarrer dans StorageGRID**
    - Sélectionnez **redémarrer en mode maintenance** pour redémarrer le contrôleur avec le nœud restant en mode de maintenance. Sélectionnez cette option si vous avez rencontré des échecs au cours de la procédure et souhaitez recommencer. Une fois le redémarrage du nœud en mode maintenance terminé, redémarrez à partir de l'étape appropriée de la procédure ayant échoué.



L'appliance peut redémarrer et rejoindre la grille en 20 minutes. Pour confirmer que le redémarrage est terminé et que le nœud a rejoint la grille, retournez à la grille Manager. La page **NODES** doit afficher un état normal (icône de coche verte à gauche du nom du nœud) pour le nœud de l'appliance, indiquant qu'aucune alerte n'est active et que le nœud est connecté à la grille.



Vérifiez la configuration du serveur DNS

Vous pouvez vérifier et modifier temporairement les serveurs DNS actuellement utilisés par ce nœud d'appliance.

Avant de commencer

L'appareil a été "passage en mode maintenance".

Description de la tâche

Vous devrez peut-être modifier les paramètres du serveur DNS si une appliance chiffrée ne peut pas se connecter au serveur de gestion des clés (KMS) ou au cluster KMS car le nom d'hôte du KMS a été spécifié en tant que nom de domaine au lieu d'une adresse IP. Toute modification apportée aux paramètres DNS de

l'appliance est temporaire et perdue lorsque vous quittez le mode de maintenance. Pour rendre ces modifications permanentes, spécifiez les serveurs DNS dans Grid Manager (**MAINTENANCE** > **réseau** > **serveurs DNS**).

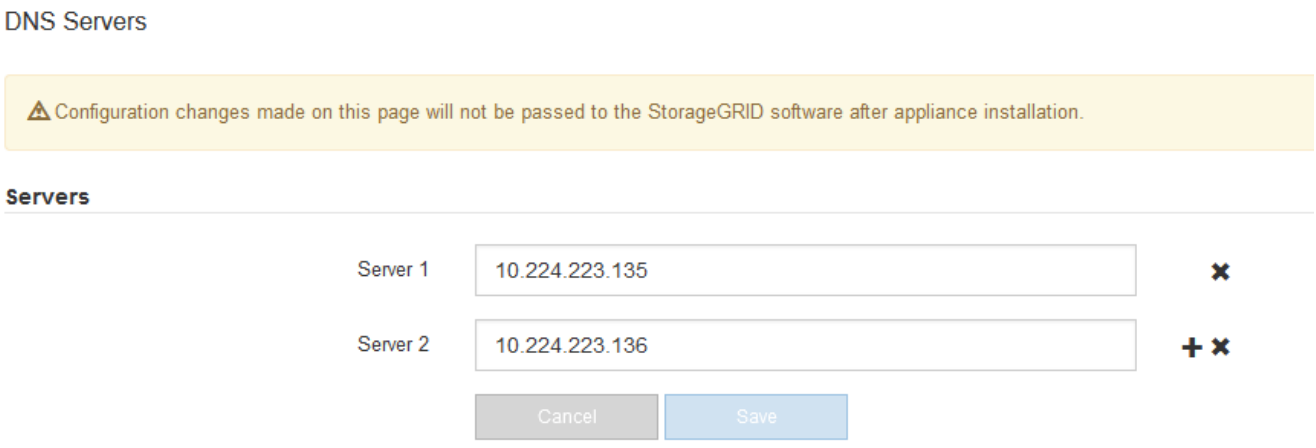
- Les modifications temporaires de la configuration DNS ne sont nécessaires que pour les appliances cryptées par nœud où le serveur KMS est défini à l'aide d'un nom de domaine complet, au lieu d'une adresse IP, pour le nom d'hôte.
- Lorsqu'une appliance chiffrée au nœud se connecte à un KMS à l'aide d'un nom de domaine, elle doit se connecter à l'un des serveurs DNS définis pour la grille. L'un de ces serveurs DNS traduit ensuite le nom de domaine en une adresse IP.
- Si le nœud ne peut pas atteindre un serveur DNS pour la grille, ou si vous avez modifié les paramètres DNS de la grille lorsqu'un nœud d'appliance chiffré par nœud était hors ligne, le nœud ne peut pas se connecter au KMS. Les données chiffrées de l'appliance ne peuvent pas être déchiffrées tant que le problème DNS n'est pas résolu.

Pour résoudre un problème DNS empêchant la connexion KMS, spécifiez l'adresse IP d'un ou plusieurs serveurs DNS dans le programme d'installation de l'appliance StorageGRID. Ces paramètres DNS temporaires permettent à l'appliance de se connecter au KMS et de décrypter les données sur le nœud.

Par exemple, si le serveur DNS de la grille change alors qu'un nœud chiffré était hors ligne, le nœud ne pourra pas atteindre le KMS lorsqu'il sera de nouveau en ligne, car il utilise toujours les valeurs DNS précédentes. La saisie de la nouvelle adresse IP du serveur DNS dans le programme d'installation de l'appliance StorageGRID permet à une connexion KMS temporaire de décrypter les données du nœud.

Étapes

1. Dans le programme d'installation de l'appliance StorageGRID, sélectionnez **configurer le réseau** > **Configuration DNS**.
2. Vérifiez que les serveurs DNS spécifiés sont corrects.



3. Si nécessaire, modifiez les serveurs DNS.

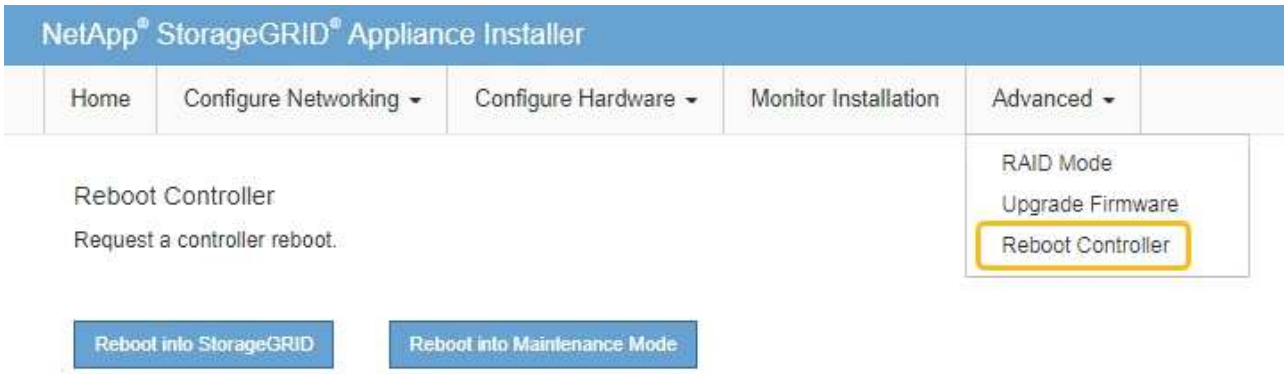
> Les modifications apportées aux paramètres DNS sont temporaires et sont perdues lorsque vous quittez le mode de maintenance.

4. Lorsque vous êtes satisfait des paramètres DNS temporaires, sélectionnez **Enregistrer**.

   Le nœud utilise les paramètres de serveur DNS spécifiés sur cette page pour se reconnecter au KMS, permettant ainsi de décrypter les données du nœud.

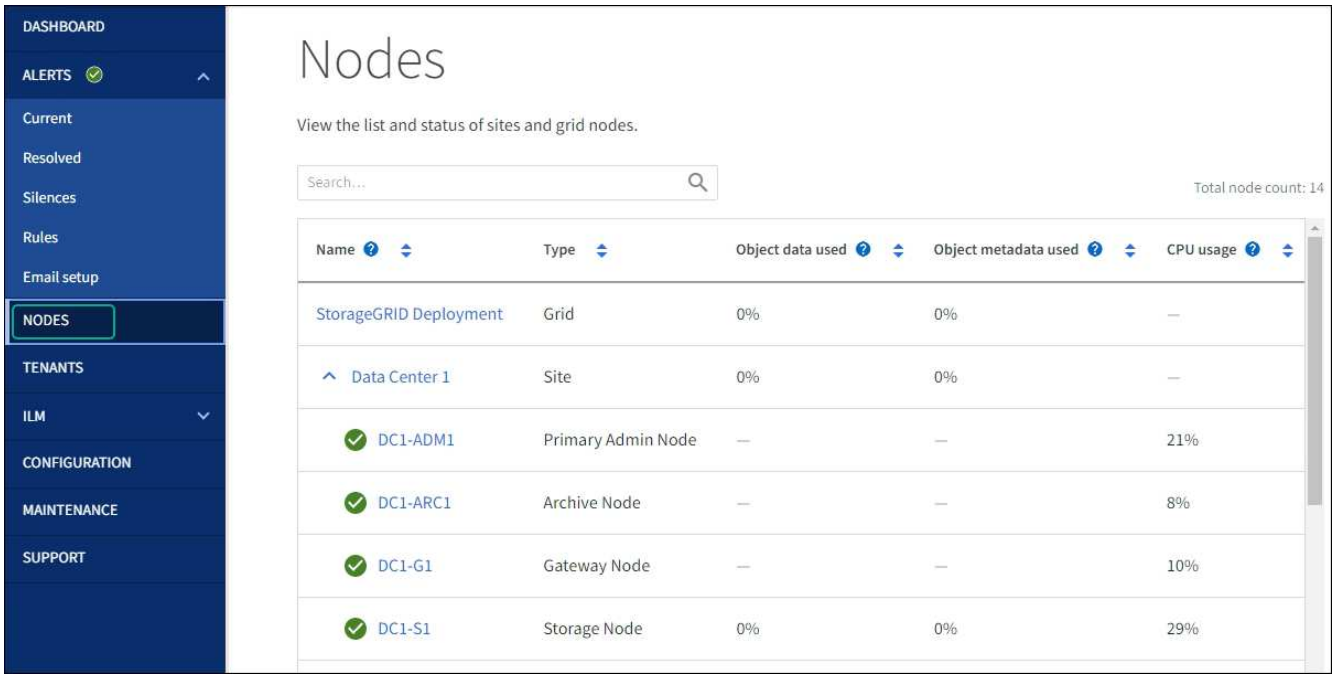
5. Une fois les données de nœud déchiffrées, redémarrez le nœud. Dans le programme d'installation de l'appliance StorageGRID, sélectionnez **Avancé** > **redémarrer le contrôleur**, puis sélectionnez l'une des options suivantes :

   - Sélectionnez **Reboot dans StorageGRID** pour redémarrer le contrôleur avec le noeud qui rejoint la grille. Sélectionnez cette option si vous avez terminé de travailler en mode maintenance et que vous êtes prêt à rétablir le fonctionnement normal du nœud.
   - Sélectionnez **redémarrer en mode maintenance** pour redémarrer le contrôleur avec le nœud restant en mode de maintenance. (Cette option n'est disponible que lorsque le contrôleur est en mode de maintenance.) Sélectionnez cette option si des opérations de maintenance supplémentaires doivent être effectuées sur le nœud avant de rejoindre la grille.



> Lorsque le nœud redémarre et rejoint la grille, il utilise les serveurs DNS du système répertoriés dans Grid Manager. Après avoir rejoint la grille, l'appliance n'utilise plus les serveurs DNS temporaires spécifiés dans le programme d'installation de l'appliance StorageGRID pendant que l'appliance était en mode de maintenance.

L'appliance peut redémarrer et rejoindre la grille en 20 minutes. Pour confirmer que le redémarrage est terminé et que le nœud a rejoint la grille, retournez à la grille Manager. La page **NODES** doit afficher un état normal (icône de coche verte à gauche du nom du nœud) pour le nœud de l'appliance, indiquant qu'aucune alerte n'est active et que le nœud est connecté à la grille.



Mettre à jour les références d'adresse MAC

Dans certains cas, vous devrez peut-être mettre à jour les références d'adresse MAC après le remplacement d'un appareil.

Description de la tâche

Si l'une des interfaces réseau d'une appliance que vous remplacez est configurée pour DHCP, vous devrez peut-être mettre à jour les attributions de bail DHCP permanentes sur les serveurs DHCP pour référencer les adresses MAC de l'appliance de remplacement. Cette mise à jour garantit que l'appliance de remplacement se voit attribuer les adresses IP attendues.

Étapes

1. Repérez l'étiquette à l'avant de l'appareil. L'étiquette indique l'adresse MAC du port de gestion BMC de l'appliance.
2. Pour déterminer l'adresse MAC du port réseau Admin, vous devez ajouter **2** au numéro hexadécimal sur l'étiquette.

   Par exemple, si l'adresse MAC de l'étiquette se termine par **09**, l'adresse MAC du port d'administration se terminera par **0B**. Si l'adresse MAC de l'étiquette se termine dans **(*y*)FF**, l'adresse MAC du port d'administration se terminera dans **(*y*+1)01**.

   Vous pouvez facilement effectuer ce calcul en ouvrant Calculator sous Windows, en le définissant en mode programmateur, en sélectionnant Hex, en saisissant l'adresse MAC, puis en tapant **+ 2 =**.

3. Demandez à votre administrateur réseau d'associer le DNS/réseau et l'adresse IP de l'appliance que vous avez retirée à l'adresse MAC du dispositif de remplacement.

> Vous devez vous assurer que toutes les adresses IP de l'appareil d'origine ont été mises à jour avant d'alimenter l'appareil de remplacement. Dans le cas contraire, l'appliance obtiendra de nouvelles adresses IP DHCP lors du démarrage et pourrait ne pas pouvoir se reconnecter à StorageGRID. Cette étape s'applique à tous les réseaux StorageGRID reliés à l'appliance.

Si l'appliance d'origine utilisait une adresse IP statique, la nouvelle appliance adopte automatiquement les adresses IP de l'appliance que vous avez retirée.

Surveillez le chiffrement des nœuds en mode de maintenance

Si vous avez activé le chiffrement des nœuds pour l'appliance lors de l'installation, vous pouvez surveiller l'état du chiffrement des nœuds de chaque nœud d'appliance, notamment les informations détaillées sur l'état de chiffrement des nœuds et le serveur de gestion des clés (KMS).

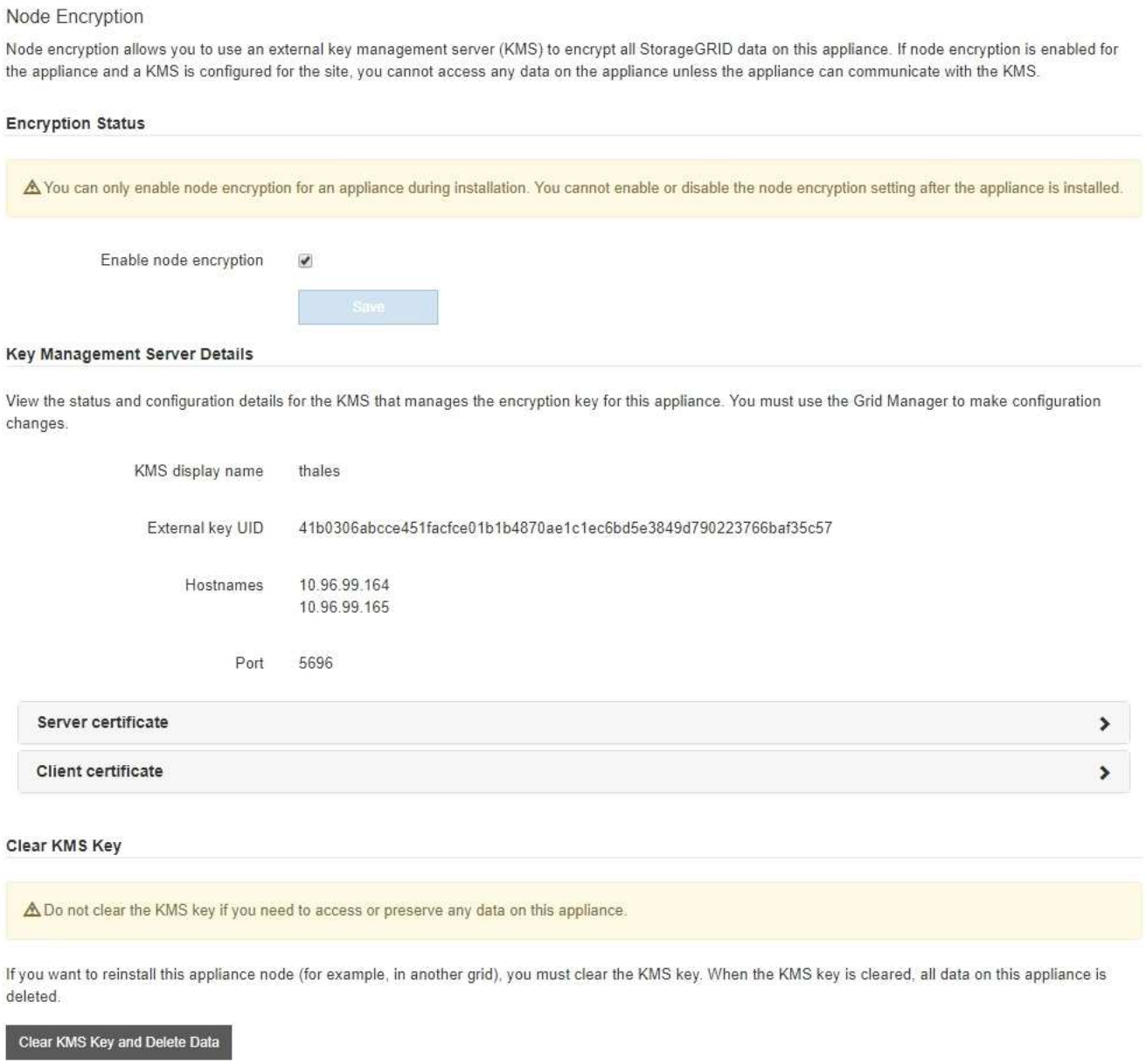
Voir "Configurer les serveurs de gestion des clés" Pour plus d'informations sur l'implémentation de KMS pour les appliances StorageGRID,

Avant de commencer

- Vous avez activé le cryptage de nœud pour l'appliance pendant l'installation. Une fois l'appliance installée, vous ne pouvez pas activer le chiffrement des nœuds.
- Vous avez "placez l'appareil en mode maintenance".

Étapes

1. Dans le programme d'installation de l'appliance StorageGRID, sélectionnez **configurer le matériel** > **cryptage de nœud**.



La page Node Encryption comprend trois sections :

- L'état du chiffrement indique si le chiffrement de nœud est activé ou désactivé pour l'appliance.
- Détails du serveur de gestion des clés affiche des informations sur le KMS utilisé pour crypter l'appliance. Vous pouvez développer les sections de certificat du serveur et du client pour afficher les détails et l'état du certificat.
  - Pour résoudre les problèmes avec les certificats eux-mêmes, tels que le renouvellement des certificats expirés, consultez le "Instructions de configuration de KMS".
  - En cas de problèmes inattendus lors de la connexion aux hôtes KMS, vérifiez que le système "Les serveurs DNS sont corrects" et ça "la mise en réseau de l'appliance est correctement configurée".
  - Si vous ne parvenez pas à résoudre les problèmes liés à votre certificat, contactez le support technique.
- Clear KMS Key désactive le chiffrement des nœuds pour l'appliance, supprime l'association entre l'appliance et le serveur de gestion des clés qui a été configuré pour le site StorageGRID et supprime toutes les données de l'appliance. Vous devez Effacez la clé KMS Avant de pouvoir installer l'appliance

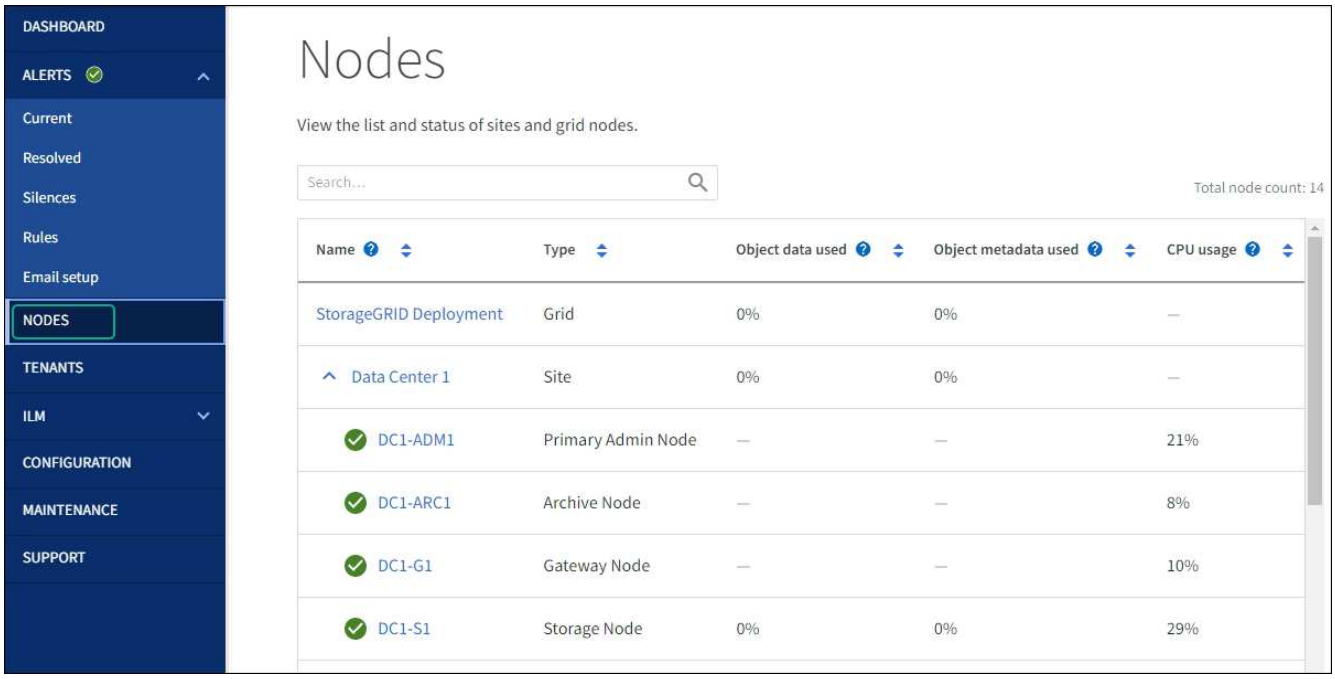
sur un autre système StorageGRID.

> L'effacement de la configuration KMS supprime les données de l'appliance, ce qui les rend définitivement inaccessibles. Ces données ne peuvent pas être récupérées.

2. Une fois que vous avez terminé de vérifier l'état du chiffrement de nœud, redémarrez le nœud. Dans le programme d'installation de l'appliance StorageGRID, sélectionnez **Avancé** > **redémarrer le contrôleur**, puis sélectionnez l'une des options suivantes :

   - Sélectionnez **Reboot dans StorageGRID** pour redémarrer le contrôleur avec le noeud qui rejoint la grille. Sélectionnez cette option si vous avez terminé de travailler en mode maintenance et que vous êtes prêt à rétablir le fonctionnement normal du nœud.
   - Sélectionnez **redémarrer en mode maintenance** pour redémarrer le contrôleur avec le nœud restant en mode de maintenance. (Cette option n'est disponible que lorsque le contrôleur est en mode de maintenance.) Sélectionnez cette option si des opérations de maintenance supplémentaires doivent être effectuées sur le nœud avant de rejoindre la grille.

L'appliance peut redémarrer et rejoindre la grille en 20 minutes. Pour confirmer que le redémarrage est terminé et que le nœud a rejoint la grille, retournez à la grille Manager. La page **NODES** doit afficher un état normal (icône de coche verte à gauche du nom du nœud) pour le nœud de l'appliance, indiquant qu'aucune alerte n'est active et que le nœud est connecté à la grille.



Effacez la configuration du serveur de gestion des clés

L'effacement de la configuration du serveur de gestion des clés (KMS) désactive le cryptage des nœuds sur votre appliance. Une fois la configuration KMS effacée, les données de votre appliance sont définitivement supprimées et ne sont plus accessibles. Ces données ne peuvent pas être récupérées.

Avant de commencer

Si vous devez conserver les données sur l'appliance, vous devez effectuer une procédure de déclassement d'un nœud ou cloner le nœud avant d'effacer la configuration du KMS.

> Lorsque le KMS est effacé, les données de l'appliance seront définitivement supprimées et ne sont plus accessibles. Ces données ne peuvent pas être récupérées.

"Mise hors service du nœud" Pour déplacer toutes les données qu'il contient vers d'autres nœuds de StorageGRID.

Description de la tâche

L'effacement de la configuration KMS de l'appliance désactive le cryptage des nœuds, supprimant ainsi l'association entre le nœud de l'appliance et la configuration KMS pour le site StorageGRID. Les données de l'appliance sont ensuite supprimées et l'appliance reste en état préinstallation. Ce processus ne peut pas être inversé.

Vous devez effacer la configuration KMS :

- Avant de pouvoir installer l'appliance dans un autre système StorageGRID, qui n'utilise pas de KMS ou qui utilise un KMS différent.

  > N'effacez pas la configuration KMS si vous prévoyez de réinstaller un nœud d'appliance dans un système StorageGRID qui utilise la même clé KMS.

- Avant de pouvoir récupérer et réinstaller un nœud où la configuration KMS était perdue et où la clé KMS n'est pas récupérable.

- Avant de retourner tout appareil déjà utilisé sur votre site.
- Après la désaffectation d'une appliance qui avait activé le chiffrement de nœud.

> Désaffectez l'appliance avant d'effacer KMS pour déplacer ses données vers d'autres nœuds de votre système StorageGRID. L'effacement de KMS avant la mise hors service de l'appareil entraînera une perte de données et pourrait rendre l'appareil inutilisable.

Étapes

1. Ouvrez un navigateur et entrez l'une des adresses IP du contrôleur de calcul de l'appliance.

   `https://Controller_IP:8443`

   `Controller_IP` Est l'adresse IP du contrôleur de calcul (pas le contrôleur de stockage) sur l'un des trois réseaux StorageGRID.

   La page d'accueil du programme d'installation de l'appliance StorageGRID s'affiche.

2. Sélectionnez **configurer le matériel** > **cryptage de nœud**.

   > Si la configuration KMS est effacée, les données de l'appliance seront définitivement supprimées. Ces données ne peuvent pas être récupérées.

3. En bas de la fenêtre, sélectionnez **Effacer la clé KMS et Supprimer les données**.
4. Si vous êtes sûr de vouloir effacer la configuration KMS, tapez **`clear`** Dans la boîte de dialogue d'avertissement et sélectionnez **Effacer la clé KMS et Supprimer les données**.

   La clé de chiffrement KMS et toutes les données sont supprimées du nœud, et l'appliance redémarre. Cette opération peut prendre jusqu'à 20 minutes.

5. Ouvrez un navigateur et entrez l'une des adresses IP du contrôleur de calcul de l'appliance.
   `https://Controller_IP:8443`

   `Controller_IP` Est l'adresse IP du contrôleur de calcul (pas le contrôleur de stockage) sur l'un des trois réseaux StorageGRID.

   La page d'accueil du programme d'installation de l'appliance StorageGRID s'affiche.

6. Sélectionnez **configurer le matériel** > **cryptage de nœud**.
7. Vérifiez que le chiffrement de nœud est désactivé et que les informations de clé et de certificat dans **Key Management Server Details** et le contrôle **clear KMS Key et Delete Data** sont supprimées de la fenêtre.

   Le chiffrement de nœud ne peut pas être réactivé sur l'appliance tant qu'il n'a pas été réinstallé dans une grille.

Une fois que vous avez terminé

Après le redémarrage de l'appliance et après avoir vérifié que KMS a été effacé et que l'appliance est dans un état de pré-installation, vous pouvez physiquement retirer l'appliance de votre système StorageGRID. Voir la "instructions de préparation de l'appareil pour la réinstallation".

Clonage de nœuds d'appliance

Clonage de nœuds de l'appliance : présentation

Vous pouvez cloner un nœud d'appliance dans StorageGRID pour utiliser une appliance plus récente ou des fonctionnalités améliorées. Le clonage transfère toutes les informations relatives au nœud existant vers la nouvelle appliance, fournit un processus de mise à niveau matérielle facile à exécuter et offre une alternative à la mise hors service et à l'extension en cas de remplacement d'appliances.

Le clonage de nœuds d'appliance vous permet de remplacer facilement un nœud d'appliance (source) existant dans votre grid par une appliance (cible) compatible faisant partie du même site StorageGRID logique. Le processus transfère toutes les données vers la nouvelle appliance, en les plaçant en service pour remplacer l'ancien nœud d'appliance et laisser l'ancienne appliance dans un état de préinstallation.

Pourquoi cloner un nœud d'appliance ?

Il est possible de cloner un nœud d'appliance si vous avez besoin de :

- Remplacez les appareils qui arrivent en fin de vie.
- Mettez à niveau les nœuds existants pour tirer parti d'une technologie d'appliance améliorée.
- Augmentez la capacité de stockage de grille sans modifier le nombre de nœuds de stockage dans votre système StorageGRID.
- Améliorez l'efficacité du stockage, par exemple en passant du mode RAID de DDP-8 à DDP-16, ou à RAID-6.
- Implémentation efficace du chiffrement des nœuds pour permettre l'utilisation de serveurs de gestion des clés externes (KMS)

Quel réseau StorageGRID est utilisé ?

Le clonage transfère les données du nœud source directement vers l'appliance cible sur l'un des trois réseaux StorageGRID. Le réseau Grid est généralement utilisé, mais vous pouvez également utiliser le réseau Admin ou le réseau client si l'appliance source est connectée à ces réseaux. Choisir le réseau à utiliser pour le trafic de clonage qui fournit les meilleures performances de transfert de données sans affecter les performances du réseau StorageGRID ni la disponibilité des données.

Lorsque vous installez l'appliance de remplacement, vous devez spécifier des adresses IP temporaires pour la connexion StorageGRID et le transfert de données. L'appliance de remplacement faisant partie des mêmes réseaux que le nœud d'appliance qu'elle remplace, vous devez spécifier des adresses IP temporaires pour chacun de ces réseaux sur l'appliance de remplacement.

Compatibilité de l'appareil cible

Les appliances de remplacement doivent être du même type que le nœud source qu'elles remplacent et doivent tous deux faire partie du même site StorageGRID logique.

- Une appliance de services de remplacement peut être différente du nœud d'administration ou du nœud de passerelle qu'elle remplace.
  - Vous pouvez cloner une appliance de nœud source SG100 sur une appliance cible de services SG1000 pour offrir une plus grande capacité au nœud d'administration ou au nœud de passerelle.
  - Vous pouvez cloner une appliance de nœud source SG1000 sur une appliance cible de services

SG100 afin de redéployer le SG1000 pour une application plus exigeante.

Par exemple, si une appliance de nœud source SG1000 est utilisée en tant que nœud d'administration et que vous souhaitez l'utiliser comme nœud d'équilibrage de charge dédié.

  - Le remplacement d'une appliance de nœud source SG1000 par un dispositif cible de services SG100 réduit la vitesse maximale des ports réseau de 100 GbE à 25 GbE.
  - Les appareils SG100 et SG1000 sont dotés de connecteurs réseau différents. Il peut être nécessaire de remplacer les câbles ou les modules SFP pour changer de type d'appliance.

- Une appliance de stockage de remplacement doit avoir une capacité supérieure à celle du nœud de stockage qu'elle remplace.

  - Si l'appliance de stockage cible dispose du même nombre de disques que le nœud source, les disques de l'appliance cible doivent avoir une capacité supérieure (en To).
  - Si vous prévoyez d'utiliser le même mode RAID sur le nœud cible que celui utilisé sur le nœud source, Ou en mode RAID moins efficace pour le stockage (par exemple, le passage de RAID 6 à DDP), les disques de l'appliance cible doivent être plus grands (en To) que les disques de l'appliance source.
  - Si le nombre de disques standard installés sur une appliance de stockage cible est inférieur au nombre de disques du nœud source, en raison de l'installation de disques SSD, la capacité de stockage globale des disques standard de l'appliance cible (en To) Doit dépasser la capacité totale du disque fonctionnel de tous les disques du nœud de stockage source.

    Par exemple, lors du clonage d'une appliance de nœud de stockage source SG5760 avec 60 disques dans une appliance SG6060 cible avec 58 disques standard, des disques plus grands doivent être installés dans l'appliance SG6060 cible avant le clonage pour maintenir la capacité de stockage. (Les deux emplacements de disque contenant des disques SSD dans l'appliance cible ne sont pas inclus dans la capacité totale de stockage de l'appliance.)

    Toutefois, si une appliance de nœud source SG5760 de 60 disques est configurée avec des pools de disques dynamiques SANtricity DDP-8, la configuration d'une appliance cible SG6060 de même taille de 58 disques avec DDP-16 peut faire de l'appliance SG6060 une cible de clone valide en raison de son efficacité du stockage améliorée.

  Vous pouvez afficher des informations sur le mode RAID actuel du nœud de l'appliance source sur la page **NODES** dans Grid Manager. Sélectionnez l'onglet **stockage** de l'appareil.

- Le nombre de volumes d'une appliance de stockage cible doit être supérieur ou égal au nombre de volumes du nœud source. Vous ne pouvez pas cloner un nœud source avec 16 volumes de magasin d'objets (rangedb) vers une appliance de stockage cible avec 12 volumes de magasin d'objets, même si l'appliance cible a une capacité supérieure au nœud source. La plupart des appliances de stockage disposent de 16 volumes de stockage objet, à l'exception de l'appliance SGF6112 qui ne dispose que de 12 volumes de stockage objet.

Quelles informations ne sont pas clonées ?

Les configurations d'appliance suivantes ne sont pas transférées vers l'appliance de remplacement pendant le clonage. Vous devez les configurer lors de la configuration initiale de l'appliance de remplacement.

- Interface BMC
- Liens réseau
- État du chiffrement de nœud
- SANtricity System Manager (pour les nœuds de stockage)

- Mode RAID (pour les nœuds de stockage)

Quels problèmes empêchent le clonage ?

Si l'un des problèmes suivants est rencontré lors du clonage, le processus de clonage s'arrête et un message d'erreur est généré :

- Configuration réseau incorrecte
- Manque de connectivité entre les appareils source et cible
- Incompatibilité entre l'appareil source et l'appareil cible
- Pour les nœuds de stockage, une appliance de remplacement de capacité insuffisante

Vous devez résoudre chaque problème pour que le clonage puisse continuer.

Considérations et configuration requise pour le clonage des nœuds d'appliance

Avant de cloner un nœud d'appliance, vous devez comprendre les considérations et les exigences.

Configuration matérielle requise pour l'appliance de remplacement

Assurez-vous que l'appareil de remplacement répond aux critères suivants :

- Le nœud source (appliance en cours de remplacement) et la cible (nouvelle) appliance doivent être du même type d'appliance :
  - Vous pouvez cloner uniquement une appliance de nœud d'administration ou une appliance de nœud de passerelle vers une nouvelle appliance de services.
  - Vous ne pouvez cloner qu'une appliance de nœud de stockage sur une nouvelle appliance de stockage.
- Pour les appliances de nœud d'administration ou de nœud de passerelle, l'appliance de nœud source et l'appliance cible n'ont pas besoin d'être du même type d'appliance. Toutefois, pour changer de type d'appliance, il peut être nécessaire de remplacer les câbles ou les modules SFP.

  Par exemple, vous pouvez remplacer une appliance SG1000 par une appliance SG100 ou remplacer une appliance SG100 par une appliance SG1000.

- Pour les appliances de nœuds de stockage, l'appliance de nœuds source et l'appliance cible n'ont pas besoin d'être du même type d'appliance ; cependant :
  - L'appliance cible doit avoir une capacité de stockage supérieure à celle de l'appliance source.

    Par exemple, vous pouvez remplacer une appliance SG5700 nœuds par une appliance SG6000.

  - L'appliance cible doit disposer d'un nombre égal ou supérieur de volumes de stockage objet à celui de l'appliance source.

    Par exemple, vous ne pouvez pas remplacer une appliance de nœuds SG6000 (16 volumes de magasin d'objets) par une appliance SGF6112 (12 volumes de magasin d'objets).

Contactez votre ingénieur commercial StorageGRID pour savoir comment choisir des appliances de remplacement compatibles afin de cloner des nœuds d'appliance spécifiques dans votre installation StorageGRID.

Préparez-vous à cloner un nœud d'appliance

Avant de cloner un nœud d'appliance, vous devez disposer des informations suivantes :

- Obtenez une adresse IP temporaire pour le réseau Grid auprès de votre administrateur réseau pour l'utiliser avec l'appliance cible lors de l'installation initiale. Si le nœud source appartient à un réseau d'administration ou à un réseau client, obtenez des adresses IP temporaires pour ces réseaux.

  Les adresses IP temporaires se trouvent généralement sur le même sous-réseau que l'appliance de nœud source clonée, et ne sont pas nécessaires une fois le clonage terminé. Les appliances source et cible doivent se connecter au nœud d'administration principal de votre StorageGRID pour établir une connexion de clonage.

- Déterminer le réseau à utiliser pour le clonage du trafic de transfert de données qui offre les meilleures performances de transfert de données sans affecter les performances du réseau StorageGRID ni la disponibilité des données.

  > ⓘ L'utilisation du réseau d'administration 1 GbE pour le transfert des données de clonage entraîne un clonage plus lent.

- Déterminez si le chiffrement des nœuds à l'aide d'un serveur de gestion des clés (KMS) sera utilisé sur l'appliance cible. Vous pouvez ainsi activer le chiffrement des nœuds lors de l'installation initiale de l'appliance cible avant le clonage. Vous pouvez vérifier si le chiffrement de nœud est activé sur le nœud de l'appliance source, comme indiqué dans la section "activation du chiffrement de nœud".

  Le nœud source et l'appliance cible peuvent avoir des paramètres de chiffrement de nœud différents. Le décryptage et le cryptage des données s'effectuent automatiquement pendant le transfert de données et lorsque le nœud cible redémarre et rejoint la grille.

- Déterminez si le mode RAID de l'appliance cible doit être modifié par défaut, afin que vous puissiez spécifier ces informations lors de l'installation initiale de l'appliance cible avant le clonage. Vous pouvez afficher des informations sur le mode RAID actuel du nœud de l'appliance source sur la page **NODES** dans Grid Manager. Sélectionnez l'onglet **stockage** de l'appareil.

  Le nœud source et l'appliance cible peuvent avoir des paramètres RAID différents.

- Planifiez le processus de clonage des nœuds suffisamment de temps. Il peut être nécessaire de plusieurs jours pour transférer les données d'un nœud de stockage opérationnel vers une appliance cible. Planifiez le clonage afin de limiter l'impact sur vos activités.
- Vous ne devez cloner qu'un seul nœud d'appliance à la fois. Le clonage peut vous empêcher d'effectuer simultanément d'autres fonctions de maintenance de StorageGRID.
- Une fois que vous avez cloné un nœud d'appliance, vous pouvez utiliser l'appliance source qui a été retournée à un état de préinstallation comme cible pour cloner une autre appliance de nœud compatible.

Clonez le nœud d'appliance

Le processus de clonage peut prendre plusieurs jours pour transférer les données entre le nœud source (appliance à remplacer) et l'appliance cible (nouvelle).

Avant de commencer

- Vous avez installé l'appareil cible compatible dans une armoire ou un rack, connecté tous les câbles et mis sous tension.

- Vous avez vérifié que la version du programme d'installation de l'appliance StorageGRID installée sur l'appliance de remplacement correspond à la version logicielle de votre système StorageGRID, en mettant à niveau le micrologiciel du programme d'installation de l'appliance StorageGRID, si nécessaire.
- L'appliance cible est configurée, y compris la configuration des connexions StorageGRID, SANtricity System Manager (dispositifs de stockage uniquement) et l'interface BMC.
  - Lors de la configuration des connexions StorageGRID, utilisez les adresses IP temporaires.
  - Lors de la configuration des liaisons réseau, utilisez la configuration de liaison finale.

> Laissez le programme d'installation de l'appliance StorageGRID ouvert une fois la configuration initiale de l'appliance cible terminée. Vous revenez à la page d'installation de l'appliance cible après avoir démarré le processus de clonage des nœuds.

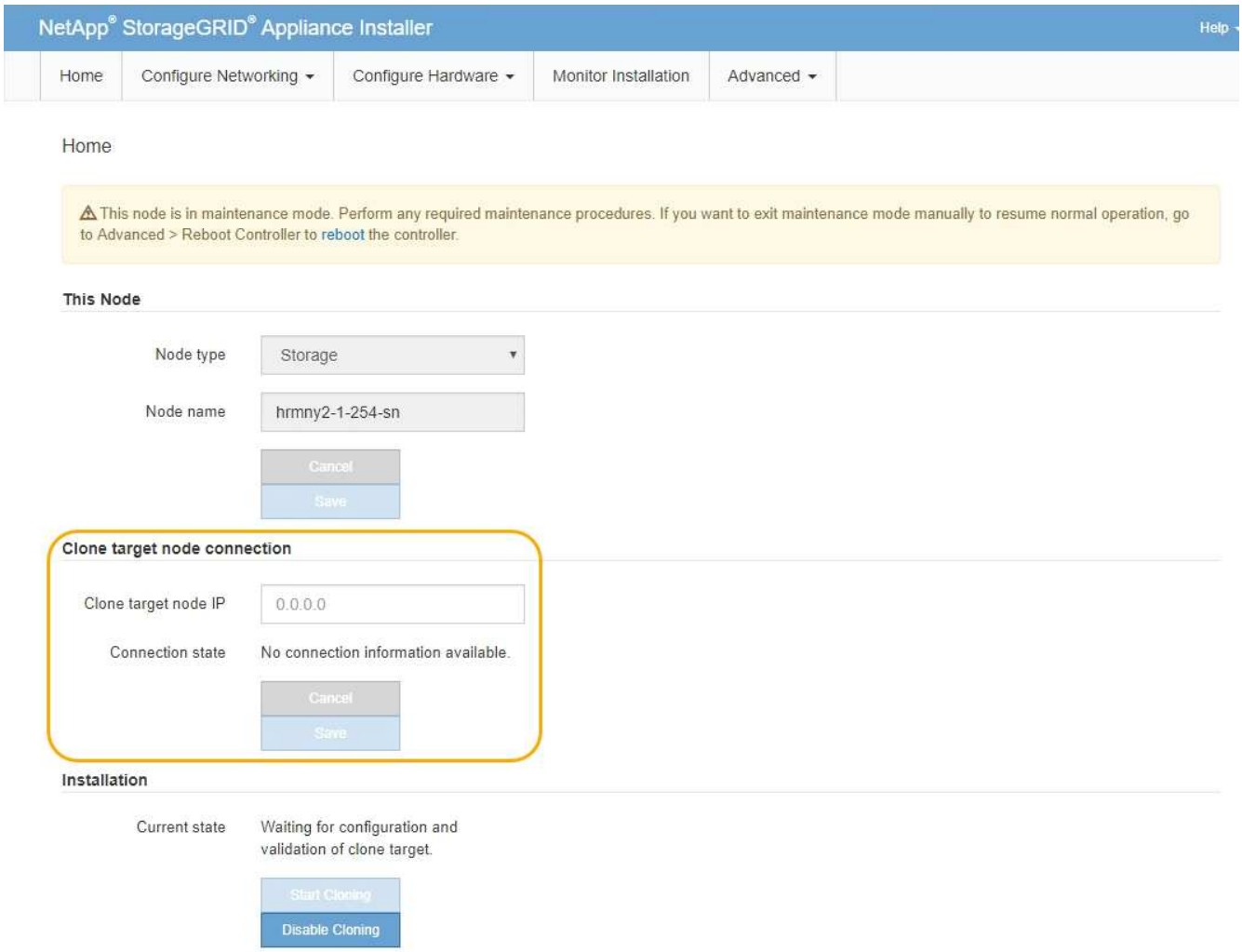
- Vous avez éventuellement activé le chiffrement de nœud pour l'appliance cible.
- Vous avez facultatif de définir le mode RAID pour l'appliance cible (dispositifs de stockage uniquement).
- Vous avez passé en revue le "considérations et conditions requises pour le clonage des nœuds de l'appliance".

Pour préserver les performances du réseau StorageGRID et la disponibilité des données, vous devez cloner un seul nœud d'appliance à la fois.

Étapes

1. "Placez le nœud source que vous clonez en mode de maintenance".
2. À partir du programme d'installation de l'appliance StorageGRID sur le nœud source, dans la section installation de la page d'accueil, sélectionnez **Activer le clonage**.

   La section connexion au nœud d'administration principal est remplacée par la section connexion au nœud cible clone.



3. Pour **Clone Target node IP**, entrez l'adresse IP temporaire attribuée au nœud cible pour que le réseau utilise pour le trafic de transfert de données clone, puis sélectionnez **Enregistrer**.

   En général, vous entrez l'adresse IP du réseau Grid, mais si vous devez utiliser un autre réseau pour le trafic de transfert de données clone, entrez l'adresse IP du nœud cible sur ce réseau.

   > L'utilisation du réseau d'administration 1 GbE pour le transfert des données de clonage entraîne un clonage plus lent.

   Une fois l'appliance cible configurée et validée, dans la section installation, **Start Cloning** est activé sur le nœud source.

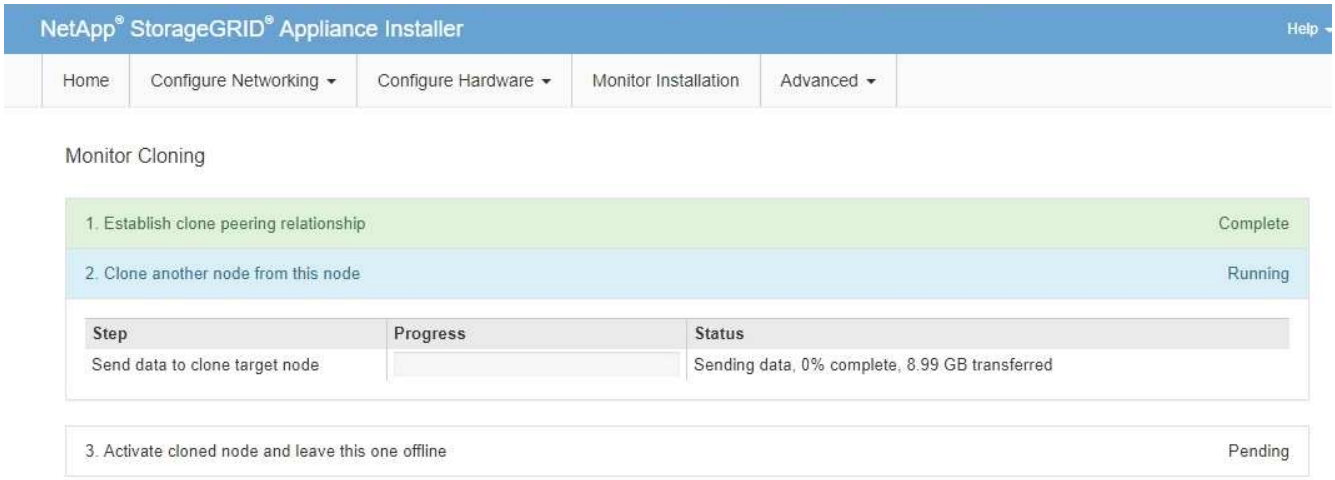
   Si des problèmes empêchent le clonage, **Démarrer le clonage** n'est pas activé et les problèmes que vous devez résoudre sont répertoriés comme l'état **connexion**. Ces problèmes sont répertoriés sur la page d'accueil du programme d'installation de l'appliance StorageGRID du nœud source et de l'appliance cible. Un seul problème s'affiche à la fois et l'état se met automatiquement à jour en fonction des changements de conditions. Résolvez tous les problèmes de clonage pour activer **Démarrer le clonage**.

   Lorsque **Démarrer le clonage** est activé, l'état **actuel** indique le réseau StorageGRID sélectionné pour le clonage du trafic, ainsi que des informations sur l'utilisation de cette connexion réseau. Voir "Considérations et configuration requise pour le clonage des nœuds d'appliance".

4. Sélectionnez **Démarrer le clonage** sur le nœud source.

5. Surveillez la progression du clonage à l'aide du programme d'installation de l'appliance StorageGRID sur le nœud source ou cible.

   Le programme d'installation de l'appliance StorageGRID sur les nœuds source et cible indique le même état.



   La page Monitor Cloning indique la progression détaillée de chaque étape du processus de clonage :

   - **Établir une relation de peering** montre la progression de la configuration et du clonage.
   - **Clone un autre noeud de ce noeud** indique la progression du transfert de données. (Cette partie du processus de clonage peut prendre plusieurs jours.)
   - **Activer le noeud cloné et le laisser hors ligne** indique la progression du transfert du contrôle vers le noeud cible et le placement du noeud source à l'état de pré-installation, une fois le transfert de données terminé.

6. Si vous devez mettre fin au processus de clonage et remettre le nœud source en service avant la fin du clonage, accédez à la page d'accueil du programme d'installation de l'appliance StorageGRID et sélectionnez **Avancé** > **redémarrer le contrôleur**, puis sélectionnez **redémarrer dans StorageGRID**.

   Si le processus de clonage est terminé :

   - Le nœud source quitte le mode de maintenance et rejoint StorageGRID.
   - Le nœud cible reste en état de pré-installation. Pour redémarrer le clonage du nœud source, redémarrez le processus de clonage à partir de l'étape 1.

Une fois le clonage terminé :

- Les nœuds source et cible échangent des adresses IP :
  - Le nœud cible utilise désormais les adresses IP initialement attribuées au nœud source pour les réseaux Grid, Admin et client.
  - Le nœud source utilise maintenant l'adresse IP temporaire initialement attribuée au nœud cible.
- Le nœud cible quitte le mode maintenance et rejoint StorageGRID, en remplaçant le nœud source.
- L'appliance source est préinstallée, comme si vous l'aviez fait "préparez-le pour la réinstallation".

Si l'appliance ne rejoint pas à nouveau la grille, accédez à la page d'accueil du programme d'installation de l'appliance StorageGRID pour le nœud source, sélectionnez **Avancé** > **redémarrer le contrôleur**, puis sélectionnez **redémarrer en mode de maintenance**. Après le redémarrage du nœud source en mode maintenance, répétez la procédure de clonage de nœuds.

- Les données utilisateur restent sur l'appliance source comme option de restauration si un problème inattendu se produit avec le nœud cible. Une fois que le nœud cible a rejoint StorageGRID, les données de l'utilisateur sur l'appliance source sont obsolètes et ne sont plus nécessaires.

  Les données utilisateur obsolètes sont écrasées lorsque vous installez ou développez l'appliance source en tant que nouveau nœud dans une autre grille.

  Vous pouvez également réinitialiser la configuration du contrôleur sur l'appliance source pour rendre ces données inaccessibles :

  a. Ouvrez le "Programme d'installation de l'appliance StorageGRID" Pour l'appliance source utilisant l'adresse IP temporaire initialement attribuée au nœud cible.
  b. Sélectionnez **aide** > **Outils de support et de débogage**.
  c. Sélectionnez **Réinitialiser la configuration du contrôleur de stockage**.

  Si nécessaire, contactez le support technique pour obtenir de l'aide sur la réinitialisation de la configuration du contrôleur de stockage.

  Le remplacement des données ou la réinitialisation de la configuration du contrôleur rendent difficile ou impossible la récupération des données obsolètes. Cependant, aucune de ces méthodes ne supprime les données de l'appliance source de manière sécurisée. Si une suppression sécurisée est nécessaire, utilisez un outil ou un service de nettoyage des données pour supprimer définitivement et en toute sécurité les données de l'appliance source.

Vous pouvez :

- Utilisez l'appliance source comme cible pour les opérations de clonage supplémentaires : aucune configuration supplémentaire n'est requise. Cette appliance dispose déjà de l'adresse IP temporaire attribuée, qui a été spécifiée à l'origine pour la première cible de clone.
- Installez et configurez l'appliance source en tant que nouveau nœud d'appliance.
- Jetez l'appareil source s'il n'est plus utilisé avec StorageGRID.

Maintenance du matériel SGF6112

Maintenance de l'appliance SGF6112

Vous devrez peut-être effectuer des procédures de maintenance sur votre appareil. Cette section présente les procédures spécifiques à la maintenance de votre système SGF6112.

Les procédures décrites dans cette section supposent que l'appliance a déjà été déployée en tant que nœud de stockage dans un système StorageGRID.

Les procédures de maintenance de la configuration sont effectuées à l'aide de l'interface Appliance installer, Grid Manager ou BMC. Ces procédures comprennent :

- Allumer et éteindre le voyant d'identification de l'appareil
- Localisez l'appliance dans le data Center
- Arrêtez l'appareil
- Modifier la configuration de la liaison de l'appliance

Les procédures de maintenance matérielle nécessitent la manipulation physique de composants SGF6112 spécifiques.

Mise à niveau du firmware des disques

Le firmware des disques du SGF6112 est automatiquement vérifié chaque fois que l'appliance est redémarrée. Si nécessaire, le micrologiciel est automatiquement mis à niveau vers la version attendue par la version actuelle de StorageGRID. En règle générale, les mises à niveau de firmware se produisent pendant les mises à niveau du logiciel StorageGRID. Toutes les mises à niveau nécessaires du micrologiciel de lecteur pour les versions StorageGRID existantes seront incluses dans les correctifs. Suivez les instructions fournies avec chaque correctif pour vous assurer que la mise à niveau est appliquée à tous les lecteurs qui pourraient en bénéficier.

SANtricity System Manager n'est pas nécessaire pour la maintenance de l'appliance SGF6112.

Procédures générales de maintenance

Voir "Procédures de maintenance courantes" pour les procédures identiques pour tous les dispositifs, telles que l'application d'un correctif, la récupération d'un nœud ou d'un site et la maintenance du réseau.

Voir "Configurez le matériel de l'appliance" pour les procédures de maintenance de l'appliance qui sont également effectuées lors de l'installation et de la configuration initiales de l'appliance.

Procédures de maintenance de la configuration

Allumer et éteindre le voyant d'identification de l'appareil

Le voyant d'identification bleu situé à l'avant et à l'arrière de l'appareil peut être allumé pour faciliter la localisation de l'appareil dans un centre de données.

Avant de commencer

Vous disposez de l'adresse IP BMC de l'appliance que vous souhaitez identifier.

Étapes

1. Accédez à l'interface BMC de l'appliance.
2. Sélectionnez **identification du serveur**.

   L'état actuel de la LED Identify est sélectionné.

3. Sélectionnez **ON** ou **OFF**, puis sélectionnez **Exécuter l'action**.

   Lorsque vous sélectionnez **ACTIVÉ**, les voyants d'identification bleus s'allument à l'avant (illustré) et à l'arrière de l'appareil.

Si un panneau est installé sur le contrôleur, il peut être difficile de voir le voyant d'identification avant.

4. Allumer et éteindre le voyant selon les besoins.

Informations associées

"Localisez l'appliance dans le data Center"

"Accéder à l'interface BMC"

Localisez l'appliance dans le data Center

Localisez l'appliance pour pouvoir effectuer les opérations de maintenance ou de mise à niveau du matériel.

Avant de commencer

- Vous avez déterminé quel appareil doit être entretenu.
- Pour localiser l'appliance dans votre data Center, "Activez le voyant d'identification bleu".

Étapes

1. Trouvez l'appliance dans le data Center.
   - Recherchez un voyant d'identification bleu allumé à l'avant ou à l'arrière de l'appareil.

     Le voyant d'identification avant se trouve derrière le cadre avant et peut être difficile à voir si le cadre est installé.

   - Vérifiez que les étiquettes apposées à l'avant de l'appareil correspondent à la référence pour vous

assurer que vous avez trouvé l'appareil approprié.

2. Retirez le cadre avant, le cas échéant, pour accéder aux commandes et aux voyants du panneau avant.
3. Éteignez le voyant d'identification bleu si vous l'avez utilisé pour localiser l'appareil.
   - Appuyez sur le commutateur LED Identify situé sur le panneau avant de l'appareil.
   - Utilisez l'interface BMC de l'appliance.

Arrêtez l'appliance SGF6112

Arrêtez l'appliance pour effectuer une maintenance matérielle.

Avant de commencer

- Vous avez "l'appareil se trouve physiquement".

Description de la tâche

Pour éviter toute interruption de service, éteignez l'appareil pendant une fenêtre de maintenance planifiée lorsque des périodes d'interruption de service sont normalement prévues.

Étapes

1. Éteignez l'appareil :

   > Vous devez effectuer un arrêt contrôlé de l'appliance en entrant les commandes indiquées ci-dessous. Il est recommandé d'effectuer un arrêt contrôlé lorsque cela est possible pour éviter les alertes inutiles, vérifier que les journaux complets sont disponibles et éviter toute interruption de service.

   a. Si vous n'avez pas encore ouvert de session sur le nœud grid, connectez-vous à l'aide de PuTTY ou d'un autre client ssh :
      i. Saisissez la commande suivante : `ssh admin@grid_node_IP`
      ii. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
      iii. Entrez la commande suivante pour passer à la racine : `su -`
      iv. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

      Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

   b. Arrêtez l'appareil :
      `shutdown -h now`

      Cette commande peut prendre jusqu'à 10 minutes.

2. Utilisez l'une des méthodes suivantes pour vérifier que l'appareil est hors tension :
   - Vérifiez que le voyant d'alimentation situé à l'avant de l'appareil est éteint.
   - Consultez la page Power Control de l'interface BMC pour vérifier que l'appliance est éteinte.

Mettez le SGF6112 sous tension et vérifiez son fonctionnement

Mettez le contrôleur sous tension après la fin de la maintenance.

Avant de commencer

- Vous avez installé le contrôleur dans une armoire ou un rack et connecté les câbles de données et d'alimentation.

  "Réinstallez le contrôleur SGF6112 dans l'armoire ou le rack"

- Vous avez physiquement situé le contrôleur dans le data Center.

  "Localisez l'appliance SGF6112 dans le data Center"

Étapes

1. Mettez l'appareil sous tension.

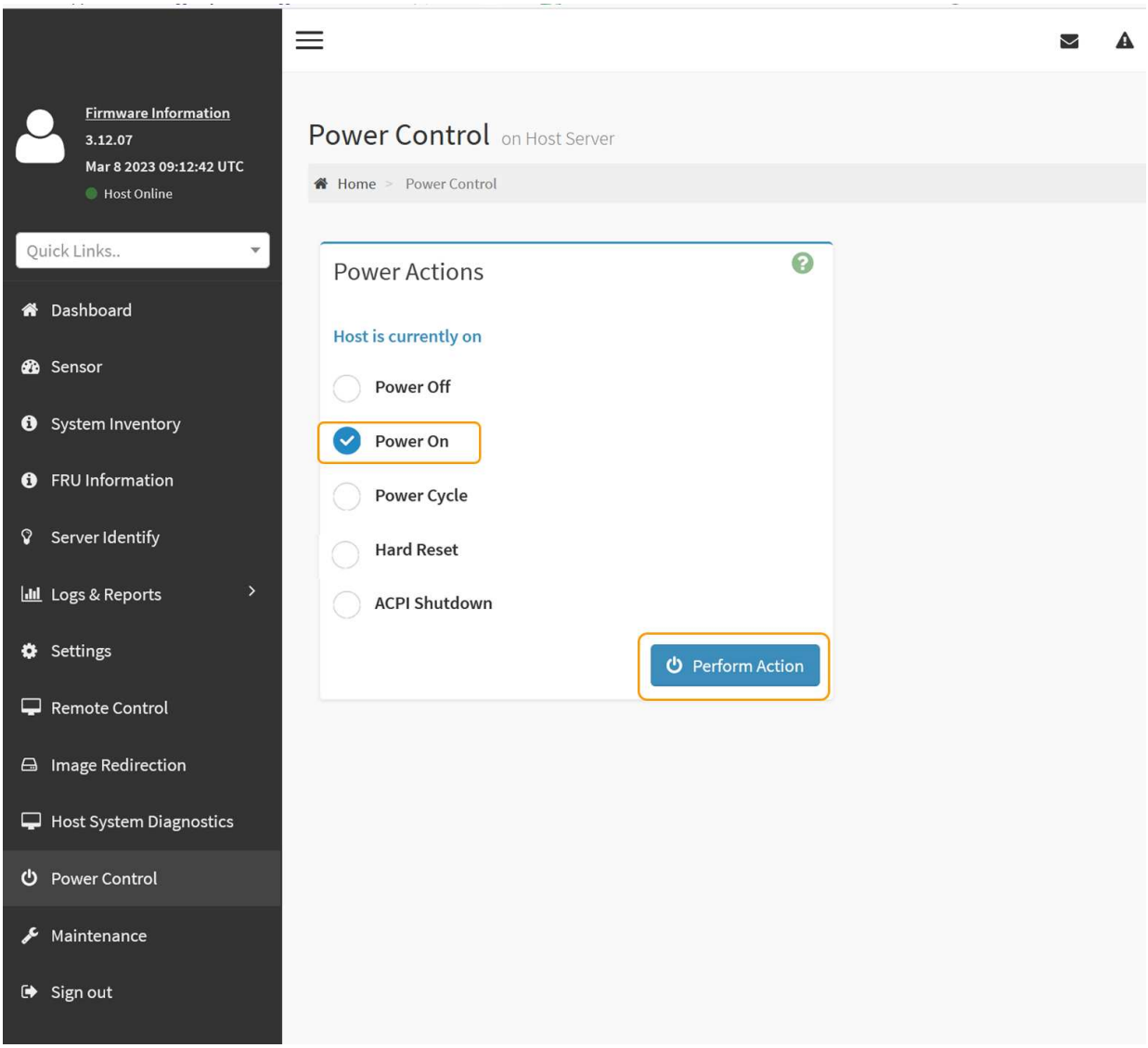
   Vous devrez peut-être retirer le cadre pour accéder à l'interrupteur d'alimentation. Si c'est le cas, n'oubliez pas de le réinstaller ensuite.

2. Surveillez les voyants du contrôleur et les codes de démarrage à l'aide de l'une des méthodes suivantes :

   - Appuyer sur le bouton de mise sous tension situé à l'avant du contrôleur.
   - Utilisez l'interface du contrôleur BMC :
     i. Accéder à l'interface du contrôleur BMC.

        "Accéder à l'interface BMC"

     ii. Sélectionnez **Power Control**.
     iii. Sélectionnez **Marche**, puis **Exécuter l'action**.



Utilisez l'interface BMC pour surveiller l'état de démarrage.

3. Vérifiez que le contrôleur de l'appliance s'affiche dans Grid Manager et sans alertes.

   L'affichage du contrôleur dans Grid Manager peut prendre jusqu'à 20 minutes.

   > Ne mettez pas un autre nœud d'appliance hors ligne sauf si cette appliance présente une icône verte.

4. Vérifiez que la nouvelle appliance est entièrement opérationnelle en vous connectant au nœud grid à l'aide de PuTTY ou d'un autre client ssh :

   a. Saisissez la commande suivante : `ssh Appliance_IP`

   b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

   c. Entrez la commande suivante pour passer à la racine : `su -`

   d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

      Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

Informations associées

"Afficher les indicateurs d'état"

Modifier la configuration de la liaison de l'appliance SGF6112

Vous pouvez modifier la configuration de la liaison Ethernet de l'appliance, notamment le mode de liaison du port, le mode de liaison réseau et la vitesse de liaison.

Avant de commencer

- Vous avez "placez l'appareil en mode maintenance".

> Dans de rares cas, le fait de placer une appliance StorageGRID en mode de maintenance peut rendre l'appliance indisponible pour l'accès à distance.

Étapes

1. Dans le programme d'installation de l'appliance StorageGRID, sélectionnez **configurer réseau** > **Configuration lien**.
2. Apportez les modifications souhaitées à la configuration de liaison.

   Pour plus d'informations sur les options, reportez-vous à la section "Configurer les liaisons réseau".

3. Lorsque vous êtes satisfait de vos sélections, cliquez sur **Enregistrer**.

   > Vous risquez de perdre votre connexion si vous avez apporté des modifications au réseau ou au lien auquel vous êtes connecté. Si vous n'êtes pas reconnecté dans un délai d'une minute, saisissez à nouveau l'URL du programme d'installation de l'appliance StorageGRID à l'aide de l'une des autres adresses IP attribuées à l'appliance : `https://appliance_IP:8443`

4. Apportez les modifications nécessaires aux adresses IP de l'appliance.

   Si vous avez modifié les paramètres VLAN, le sous-réseau de l'appliance a peut-être changé. Si vous devez modifier les adresses IP de l'appliance, reportez-vous à la section "Configurez les adresses IP StorageGRID".

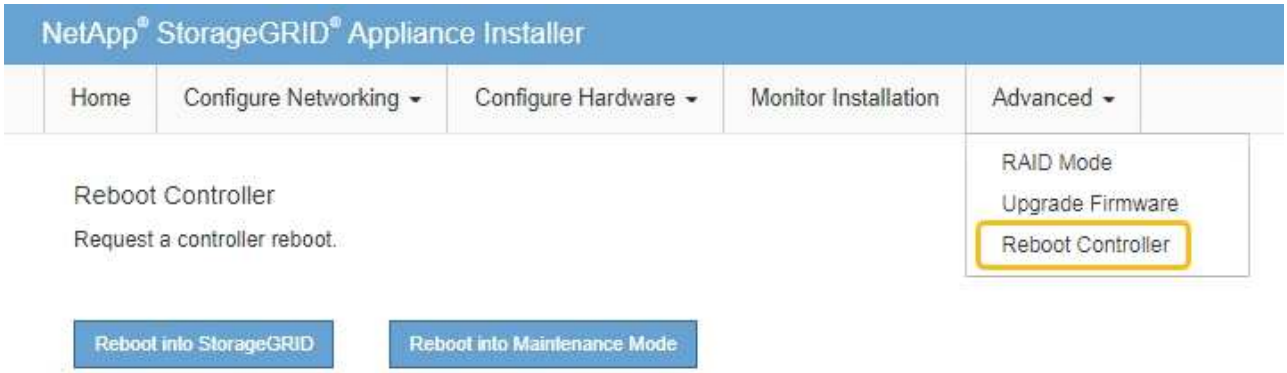
5. Sélectionnez **configurer réseau** > **Test Ping** dans le menu.
6. Utilisez l'outil de test Ping pour vérifier la connectivité aux adresses IP sur tous les réseaux susceptibles d'avoir été affectés par les modifications de configuration de liaison effectuées lors de la configuration de l'appliance.

   En plus des autres tests que vous choisissez d'effectuer, confirmez que vous pouvez envoyer une commande ping à l'adresse IP du réseau de la grille du nœud d'administration principal et à l'adresse IP du réseau de la grille d'au moins un autre nœud. Si nécessaire, revenez aux instructions de configuration des liaisons réseau et corrigez tout problème.

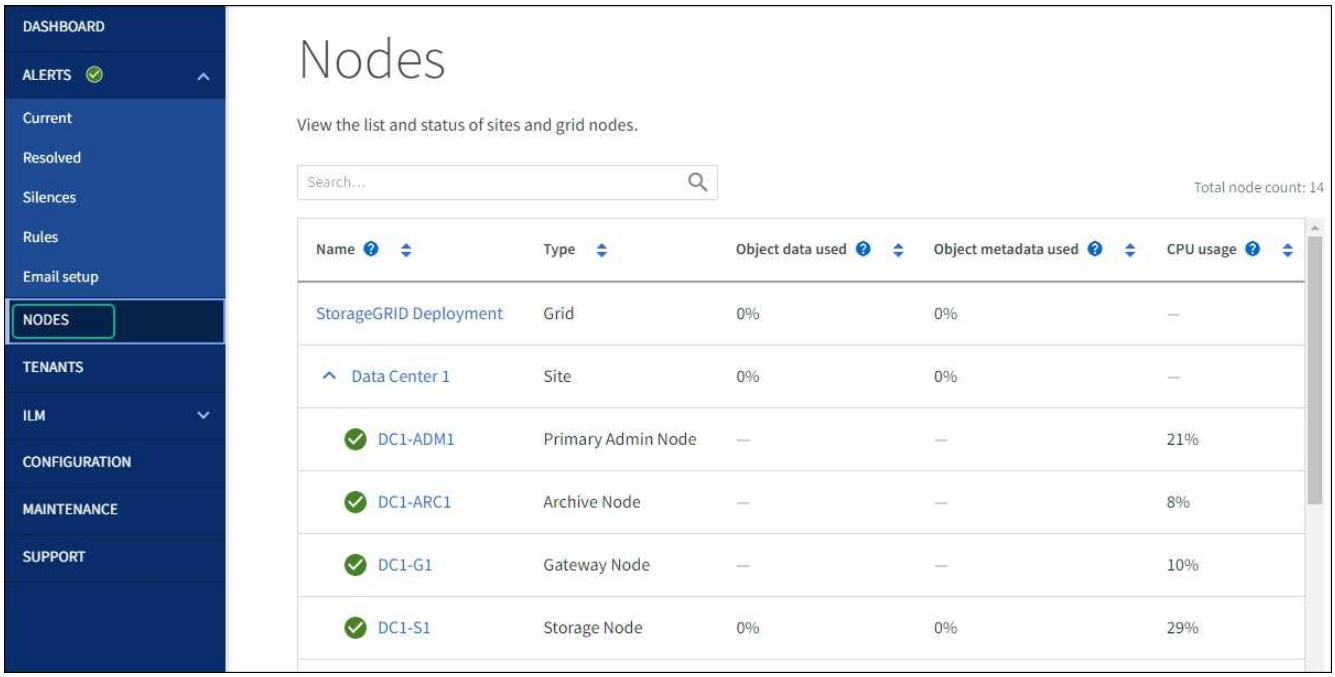
7. Une fois que vous êtes satisfait du fait que les modifications de configuration du lien fonctionnent, redémarrez le nœud. Dans le programme d'installation de l'appliance StorageGRID, sélectionnez **Avancé** > **redémarrer le contrôleur**, puis sélectionnez l'une des options suivantes :

   - Sélectionnez **Reboot into StorageGRID** pour redémarrer le contrôleur de calcul avec le nœud rejoignant la grille. Sélectionnez cette option si vous avez terminé de travailler en mode maintenance et que vous êtes prêt à rétablir le fonctionnement normal du nœud.

◦ Sélectionnez **redémarrer en mode maintenance** pour redémarrer le contrôleur de calcul avec le nœud restant en mode maintenance. (Cette option est disponible uniquement lorsque le contrôleur est en mode maintenance.) Sélectionnez cette option si des opérations de maintenance supplémentaires doivent être effectuées sur le nœud avant de rejoindre à nouveau la grille.



L'appliance peut redémarrer et rejoindre la grille en 20 minutes. Pour confirmer que le redémarrage est terminé et que le nœud a rejoint la grille, retournez à la grille Manager. La page **NODES** doit afficher un état normal (icône de coche verte à gauche du nom du nœud) pour le nœud de l'appliance, indiquant qu'aucune alerte n'est active et que le nœud est connecté à la grille.



Procédures de maintenance du matériel

Vérifiez le composant à remplacer dans le SGF6112

Si vous n'êtes pas sûr du composant matériel à remplacer dans votre appareil, suivez cette procédure pour identifier le composant et l'emplacement de l'appareil dans le centre de données.

Avant de commencer

- Vous disposez du numéro de série du dispositif de stockage sur lequel le composant doit être remplacé.
- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".

Description de la tâche

Utilisez cette procédure pour identifier l'appareil dont le matériel est défectueux et lequel des composants matériels remplaçables suivants ne fonctionne pas correctement :

- Blocs d'alimentation
- Ventilateurs
- Disques SSD
- Cartes d'interface réseau (NIC)
- Pile CMOS

Étapes

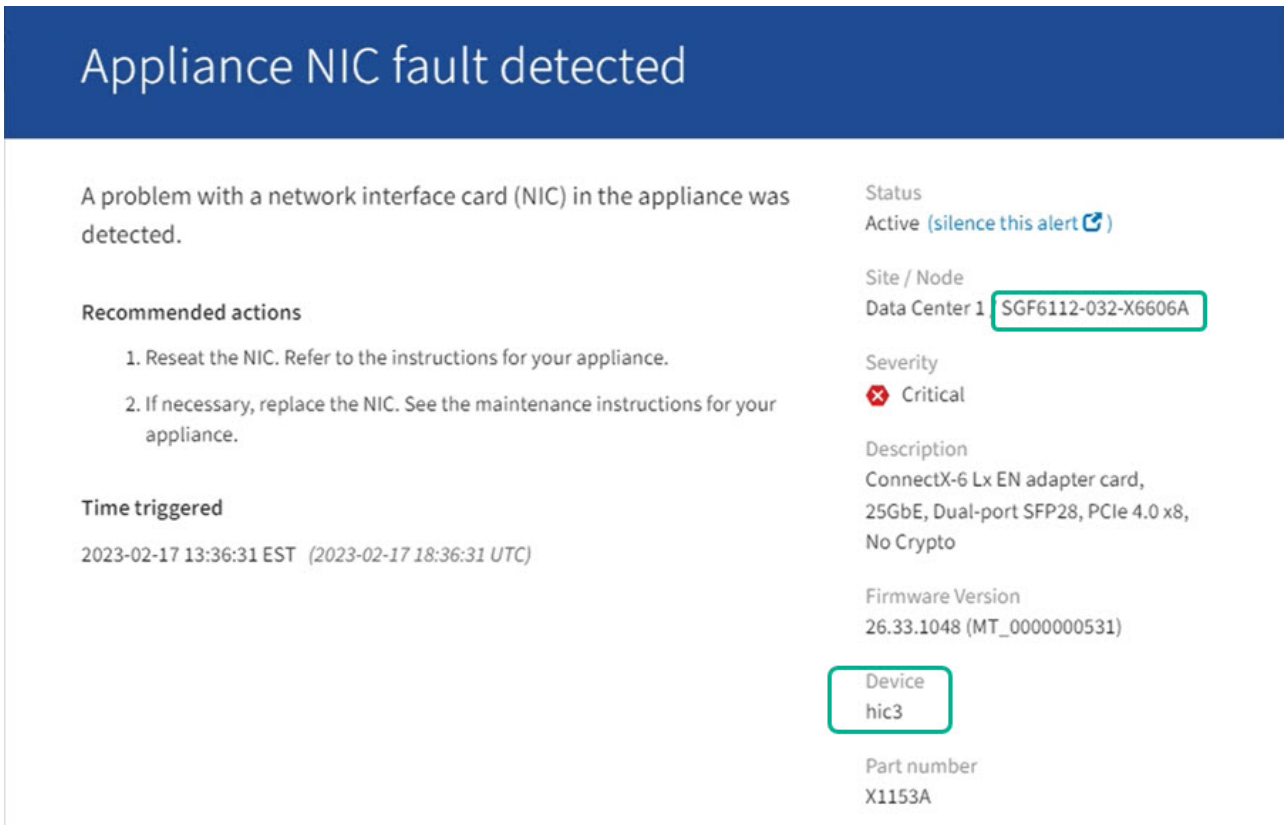
1. Identifiez le composant défectueux et le nom de l'appliance dans laquelle il est installé.
   a. Dans Grid Manager, sélectionnez **ALERTES** > **Current**.

      La page alertes s'affiche.

   b. Sélectionnez l'alerte pour afficher les détails de l'alerte.

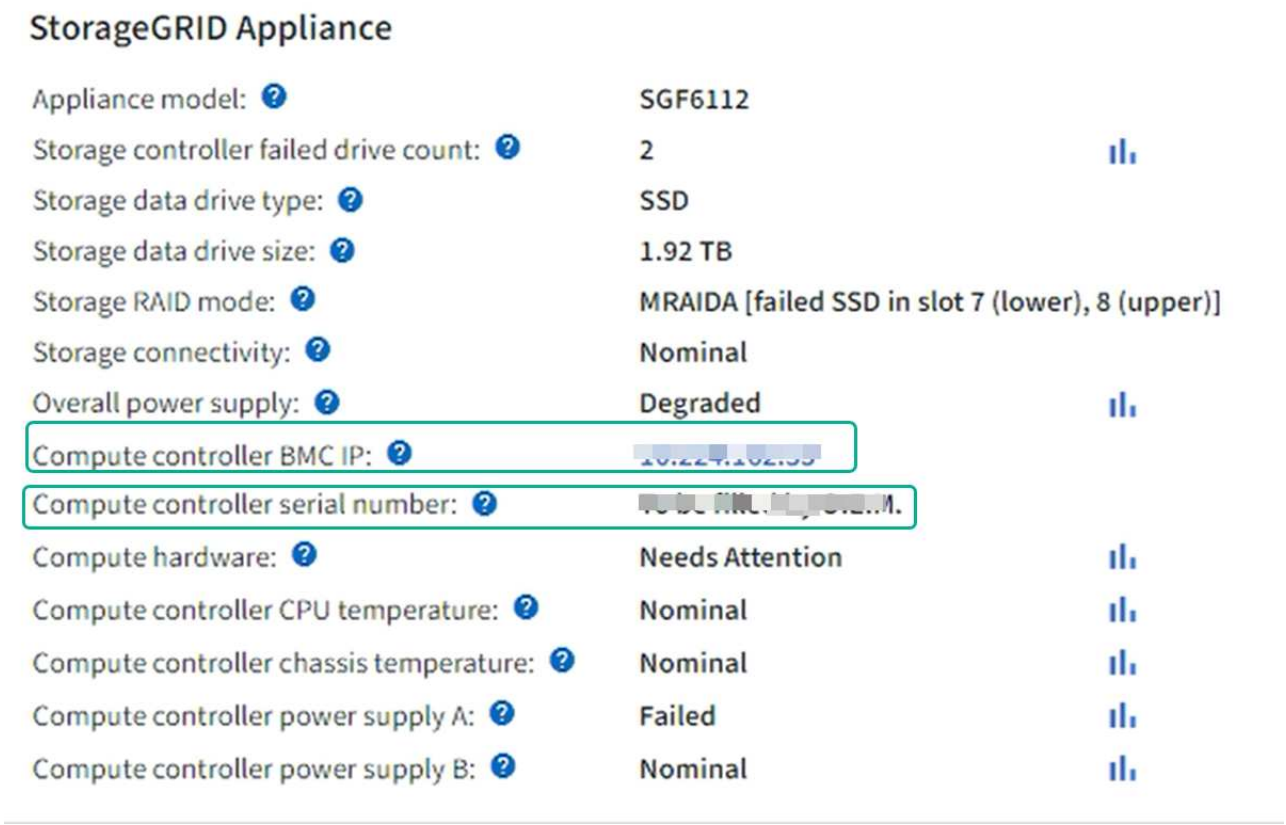
      Sélectionnez l'alerte, et non l'en-tête d'un groupe d'alertes.

   c. Notez le nom du nœud et l'étiquette d'identification unique du composant qui a échoué.



2. Identifiez le châssis avec le composant qui doit être remplacé.
   a. Dans Grid Manager, sélectionnez **NODES**.
   b. Dans le tableau de la page nœuds, sélectionnez le nom du nœud de stockage de l'appliance avec le composant défaillant.
   c. Sélectionnez l'onglet **matériel**.

      Vérifiez le **numéro de série du contrôleur de calcul** dans la section appareil StorageGRID. Vérifiez si le numéro de série correspond au numéro de série du dispositif de stockage sur lequel vous remplacez le composant. Si le numéro de série correspond, vous avez trouvé l'appareil approprié.



      - Si la section StorageGRID Appliance du Gestionnaire de grille ne s'affiche pas, le nœud sélectionné n'est pas une appliance StorageGRID. Sélectionnez un nœud différent dans l'arborescence.
      - Si les numéros de série ne correspondent pas, sélectionnez un autre nœud dans l'arborescence.

3. Après avoir localisé le nœud sur lequel le composant doit être remplacé, notez l'adresse IP du contrôleur BMC de l'appliance indiquée dans la section appareil StorageGRID.

   Pour vous aider à localiser l'appliance dans le centre de données, vous pouvez utiliser l'adresse IP du contrôleur BMC pour allumer le voyant d'identification de l'appliance.

   "Allumez et éteignez le voyant d'identification de l'appareil"

Remplacez l'une des alimentations ou les deux par le SGF6112

L'appliance SGF6112 dispose de deux blocs d'alimentation pour la redondance. Si l'un des blocs d'alimentation tombe en panne, vous devez le remplacer dès que possible pour

vous assurer que l'appareil est alimenté de manière redondante. Les deux blocs d'alimentation fonctionnant dans l'appareil doivent être de même modèle et de même puissance.

Avant de commencer

- Vous avez "l'appareil se trouve physiquement" avec l'alimentation à remplacer.
- Vous avez "déterminez l'emplacement du bloc d'alimentation à remplacer - effectué".
- Si vous remplacez une seule alimentation :
  - Vous avez déballé le bloc d'alimentation de remplacement et vous êtes assuré qu'il est le même modèle et la même puissance que l'unité d'alimentation que vous remplacez.
  - Vous avez confirmé que l'autre bloc d'alimentation est installé et en cours d'exécution.
- Si vous remplacez les deux alimentations en même temps :
  - Vous avez déballé les blocs d'alimentation de remplacement et vous êtes assuré qu'ils sont du même modèle et de la même puissance.

Description de la tâche

La figure illustre les deux blocs d'alimentation du SGF6112. Les blocs d'alimentation sont accessibles depuis l'arrière de l'appareil.

Étapes

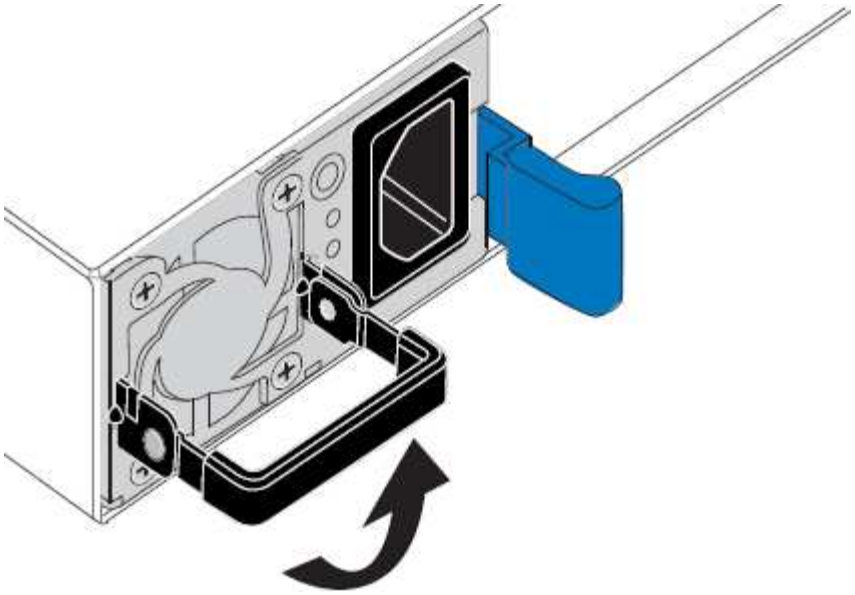
1. Si vous ne remplacez qu'une seule alimentation, vous n'avez pas besoin d'éteindre l'appareil. Accédez au Débranchez le cordon d'alimentation étape. Si vous remplacez les deux blocs d'alimentation en même temps, procédez comme suit avant de débrancher les cordons d'alimentation :
   a. "Arrêtez l'appareil".

   > Si vous avez déjà utilisé une règle ILM pour créer une seule copie d'un objet et que vous remplacez les deux blocs d'alimentation en même temps, vous devez remplacer les blocs d'alimentation durant une fenêtre de maintenance planifiée. Sinon, vous risquez de perdre temporairement l'accès à ces objets au cours de cette procédure. Voir informations sur "pourquoi ne pas utiliser la réplication à copie unique".

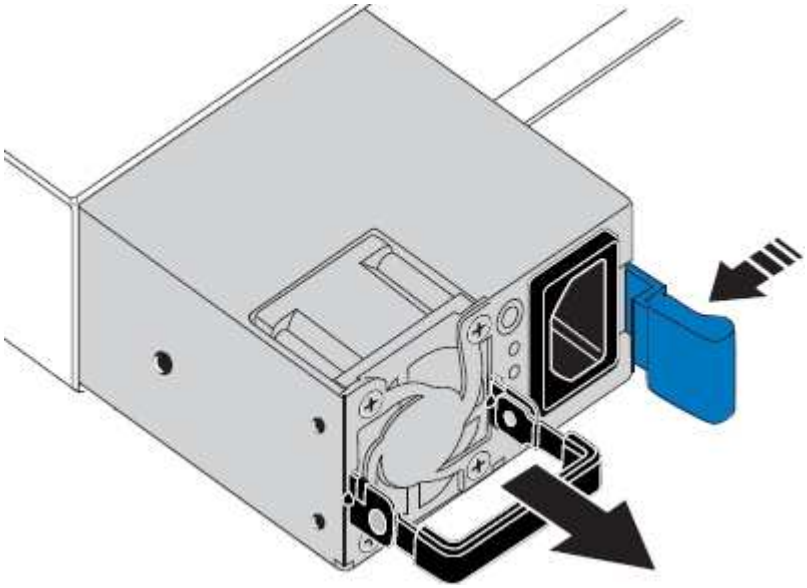
2. débranchez le cordon d'alimentation de chaque alimentation à remplacer.

   Vu de l'arrière de l'appareil, le bloc D'alimentation A (PSU0) se trouve à droite et le bloc d'alimentation B (PSU1) à gauche.

3. Soulevez la poignée de la première alimentation à remplacer.



4. Appuyez sur le loquet bleu et retirez le bloc d’alimentation.

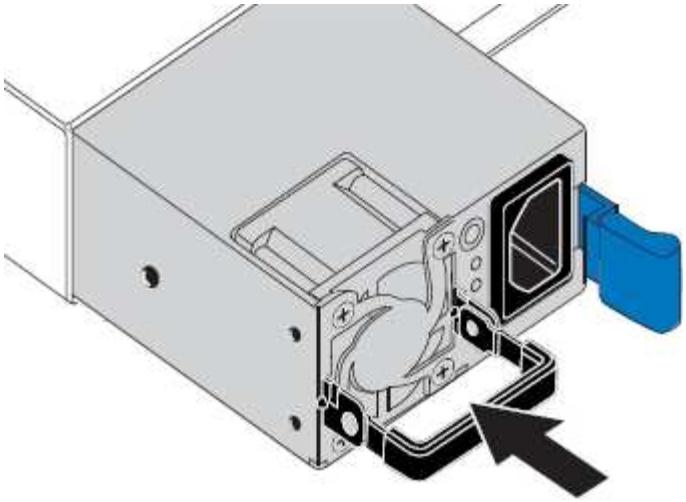


5. Avec le loquet bleu sur la droite, faites glisser le bloc d’alimentation de remplacement dans le châssis.

> Les deux blocs d’alimentation installés doivent être du même modèle et de la même puissance.

Assurez-vous que le loquet bleu se trouve sur le côté droit lorsque vous faites glisser l’unité de rechange.

Vous sentirez un clic lorsque le bloc d’alimentation est verrouillé en place.



6. Poussez la poignée vers le bas contre le corps du bloc d'alimentation.
7. Si vous remplacez les deux blocs d'alimentation, répétez les étapes 2 à 6 pour remplacer la seconde.
8. "Branchez les câbles d'alimentation aux unités remplacées et mettez-les sous tension".

Après le remplacement de la pièce, renvoyez la pièce défectueuse à NetApp, en suivant les instructions RMA (retour de matériel) livrées avec le kit. Voir la "Retour de pièce et amp ; remplacements" pour plus d'informations.

Remplacez le ventilateur dans une appliance SGF6112

L'appliance SGF6112 est équipée de huit ventilateurs. Si l'un des ventilateurs tombe en panne, vous devez le remplacer dès que possible pour vous assurer que l'appareil est bien refroidi.

Avant de commencer

- Vous disposez du ventilateur de remplacement approprié.
- Vous avez déterminé l'emplacement du ventilateur à remplacer.

  "Vérifier le composant à remplacer"

- Vous avez physiquement localisé l'appliance SGF6112 où vous remplacez le ventilateur dans le centre de données.

  "Localisez l'appliance dans le data Center"

  A "arrêt contrôlé de l'appareil" est nécessaire avant de retirer l'appareil du rack.

- Vous avez débranché tous les câbles et retiré le capot de l'appareil.

  "Retirer le couvercle du SGF6112"

- Vous avez confirmé que les autres ventilateurs sont installés et en cours d'exécution.

Description de la tâche

Pour éviter toute interruption de service, vérifiez que tous les autres nœuds de stockage sont connectés à la grille avant de commencer le remplacement du ventilateur ou remplacez le ventilateur dans une fenêtre de

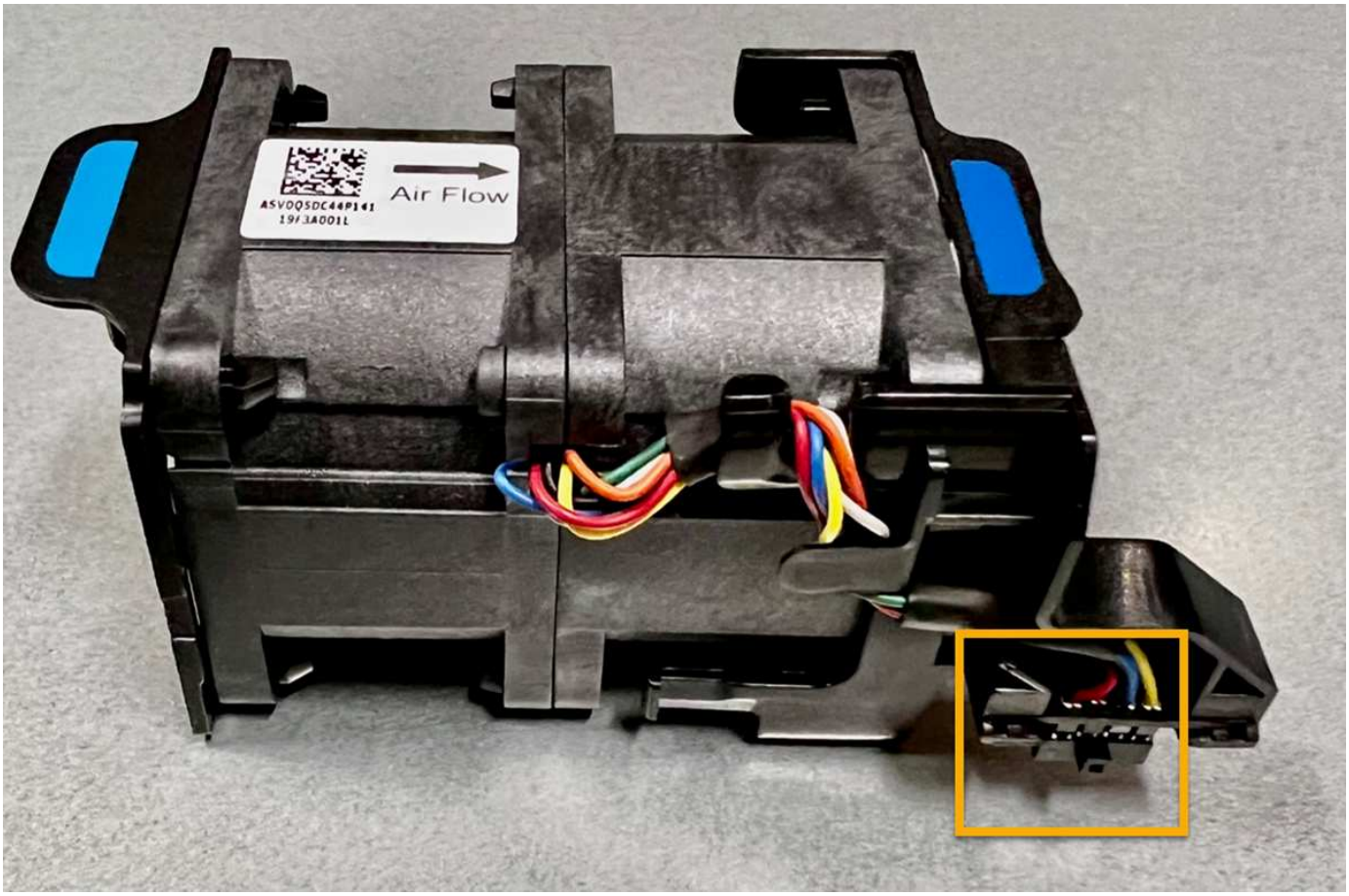
maintenance planifiée lorsque des périodes d'interruption de service sont normalement prévues. Voir les informations sur "contrôle de l'état de connexion du nœud".

> Si vous avez déjà utilisé une règle ILM pour créer une seule copie d'un objet, vous devez remplacer le ventilateur lors d'une fenêtre de maintenance planifiée. Sinon, vous risquez de perdre temporairement l'accès à ces objets au cours de cette procédure. Voir informations sur "pourquoi ne pas utiliser la réplication à copie unique".

Le nœud d'appliance ne sera pas accessible pendant le remplacement du ventilateur.

La photo montre un ventilateur pour l'appareil. Le connecteur électrique est mis en surbrillance. Les ventilateurs de refroidissement sont accessibles après avoir pris le capot supérieur de l'appareil.

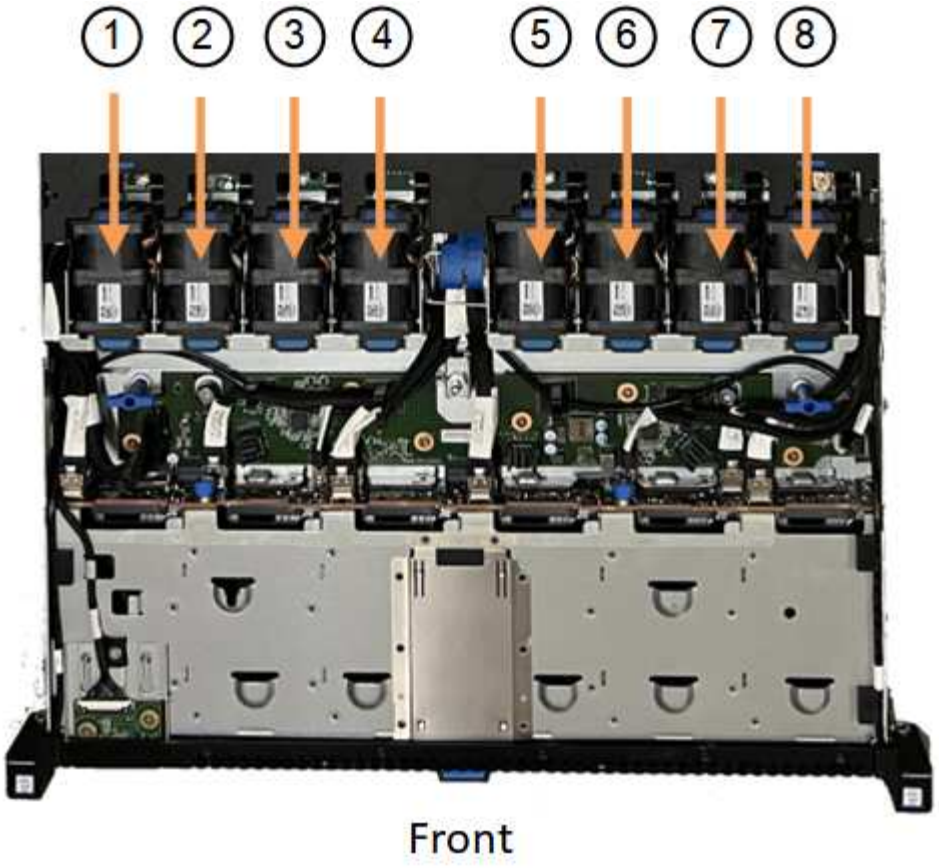
> Chacun des deux blocs d'alimentation contient également un ventilateur. Les ventilateurs du bloc d'alimentation ne sont pas inclus dans cette procédure.



Étapes

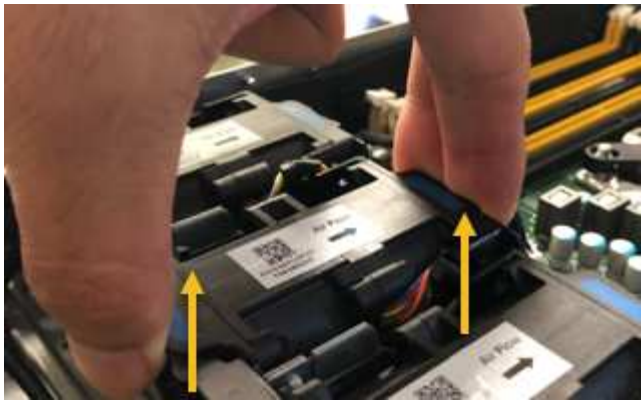
1. Enroulez l'extrémité du bracelet antistatique autour de votre poignet et fixez l'extrémité du clip à une masse métallique afin d'éviter toute décharge statique.
2. Localisez le ventilateur que vous devez remplacer.

   Les huit ventilateurs se trouvent dans les positions suivantes dans le châssis (la moitié avant du SGF6112 avec le capot supérieur retiré est illustrée) :



	Ventilateur
1	Fan_SYS0
2	Ventilateur_SYS1
3	Ventilateur_SYS2
4	FAN_SYS3
5	Ventilateur_SYS4
6	Ventilateur_SYS5
7	Ventilateur_SYS6
8	FAN_SYS7

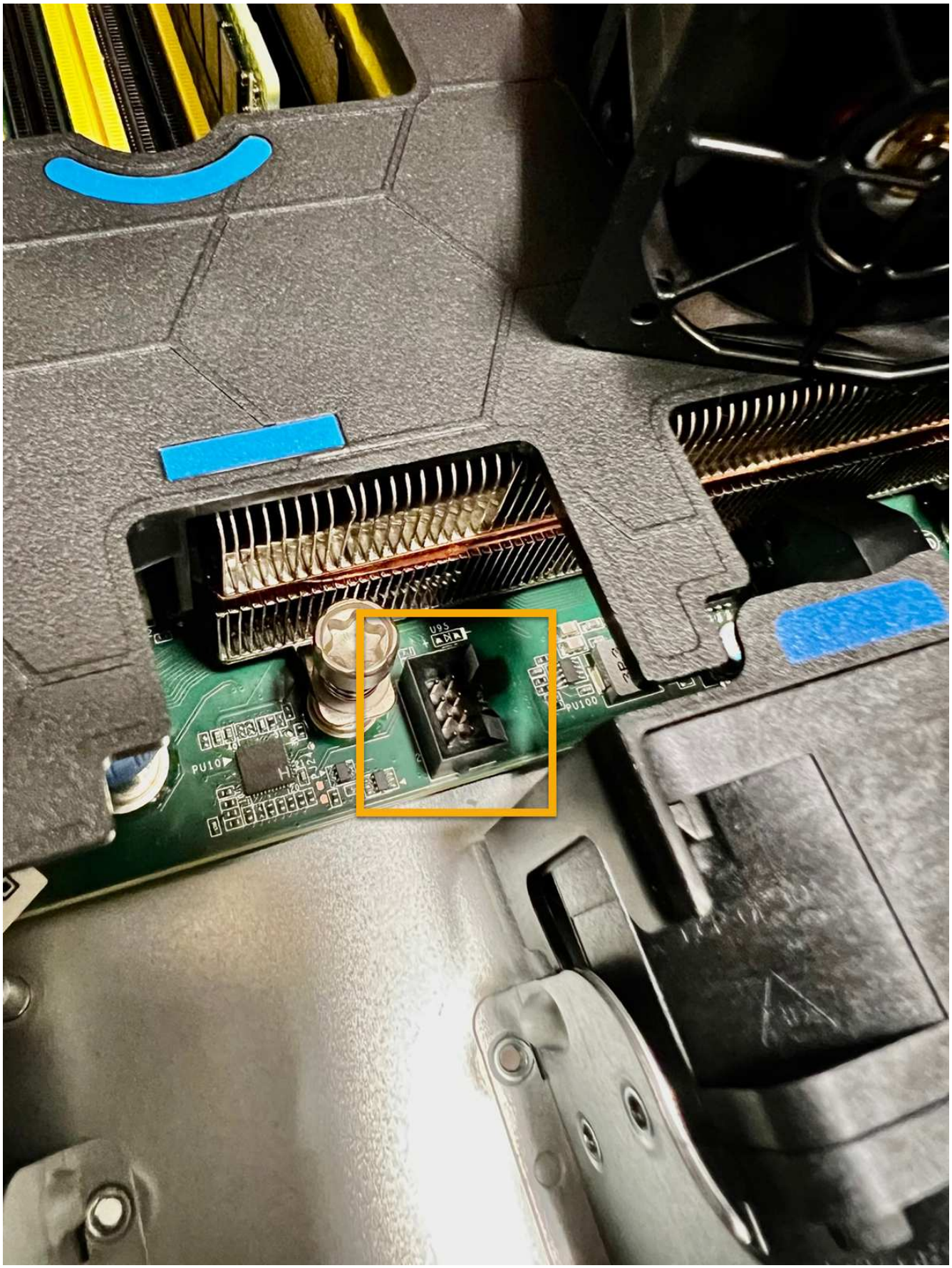
1. Soulevez le ventilateur défectueux hors du châssis à l'aide des languettes bleues.



2. Faites glisser le ventilateur de remplacement dans le logement ouvert du châssis.

   Veillez à aligner le connecteur du ventilateur avec la prise de la carte de circuit imprimé.

3. Enfoncez fermement le connecteur du ventilateur dans la carte de circuit imprimé (prise en surbrillance).



4. Replacez le capot supérieur sur l’appareil et appuyez sur le loquet pour fixer le capot en place.

5. Mettez l’appareil sous tension et surveillez les voyants et les codes de démarrage de l’appareil.

   Utilisez l’interface BMC pour surveiller l’état de démarrage.

6. Vérifiez que le nœud de l’appliance s’affiche dans Grid Manager et qu’aucune alerte n’apparaît.

Après le remplacement de la pièce, renvoyez la pièce défectueuse à NetApp, en suivant les instructions RMA (retour de matériel) livrées avec le kit. Voir la "Retour de pièce et amp ; remplacements" pour plus d’informations.

Remplacez les disques de l’appliance SGF6112

Le dispositif de stockage SGF6112 contient 12 disques SSD. Les données des disques sont protégées par un schéma RAID qui permet à l’appliance de restaurer les données en cas de panne d’un disque sans avoir à copier les données à partir d’un autre nœud.

La défaillance d’un second disque avant la correction d’une panne initiale peut nécessiter la copie des données des autres nœuds pour restaurer la redondance. Cette restauration de redondance peut prendre plus de temps et peut être impossible si des règles ILM à une seule copie sont utilisées ou étaient utilisées auparavant, ou si la redondance des données a été affectée par des défaillances sur d’autres nœuds. Par conséquent, si l’un des disques SGF6112 tombe en panne, vous devez le remplacer dès que possible pour assurer la redondance.

Avant de commencer

- Vous avez "l’appareil se trouve physiquement".
- Vous avez vérifié quel disque est défaillant en notant que le voyant de gauche du disque est orange fixe ou en utilisant Grid Manager pour "afficher l’alerte causée par le disque défectueux".

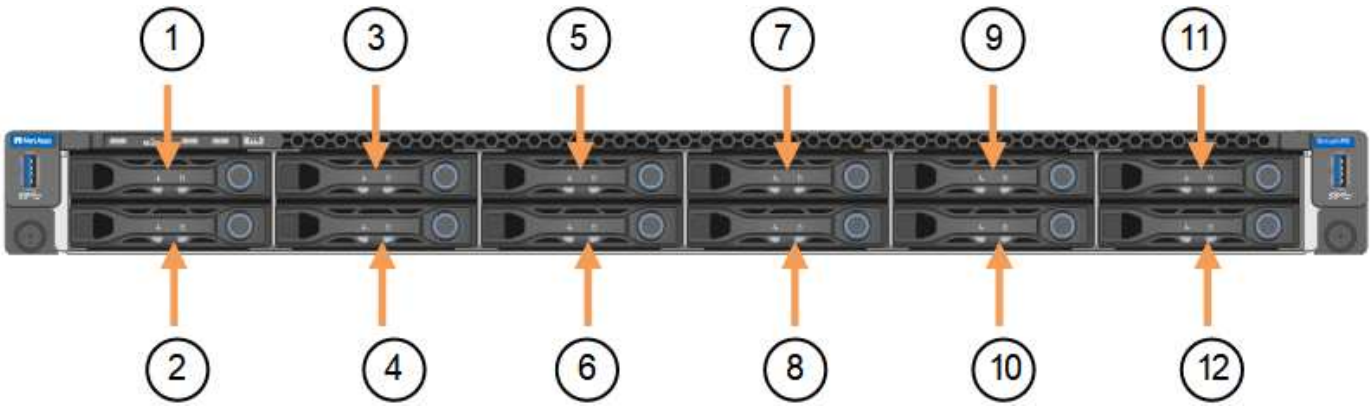
  Reportez-vous aux informations sur l’affichage des indicateurs d’état pour vérifier l’échec.

- Vous avez obtenu le disque de remplacement.
- Vous avez obtenu une protection ESD appropriée.

Étapes

1. Vérifiez que le voyant de panne gauche du disque est orange ou utilisez l’ID de logement de disque de l’alerte pour localiser le disque.

   Les douze disques se trouvent aux emplacements suivants dans le châssis (avant du châssis avec le cadre retiré) :



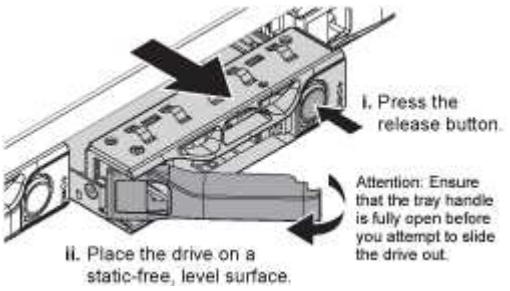
Position	Lecteur
1	HDD00
2	HDD01
3	HDD02
4	HDD03
5	HDD04
6	HDD05
7	HDD06
8	HDD07
9	HDD08
10	HDD09
11	HDD10
12	HDD11

Vous pouvez également utiliser Grid Manager pour contrôler l'état des disques SSD. Sélectionnez **NOEUDS**. Puis faire `Storage Node` > **matériel**. Si un lecteur est défectueux, le champ Storage RAID mode contient un message indiquant quel lecteur est défectueux.

1. Enroulez l'extrémité du bracelet antistatique autour de votre poignet et fixez l'extrémité du clip à une masse métallique afin d'éviter toute décharge statique.
2. Déballez le lecteur de remplacement et placez-le sur une surface plane et sans électricité statique près de l'appareil.

   Conservez tous les matériaux d'emballage.

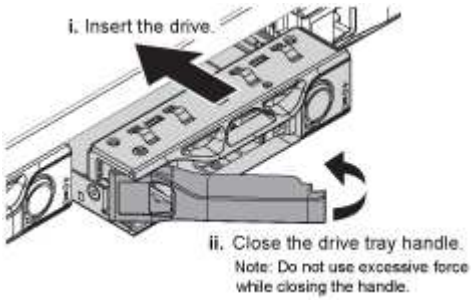
3. Appuyez sur le bouton de déverrouillage du disque défectueux.



   La poignée des ressorts d'entraînement s'ouvre partiellement et l'entraînement se relâche de la fente.

4. Ouvrez la poignée, faites glisser l'entraînement vers l'extérieur et placez-le sur une surface plane et non statique.
5. Appuyez sur le bouton de dégagement du disque de remplacement avant de l'insérer dans le slot.

   Les ressorts de verrouillage s'ouvrent.



6. Insérez le lecteur de remplacement dans son logement, puis fermez la poignée du lecteur.

   Ne forcez pas trop lorsque vous fermez la poignée.

   Lorsque le lecteur est complètement inséré, vous entendez un clic.

   Le lecteur remplacé est automatiquement reconstruit avec les données en miroir des lecteurs en fonctionnement. Le voyant du lecteur doit d'abord clignoter, mais cesse de clignoter dès que le système détermine que le lecteur dispose d'une capacité suffisante et qu'il est fonctionnel.

   Vous pouvez vérifier l'état de la reconstruction à l'aide du Gestionnaire de grille.

7. Si plusieurs disques sont défectueux et ont été remplacés, des alertes vous indiquent que certains volumes doivent être restaurés. Si vous recevez une alerte, avant de tenter une récupération de volume, sélectionnez **NODES** > **`appliance Storage Node`** > **matériel**. Dans la section dispositif StorageGRID de la page, vérifiez que le mode RAID de stockage est en bon état ou qu'il est en cours de reconstruction. Si l'état indique un ou plusieurs disques défaillants, corrigez cette condition avant de tenter la restauration du volume.
8. Dans le Gestionnaire de grille, accédez à **NODES** > **`appliance Storage Node`** > **matériel**. Dans la section dispositif StorageGRID de la page, vérifiez que le mode RAID de stockage fonctionne correctement.

Après le remplacement de la pièce, renvoyez la pièce défectueuse à NetApp, en suivant les instructions RMA (retour de matériel) livrées avec le kit. Voir la "Retour de pièce et amp ; remplacements" pour plus d'informations.

Remplacez la carte réseau dans le SGF6112

Vous devrez peut-être remplacer une carte d'interface réseau (NIC) dans le SGF6112 s'il ne fonctionne pas de manière optimale ou s'il est défectueux.

Suivez ces procédures pour :

- Retirez la carte réseau
- Réinstallez la carte réseau

Retirez la carte réseau

Avant de commencer

- Vous avez la carte réseau de remplacement correcte.
- Vous avez déterminé l'emplacement de la carte réseau à remplacer.

  "Vérifiez l'emplacement du composant à remplacer"

- Vous avez physiquement localisé l'appliance SGF6112 où vous remplacez la carte réseau dans le centre de données.

  "Localisez l'appliance dans le data Center"

  A "arrêt contrôlé de l'appareil" est nécessaire avant de retirer l'appareil du rack.

- Vous avez débranché tous les câbles et retiré le capot de l'appareil.

  "Retirer le couvercle du SGF6112"

Description de la tâche

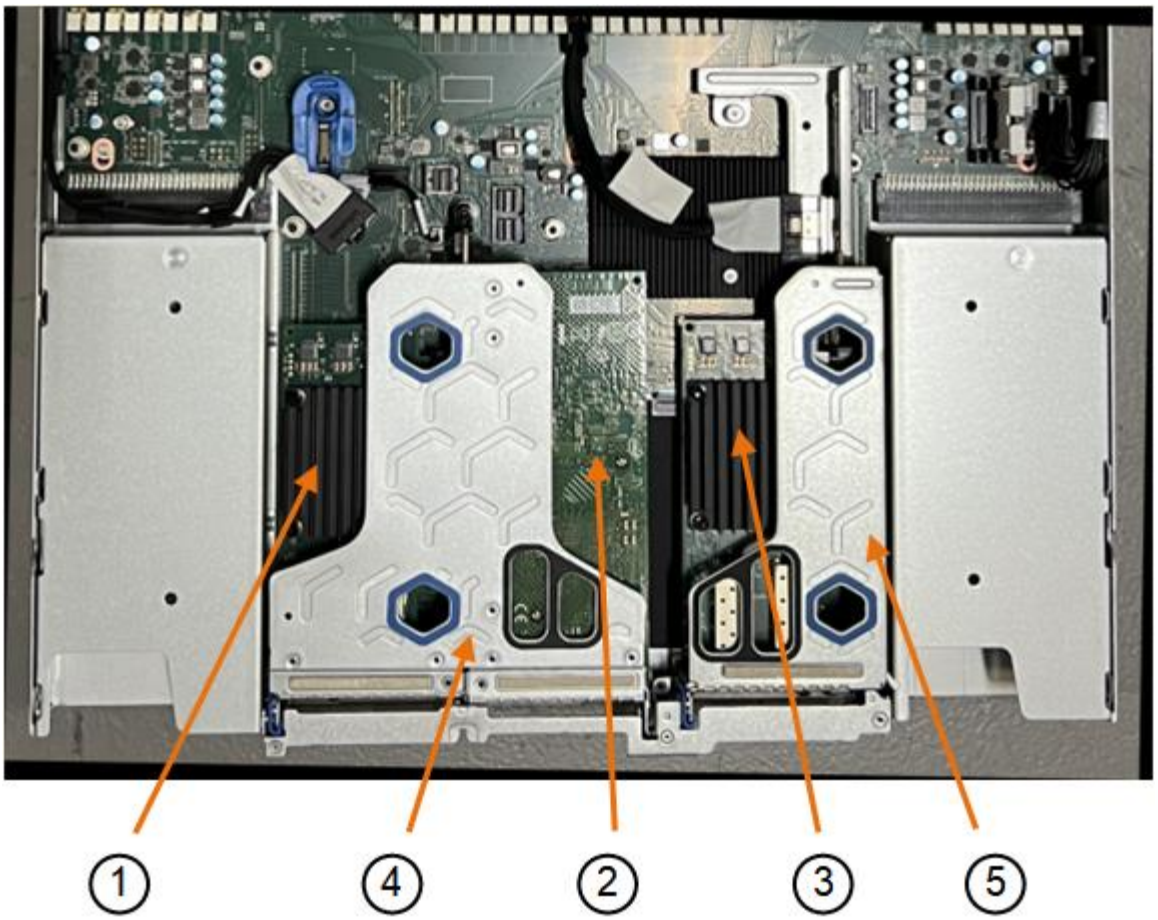
Pour éviter toute interruption de service, vérifiez que tous les autres nœuds de stockage sont connectés à la grille avant de commencer le remplacement de la carte d'interface réseau (NIC) ou remplacez-la lors d'une fenêtre de maintenance planifiée lorsque des périodes d'interruption de service sont normalement prévues. Voir les informations sur "contrôle de l'état de connexion du nœud".

Si vous avez déjà utilisé une règle ILM qui ne crée qu'une seule copie d'un objet, vous devez remplacer la carte réseau au cours d'une fenêtre de maintenance planifiée. Sinon, vous risquez de perdre temporairement l'accès à ces objets au cours de cette procédure. Voir informations sur "pourquoi ne pas utiliser la réplication à copie unique".

Étapes

1. Enroulez l'extrémité du bracelet antistatique autour de votre poignet et fixez l'extrémité du clip à une masse métallique afin d'éviter toute décharge statique.
2. Repérez le dispositif de montage contenant la carte réseau à l'arrière de l'appareil.

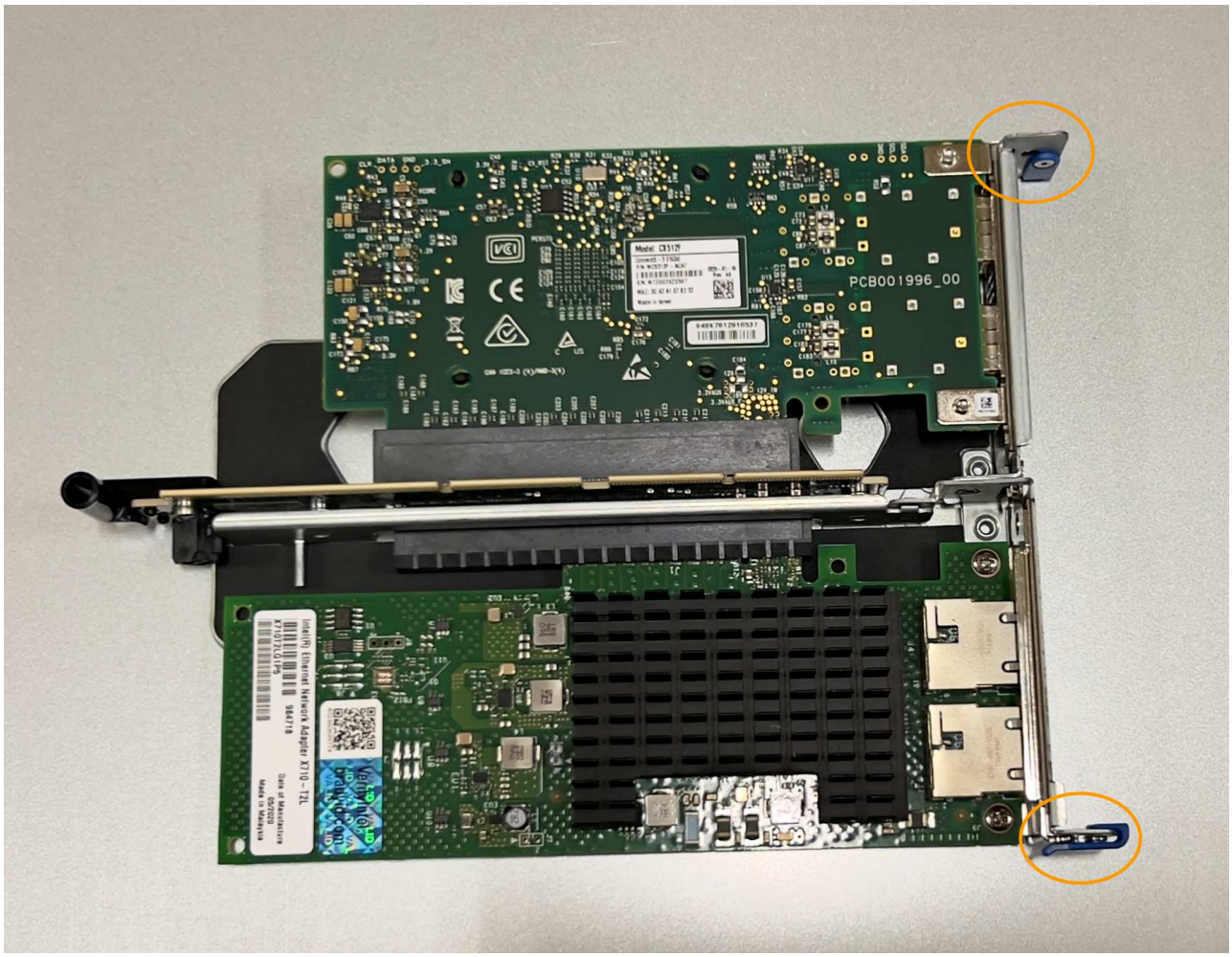
   Les trois cartes d'interface réseau du SGF6112 se trouvent dans deux ensembles de carte de montage dans les positions indiquées dans le châssis (arrière du SGF6112 avec le capot supérieur retiré) :



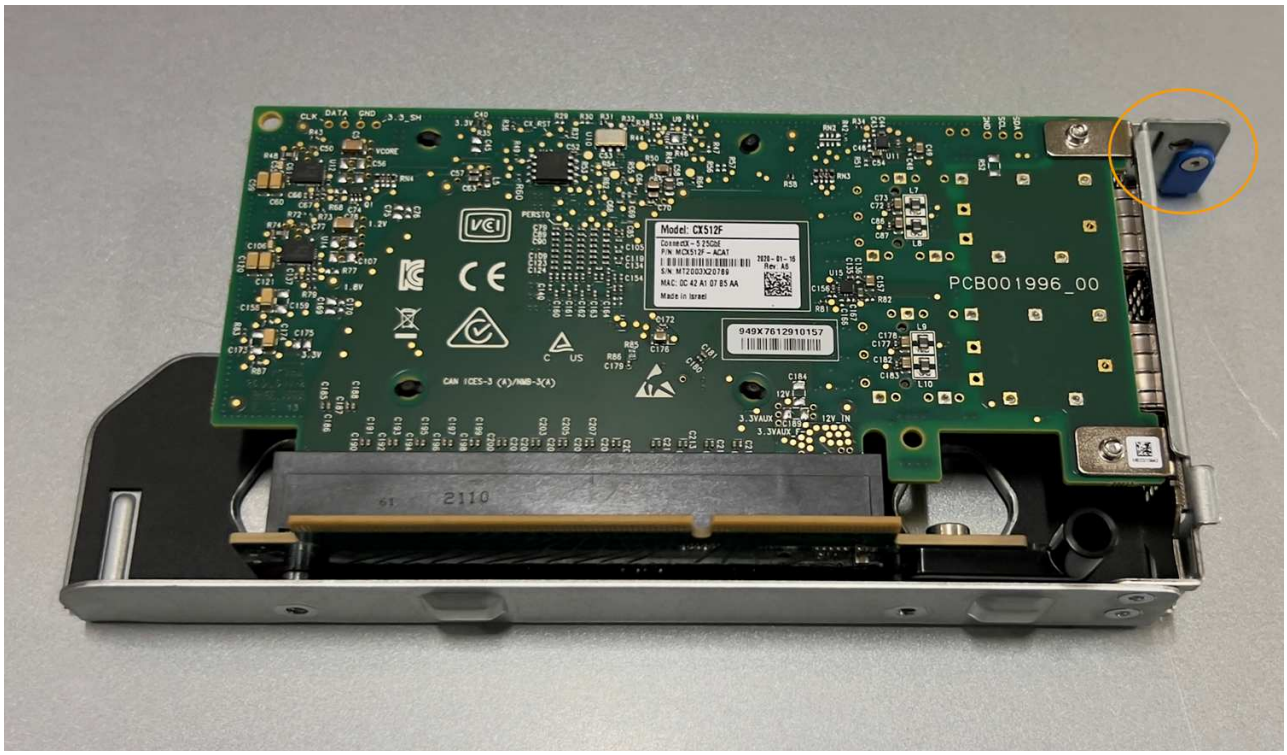
	Nom du périphérique ou de la pièce	Description
1	hic1/hic2	Ports réseau Ethernet 10/25-GbE dans l'ensemble de carte de montage à deux ports
2	mtc1/mtc2	Ports de gestion 1/10GBase-T dans l'ensemble de montage à deux ports
3	hic3/hic4	Ports réseau Ethernet 10/25-GbE dans l'ensemble de carte de montage à un port
4	Assemblage de la carte de montage à deux emplacements	Prise en charge de l'une des cartes réseau 10/25-GbE et de la carte réseau 1/10GBase-T.
5	Assemblage de la carte de montage à une position	Prise en charge de l'une des cartes réseau 10/25 GbE

1. Saisissez l'ensemble de la carte de montage avec la carte réseau défectueuse dans les trous marqués en bleu et soulevez-le avec précaution vers le haut. Déplacez l'ensemble de carte de montage vers l'avant du châssis tout en le soulevant pour permettre aux connecteurs externes de ses cartes réseau installées de se dégager du châssis.

2. Placez la carte de montage sur une surface antistatique plane, avec le cadre métallique vers le bas pour accéder aux cartes réseau.
   - **Assemblage de carte de montage à deux emplacements avec deux cartes réseau**



   - **Assemblage de carte de montage à un emplacement avec une carte d'interface réseau**



3. Ouvrez le loquet bleu (entouré) de la carte réseau à remplacer et retirez avec précaution la carte réseau de l'ensemble de carte de montage. Secouez légèrement la carte réseau pour la retirer de son connecteur. N'utilisez pas de force excessive.
4. Placez la carte réseau sur une surface antistatique plane.

Réinstallez la carte réseau

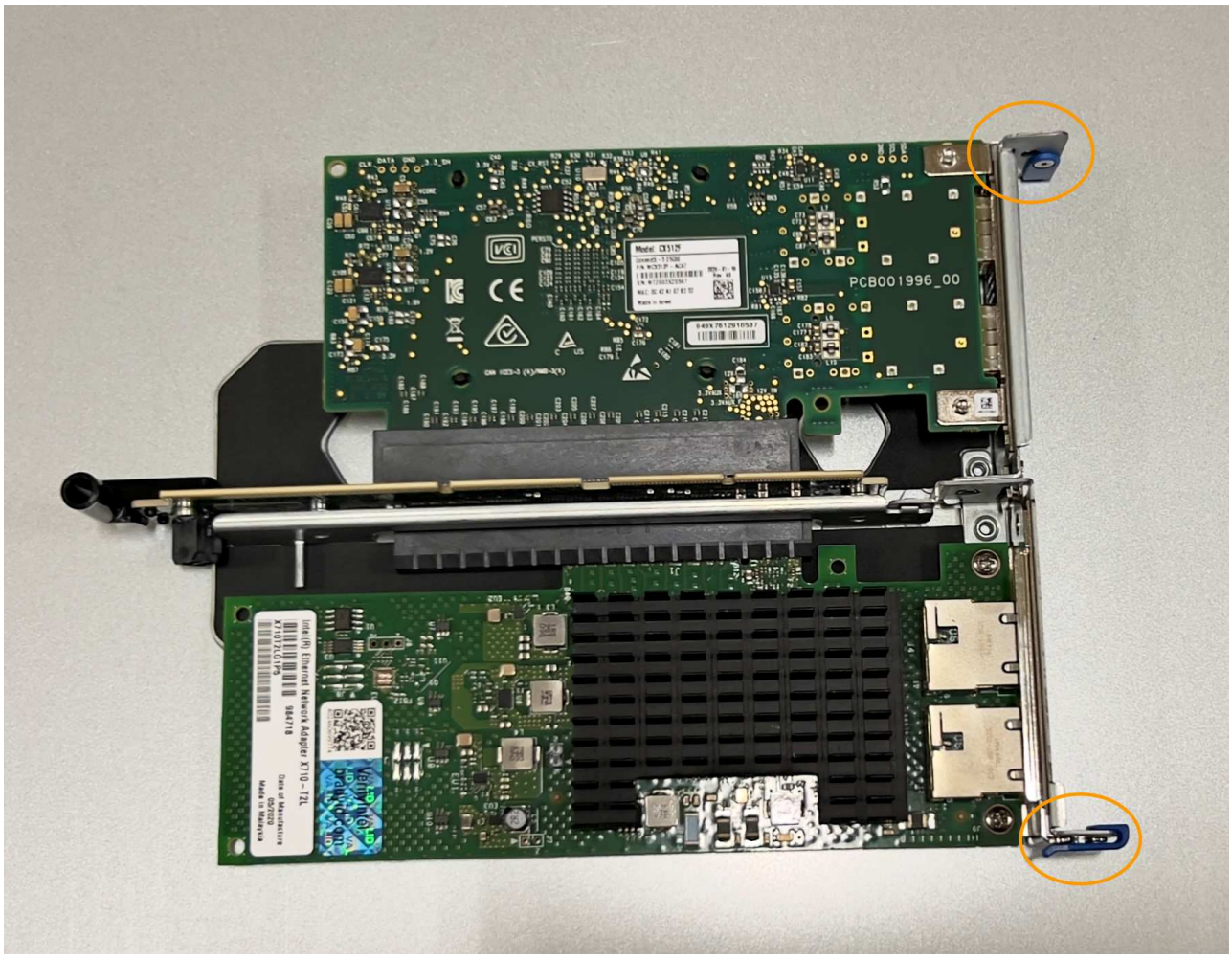
Installez la carte réseau de remplacement au même emplacement que celui qui a été retiré.

Avant de commencer

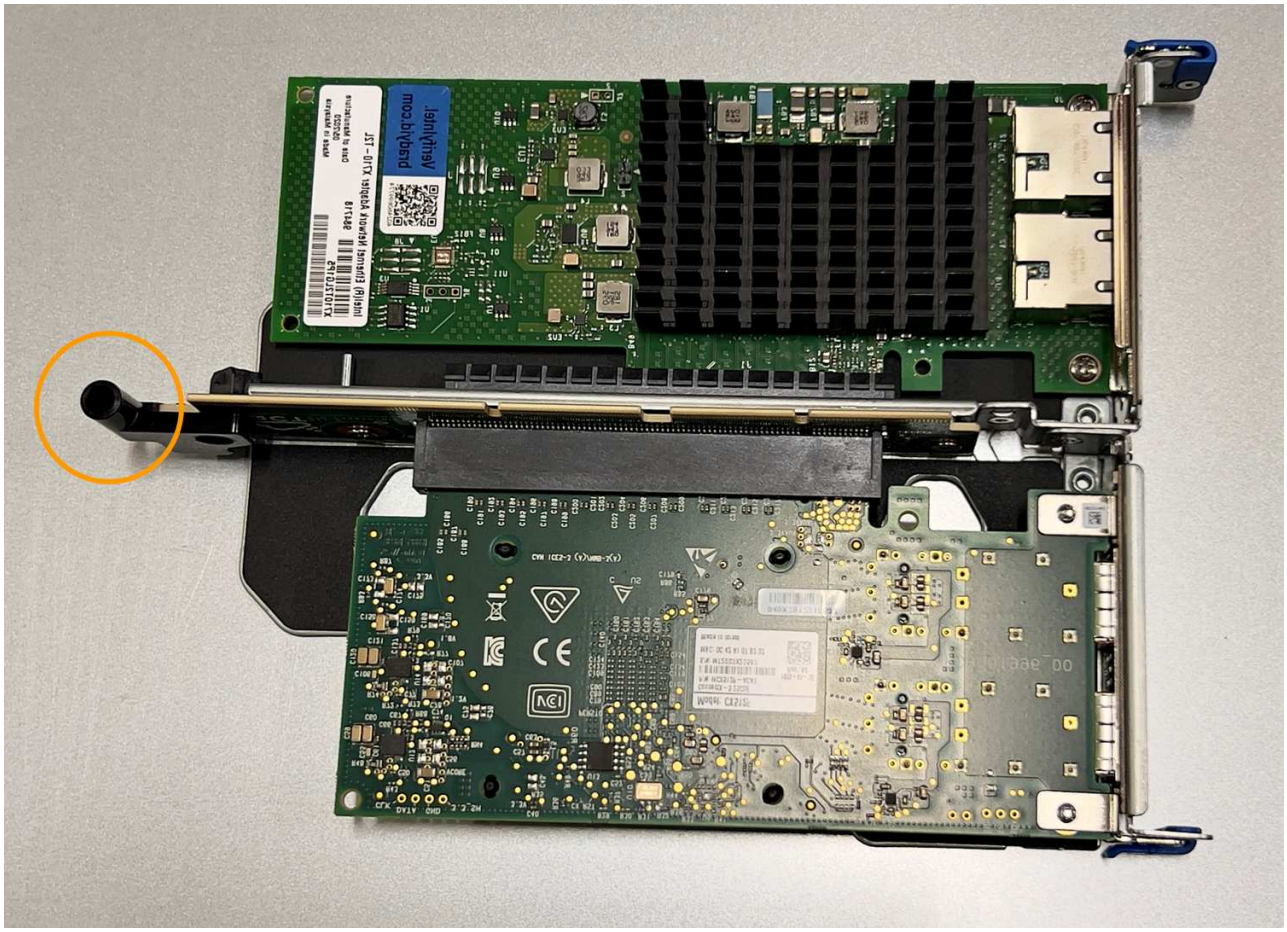
- Vous avez la carte réseau de remplacement correcte.
- Vous avez supprimé la carte réseau défectueuse existante.

Étapes

1. Enroulez l'extrémité du bracelet antistatique autour de votre poignet et fixez l'extrémité du clip à une masse métallique afin d'éviter toute décharge statique.
2. Retirez la carte réseau de remplacement de son emballage.
3. Si vous remplacez l'une des cartes réseau de l'ensemble de carte de montage à deux emplacements, procédez comme suit :
   a. Assurez-vous que le loquet bleu est en position ouverte.
   b. Alignez la carte réseau avec son connecteur sur l'ensemble de carte de montage. Appuyez avec précaution sur la carte réseau dans le connecteur jusqu'à ce qu'elle soit bien en place, comme indiqué sur la photo, puis fermez le loquet bleu.



c. Repérez le trou d’alignement de l’ensemble de carte de montage à deux emplacements (encerclé) qui s’aligne sur une broche de guidage de la carte système afin de garantir un positionnement correct de l’ensemble de carte de montage.



d. Repérez la broche de guidage sur la carte système

e. Positionnez l’ensemble de carte de montage dans le châssis, en vous assurant qu’il est aligné avec le

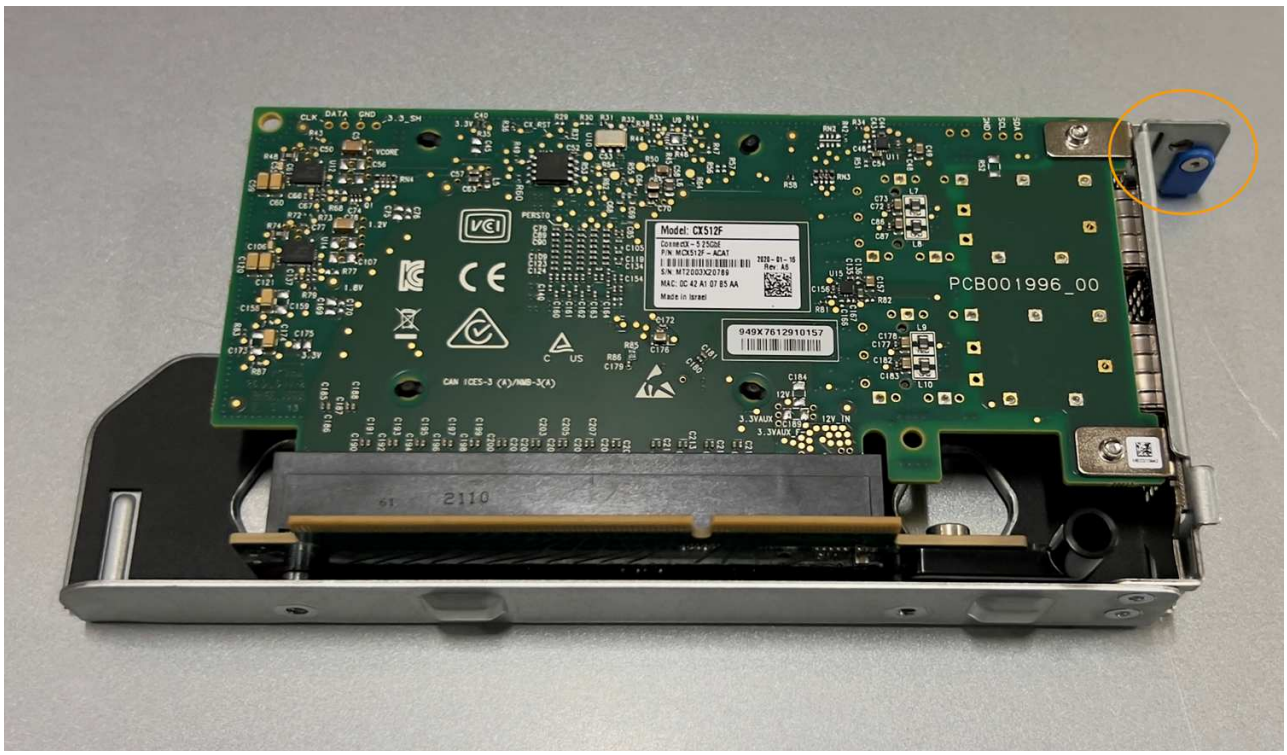
connecteur de la carte système et la broche de guidage.

f. Appuyez avec précaution sur l'ensemble de montage à deux fentes le long de sa ligne centrale, près des trous marqués en bleu, jusqu'à ce qu'il soit bien en place.

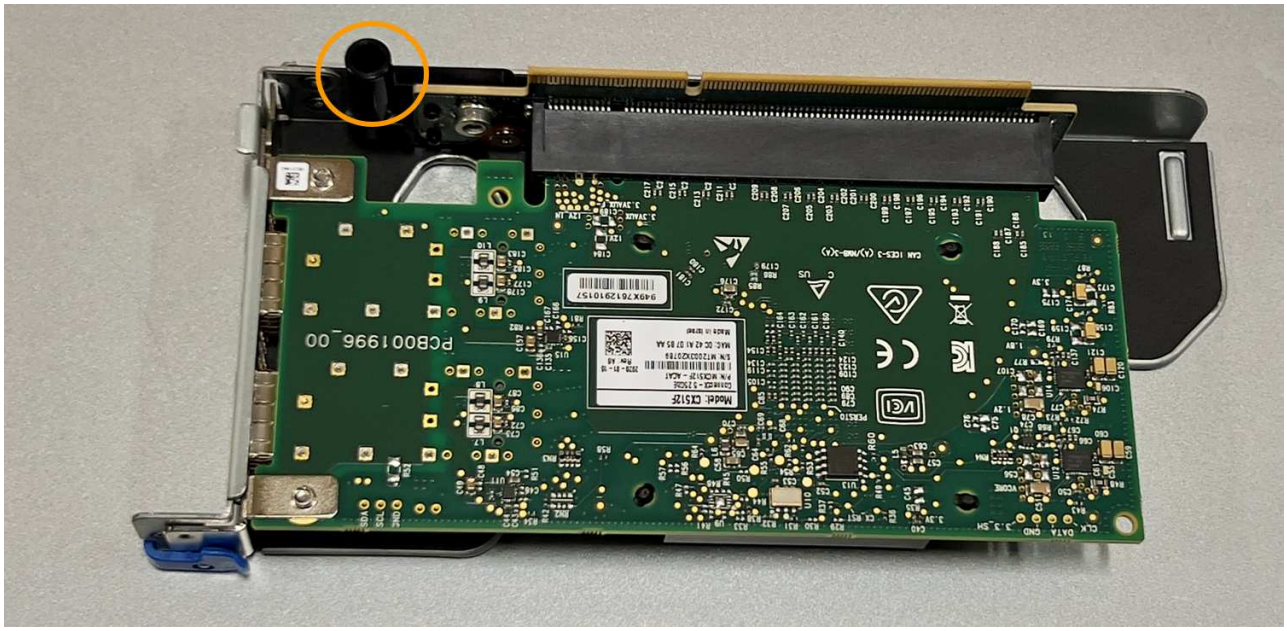
4. Si vous remplacez la carte réseau dans le dispositif de montage à un emplacement, procédez comme suit :

a. Assurez-vous que le loquet bleu est en position ouverte.

b. Alignez la carte réseau avec son connecteur sur l'ensemble de carte de montage. Appuyez avec précaution sur la carte réseau dans le connecteur jusqu'à ce qu'elle soit bien en place, comme indiqué sur la photo, puis fermez le loquet bleu.



c. Repérez le trou d'alignement de l'assemblage de la carte de montage à un emplacement (encerclé) qui s'aligne sur une broche de guidage de la carte système afin de garantir un positionnement correct de l'assemblage de la carte de montage.



d. Repérez la broche de guidage sur la carte système

e. Positionnez l'ensemble de carte de montage à un emplacement dans le châssis, en vous assurant qu'il est aligné avec le connecteur de la carte système et la broche de guidage.

f. Appuyez avec précaution sur le dispositif de montage à une fente le long de sa ligne centrale, à côté des trous marqués en bleu, jusqu'à ce qu'il soit bien en place.

5. Retirez les caches de protection des ports de carte réseau sur lesquels vous allez réinstaller les câbles.

Une fois que vous avez terminé

Si vous n'avez aucune autre procédure de maintenance à effectuer dans l'appareil, réinstallez le capot de l'appareil, replacez l'appareil sur le rack, branchez les câbles et mettez l'appareil sous tension.

Après le remplacement de la pièce, renvoyez la pièce défectueuse à NetApp, en suivant les instructions RMA

(retour de matériel) livrées avec le kit. Voir la "Retour de pièce et amp ; remplacements" pour plus d'informations.

Remplacez la pile CMOS du SGF6112

Utilisez cette procédure pour remplacer la pile bouton CMOS de la carte système.

Suivez ces procédures pour :

- Retirez la pile CMOS
- Réinstallez la pile CMOS

Retirez la pile CMOS

Avant de commencer

- Vous avez vérifié que la pile CMOS du SGF6112 doit être remplacée.

  "Vérifier le composant à remplacer"

- Vous avez physiquement localisé l'appliance SGF6112 où vous remplacez la pile CMOS dans le centre de données.

  "Localisez l'appliance dans le data Center"

  A "arrêt contrôlé de l'appareil" est nécessaire avant de retirer l'appareil du rack.

- Vous avez débranché tous les câbles et retiré le capot de l'appareil.

  "Retirer le couvercle du SGF6112"

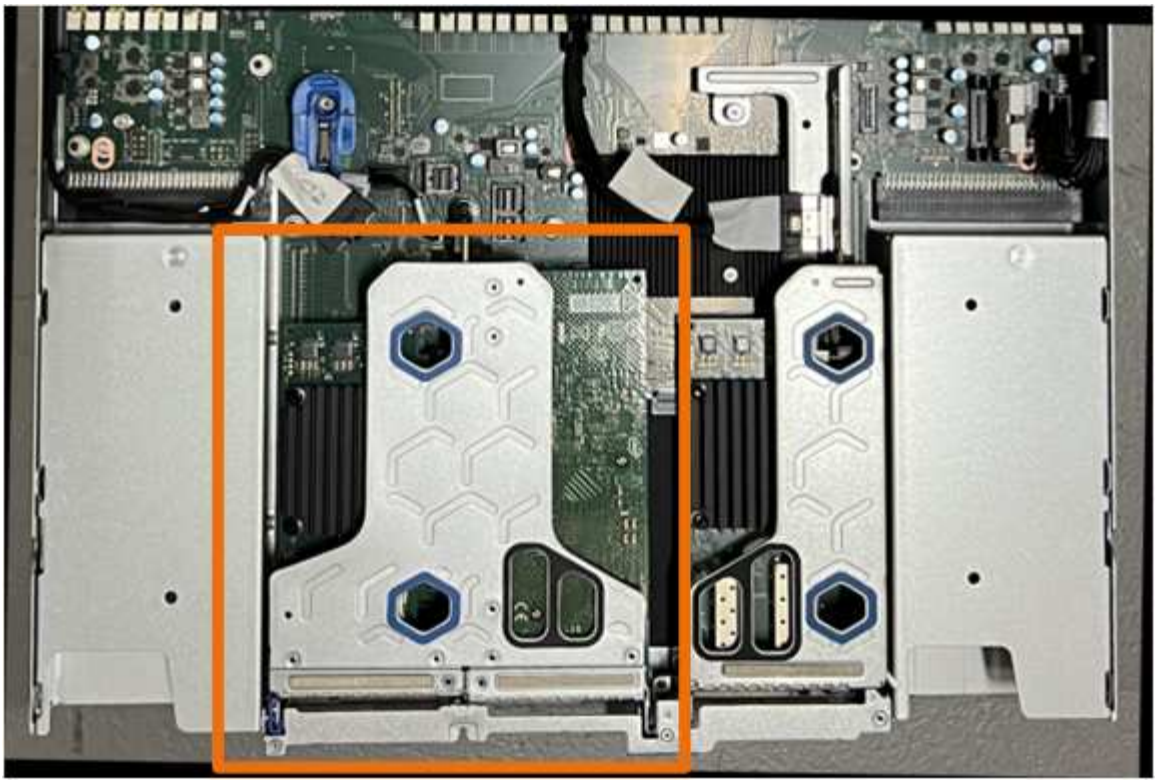
Description de la tâche

Pour éviter toute interruption de service, vérifiez que tous les autres nœuds de stockage sont connectés à la grille avant de commencer le remplacement de la batterie CMOS ou remplacez la batterie pendant une fenêtre de maintenance planifiée lorsque des périodes d'interruption de service sont normalement prévues. Voir les informations sur "contrôle de l'état de connexion du nœud".

Si vous avez déjà utilisé une règle ILM pour créer une seule copie d'un objet, vous devez remplacer la batterie lors d'une fenêtre de maintenance planifiée. Sinon, vous risquez de perdre temporairement l'accès à ces objets au cours de cette procédure. Voir informations sur "pourquoi ne pas utiliser la réplication à copie unique".

Étapes

1. Enroulez l'extrémité du bracelet antistatique autour de votre poignet et fixez l'extrémité du clip à une masse métallique afin d'éviter toute décharge statique.
2. Repérez l'ensemble de montage à deux emplacements à l'arrière de l'appareil.



3. Saisissez l’ensemble de montage dans les trous marqués de couleur bleue et soulevez-le avec précaution vers le haut. Déplacez l’ensemble de carte de montage vers l’avant du châssis tout en le soulevant pour permettre aux connecteurs externes de ses cartes réseau installées de se dégager du châssis.
4. Placez la carte de montage sur une surface antistatique plane, le cadre métallique étant orienté vers le bas.
5. Repérez la pile CMOS sur la carte système dans la position sous le dispositif de montage retiré.

6. Utilisez votre doigt ou un levier en plastique pour écarter le clip de retenue (mis en surbrillance) de la batterie et le retirer de la prise.

7. Retirez la batterie et mettez-la au rebut de façon appropriée.

Réinstallez la pile CMOS

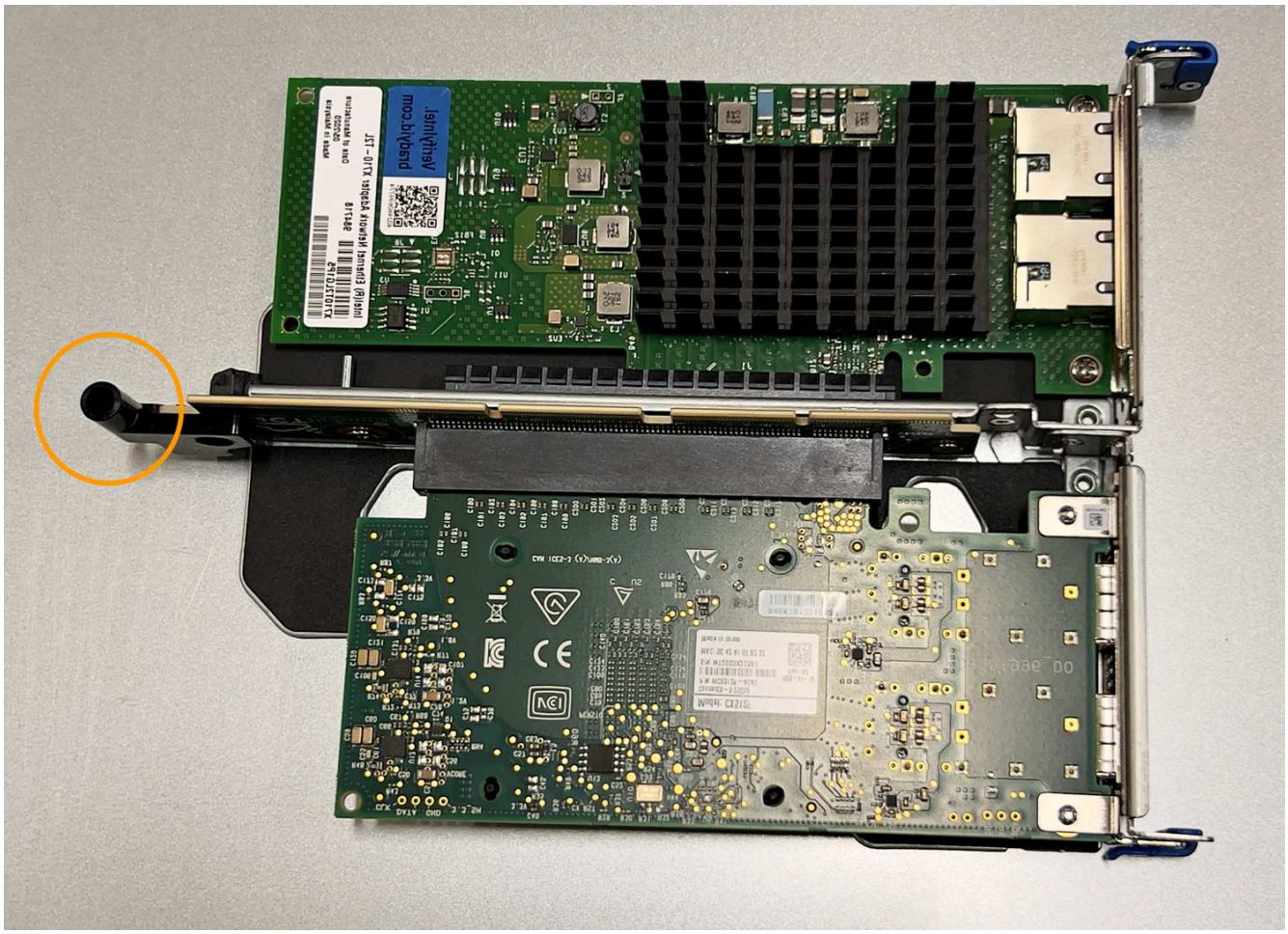
Installez la pile CMOS de remplacement dans le support de la carte système.

Avant de commencer

- Vous disposez de la pile CMOS de remplacement correcte (CR2032).
- Vous avez retiré la pile CMOS défectueuse.

Étapes

1. Enroulez l’extrémité du bracelet antistatique autour de votre poignet et fixez l’extrémité du clip à une masse métallique afin d’éviter toute décharge statique.
2. Retirez la pile CMOS de son emballage.
3. Appuyez sur la batterie de remplacement dans le support vide de la carte système, côté positif (+) vers le haut jusqu’à ce que la batterie s’enclenche.
4. Repérez le trou d’alignement de l’assemblage de la carte de montage à deux emplacements (encerclé) qui s’aligne sur la broche de guidage de la carte système afin de garantir un positionnement correct de l’assemblage de la carte de montage.



5. Repérez la broche de guidage sur la carte système

6. Positionnez l'ensemble de carte de montage dans le châssis, en vous assurant qu'il est aligné avec le connecteur de la carte système et la broche de guidage.
7. Appuyez avec précaution sur l'ensemble de montage à deux fentes le long de sa ligne centrale, près des trous marqués en bleu, jusqu'à ce qu'il soit bien en place.
8. Si vous n'avez aucune autre procédure de maintenance à effectuer dans l'appareil, réinstallez le capot de l'appareil, replacez l'appareil sur le rack, branchez les câbles et mettez l'appareil sous tension.
9. Si l'appliance que vous avez remplacée utilisait un serveur de gestion des clés (KMS) pour chiffrer les données, il est possible que vous ayez besoin d'une configuration supplémentaire avant que le nœud puisse rejoindre la grille. Si le nœud ne rejoint pas automatiquement la grille, assurez-vous que ces paramètres de configuration ont été transférés vers la nouvelle appliance et configurez manuellement les paramètres qui ne possèdent pas la configuration attendue :
   - "Configurer les connexions StorageGRID"
   - "Configurez le chiffrement des nœuds pour l'appliance"
10. Connectez-vous à l'appliance :
    a. Saisissez la commande suivante : `ssh admin@grid_node_IP`
    b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
    c. Entrez la commande suivante pour passer à la racine : `su -`
    d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
11. Restaurez la connectivité réseau du contrôleur BMC pour l'appliance. Deux options sont disponibles :
    - Utilisez une adresse IP statique, un masque de réseau et une passerelle
    - Utilisez DHCP pour obtenir une adresse IP, un masque de réseau et une passerelle

      i. Pour restaurer la configuration du contrôleur BMC afin d'utiliser une adresse IP statique, un masque de réseau et une passerelle, entrez les commandes suivantes :

      `run-host-command ipmitool lan set 1 ipsrc static`

      `run-host-command ipmitool lan set 1 ipaddr Appliance_IP`

      `run-host-command ipmitool lan set 1 netmask Netmask_IP`

      `run-host-command ipmitool lan set 1 defgw ipaddr Default_gateway`

      i. Pour restaurer la configuration du contrôleur BMC afin d'utiliser DHCP pour obtenir une adresse IP, un masque de réseau et une passerelle, entrez la commande suivante :

      `run-host-command ipmitool lan set 1 ipsrc dhcp`

12. Après avoir restauré la connectivité réseau du contrôleur BMC, connectez-vous à l'interface du contrôleur BMC pour vérifier et restaurer toute configuration BMC personnalisée supplémentaire que vous avez éventuellement appliquée. Par exemple, vous devez confirmer les paramètres des destinations d'interruption SNMP et des notifications par e-mail. Voir "Configurer l'interface BMC".
13. Vérifiez que le nœud de l'appliance s'affiche dans Grid Manager et qu'aucune alerte n'apparaît.

Remplacez l'appliance SGF6112

Vous devrez peut-être remplacer l'appareil s'il ne fonctionne pas de manière optimale ou s'il est défectueux.

Avant de commencer

- Vous disposez d'un appareil de remplacement avec le même numéro de pièce que l'appareil que vous remplacez.
- Vous disposez d'étiquettes pour identifier chaque câble connecté à l'appareil.
- Vous avez "l'appareil se trouve physiquement".

Description de la tâche

Le nœud StorageGRID ne sera pas accessible lors du remplacement de l'appliance. Si l'appareil fonctionne correctement, vous pouvez procéder à un arrêt contrôlé au début de cette procédure.

> ⓘ Si vous remplacez l'appliance avant d'installer le logiciel StorageGRID, il se peut que vous ne puissiez pas accéder immédiatement au programme d'installation de l'appliance StorageGRID après avoir terminé cette procédure. Bien que vous puissiez accéder au programme d'installation de l'appliance StorageGRID à partir d'autres hôtes situés sur le même sous-réseau que l'appliance, vous ne pouvez pas y accéder à partir d'hôtes situés sur d'autres sous-réseaux. Cette condition doit se résoudre dans les 15 minutes (lorsque les entrées du cache ARP pour l'appliance d'origine sont écoulées), ou vous pouvez effacer immédiatement la condition en éliminant manuellement les anciennes entrées du cache ARP à partir du routeur ou de la passerelle local.

Étapes

1. Affichez les configurations actuelles de l'appareil et enregistrez-les.
   a. Connectez-vous à l'appliance à remplacer :
      i. Saisissez la commande suivante : `ssh admin@grid_node_IP`
      ii. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
      iii. Entrez la commande suivante pour passer à la racine : `su -`
      iv. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

      Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

   b. Entrez : **`run-host-command ipmitool lan print`** Pour afficher les configurations BMC actuelles de l'appliance.
2. Éteignez l'appareil :

   "Arrêtez le SGF6112"

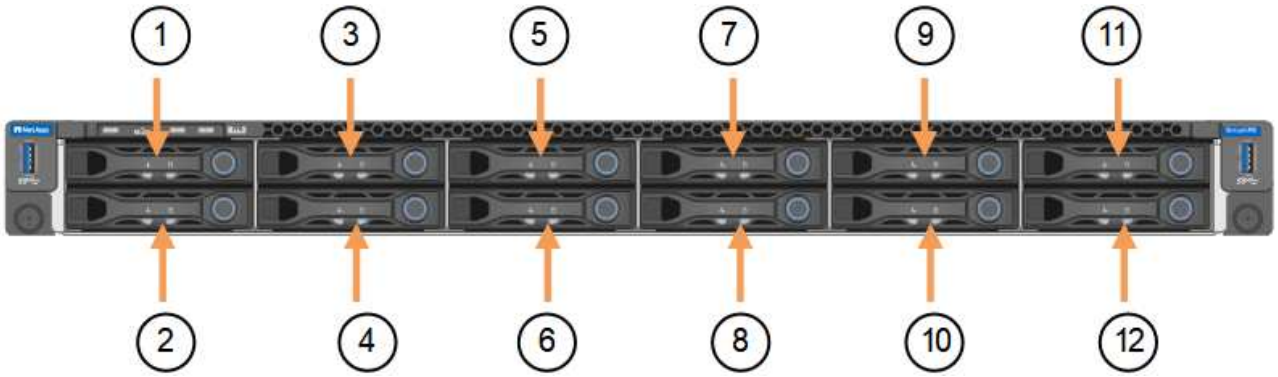
3. Si l'une des interfaces réseau de cette appliance StorageGRID est configurée pour DHCP, vous devrez peut-être mettre à jour les attributions de bail DHCP permanentes sur les serveurs DHCP pour référencer les adresses MAC de l'appliance de remplacement, afin de vous assurer que l'appliance se voit attribuer les adresses IP attendues. Voir "Mettre à jour les références d'adresse MAC".
4. Retirez et remplacez l'appareil :
   a. Etiqueter les câbles, puis débrancher les câbles et les émetteurs-récepteurs réseau.

Pour éviter toute dégradation des performances, ne tordez pas, ne pliez pas, ne pincez pas ou ne montez pas sur les câbles.

b. Retirez l'appliance défectueuse de l'armoire ou du rack.

c. Notez la position des composants remplaçables (deux blocs d'alimentation, huit ventilateurs, trois cartes réseau et douze disques SSD) dans l'appliance défectueuse.

   Les douze disques se trouvent aux emplacements suivants dans le châssis (avant du châssis avec le cadre retiré) :



	Lecteur
1	HDD00
2	HDD01
3	HDD02
4	HDD03
5	HDD04
6	HDD05
7	HDD06
8	HDD07
9	HDD08
10	HDD09
11	HDD10
12	HDD11

d. Transférez les composants remplaçables sur l'appareil de remplacement.

   Suivez les instructions de maintenance fournies pour réinstaller les composants remplaçables.

   > Si vous souhaitez conserver les données sur les disques, veillez à insérer les disques SSD dans les emplacements de disque qu'ils occupaient dans l'appliance en panne. Si ce n'est pas le cas, le programme d'installation de l'appliance affichera un message d'avertissement et vous devrez placer les disques dans les emplacements appropriés et redémarrer l'appliance avant que l'appliance puisse rejoindre à nouveau la grille.

a. Installez l'appliance de remplacement dans l'armoire ou le rack.

b. Remplacez les câbles et les émetteurs-récepteurs optiques.

c. Mettez l'appareil sous tension et attendez qu'il rejoigne à nouveau la grille. Si l'appliance ne rejoint pas la grille, suivez les instructions de la page d'accueil du programme d'installation de l'appliance StorageGRID pour résoudre le problème.

   > Pour éviter toute perte de données si le programme d'installation de l'appliance indique que des modifications matérielles sont nécessaires, telles que le déplacement de disques vers différents emplacements, mettez l'appliance hors tension avant de procéder à des modifications matérielles.

5. Si l'appliance que vous avez remplacée utilisait un serveur de gestion des clés (KMS) pour chiffrer les données, il est possible que vous ayez besoin d'une configuration supplémentaire avant que le nœud puisse rejoindre la grille. Si le nœud ne rejoint pas automatiquement la grille, assurez-vous que ces paramètres de configuration ont été transférés vers la nouvelle appliance et configurez manuellement les paramètres qui ne possèdent pas la configuration attendue :
   - "Configurer les connexions StorageGRID"
   - "Configurez le chiffrement des nœuds pour l'appliance"
6. Connectez-vous à l'appliance remplacée :
   a. Saisissez la commande suivante : `ssh admin@grid_node_IP`
   b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
   c. Entrez la commande suivante pour passer à la racine : `su -`
   d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
7. Restaurez la connectivité réseau du contrôleur BMC pour l'appliance remplacée. Deux options sont disponibles :
   - Utilisez une adresse IP statique, un masque de réseau et une passerelle
   - Utilisez DHCP pour obtenir une adresse IP, un masque de réseau et une passerelle

     i. Pour restaurer la configuration du contrôleur BMC afin d'utiliser une adresse IP statique, un masque de réseau et une passerelle, entrez les commandes suivantes :

     `run-host-command ipmitool lan set 1 ipsrc static`

     `run-host-command ipmitool lan set 1 ipaddr *Appliance_IP*`

`run-host-command ipmitool lan set 1 netmask *Netmask_IP*`

```
run-host-command ipmitool lan set 1 defgw ipaddr Default_gateway
```

i. Pour restaurer la configuration du contrôleur BMC afin d'utiliser DHCP pour obtenir une adresse IP, un masque de réseau et une passerelle, entrez la commande suivante :

```
run-host-command ipmitool lan set 1 ipsrc dhcp
```

8. Après avoir restauré la connectivité réseau du contrôleur BMC, connectez-vous à l'interface du contrôleur BMC pour vérifier et restaurer toute configuration BMC personnalisée supplémentaire que vous avez éventuellement appliquée. Par exemple, vous devez confirmer les paramètres des destinations d'interruption SNMP et des notifications par e-mail. Voir "Configurer l'interface BMC".
9. Vérifiez que le nœud de l'appliance s'affiche dans Grid Manager et qu'aucune alerte n'apparaît.

Informations associées

"Installation de l'appliance dans une armoire ou un rack (SGF6112)"

"Afficher les indicateurs d'état"

"Afficher les codes de démarrage de l'appareil"

Après le remplacement de la pièce, renvoyez la pièce défectueuse à NetApp, en suivant les instructions RMA (retour de matériel) livrées avec le kit. Voir la "Retour de pièce et amp ; remplacements" pour plus d'informations.

Déplacez le SGF6112 dans l'armoire ou le rack

Retirez le SGF6112 d'une armoire ou d'un rack pour accéder au capot supérieur ou pour déplacer l'appliance vers un autre emplacement, puis réinstallez l'appliance dans une armoire ou un rack une fois la maintenance matérielle terminée.

Retirez le SGF6112 de l'armoire ou du rack

Avant de commencer

- Vous disposez d'étiquettes pour identifier chaque câble connecté au SGF6112.
- Vous avez physiquement localisé le SGF6112 où vous effectuez la maintenance dans le data Center.

  "Localisez le SGF6112 dans le data Center"

- Vous avez arrêté le SGF6112.

  "Arrêtez le SGF6112"

  N'éteignez pas l'appareil à l'aide de l'interrupteur d'alimentation.

Étapes

1. Etiquetez puis débranchez les câbles d'alimentation de l'appareil.
2. Enroulez l'extrémité du bracelet antistatique autour de votre poignet et fixez l'extrémité du clip à une masse métallique afin d'éviter toute décharge statique.
3. Etiquetez puis débranchez les câbles de données de l'appliance et les émetteurs-récepteurs SFP+ ou SFP28.

Pour éviter toute dégradation des performances, ne tordez pas, ne pliez pas, ne pincez pas ou ne montez pas sur les câbles.

4. Desserrez les deux vis imperdables situées sur le panneau avant de l'appareil.

5. Faites glisser le SGF6112 vers l'avant pour le sortir du rack jusqu'à ce que les rails de montage soient complètement sortis et que vous entendiez un clic sur les loquets des deux côtés.

   Le capot supérieur de l'appareil est accessible.

6. Facultatif : si vous retirez complètement l'appareil de l'armoire ou du rack, suivez les instructions du kit de rails pour retirer l'appareil des rails.

Après le remplacement de la pièce, renvoyez la pièce défectueuse à NetApp, en suivant les instructions RMA (retour de matériel) livrées avec le kit. Voir la "Retour de pièce et amp ; remplacements" pour plus d'informations.

Réinstallez le SGF6112 dans l'armoire ou le rack

Avant de commencer

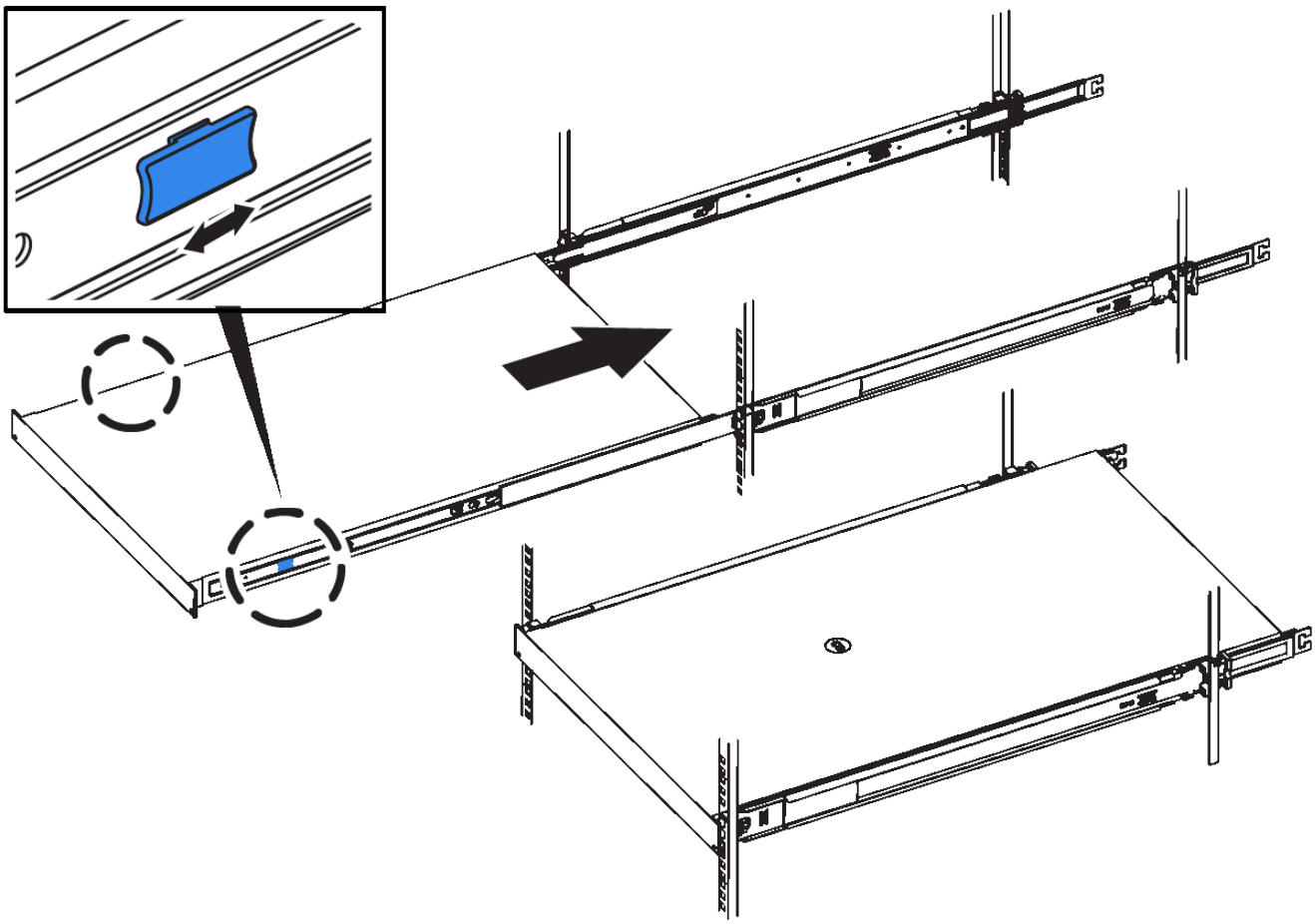
Vous avez réinstallé le capot de l'appareil.

"Réinstallez le couvercle du SGF6112"

Étapes

1. Appuyez simultanément sur le rail bleu pour libérer les deux rails du rack et faites glisser le SGF6112 dans le rack jusqu'à ce qu'il soit bien en place.

   Lorsque vous ne pouvez plus déplacer le contrôleur, tirez sur les loquets bleus des deux côtés du châssis pour faire glisser le contrôleur complètement vers l'intérieur.



Ne fixez le panneau avant qu'après la mise sous tension du contrôleur.

2. Serrez les vis imperdables du panneau avant du contrôleur pour fixer le contrôleur dans le rack.

3. Enroulez l'extrémité du bracelet antistatique autour de votre poignet et fixez l'extrémité du clip à une masse métallique afin d'éviter toute décharge statique.
4. Reconnectez les câbles de données du contrôleur et les émetteurs-récepteurs SFP+ ou SFP28.

Pour éviter toute dégradation des performances, ne tordez pas, ne pliez pas, ne pincez pas ou ne montez pas sur les câbles.

"Cable appliance (SGF6112)"

5. Reconnectez les câbles d'alimentation du contrôleur.

"Branchement des câbles d'alimentation et mise sous tension (SGF6112)"

Une fois que vous avez terminé

L'appareil peut être redémarré.

"Mettez le SGF6112 sous tension et vérifiez son fonctionnement"

Replacez le couvercle du SGF6112

Retirez le couvercle de l'appareil pour accéder aux composants internes à des fins d'entretien et remettez-le en place une fois l'opération terminée.

Déposer le couvercle

Avant de commencer

Retirez l'appareil de l'armoire ou du rack pour accéder au capot supérieur.

"Retirez le SGF6112 de l'armoire ou du rack"

Étapes

1. Assurez-vous que le loquet du capot du SGF6112 n'est pas verrouillé. Si nécessaire, tournez le verrou en plastique bleu d'un quart de tour dans le sens de déverrouillage, comme illustré sur le verrou.
2. Faites pivoter le loquet vers le haut et vers l'arrière du châssis SGF6112 jusqu'à ce qu'il s'arrête, puis soulevez avec précaution le capot du châssis et mettez-le de côté.

Enroulez l'extrémité de la sangle d'un bracelet antistatique autour de votre poignet et fixez l'extrémité de la pince à une terre métallique pour éviter toute décharge statique lors d'une intervention à l'intérieur du SGF6112.

Réinstallez le couvercle

Avant de commencer

Vous avez effectué toutes les procédures de maintenance à l'intérieur de l'appareil.

Étapes

1. Avec le loquet du capot ouvert, tenez le capot au-dessus du châssis et alignez le trou du loquet du capot supérieur avec la broche du châssis. Lorsque le capot est aligné, abaissez-le sur le châssis.

2. Faites pivoter le loquet du capot vers l'avant et vers le bas jusqu'à ce qu'il s'arrête et que le capot s'insère complètement dans le châssis. Vérifier qu'il n'y a pas d'espace le long du bord avant du couvercle.

   Si le capot n'est pas bien en place, il se peut que vous ne puissiez pas faire glisser le SGF6112 dans le rack.

3. En option : tournez d'un quart de tour le verrou en plastique bleu dans le sens de verrouillage, comme illustré sur le verrou, pour le verrouiller.

Une fois que vous avez terminé

Réinstallez l'appareil dans l'armoire ou le rack.

"Réinstallez le SGF6112 dans l'armoire ou le rack"

Maintenance du matériel SG6000

Entretenir l'appareil SG6000

Vous devrez peut-être effectuer des procédures de maintenance sur l'appareil SG6000.

Les procédures spécifiques à la maintenance de votre appliance SG6000 sont décrites dans cette section et supposent que l'appliance a déjà été déployée en tant que nœud de stockage dans un système StorageGRID.

Voir "Procédures courantes" pour les procédures de maintenance utilisées par tous les appareils.

Voir "Configurer le matériel" pour les procédures de maintenance qui sont également effectuées lors de l'installation et de la configuration initiales de l'appliance.

Pour éviter toute interruption de service, vérifiez que tous les autres nœuds de stockage sont connectés au grid avant d'arrêter l'appliance ou de l'arrêter durant une fenêtre de maintenance planifiée en cas d'interruption de service. Voir les informations sur "contrôle de l'état de connexion du nœud".

> Si vous avez déjà utilisé une règle ILM pour créer une seule copie d'un objet, vous devez arrêter l'appliance durant une fenêtre de maintenance planifiée. Sinon, vous risquez de perdre temporairement l'accès à ces objets pendant toute procédure de maintenance qui met un nœud de stockage hors service. Voir les informations sur "gestion des objets avec gestion du cycle de vie des informations".

Procédures de configuration de la maintenance

Mettez à niveau votre système d'exploitation SANtricity sur les contrôleurs de stockage

Pour optimiser le fonctionnement du contrôleur de stockage, vous devez effectuer une mise à niveau vers la dernière version de maintenance du système d'exploitation SANtricity compatible avec votre appliance StorageGRID.

Consulter le "Matrice d'interopérabilité NetApp (IMT)" pour déterminer la version que vous devez utiliser.

Téléchargez le nouveau fichier du logiciel SANtricity OS sur "Téléchargement NetApp : appliance StorageGRID".

Utilisez l'une des procédures suivantes basées sur la version de SANtricity OS actuellement installée :

- Si le contrôleur de stockage utilise SANtricity OS 08.42.20.00 (11.42) ou une version ultérieure, utilisez Grid Manager pour effectuer la mise à niveau.

  "Mettez à niveau le système d'exploitation SANtricity sur les contrôleurs de stockage à l'aide de Grid Manager"

- Si le contrôleur de stockage utilise une version de SANtricity OS antérieure à 08.42.20.00 (11.42), utilisez le mode de maintenance pour effectuer la mise à niveau.

  "Mettre à niveau le système d'exploitation SANtricity sur les contrôleurs de stockage à l'aide du mode de maintenance"

> Lorsque vous mettez à niveau SANtricity OS pour votre appliance de stockage, vous devez suivre les instructions de la documentation StorageGRID. Si vous utilisez d'autres instructions, votre appareil risque de ne plus fonctionner.

Mettez à niveau le système d'exploitation SANtricity sur les contrôleurs de stockage à l'aide de Grid Manager

Pour les contrôleurs de stockage qui utilisent actuellement SANtricity OS 08.42.20.00 (11.42) ou version ultérieure, vous devez utiliser le gestionnaire grid pour appliquer une mise à niveau.

Avant de commencer

- Vous avez consulté le "Matrice d'interopérabilité NetApp (IMT)" Pour vérifier que la version de SANtricity OS utilisée pour la mise à niveau est compatible avec votre appliance.
- Vous avez le "Maintenance ou autorisation d'accès racine".
- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous avez la phrase secrète pour le provisionnement.
- Vous avez accès à "Téléchargement NetApp : appliance StorageGRID".

Description de la tâche

Vous ne pouvez pas effectuer d'autres mises à jour logicielles (mise à niveau du logiciel StorageGRID ou correctif) tant que vous n'avez pas terminé le processus de mise à niveau du système d'exploitation SANtricity. Si vous tentez de lancer un correctif ou une mise à niveau du logiciel StorageGRID avant la fin du processus de mise à niveau de SANtricity OS, vous êtes redirigé vers la page de mise à niveau de SANtricity OS.

La procédure ne sera terminée qu'une fois la mise à niveau de SANtricity OS appliquée avec succès à tous les nœuds applicables sélectionnés pour la mise à niveau. Cela peut prendre plus de 30 minutes pour charger le système d'exploitation SANtricity sur chaque nœud (de façon séquentielle) et jusqu'à 90 minutes pour redémarrer chaque appliance de stockage StorageGRID. Les nœuds de votre grille qui n'utilisent pas SANtricity OS ne seront pas affectés par cette procédure.

> Les étapes suivantes s'appliquent uniquement lorsque vous utilisez le gestionnaire de grille pour effectuer la mise à niveau. Les contrôleurs de stockage de l'appliance ne peuvent pas être mis à niveau à l'aide du gestionnaire de grid lorsque les contrôleurs utilisent un système d'exploitation SANtricity antérieur à 08.42.20.00 (11.42).

> Cette procédure met automatiquement à niveau la NVSRAM vers la version la plus récente associée à la mise à niveau du système d'exploitation SANtricity. Vous n'avez pas besoin d'appliquer un fichier de mise à niveau NVSRAM distinct.

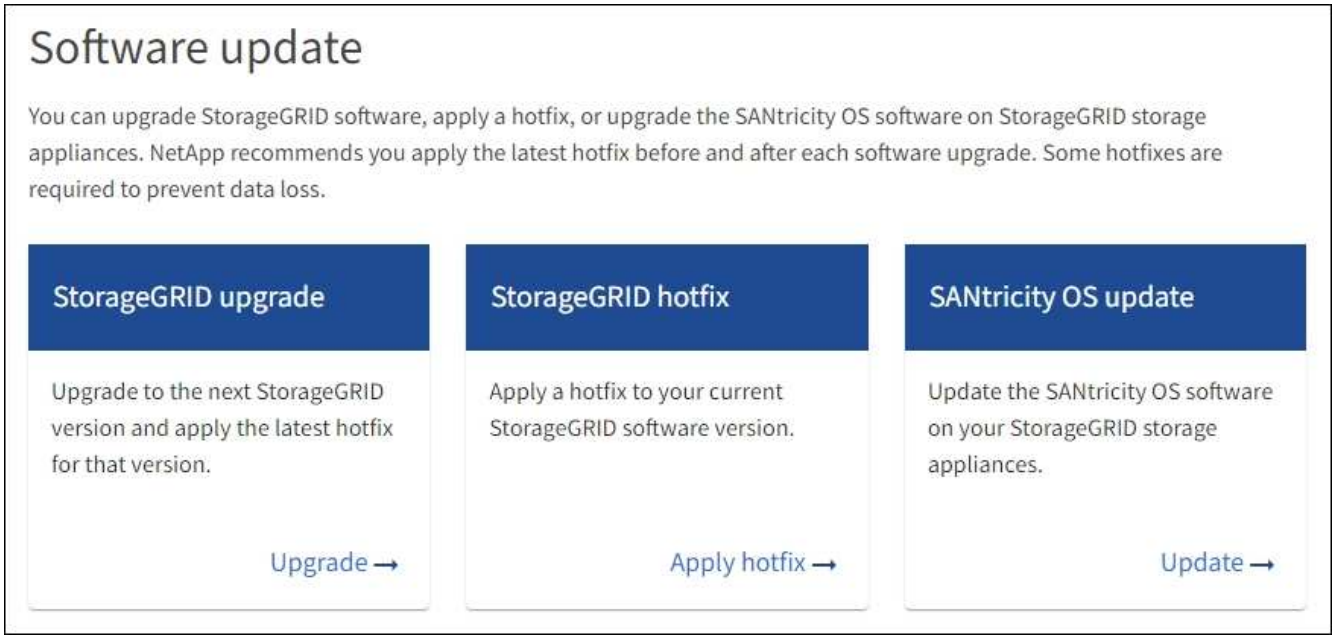
> Veillez à appliquer le dernier correctif StorageGRID avant de commencer cette procédure. Voir "Procédure de correctif StorageGRID" pour plus d'informations.

Étapes

1. Téléchargez le nouveau fichier du logiciel SANtricity OS depuis le site "Téléchargement NetApp : appliance StorageGRID".

   Veillez à choisir la version de système d'exploitation SANtricity pour vos contrôleurs de stockage.

2. Sélectionnez **MAINTENANCE** > **système** > **mise à jour logicielle**.



3. Dans la section mise à jour de SANtricity OS, sélectionnez **mise à jour**.

   La page de mise à niveau de SANtricity OS s'affiche et répertorie les détails de chaque nœud d'appliance, notamment :

   - Nom du nœud
   - Le site

- Modèle de type appliance
- Version du système d'exploitation SANtricity
- État
- État de la dernière mise à niveau

4. Consultez les informations du tableau pour tous vos appareils pouvant être mis à niveau. Vérifiez que tous les contrôleurs de stockage ont l'état **nominal**. Si l'état d'un contrôleur est **Inconnu**, passez à **nœuds** > ***appliance node*** > **matériel** pour rechercher et résoudre le problème.
5. Sélectionnez le fichier de mise à niveau du système d'exploitation SANtricity que vous avez téléchargé depuis le site du support NetApp.

   a. Sélectionnez **Parcourir**.

   b. Localisez et sélectionnez le fichier.

   c. Sélectionnez **Ouvrir**.

   Le fichier est téléchargé et validé. Une fois le processus de validation terminé, le nom du fichier est affiché avec une coche verte à côté du bouton **Browse**. Ne modifiez pas le nom du fichier car il fait partie du processus de vérification.

6. Entrez la phrase de passe de provisionnement et sélectionnez **Continuer**.

   Un message d'avertissement s'affiche indiquant que la connexion de votre navigateur peut être perdue temporairement car les services sur les nœuds mis à niveau sont redémarrés.

7. Sélectionnez **Oui** pour placer le fichier de mise à niveau de SANtricity OS sur le nœud d'administration principal.

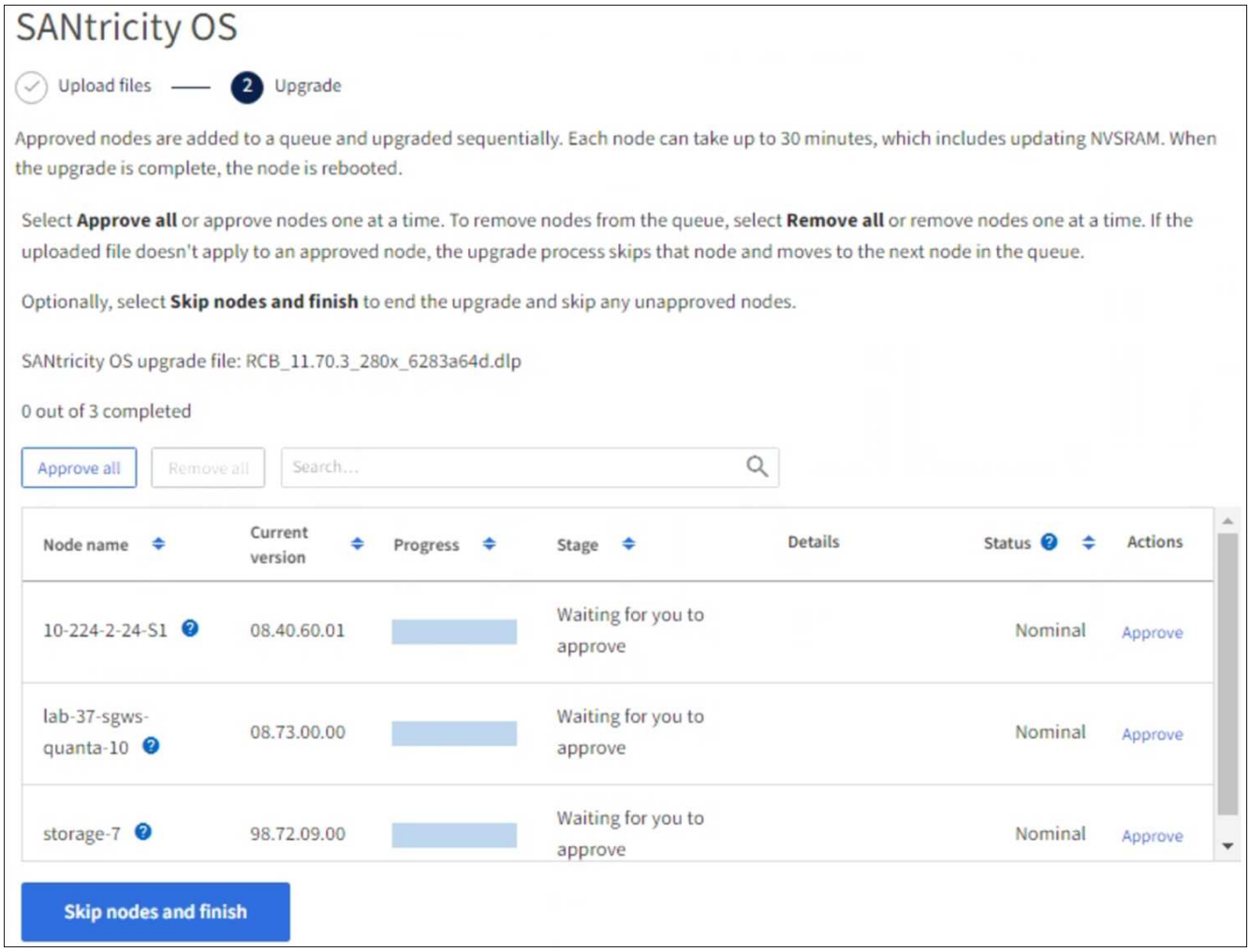
   Lorsque la mise à niveau de SANtricity OS démarre :

   a. Le contrôle de l'état est exécuté. Ce processus vérifie qu'aucun nœud ne présente l'état nécessite une intervention.

      Si des erreurs sont signalées, résolvez-les et sélectionnez à nouveau **Démarrer**.

   b. Le tableau de progression de la mise à niveau de SANtricity OS s'affiche. Ce tableau affiche tous les nœuds de stockage de votre grille ainsi que l'étape actuelle de la mise à niveau de chaque nœud.

      Le tableau indique tous les nœuds de stockage de l'appliance. Les nœuds de stockage logiciels ne sont pas affichés. Sélectionnez **Approve** pour tous les nœuds nécessitant la mise à niveau.



8. Vous pouvez également trier la liste des nœuds par ordre croissant ou décroissant :
   - Nom du nœud
   - Version actuelle
   - Progression
   - Étape
   - État

   Vous pouvez également saisir un terme dans la zone de recherche pour rechercher des nœuds spécifiques.

9. Approuver les nœuds de grille que vous êtes prêt à ajouter à la file d'attente de mise à niveau. Les nœuds approuvés sont mis à niveau un par un.

   > N'approuvez pas la mise à niveau de SANtricity OS pour un nœud de stockage d'appliance, sauf si vous êtes sûr que le nœud est prêt à être arrêté et redémarré. Lorsque la mise à niveau de SANtricity OS est approuvée sur un nœud, les services qui y sont arrêtés et le processus de mise à niveau commence. Plus tard, lorsque la mise à niveau du nœud est terminée, le nœud d'appliance est redémarré. Ces opérations peuvent entraîner des interruptions de service pour les clients qui communiquent avec le nœud.

   - Sélectionnez le bouton **Approve All** pour ajouter tous les nœuds de stockage à la file d'attente de mise à niveau de SANtricity OS.

> Si l'ordre dans lequel les nœuds sont mis à niveau est important, approuvez les nœuds ou les groupes de nœuds un par un et attendez que la mise à niveau soit terminée sur chaque nœud avant d'approuver le nœud suivant.

- Sélectionnez un ou plusieurs boutons **Approve** pour ajouter un ou plusieurs nœuds à la file d'attente de mise à niveau de SANtricity OS. Le bouton **Approve** est désactivé si l'état n'est pas nominal.

  Après avoir sélectionné **Approve**, le processus de mise à niveau détermine si le noeud peut être mis à niveau. Si un nœud peut être mis à niveau, il est ajouté à la file d'attente de mise à niveau.

Pour certains noeuds, le fichier de mise à niveau sélectionné n'est pas appliqué intentionnellement et vous pouvez terminer le processus de mise à niveau sans mettre à niveau ces noeuds spécifiques. Les nœuds volontairement non mis à niveau affichent une étape terminée (tentative de mise à niveau) et indiquent la raison pour laquelle le nœud n'a pas été mis à niveau dans la colonne Détails.

10. Si vous devez supprimer un nœud ou tous les nœuds de la file d'attente de mise à niveau de SANtricity OS, sélectionnez **Supprimer** ou **tout supprimer**.

    Lorsque l'étape dépasse la mise en file d'attente, le bouton **Supprimer** est masqué et vous ne pouvez plus supprimer le nœud du processus de mise à niveau de SANtricity OS.

11. Attendez que la mise à niveau de SANtricity OS soit appliquée à chaque nœud de grid approuvé.

    - Si un nœud affiche une étape d'erreur alors que la mise à niveau de SANtricity OS est appliquée, la mise à niveau a échoué pour le nœud. Avec l'aide du support technique, vous devrez peut-être placer l'appliance en mode maintenance pour la restaurer.
    - Si le firmware du nœud est trop ancien pour être mis à niveau avec le Gestionnaire de grille, le nœud affiche un stade d'erreur avec les détails que vous devez utiliser le mode de maintenance pour mettre à niveau SANtricity OS sur le nœud. Pour résoudre l'erreur, procédez comme suit :
      i. Utilisez le mode de maintenance pour mettre à niveau SANtricity OS sur le nœud qui affiche une étape d'erreur.
      ii. Utilisez Grid Manager pour redémarrer et terminer la mise à niveau de SANtricity OS.

    Une fois la mise à niveau du système d'exploitation SANtricity terminée sur tous les nœuds approuvés, le tableau de progression de la mise à niveau du système d'exploitation SANtricity se ferme et une bannière verte indique le nombre de nœuds mis à niveau, ainsi que la date et l'heure de fin de la mise à niveau.

12. Si un nœud ne peut pas être mis à niveau, notez la raison indiquée dans la colonne Détails et prenez l'action appropriée.

> La mise à niveau de SANtricity OS n'est terminée qu'une fois la mise à niveau de SANtricity OS approuvée sur tous les nœuds de stockage répertoriés.

Raison	Action recommandée
Le nœud de stockage a déjà été mis à niveau.	Aucune autre action n'est requise.
La mise à niveau de SANtricity OS n'est pas applicable à ce nœud.	Le nœud ne dispose d'aucun contrôleur de stockage qui peut être géré par le système StorageGRID. Terminez le processus de mise à niveau sans mettre à niveau le nœud affichant ce message.

Raison	Action recommandée
SANtricity OS fichier n'est pas compatible avec ce nœud.	Le nœud nécessite un fichier SANtricity OS différent de celui que vous avez sélectionné. Une fois la mise à niveau actuelle terminée, téléchargez le fichier SANtricity OS approprié pour le nœud et répétez le processus de mise à niveau.

13. Si vous souhaitez mettre fin à l'approbation des nœuds et revenir à la page SANtricity OS pour permettre le téléchargement d'un nouveau fichier SANtricity OS, procédez comme suit :
    a. Sélectionnez **Ignorer les nœuds et Terminer**.

       Un avertissement s'affiche vous demandant si vous êtes sûr de vouloir terminer le processus de mise à niveau sans mettre à niveau tous les nœuds applicables.

    b. Sélectionnez **OK** pour revenir à la page **SANtricity OS**.
    c. Lorsque vous êtes prêt à poursuivre l'approbation des nœuds, Téléchargez SANtricity OS pour redémarrer le processus de mise à niveau.

       Les nœuds déjà approuvés et mis à niveau sans erreur restent mis à niveau.

14. Répétez cette procédure de mise à niveau pour tous les nœuds dont la procédure de fin nécessite un fichier de mise à niveau SANtricity OS différent.

    Pour les nœuds avec un état de nécessite une intervention, utilisez le mode maintenance pour effectuer la mise à niveau.

Informations associées

"Matrice d'interopérabilité NetApp"

"Mettre à niveau le système d'exploitation SANtricity sur les contrôleurs de stockage à l'aide du mode de maintenance"

Mettre à niveau le système d'exploitation SANtricity sur les contrôleurs de stockage à l'aide du mode de maintenance

Pour les contrôleurs de stockage qui utilisent actuellement SANtricity OS antérieurs à la version 08.42.20.00 (11.42), vous devez utiliser la procédure du mode de maintenance pour appliquer une mise à niveau.

Avant de commencer

- Vous avez consulté le "Matrice d'interopérabilité NetApp (IMT)" Pour vérifier que la version de SANtricity OS utilisée pour la mise à niveau est compatible avec votre appliance.
- Si l'appliance StorageGRID s'exécute sur un système StorageGRID, vous avez placé le contrôleur SG6000-CN dans "mode maintenance".

  Le mode maintenance interrompt la connexion au contrôleur de stockage.

Description de la tâche

Ne mettez pas à niveau le système d'exploitation SANtricity ou la NVSRAM du contrôleur E-Series sur plusieurs appliances StorageGRID à la fois.

La mise à niveau de plusieurs appliances StorageGRID peut entraîner une indisponibilité des données, en fonction du modèle de déploiement et des règles ILM.

Étapes

1. Vérifiez que l'appareil est dans "mode maintenance".
2. Depuis un ordinateur portable de service, accédez à SANtricity System Manager et connectez-vous.
3. Téléchargez le nouveau fichier du logiciel SANtricity OS et le fichier NVSRAM sur le client de gestion.

   La NVSRAM est spécifique à l'appliance StorageGRID. N'utilisez pas le téléchargement standard de NVSRAM.

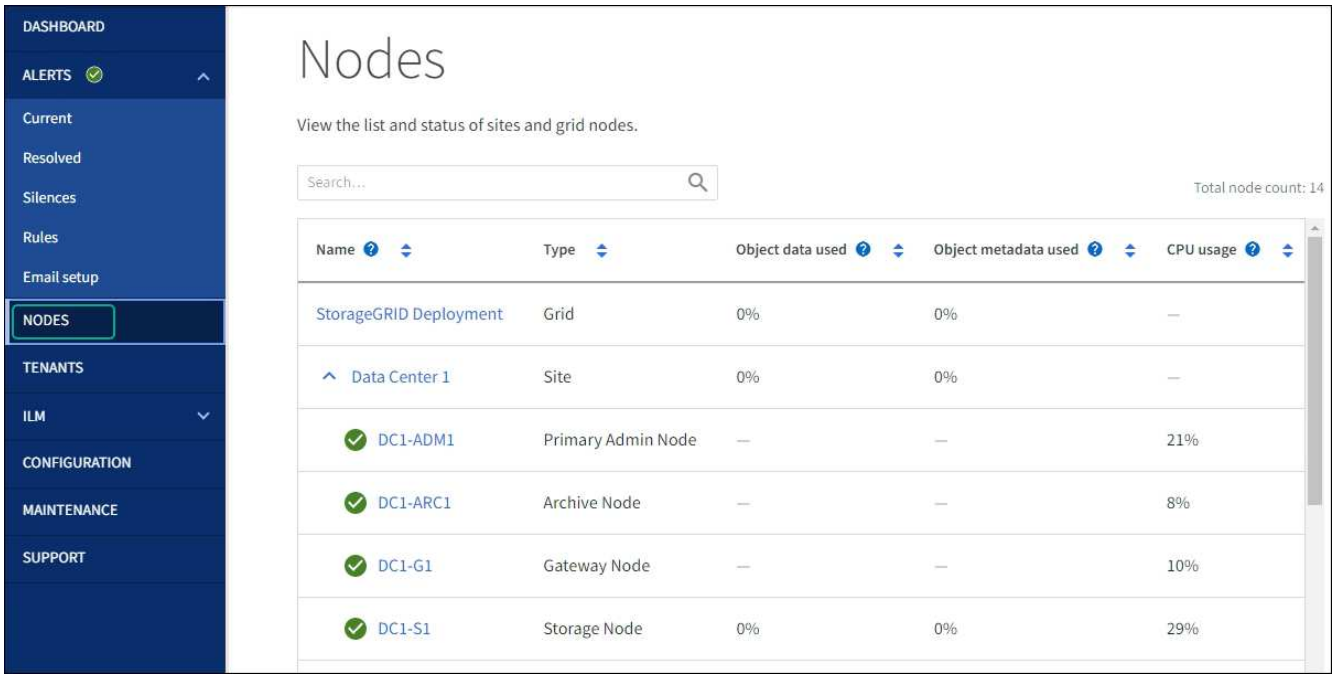
4. Suivez les instructions du *Upgrade SANtricity OS* guide ou de l'aide en ligne de SANtricity System Manager pour mettre à niveau le micrologiciel et la NVSRAM.

   Activez immédiatement les fichiers de mise à niveau. Ne différez pas l'activation.

5. Si cette procédure s'est terminée avec succès et que vous disposez de procédures supplémentaires pour effectuer cette opération pendant que le nœud est en mode de maintenance, effectuez-les maintenant. Lorsque vous avez terminé, ou si vous avez rencontré des échecs et souhaitez recommencer, sélectionnez **Avancé** > **redémarrer le contrôleur**, puis sélectionnez l'une des options suivantes :

   - Sélectionnez **redémarrer dans StorageGRID**
   - Sélectionnez **redémarrer en mode maintenance** pour redémarrer le contrôleur avec le nœud restant en mode de maintenance. Sélectionnez cette option si vous avez rencontré des échecs au cours de la procédure et souhaitez recommencer. Une fois le redémarrage du nœud en mode maintenance terminé, redémarrez à partir de l'étape appropriée de la procédure ayant échoué.

   L'appliance peut redémarrer et rejoindre la grille en 20 minutes. Pour confirmer que le redémarrage est terminé et que le nœud a rejoint la grille, retournez à la grille Manager. La page nœuds doit afficher un état normal (icône en forme de coche verte) à gauche du nom du nœud) pour le nœud de l'appliance, indiquant qu'aucune alerte n'est active et que le nœud est connecté à la grille.



Informations associées

"Matrice d'interopérabilité NetApp"

"Mettez à niveau le système d'exploitation SANtricity sur les contrôleurs de stockage à l'aide de Grid Manager"

Mise à niveau du firmware des disques à l'aide de SANtricity System Manager

Mettez à niveau le firmware du disque SG6000 à l'aide du Gestionnaire système SANtricity en utilisant la méthode en ligne

Utilisez la méthode en ligne du Gestionnaire système SANtricity pour mettre à niveau le firmware des disques de votre appliance et vous assurer que vous disposez des dernières fonctionnalités et des derniers correctifs.

Avant de commencer

- Le dispositif de stockage est à l'état optimal.
- Tous les disques ont un état optimal.

> Ne mettez pas à niveau le firmware du disque sur plusieurs appliances StorageGRID à la fois. Cela pourrait entraîner une indisponibilité des données, selon votre modèle de déploiement et votre politique ILM.

Description de la tâche

Les disques sont mis à niveau un par un pendant que l'appliance effectue des E/S. Cette méthode ne nécessite pas le passage de l'appareil en mode de maintenance. Cependant, les performances du système peuvent être affectées et la mise à niveau peut prendre plusieurs heures de plus que la méthode hors ligne.

Les disques appartenant à des volumes qui ne sont pas redondants doivent être mis à jour à l'aide du "méthode hors ligne". La méthode hors ligne doit être utilisée pour tout disque associé au cache de lecture Flash (par exemple, des disques SSD dans le SG6060) ou tout pool ou groupe de volumes actuellement dégradé.
Il existe deux types de disques : les disques SSD et les disques durs. Vous devez utiliser le "méthode hors ligne" Pour mettre à niveau le firmware sur les disques SSD (par exemple, des disques SSD dans le SG6060). Vous pouvez utiliser la méthode en ligne ou hors ligne pour mettre à niveau le micrologiciel sur les disques durs.

Étapes

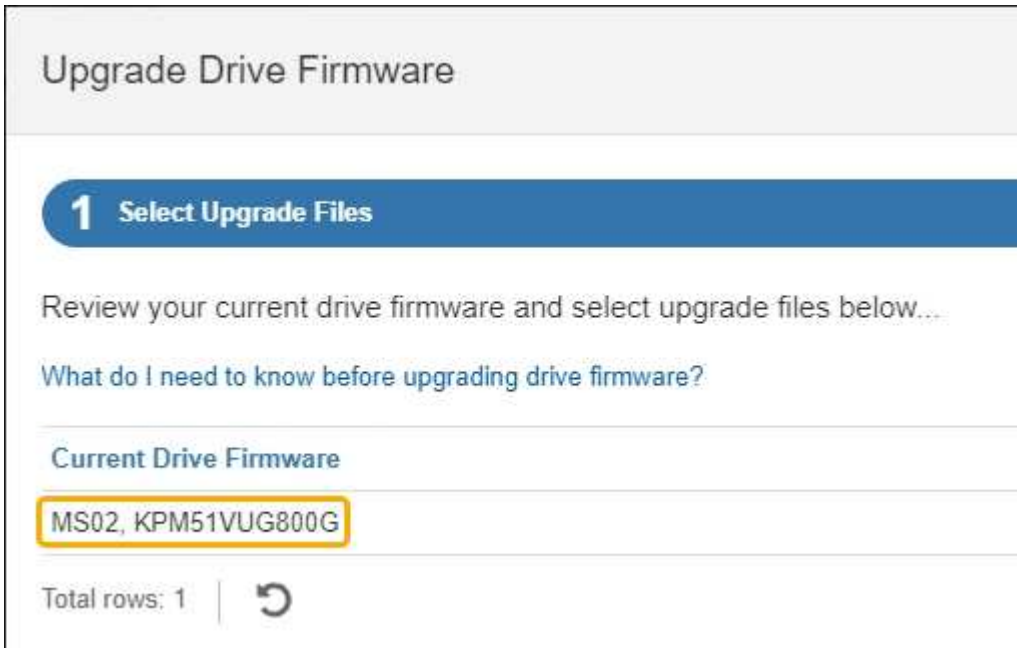
1. Pour accéder à SANtricity System Manager, utilisez l'une des méthodes suivantes :
   - Utilisez le programme d'installation de l'appliance StorageGRID et sélectionnez **Avancé** > **Gestionnaire système SANtricity**
   - Utilisez le Gestionnaire de grille et sélectionnez **NODES** > ***noeud de stockage*** > **Gestionnaire système SANtricity**
   - Pour utiliser SANtricity System Manager, accédez à l'adresse IP du contrôleur de stockage :

     `https://Storage_Controller_IP`

2. Entrez le nom d'utilisateur et le mot de passe de l'administrateur SANtricity System Manager si nécessaire.
3. Vérifiez la version du micrologiciel du lecteur actuellement installé sur l'appliance de stockage :
   a. Dans le Gestionnaire système SANtricity, sélectionnez **SUPPORT** > **Centre de mise à niveau**.
   b. Sous mise à niveau du micrologiciel du lecteur, sélectionnez **commencer la mise à niveau**.

      La page mettre à niveau le micrologiciel du lecteur affiche les fichiers du micrologiciel du lecteur actuellement installés.

   c. Notez les révisions actuelles du micrologiciel du lecteur et les identificateurs de lecteur dans la colonne micrologiciel du lecteur en cours.



Dans cet exemple :

- La version du micrologiciel du lecteur est **MS02**.
- L'identifiant du lecteur est **KPM51VUG800G**.

d. Sélectionnez **Afficher les lecteurs** dans la colonne lecteurs associés pour afficher l'emplacement d'installation de ces lecteurs dans votre appliance de stockage.

e. Fermez la fenêtre mise à niveau du micrologiciel du lecteur.

4. Téléchargez et préparez la mise à niveau disponible du firmware des disques :

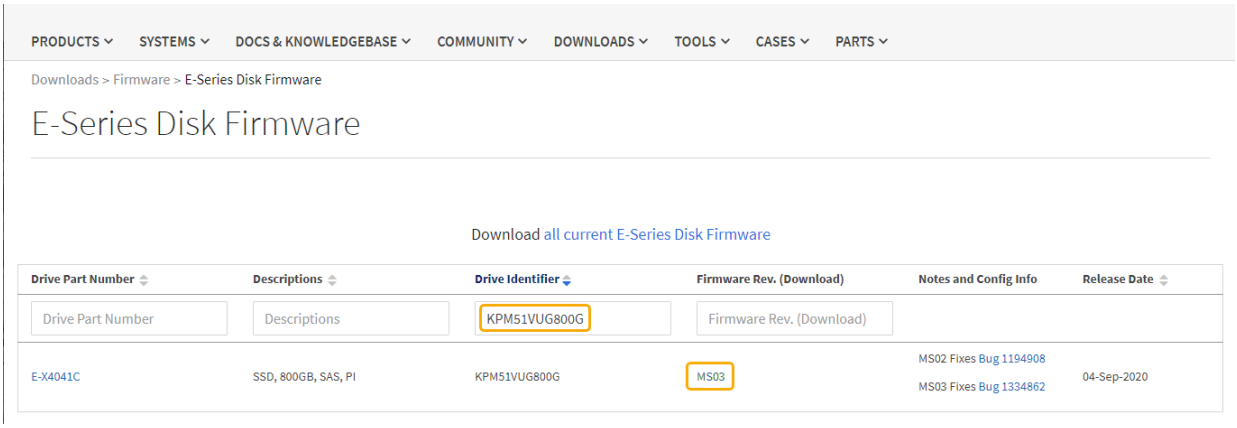
a. Sous mise à niveau du micrologiciel des disques, sélectionnez **NetApp support**.

b. Sur le site de support NetApp, sélectionnez l'onglet **Téléchargements**, puis sélectionnez **micrologiciel de lecteur de disque E-Series**.

La page firmware des disques E-Series s'affiche.

c. Recherchez chaque **Drive identifier** installé dans votre appliance de stockage et vérifiez que chaque identificateur de lecteur dispose de la dernière révision du micrologiciel.

- Si la révision du micrologiciel n'est pas un lien, cet identificateur de lecteur a la dernière révision du micrologiciel.
- Si un ou plusieurs numéros de référence de lecteur sont répertoriés pour un identificateur de lecteur, une mise à niveau du micrologiciel est disponible pour ces lecteurs. Vous pouvez sélectionner n'importe quel lien pour télécharger le fichier de micrologiciel.



d. Si une version ultérieure du micrologiciel est répertoriée, sélectionnez le lien dans la révision du micrologiciel (Télécharger) pour télécharger un `.zip` archive contenant le fichier du micrologiciel.

e. Extrayez (décompressez le fichier d'archive du micrologiciel du lecteur que vous avez téléchargé sur le site de support.

5. Installez la mise à niveau du micrologiciel du lecteur :

a. Dans le Gestionnaire système SANtricity, sous mise à niveau du micrologiciel du lecteur, sélectionnez **commencer la mise à niveau**.

b. Sélectionnez **Browse**, puis sélectionnez les nouveaux fichiers de micrologiciel de lecteur que vous avez téléchargés à partir du site de support.

Les fichiers du micrologiciel du lecteur ont un nom de fichier similaire à `D_HUC101212CSS600_30602291_MS01_2800_0002.dlp`.

Vous pouvez sélectionner jusqu'à quatre fichiers de micrologiciel de lecteur, un par un. Si plusieurs fichiers de micrologiciel de lecteur sont compatibles avec le même lecteur, vous obtenez une erreur de

conflit de fichier. Choisissez le fichier de micrologiciel de lecteur que vous souhaitez utiliser pour la mise à niveau et supprimez l'autre.

c. Sélectionnez **Suivant**.

Sélectionner les lecteurs répertorie les lecteurs que vous pouvez mettre à niveau avec les fichiers de micrologiciel sélectionnés.

Seuls les lecteurs compatibles apparaissent.

Le micrologiciel sélectionné pour le lecteur apparaît dans la colonne **micrologiciel proposé**. Si vous devez modifier ce micrologiciel, sélectionnez **Retour**.

d. Sélectionnez **mettre à niveau tous les lecteurs en ligne** — met à niveau les lecteurs qui peuvent prendre en charge le téléchargement du micrologiciel pendant que la matrice de stockage traite les E/S. Lorsque vous sélectionnez cette méthode de mise à niveau, vous n'avez pas besoin d'arrêter les E/S sur les volumes associés utilisant ces disques.

> Une mise à niveau en ligne peut prendre plusieurs heures de plus qu'une mise à niveau hors ligne.
>
> Vous devez utiliser le "méthode hors ligne" Pour mettre à niveau le firmware des disques SSD.

e. Dans la première colonne du tableau, sélectionnez le ou les lecteurs que vous souhaitez mettre à niveau.

La meilleure pratique consiste à mettre à niveau tous les lecteurs du même modèle vers la même révision du micrologiciel.

f. Sélectionnez **Démarrer** et confirmez que vous souhaitez effectuer la mise à niveau.

Si vous devez arrêter la mise à niveau, sélectionnez **Stop**. Tous les téléchargements de micrologiciel en cours sont terminés. Tous les téléchargements de micrologiciel qui n'ont pas démarré sont annulés.

> L'arrêt de la mise à niveau du micrologiciel du lecteur peut entraîner une perte de données ou l'indisponibilité des disques.

g. (Facultatif) pour afficher la liste des mises à niveau, sélectionnez **Enregistrer le journal**.

Le fichier journal est enregistré dans le dossier des téléchargements de votre navigateur portant le nom `latest-upgrade-log-timestamp.txt`.

"Si nécessaire, dépannez les erreurs de mise à niveau du micrologiciel du pilote".

Mettez à niveau le micrologiciel du lecteur SG6000 à l'aide du Gestionnaire système SANtricity en utilisant la méthode hors ligne

Utilisez la méthode hors ligne du Gestionnaire système SANtricity pour mettre à niveau le firmware des disques de votre appliance et vous assurer que vous disposez des dernières fonctionnalités et des derniers correctifs.

Avant de commencer

- Le dispositif de stockage est à l'état optimal.
- Tous les disques ont un état optimal.
- Vous avez "Mettez l'appliance StorageGRID en mode de maintenance - effectué".

> Lorsque l'appliance est en mode de maintenance, les opérations d'E/S (entrée/sortie) vers le contrôleur de stockage sont arrêtées pour la sécurité des interruptions.

> Ne mettez pas à niveau le firmware du disque sur plusieurs appliances StorageGRID à la fois. Cela pourrait entraîner une indisponibilité des données, selon votre modèle de déploiement et votre politique ILM.

Description de la tâche

Les disques sont mis à niveau en parallèle lorsque l'appliance est en mode de maintenance. Si le pool ou le groupe de volumes ne prend pas en charge la redondance ou est dégradé, vous devez utiliser la méthode hors ligne pour mettre à niveau le micrologiciel du lecteur. Vous devez également utiliser la méthode offline pour tout disque associé au cache de lecture Flash ou tout pool ou groupe de volumes actuellement dégradé. La méthode hors ligne met à niveau le micrologiciel uniquement lorsque toutes les activités d'E/S sont arrêtées sur les disques à mettre à niveau. Pour arrêter les E/S, placez le nœud en mode de maintenance.

La méthode hors ligne est plus rapide que la méthode en ligne et sera beaucoup plus rapide lorsque de nombreux lecteurs d'une seule appliance auront besoin de mises à niveau. Cependant, il requiert la mise hors service des nœuds. Cela peut nécessiter la planification d'une fenêtre de maintenance et le suivi de l'avancement. Choisissez la méthode la mieux adaptée à vos procédures opérationnelles et le nombre de lecteurs à mettre à niveau.

> Il existe deux types de disques : les disques SSD et les disques durs. Vous devez utiliser la méthode hors ligne pour mettre à niveau le firmware sur les disques SSD (par exemple, des disques SSD dans le SG6060). Vous pouvez utiliser la méthode en ligne ou hors ligne pour mettre à niveau le micrologiciel sur les disques durs.

Étapes

1. Vérifiez que l'appareil est dans "mode maintenance".

   > Si vous mettez à niveau le micrologiciel de disques SSD faisant partie d'un groupe de cache, vous devez vous assurer qu'aucune E/S n'est envoyée aux volumes mis en cache pendant la mise à niveau. Lorsque l'appliance est en mode de maintenance, aucune E/S n'est envoyée aux volumes pendant la mise à niveau.

2. Pour accéder à SANtricity System Manager, utilisez l'une des méthodes suivantes :
   - Utilisez le programme d'installation de l'appliance StorageGRID et sélectionnez **Avancé** > **Gestionnaire système SANtricity**
   - Utilisez le Gestionnaire de grille et sélectionnez **NODES** > ***noeud de stockage*** > **Gestionnaire système SANtricity**
   - Pour utiliser SANtricity System Manager, accédez à l'adresse IP du contrôleur de stockage :

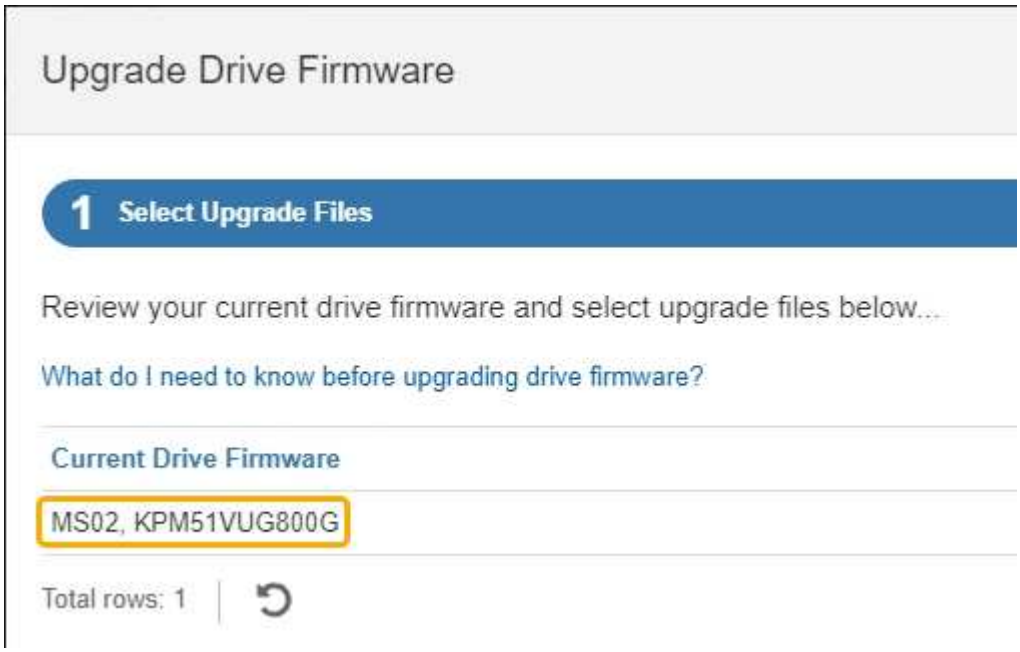
     `https://Storage_Controller_IP`

3. Entrez le nom d'utilisateur et le mot de passe de l'administrateur SANtricity System Manager si nécessaire.

4. Vérifiez la version du micrologiciel du lecteur actuellement installé sur l'appliance de stockage :
   a. Dans le Gestionnaire système SANtricity, sélectionnez **SUPPORT** > **Centre de mise à niveau**.
   b. Sous mise à niveau du micrologiciel du lecteur, sélectionnez **commencer la mise à niveau**.

      La page mettre à niveau le micrologiciel du lecteur affiche les fichiers du micrologiciel du lecteur actuellement installés.

   c. Notez les révisions actuelles du micrologiciel du lecteur et les identificateurs de lecteur dans la colonne micrologiciel du lecteur en cours.



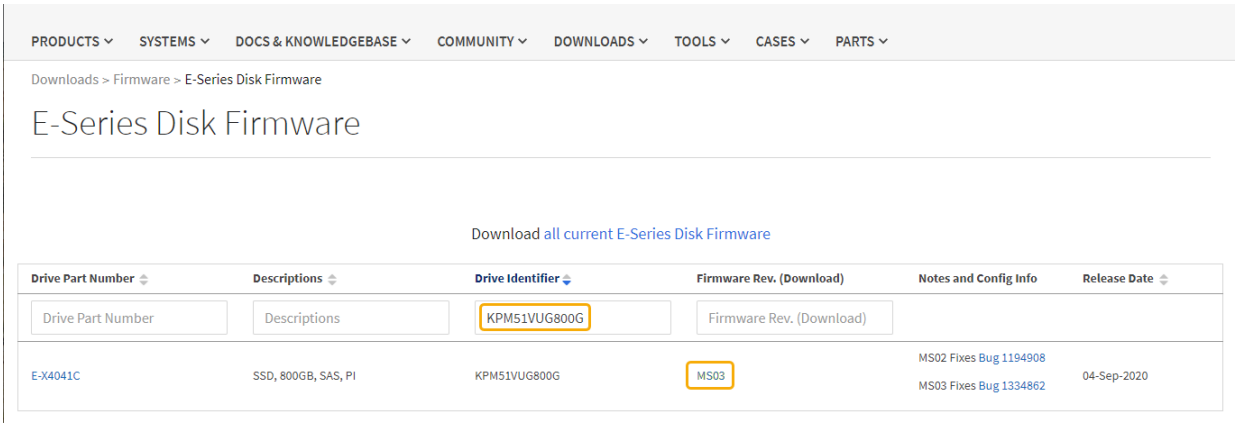
      Dans cet exemple :

      - La version du micrologiciel du lecteur est **MS02**.
      - L'identifiant du lecteur est **KPM51VUG800G**.

   d. Sélectionnez **Afficher les lecteurs** dans la colonne lecteurs associés pour afficher l'emplacement d'installation de ces lecteurs dans votre appliance de stockage.
   e. Fermez la fenêtre mise à niveau du micrologiciel du lecteur.
5. Téléchargez et préparez la mise à niveau disponible du firmware des disques :
   a. Sous mise à niveau du micrologiciel des disques, sélectionnez **NetApp support**.
   b. Sur le site de support NetApp, sélectionnez l'onglet **Téléchargements**, puis sélectionnez **micrologiciel de lecteur de disque E-Series**.

      La page firmware des disques E-Series s'affiche.

   c. Recherchez chaque **Drive identifier** installé dans votre appliance de stockage et vérifiez que chaque identificateur de lecteur dispose de la dernière révision du micrologiciel.
      - Si la révision du micrologiciel n'est pas un lien, cet identificateur de lecteur a la dernière révision du micrologiciel.
      - Si un ou plusieurs numéros de référence de lecteur sont répertoriés pour un identificateur de lecteur, une mise à niveau du micrologiciel est disponible pour ces lecteurs. Vous pouvez sélectionner n'importe quel lien pour télécharger le fichier de micrologiciel.



d. Si une version ultérieure du micrologiciel est répertoriée, sélectionnez le lien dans la révision du micrologiciel (Télécharger) pour télécharger un `.zip` archive contenant le fichier du micrologiciel.

e. Extrayez (décompressez le fichier d'archive du micrologiciel du lecteur que vous avez téléchargé sur le site de support.

6. Installez la mise à niveau du micrologiciel du lecteur :

a. Dans le Gestionnaire système SANtricity, sous mise à niveau du micrologiciel du lecteur, sélectionnez **commencer la mise à niveau**.

b. Sélectionnez **Browse**, puis sélectionnez les nouveaux fichiers de micrologiciel de lecteur que vous avez téléchargés à partir du site de support.

Les fichiers du micrologiciel du lecteur ont un nom de fichier similaire à `D_HUC101212CSS600_30602291_MS01_2800_0002.dlp`.

Vous pouvez sélectionner jusqu'à quatre fichiers de micrologiciel de lecteur, un par un. Si plusieurs fichiers de micrologiciel de lecteur sont compatibles avec le même lecteur, vous obtenez une erreur de conflit de fichier. Choisissez le fichier de micrologiciel de lecteur que vous souhaitez utiliser pour la mise à niveau et supprimez l'autre.

c. Sélectionnez **Suivant**.

Sélectionner les lecteurs répertorie les lecteurs que vous pouvez mettre à niveau avec les fichiers de micrologiciel sélectionnés.

Seuls les lecteurs compatibles apparaissent.

Le micrologiciel sélectionné pour le lecteur apparaît dans la colonne **micrologiciel proposé**. Si vous devez modifier ce micrologiciel, sélectionnez **Retour**.

d. Sélectionnez **mettre à niveau tous les lecteurs hors ligne (parallèle)** — met à niveau les lecteurs qui peuvent prendre en charge un téléchargement de micrologiciel uniquement lorsque toutes les activités d'E/S sont arrêtées sur tous les volumes qui utilisent les lecteurs.

Vous devez mettre l'appareil en mode maintenance avant d'utiliser cette méthode. Vous devez utiliser la méthode **Offline** pour mettre à niveau le micrologiciel du lecteur.

> Si vous souhaitez utiliser la mise à niveau hors ligne (parallèle), ne continuez pas, sauf si vous êtes certain que l'appliance est en mode de maintenance. Si vous ne mettez pas l'appliance en mode de maintenance avant d'effectuer une mise à jour hors ligne du firmware des disques, vous risquez de perdre des données.

e. Dans la première colonne du tableau, sélectionnez le ou les lecteurs que vous souhaitez mettre à niveau.

   La meilleure pratique consiste à mettre à niveau tous les lecteurs du même modèle vers la même révision du micrologiciel.

f. Sélectionnez **Démarrer** et confirmez que vous souhaitez effectuer la mise à niveau.

   Si vous devez arrêter la mise à niveau, sélectionnez **Stop**. Tous les téléchargements de micrologiciel en cours sont terminés. Tous les téléchargements de micrologiciel qui n'ont pas démarré sont annulés.

   > L'arrêt de la mise à niveau du micrologiciel du lecteur peut entraîner une perte de données ou l'indisponibilité des disques.

g. (Facultatif) pour afficher la liste des mises à niveau, sélectionnez **Enregistrer le journal**.

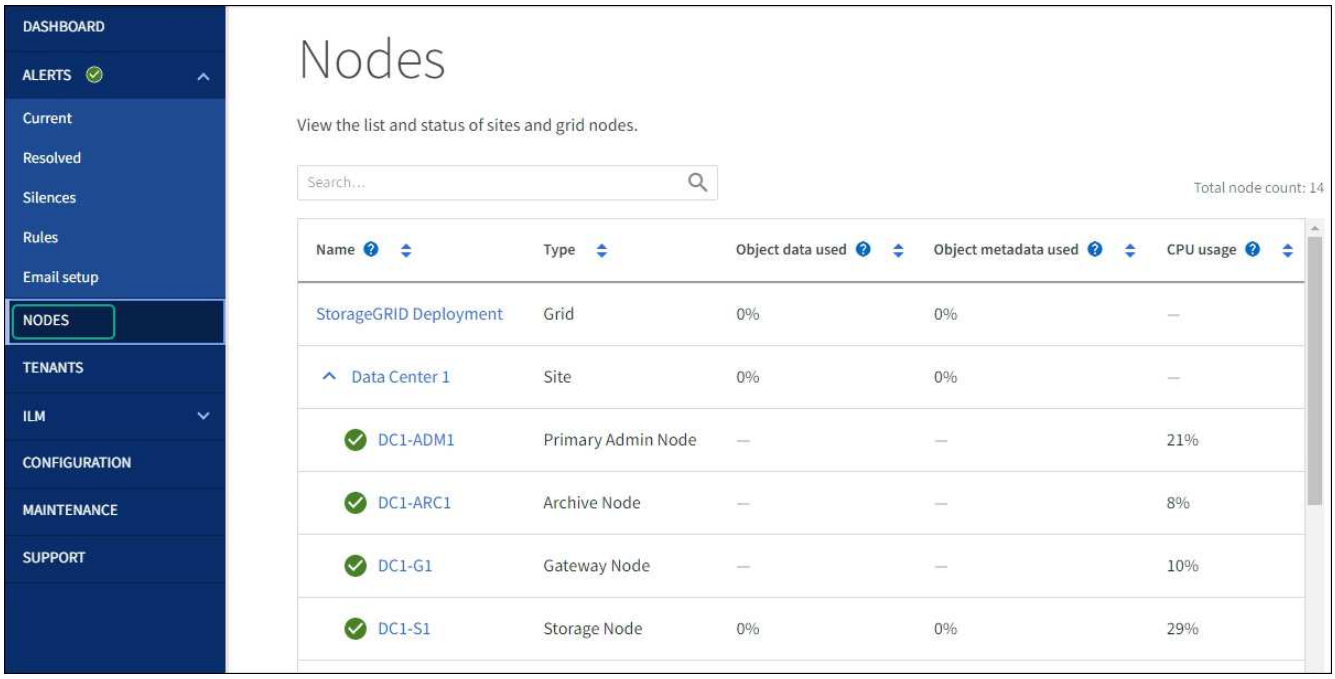
   Le fichier journal est enregistré dans le dossier des téléchargements de votre navigateur portant le nom `latest-upgrade-log-timestamp.txt`.

"Si nécessaire, dépannez les erreurs de mise à niveau du micrologiciel du pilote".

7. Une fois la procédure terminée, effectuez les éventuelles procédures de maintenance supplémentaires lorsque le nœud est en mode maintenance. Lorsque vous avez terminé, ou si vous avez rencontré des défaillances et que vous souhaitez recommencer, accédez au programme d'installation de l'appliance StorageGRID et sélectionnez **Avancé** > **redémarrer le contrôleur**. Sélectionnez ensuite l'une des options suivantes :

   - **Redémarrer dans StorageGRID**.
   - **Redémarrer en mode Maintenance**. Redémarrez le contrôleur et laissez le nœud en mode de maintenance. Sélectionnez cette option si des échecs se sont produits au cours de la procédure et que vous souhaitez recommencer. Une fois le redémarrage du nœud en mode maintenance terminé, redémarrez à partir de l'étape appropriée de la procédure ayant échoué.

     L'appliance peut redémarrer et rejoindre la grille en 20 minutes. Pour confirmer que le redémarrage est terminé et que le nœud a rejoint la grille, retournez à la grille Manager. La page nœuds doit afficher un état normal (icône en forme de coche verte) à gauche du nom du nœud) pour le nœud de l'appliance, indiquant qu'aucune alerte n'est active et que le nœud est connecté à la grille.



Dépannez les erreurs de mise à niveau du firmware des disques

Résolvez les erreurs qui peuvent se produire lorsque vous utilisez SANtricity System Manager pour mettre à niveau le firmware des disques de votre appliance.

- **Disques affectés en échec**
  - L'une des raisons de la défaillance est que le lecteur ne possède pas la signature appropriée. Assurez-vous que le disque concerné est un disque autorisé. Contactez le support technique pour plus d'informations.
  - Lorsque vous remplacez un lecteur, assurez-vous que sa capacité est supérieure ou égale à celle du lecteur défectueux que vous remplacez.
  - Vous pouvez remplacer le disque défectueux alors que la matrice de stockage reçoit des E/S.
- **Vérifier la matrice de stockage**
  - Assurez-vous qu'une adresse IP a été attribuée à chaque contrôleur.
  - Assurez-vous que tous les câbles connectés au contrôleur ne sont pas endommagés.
  - Assurez-vous que tous les câbles sont bien connectés.
- **Disques de secours intégrés**

  Ce problème d'erreur doit être corrigé avant de pouvoir mettre à niveau le micrologiciel.
- **Groupes de volumes incomplets**

  Si un ou plusieurs groupes de volumes ou pools de disques sont incomplets, vous devez corriger cette condition d'erreur avant de pouvoir mettre à niveau le micrologiciel.
- **Opérations exclusives (autres que l'analyse des supports/parité en arrière-plan) actuellement en cours d'exécution sur n'importe quel groupe de volumes**

  Si une ou plusieurs opérations exclusives sont en cours, les opérations doivent être effectuées avant la mise à niveau du micrologiciel. Utilisez System Manager pour surveiller la progression des opérations.

- **Volumes manquants**

  Vous devez corriger la condition de volume manquant avant de pouvoir mettre à niveau le micrologiciel.

- **L'un ou l'autre des contrôleurs dans un état autre que optimal**

  L'un des contrôleurs de la baie de stockage doit faire attention. Ce problème doit être résolu avant la mise à niveau du firmware.

- **Discordance des informations de partition de stockage entre les graphiques d'objet du contrôleur**

  Une erreur s'est produite lors de la validation des données sur les contrôleurs. Contactez le support technique pour résoudre ce problème.

- **Échec de la vérification du contrôleur de base de données SPM**

  Une erreur de mappage de la base de données de mappage des partitions de stockage s'est produite sur un contrôleur. Contactez le support technique pour résoudre ce problème.

- **Validation de la base de données de configuration (si prise en charge par la version du contrôleur de la matrice de stockage)**

  Une erreur de base de données de configuration s'est produite sur un contrôleur. Contactez le support technique pour résoudre ce problème.

- **Vérifications liées au MEL**

  Contactez le support technique pour résoudre ce problème.

- **Plus de 10 événements MEL informationnels ou critiques de la DDE ont été rapportés au cours des 7 derniers jours**

  Contactez le support technique pour résoudre ce problème.

- **Plus de 2 pages 2C des événements MEL critiques ont été rapportés au cours des 7 derniers jours**

  Contactez le support technique pour résoudre ce problème.

- **Plus de 2 événements MEL critiques de canal d'entraînement dégradés ont été signalés au cours des 7 derniers jours**

  Contactez le support technique pour résoudre ce problème.

- **Plus de 4 entrées MEL critiques au cours des 7 derniers jours**

  Contactez le support technique pour résoudre ce problème.

Allumer et éteindre la LED d'identification du contrôleur

Il est possible d'allumer la LED d'identification bleue à l'avant et à l'arrière du contrôleur pour localiser l'appliance dans un data Center.

Avant de commencer

Vous disposez de l'adresse IP du contrôleur BMC que vous souhaitez identifier.

Étapes

1. Accéder à l'interface du contrôleur BMC.
2. Sélectionnez **identification du serveur**.

   L'état actuel de la LED Identify est sélectionné.

3. Sélectionnez **ON** ou **OFF**, puis sélectionnez **Exécuter l'action**.

   Lorsque vous sélectionnez **ACTIVÉ**, les voyants d'identification bleus s'allument à l'avant (illustré) et à l'arrière de l'appareil.

> Si un panneau est installé sur le contrôleur, il peut être difficile de voir le voyant d'identification avant.

4. Allumer et éteindre le voyant selon les besoins.

Informations associées

"Vérifiez que la carte HBA Fibre Channel doit être remplacée"

"Localiser le contrôleur dans le data Center"

"Accéder à l'interface BMC"

Localiser le contrôleur dans le data Center

Identifiez le contrôleur pour effectuer des opérations de maintenance ou de mise à niveau du matériel.

Avant de commencer

- Vous avez déterminé quel contrôleur doit être entretenu.

  (Facultatif) pour localiser le contrôleur dans votre centre de données, activez le voyant d'identification bleu.

  "Allumer et éteindre la LED d'identification du contrôleur"

Étapes

1. Trouver le contrôleur qui nécessite une maintenance dans le data Center.
   - Recherchez une LED d'identification bleue allumée à l'avant ou à l'arrière du contrôleur.

Le voyant d'identification avant se trouve derrière le panneau avant du contrôleur et il peut être difficile de voir si le panneau est installé.

- Vérifiez que les étiquettes fixées à l'avant de chaque contrôleur correspondent à un numéro de pièce.

2. Retirez le cadre avant du contrôleur, le cas échéant, pour accéder aux commandes et aux indicateurs du panneau avant.
3. Facultatif : si vous l'utilisez pour localiser le contrôleur, désactivez le voyant d'identification bleu.
   - Appuyez sur le commutateur LED identifier sur le panneau avant du contrôleur.
   - Utilisez l'interface du contrôleur BMC.

     "Allumer et éteindre la LED d'identification du contrôleur"

Informations associées

"Retirez l'adaptateur HBA Fibre Channel"

"Retirez le contrôleur SG6000-CN de l'armoire ou du rack"

"Arrêtez le contrôleur SG6000-CN"

Met le contrôleur sous et hors tension

Arrêtez le contrôleur SG6000-CN

Arrêtez le contrôleur SG6000-CN pour effectuer la maintenance du matériel.

Avant de commencer

- Vous avez installé physiquement le contrôleur SG6000-CN nécessitant une maintenance dans le centre de données. Voir "Localiser le contrôleur dans le data Center".

Description de la tâche

Pour éviter les interruptions de service, vérifiez que tous les autres nœuds de stockage sont connectés à la grille avant d'arrêter le contrôleur ou d'arrêter le contrôleur durant une fenêtre de maintenance planifiée en cas d'interruption de service. Voir les informations sur "contrôle de l'état de connexion du nœud".

> Si vous avez déjà utilisé une règle ILM pour créer une seule copie d'un objet, vous devez arrêter le contrôleur durant la fenêtre de maintenance planifiée. Sinon, vous risquez de perdre temporairement l'accès à ces objets au cours de cette procédure. + Voir les informations sur la gestion des objets avec la gestion du cycle de vie des informations.

Étapes

1. Arrêtez le contrôleur SG6000-CN.

   Vous devez effectuer un arrêt contrôlé de l'appliance en entrant les commandes indiquées ci-dessous. Il est recommandé d'effectuer un arrêt contrôlé lorsque cela est possible pour éviter les alertes inutiles, vérifier que les journaux complets sont disponibles et éviter toute interruption de service.

   a. Si vous n'avez pas encore ouvert de session sur le nœud grid, connectez-vous à l'aide de PuTTY ou d'un autre client ssh :

      i. Saisissez la commande suivante : `ssh admin@grid_node_IP`

      ii. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

      iii. Entrez la commande suivante pour passer à la racine : `su -`

      iv. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

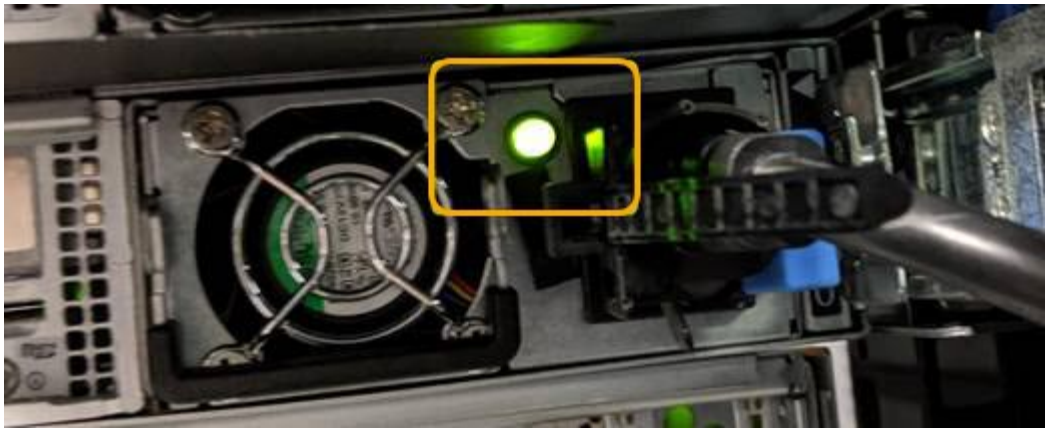
      Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

   b. Arrêtez le contrôleur SG6000-CN :
   `shutdown -h now`

   Cette commande peut prendre jusqu'à 10 minutes.

2. Utilisez l'une des méthodes suivantes pour vérifier que le contrôleur SG6000-CN est hors tension :
   - Observer la LED bleue d'alimentation à l'avant du contrôleur et vérifier qu'elle est éteinte.

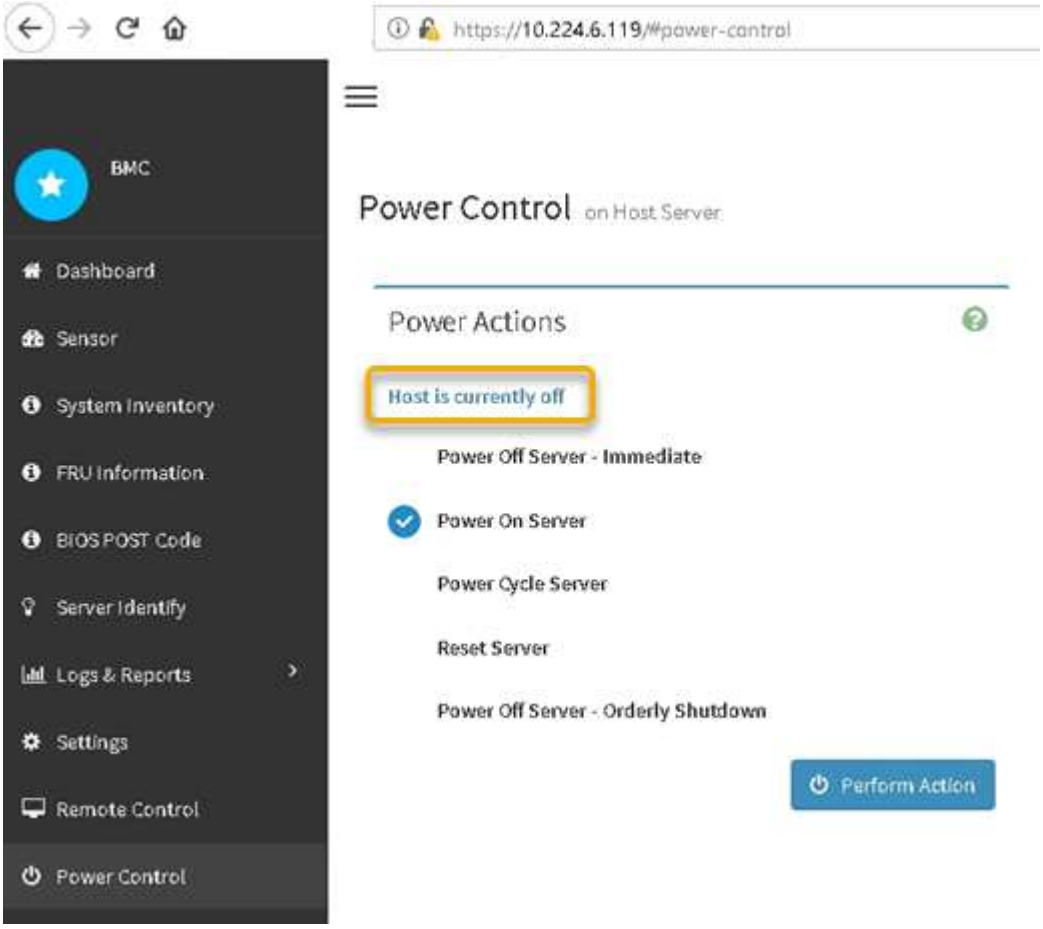
   - Observez les LED vertes des deux blocs d'alimentation à l'arrière du contrôleur et vérifiez qu'ils clignotent à une fréquence régulière (environ un clignotement par seconde).



- Utilisez l’interface du contrôleur BMC :
  i. Accéder à l’interface du contrôleur BMC.

     "Accéder à l’interface BMC"

  ii. Sélectionnez **Power Control**.
  iii. Vérifiez que les actions d’alimentation indiquent que l’hôte est actuellement éteint.



Informations associées

"Retirez le contrôleur SG6000-CN de l’armoire ou du rack"

Mettez le contrôleur sous tension après la fin de la maintenance.

Avant de commencer

- Vous avez installé le contrôleur dans une armoire ou un rack et connecté les câbles de données et d'alimentation.

  "Réinstallez le contrôleur SG6000-CN dans l'armoire ou le rack"

- Vous avez physiquement situé le contrôleur dans le data Center.

  "Localiser le contrôleur dans le data Center"

Étapes

1. Mettez le contrôleur SG6000-CN sous tension et surveillez les voyants du contrôleur et les codes de démarrage à l'aide de l'une des méthodes suivantes :

   - Appuyer sur le bouton de mise sous tension situé à l'avant du contrôleur.

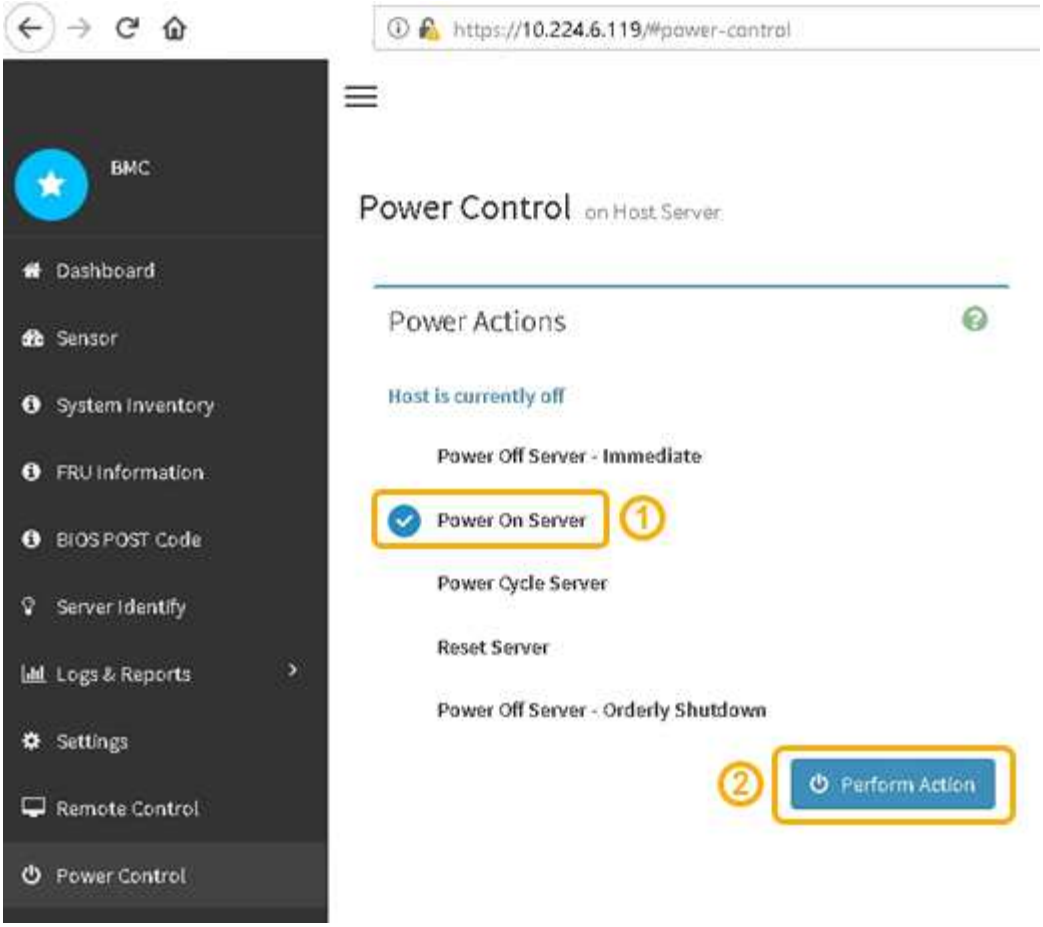
   - Utilisez l'interface du contrôleur BMC :

     i. Accéder à l'interface du contrôleur BMC.

        "Accéder à l'interface BMC"

     ii. Sélectionnez **Power Control**.

     iii. Sélectionnez **Power On Server**, puis **Perform action**.



Utilisez l'interface BMC pour surveiller l'état de démarrage.

2. Vérifiez que le contrôleur de l'appliance s'affiche dans Grid Manager et sans alertes.

   L'affichage du contrôleur dans Grid Manager peut prendre jusqu'à 20 minutes.

3. Vérifier que le nouveau contrôleur SG6000-CN est entièrement opérationnel :

   a. Connectez-vous au nœud de la grille à l'aide de PuTTY ou d'un autre client ssh :

      i. Saisissez la commande suivante : `ssh admin@grid_node_IP`

      ii. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

      iii. Entrez la commande suivante pour passer à la racine : `su -`

      iv. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

      Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

   b. Entrez la commande suivante et vérifiez qu'elle renvoie la sortie attendue : `cat /sys/class/fc_host/*/port_state`

      Sortie attendue :

```
Online
Online
Online
Online
```

Si le résultat attendu n'est pas renvoyé, contactez le support technique.

c. Entrez la commande suivante et vérifiez qu'elle renvoie la sortie attendue :
`cat /sys/class/fc_host/*/speed`

Sortie attendue :

```
16 Gbit
16 Gbit
16 Gbit
16 Gbit
```

+
Si le résultat attendu n'est pas renvoyé, contactez le support technique.

a. Dans la page nœuds de Grid Manager, assurez-vous que le nœud d'appliance est connecté à la grille et qu'il n'y a aucune alerte.

> Ne mettez pas un autre nœud d'appliance hors ligne sauf si cette appliance présente une icône verte.

4. Facultatif : installez le cadre avant, si l'un d'eux a été retiré.

Informations associées

"Afficher les indicateurs d'état"

Modifier la configuration de la liaison du contrôleur SG6000-CN

Vous pouvez modifier la configuration de la liaison Ethernet du contrôleur SG6000-CN. Vous pouvez modifier le mode de liaison du port, le mode de liaison réseau et la vitesse de liaison.

Avant de commencer

L'appareil a été "passage en mode maintenance".

Description de la tâche

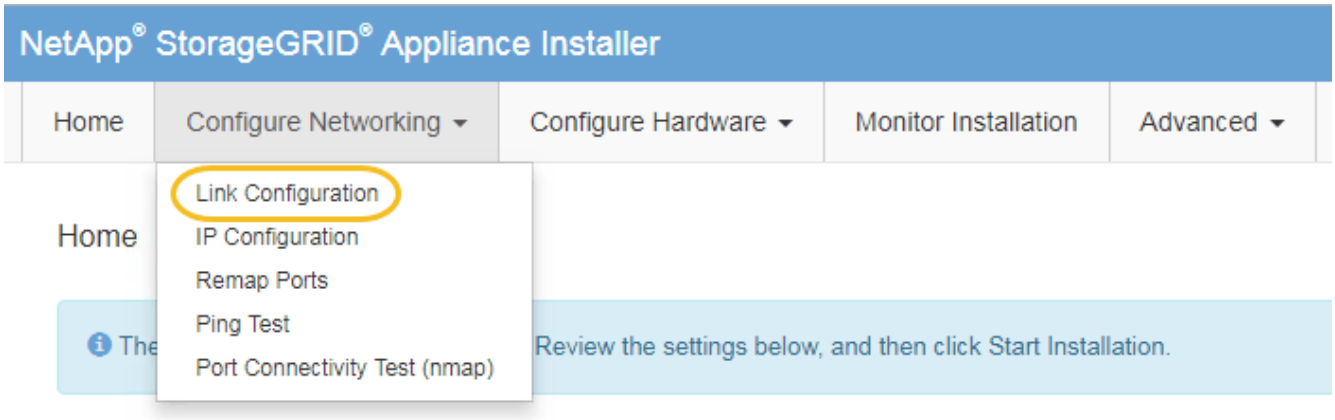
Les options permettant de modifier la configuration de la liaison Ethernet du contrôleur SG6000-CN sont les suivantes :

- Changement du mode **Port bond** de fixe à agrégé, ou d'agrégat à fixe
- Passage du mode de liaison réseau * d'Active-Backup à LACP, ou de LACP à Active-Backup
- Activation ou désactivation du balisage VLAN ou modification de la valeur d'une balise VLAN

- Modification de la vitesse de liaison.

Étapes

1. Dans le programme d'installation de l'appliance StorageGRID, sélectionnez **configurer réseau** > **Configuration lien**.



2. apportez les modifications souhaitées à la configuration de liaison.

   Pour plus d'informations sur les options, reportez-vous à la section "Configurer les liaisons réseau".

3. Lorsque vous êtes satisfait de vos sélections, cliquez sur **Enregistrer**.

   > Vous risquez de perdre votre connexion si vous avez apporté des modifications au réseau ou au lien auquel vous êtes connecté. Si vous n'êtes pas reconnecté dans un délai d'une minute, saisissez à nouveau l'URL du programme d'installation de l'appliance StorageGRID à l'aide de l'une des autres adresses IP attribuées à l'appliance : **`https://Appliance_Controller_IP:8443`**

   Si vous avez modifié les paramètres VLAN, le sous-réseau de l'appliance a peut-être changé. Si vous devez modifier les adresses IP de l'appareil, suivez la "Configurez les adresses IP" instructions.

   "Configurez les adresses IP StorageGRID"

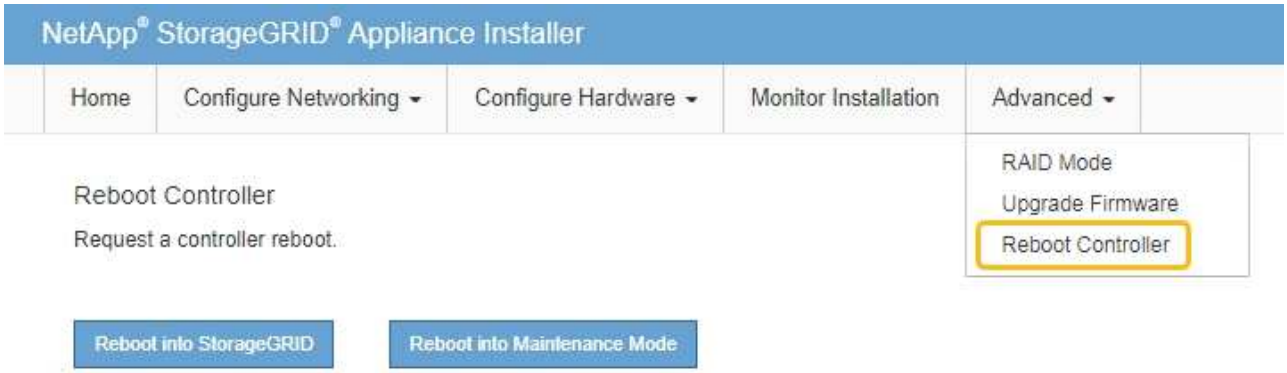
4. Sélectionnez **configurer réseau** > **Test Ping** dans le menu.
5. Utilisez l'outil Test Ping pour vérifier la connectivité aux adresses IP sur tous les réseaux susceptibles d'avoir été affectés par les modifications de configuration de liaison que vous avez effectuées dans modification de la configuration des liens étape.

   En plus des autres tests que vous choisissez d'effectuer, vérifiez que vous pouvez envoyer une requête ping à l'adresse IP du réseau de la grille du nœud d'administration principal et à l'adresse IP du réseau de la grille d'au moins un autre nœud de stockage. Si nécessaire, retourner à l' modification de la configuration des liens corrigez tout problème de configuration de lien.

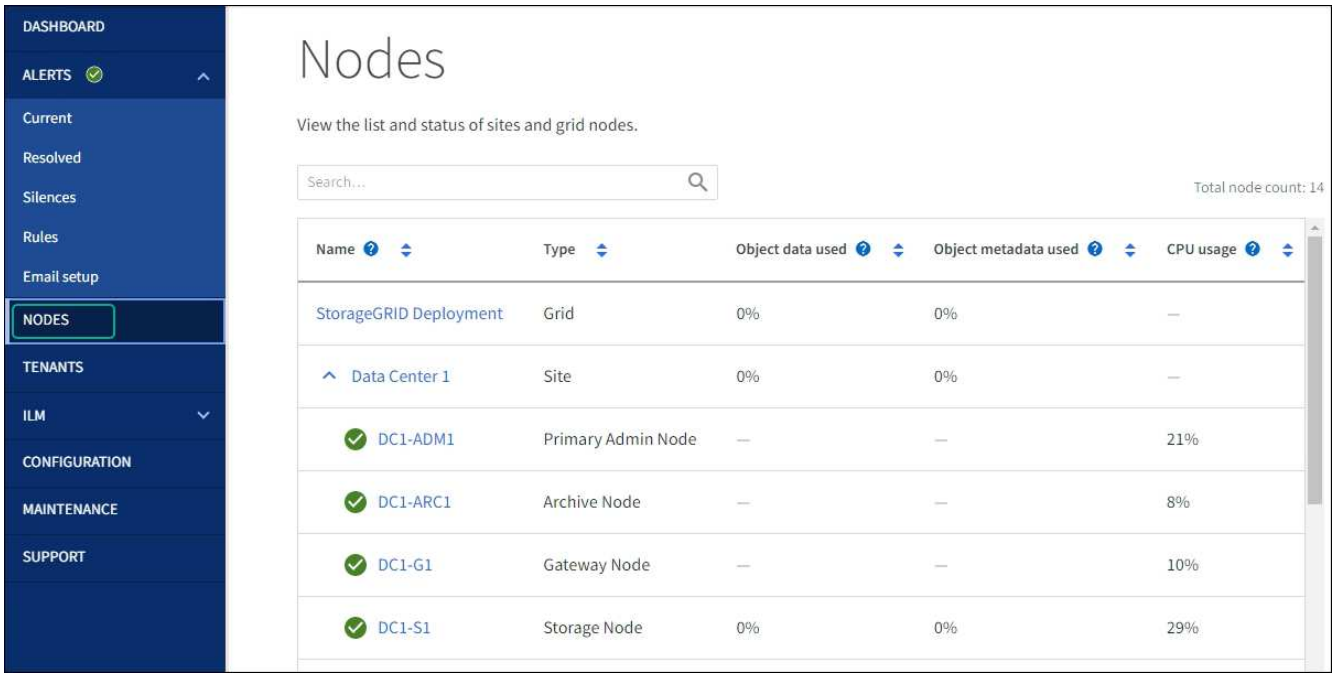
6. Lorsque vous êtes satisfait du fait que vos modifications de configuration de liaison fonctionnent et que vous disposez de procédures supplémentaires à effectuer lorsque le nœud est en mode maintenance, effectuez-les maintenant. Lorsque vous avez terminé, ou si vous avez rencontré des échecs et souhaitez recommencer, sélectionnez **Avancé** > **redémarrer le contrôleur**, puis sélectionnez l'une des options suivantes :

   - Sélectionnez **redémarrer dans StorageGRID**

◦ Sélectionnez **redémarrer en mode maintenance** pour redémarrer le contrôleur avec le nœud restant en mode de maintenance. Sélectionnez cette option si vous avez rencontré des échecs au cours de la procédure et souhaitez recommencer. Une fois le redémarrage du nœud en mode maintenance terminé, redémarrez à partir de l'étape appropriée de la procédure ayant échoué.



L'appliance peut redémarrer et rejoindre la grille en 20 minutes. Pour confirmer que le redémarrage est terminé et que le nœud a rejoint la grille, retournez à la grille Manager. La page **NODES** doit afficher un état normal (icône de coche verte à gauche du nom du nœud) pour le nœud de l'appliance, indiquant qu'aucune alerte n'est active et que le nœud est connecté à la grille.



Procédures matérielles

Ajoutez un tiroir d'extension à SG6060 déployé

Pour augmenter la capacité de stockage, vous pouvez ajouter une ou deux tiroirs d'extension à une SG6060 déjà déployée dans un système StorageGRID.

Avant de commencer

- Vous devez disposer de la phrase secrète pour le provisionnement.
- Vous devez exécuter StorageGRID 11.4 ou version ultérieure.
- Le tiroir d'extension et deux câbles SAS pour chaque tiroir d'extension sont disponibles.
- Vous avez trouvé l'appliance de stockage où vous ajoutez le tiroir d'extension dans le data Center.

  "Localiser le contrôleur dans le data Center"

Description de la tâche

Pour ajouter un tiroir d'extension, procédez comme suit :

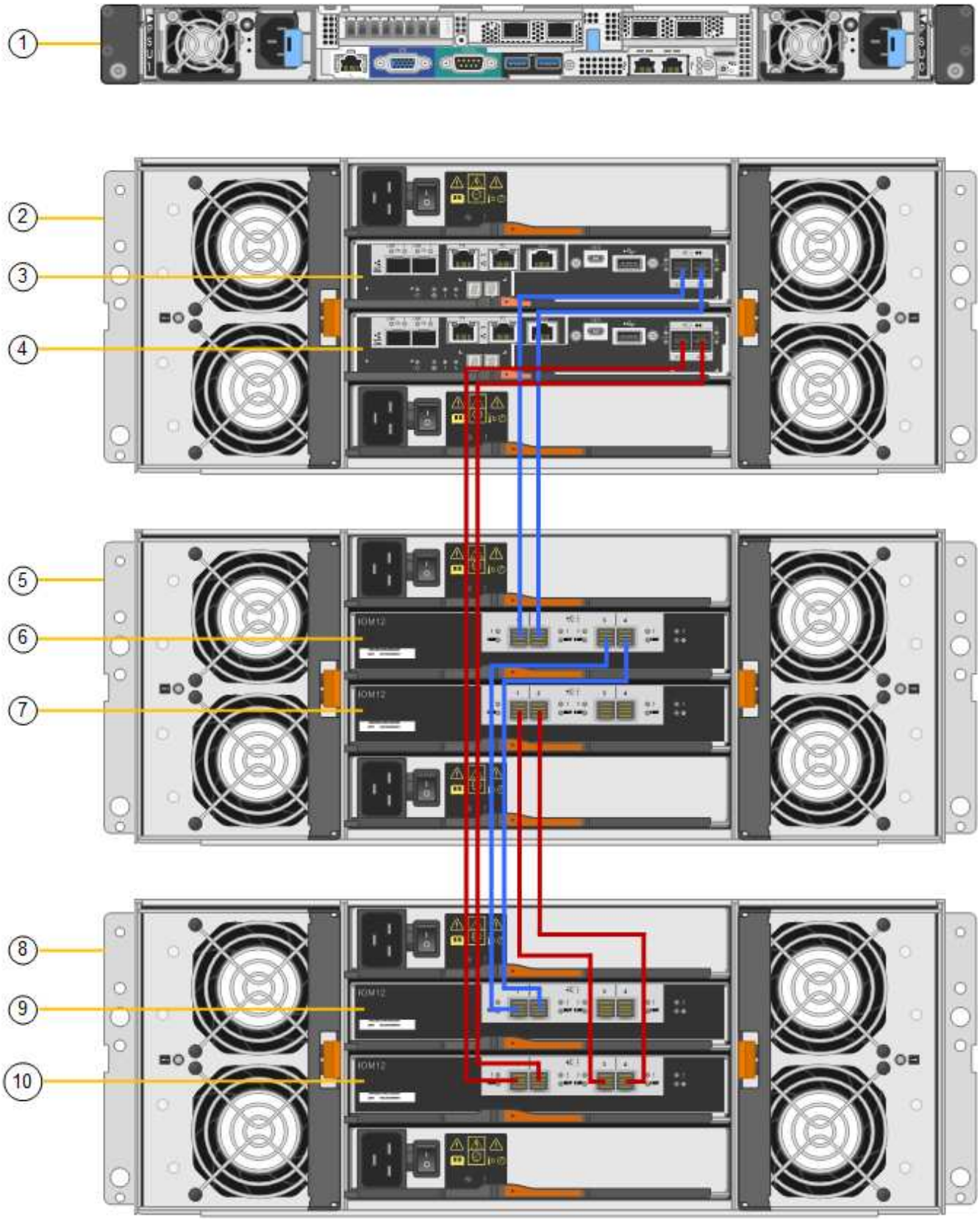
- Installez le matériel dans l'armoire ou le rack.
- Mettez le SG6060 en mode de maintenance.
- Connectez le tiroir d'extension au tiroir contrôleur E2860 ou à un autre tiroir d'extension.
- Démarrez l'extension à l'aide du programme d'installation de l'appliance StorageGRID
- Attendez que les nouveaux volumes soient configurés.

En procédant à une ou deux tiroirs d'extension, chaque nœud d'appliance doit prendre moins d'une heure. Pour réduire les temps d'indisponibilité, procédez comme suit afin d'installer les nouveaux tiroirs et disques d'extension avant de placer le SG6060 en mode de maintenance. La durée restante de la procédure doit être d'environ 20 à 30 minutes par nœud d'appliance.

Étapes

1. Suivez les instructions de la section "installation des tiroirs de 60 disques dans une armoire ou un rack".
2. Suivez les instructions de la section "installation des lecteurs".
3. Dans Grid Manager, "Placez le contrôleur SG6000-CN en mode maintenance".
4. Connectez chaque tiroir d'extension au tiroir contrôleur E2860, comme indiqué sur le schéma.

   Cette mise en plan montre deux tiroirs d'extension. Si vous n'en avez qu'un, connectez l'E/S A au contrôleur A et connectez l'E/S B au contrôleur B.



Légende	Description
1	SG6000-CN

Légende	Description
2	Tiroir contrôleur E2860
3	Contrôleur A
4	Contrôleur B
5	Tiroir d’extension 1
6	Module d’E/S A pour le tiroir d’extension 1
7	Module d’E/S B pour le tiroir d’extension 1
8	Tiroir d’extension 2
9	Module d’E/S A pour le tiroir d’extension 2
10	Module d’E/S B pour le tiroir d’extension 2

5. Branchez les câbles d’alimentation et mettez les tiroirs d’extension sous tension.
   a. Connectez un cordon d’alimentation à chacune des deux unités d’alimentation de chaque shelf d’extension.
   b. Connectez les deux cordons d’alimentation de chaque tiroir d’extension à deux PDU différentes dans l’armoire ou le rack.
   c. Allumer les deux boutons d’alimentation pour chaque tiroir d’extension.
      - N’éteignez pas les interrupteurs d’alimentation pendant le processus de mise sous tension.
      - Les ventilateurs des tiroirs d’extension peuvent être très bruyants lors du premier démarrage. Le bruit est normal au démarrage.
6. Surveillez la page d’accueil du programme d’installation de l’appliance StorageGRID.

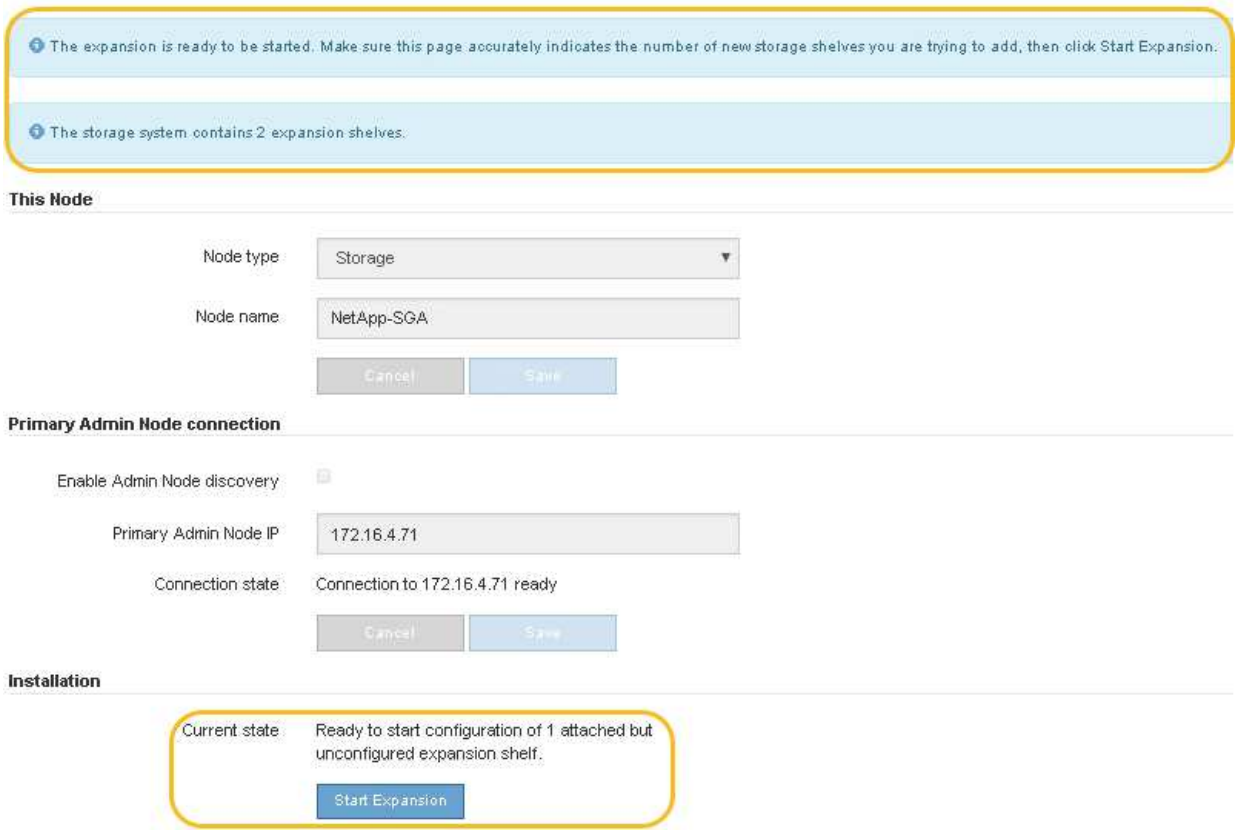
   En cinq minutes environ, les tiroirs d’extension sont mis sous tension et détectés par le système. La page d’accueil indique le nombre de nouveaux tiroirs d’extension détectés et le bouton Démarrer l’extension est activé.

   La capture d’écran présente des exemples de messages qui peuvent apparaître sur la page d’accueil, selon le nombre de tiroirs d’extension existants ou nouveaux, comme suit :

   - La bannière entourée en haut de la page indique le nombre total de étagères d’extension détectées.
     - La bannière indique le nombre total de tiroirs d’extension, que ceux-ci soient configurés et déployés ou nouveaux et non configurés.
     - Si aucun tiroir d’extension n’est détecté, la bannière n’apparaît pas.
   - Le message encerclé en bas de la page indique qu’une extension est prête à être démarrée.
     - Ce message indique le nombre de nouveaux tiroirs d’extension détectés par StorageGRID. « Connecté » indique que la tablette est détectée. « Non configuré » indique que le tiroir est nouveau et qu’il n’est pas encore configuré à l’aide du programme d’installation de l’appliance StorageGRID.

Les tiroirs d'extension déjà déployés ne sont pas inclus dans ce message. Ils sont inclus dans le compte dans la bannière en haut de la page.

- Le message ne s'affiche pas si de nouveaux tiroirs d'extension ne sont pas détectés.



7. Si nécessaire, résolvez les problèmes décrits dans les messages de la page d'accueil.

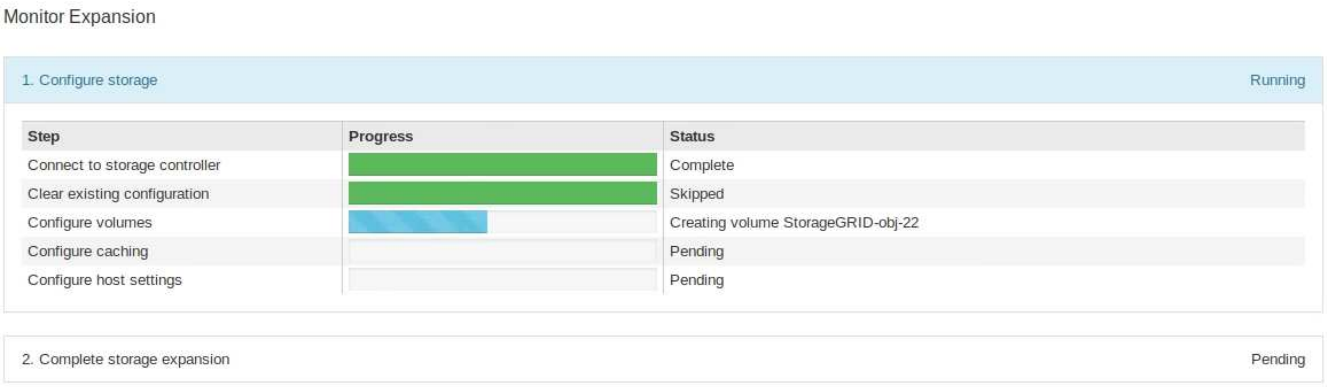
   Utilisez SANtricity System Manager, par exemple, pour résoudre les problèmes matériels de stockage.

8. Vérifiez que le nombre de tiroirs d'extension affichés sur la page d'accueil correspond au nombre de tiroirs d'extension que vous ajoutez.

   Si les nouveaux tiroirs d'extension n'ont pas été détectés, vérifiez qu'ils sont correctement câblés et mis sous tension.

9. cliquez sur **Start expansion** pour configurer les tiroirs d'extension et les rendre disponibles pour le stockage d'objets.
10. Surveiller la progression de la configuration du tiroir d'extension.

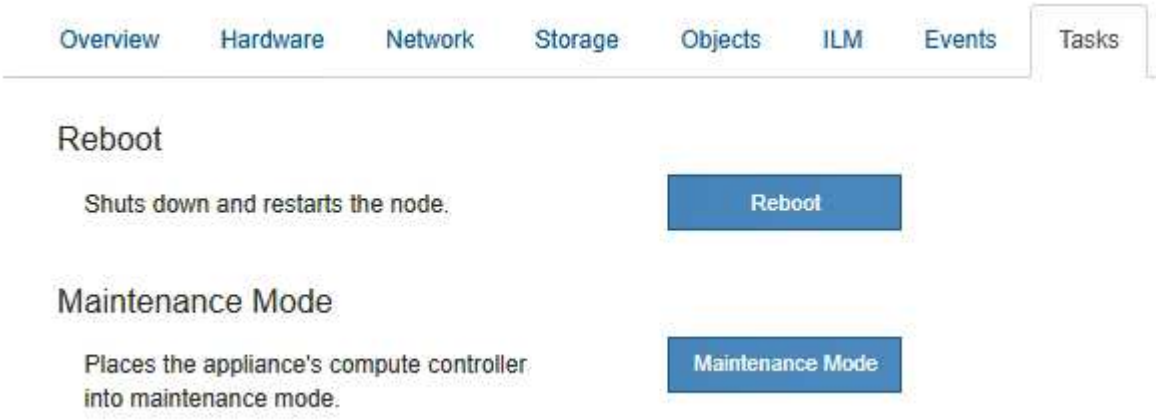
    Des barres de progression apparaissent sur la page Web, comme elles le font lors de l'installation initiale.



Une fois la configuration terminée, l'appliance redémarre automatiquement pour quitter le mode de maintenance et rejoindre à nouveau la grille. Ce processus peut prendre jusqu'à 20 minutes.

> Pour relancer la configuration du tiroir d'extension en cas d'échec, accédez au programme d'installation de l'appliance StorageGRID, sélectionnez **Avancé** > **redémarrer le contrôleur**, puis sélectionnez **redémarrer en mode de maintenance**. Une fois le nœud redémarré, réessayez dans configuration des tiroirs d'extension.

Une fois le redémarrage terminé, l'onglet **tâches** ressemble à la capture d'écran suivante :



11. Vérifiez l'état du nœud de stockage de l'appliance et des nouveaux tiroirs d'extension.
    a. Dans le Gestionnaire de grille, sélectionnez **NODES** et vérifiez que le noeud de stockage de l'appliance possède une icône de coche verte.

       L'icône de coche verte signifie qu'aucune alerte n'est active et que le nœud est connecté à la grille. Pour une description des icônes de nœuds, reportez-vous à la section "Surveiller les États de connexion du nœud".

    b. Sélectionnez l'onglet **stockage** et vérifiez que 16 nouveaux magasins d'objets sont affichés dans la table stockage d'objets pour chaque étagère d'extension ajoutée.
    c. Vérifier que chaque nouveau tiroir d'extension dispose d'un état de tiroir nominal et d'un état de configuration configuré.

Remplacez le contrôleur de stockage dans le SG6000

Vous devrez peut-être remplacer un contrôleur E2800 Series ou un contrôleur EF570 si

ce dernier ne fonctionne pas de manière optimale ou en cas de défaillance.

Avant de commencer

- Vous disposez d'un contrôleur de remplacement avec la même référence que le contrôleur que vous remplacez.
- Vous avez des étiquettes pour identifier chaque câble connecté au contrôleur.
- Vous avez un bracelet ESD, ou vous avez pris d'autres précautions antistatiques.
- Vous avez un tournevis cruciforme n° 1.
- Vous avez trouvé physiquement l'appliance de stockage où vous remplacez le contrôleur dans le data Center.

  "Localiser le contrôleur dans le data Center"

> Ne vous fiez pas aux instructions E-Series pour remplacer un contrôleur de l'appliance StorageGRID, car les procédures ne sont pas identiques.

Description de la tâche

Vous pouvez déterminer si vous avez un contrôleur défectueux de deux manières :

- Il vous est alors dirigé vers le remplacement du contrôleur dans SANtricity System Manager.
- La LED d'avertissement orange située sur le contrôleur est allumée, ce qui indique que le contrôleur est en panne.

> Si les deux contrôleurs du tiroir disposent de leurs LED d'avertissement, contactez le support technique pour obtenir de l'aide.

Si votre appliance contient deux contrôleurs de stockage, vous pouvez remplacer l'un des contrôleurs lorsque votre appliance est sous tension et effectuer des opérations de lecture/écriture, tant que les conditions suivantes sont réunies :

- Le second contrôleur du tiroir est à l'état optimal.
- Le champ **OK à supprimer** de la zone Détails du gourou de la restauration dans le Gestionnaire de système SANtricity affiche **Oui**, indiquant qu'il est sûr de supprimer ce composant.

> Si possible, placez l'appareil en mode de maintenance pour cette procédure de remplacement afin de minimiser l'impact potentiel d'erreurs ou de défaillances imprévues.

> Si le second contrôleur du tiroir n'a pas l'état optimal ou si le gourou de la restauration indique qu'il n'est pas OK pour retirer le contrôleur, contactez le support technique.

Lorsque vous remplacez un contrôleur, vous devez retirer la batterie du contrôleur d'origine et l'installer dans le contrôleur de remplacement. Dans certains cas, vous devrez également retirer la carte d'interface hôte du contrôleur d'origine et l'installer dans le contrôleur de remplacement.

> Dans la plupart des modèles d'appliance, les contrôleurs de stockage n'incluent pas de cartes d'interface hôte (HIC).

Étape 1 : préparer le contrôleur de remplacement

Préparez le contrôleur E2800A ou E2800B de rechange.

Étapes

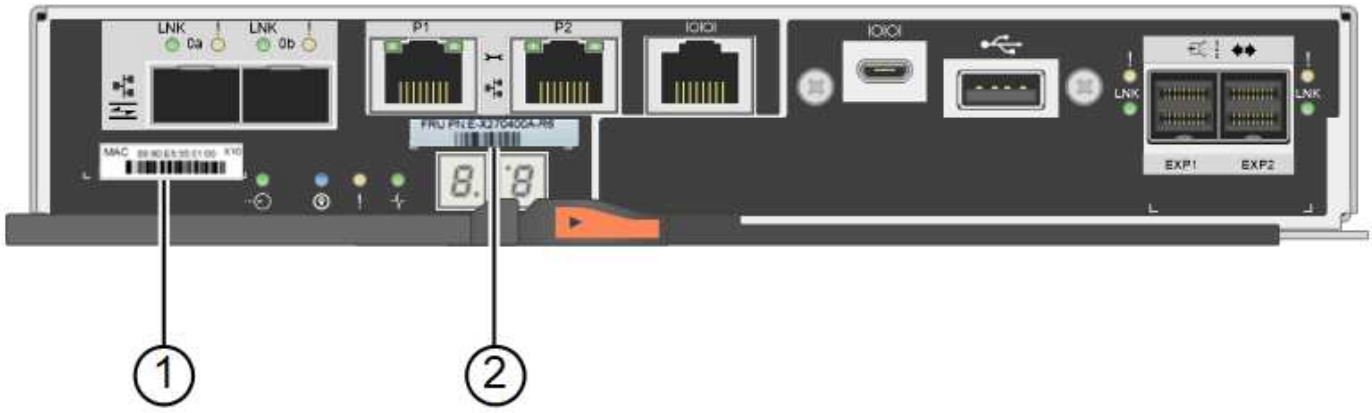
1. Déballez le nouveau contrôleur et placez-le sur une surface plane et sans électricité statique.

   Conservez les matériaux d'emballage à utiliser lors de l'expédition du contrôleur défectueux.

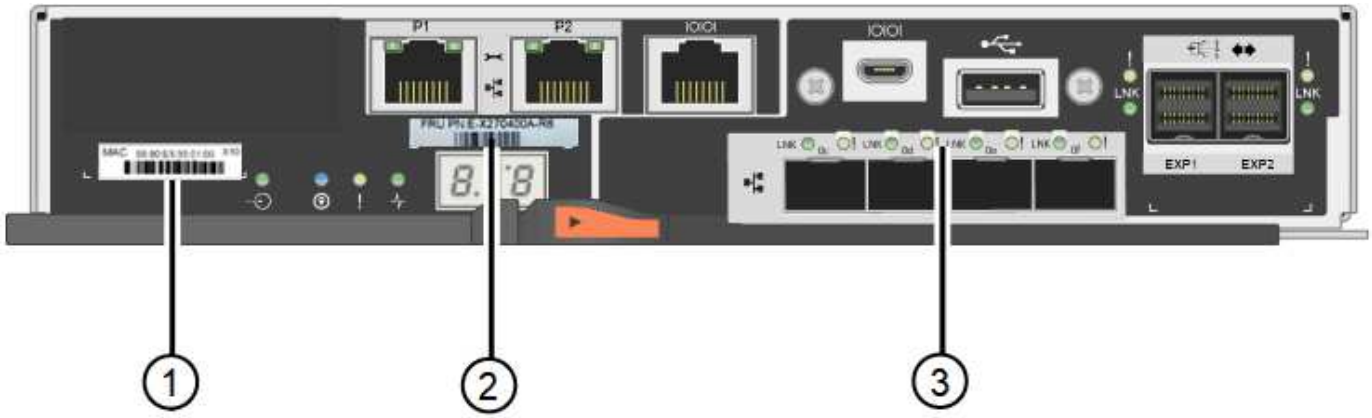
2. Localisez les étiquettes d'adresse MAC et de référence des FRU à l'arrière du contrôleur de remplacement.

Ces figures illustrent le contrôleur E2800A et le contrôleur E2800B. La procédure de remplacement des contrôleurs E2800 Series et du contrôleur EF570 est identique.

Contrôleur de stockage E2800A :



Contrôleur de stockage E2800B :



Étiquette	composant	Description
1	Adresse MAC	L'adresse MAC du port de gestion 1 (« P1 sur le E2800A et 0a sur le E2800B »). Si vous avez utilisé DHCP pour obtenir l'adresse IP du contrôleur d'origine, vous devez disposer de cette adresse pour vous connecter au nouveau contrôleur.

Étiquette	composant	Description
2	Référence de l'unité remplaçable sur site	Numéro de référence de l'unité remplaçable sur site. Ce numéro doit correspondre au numéro de référence de remplacement du contrôleur actuellement installé.
3	HIC 4 ports	La carte d'interface hôte 4 ports (HIC). Cette carte doit être déplacée vers le nouveau contrôleur lors du remplacement. **Remarque** : le contrôleur E2800A n'a pas de HIC.

Ste 2 : mettre le contrôleur hors ligne

Vous préparer à retirer le contrôleur défectueux et à le mettre hors ligne.

Étapes

1. Préparez-vous à retirer le contrôleur. Ces étapes sont réalisées à l'aide de SANtricity System Manager.

   a. Vérifiez que le numéro de référence de la référence de remplacement du contrôleur défectueux est identique à celui de la référence de l'unité remplaçable sur site du contrôleur de remplacement.

      Lorsqu'un contrôleur présente une défaillance et doit être remplacé, la référence du remplacement est affichée dans la zone Détails du Recovery Guru. Si vous avez besoin de trouver ce numéro manuellement, vous pouvez consulter l'onglet **base** du contrôleur.

      Perte possible de l'accès aux données et#8212; si les deux numéros de pièce ne sont pas les mêmes, ne pas tenter cette procédure.

   a. Sauvegardez la base de données de configuration.

      Si un problème survient lorsque vous supprimez un contrôleur, vous pouvez utiliser le fichier enregistré pour restaurer votre configuration.

   b. Collecte des données d'assistance pour l'appareil.

      La collecte des données de support avant et après le remplacement d'un composant vous permet d'envoyer un ensemble complet de journaux au support technique si le remplacement ne résout pas le problème.

   c. Mettre le contrôleur que vous prévoyez de remplacer hors ligne.

2. Met le tiroir contrôleur hors tension.

Étape 3 : retirez le contrôleur

Retirez le contrôleur de l'appareil.

Étapes

1. Placez un bracelet antistatique ou prenez d'autres précautions antistatiques.
2. Etiqueter les câbles puis débrancher les câbles et les SFP.

Pour éviter toute dégradation des performances, ne tordez pas, ne pliez pas, ne pincez pas ou ne montez pas sur les câbles.

3. Libérez le contrôleur de l'appareil en appuyant sur le loquet de la poignée de came jusqu'à ce qu'il se relâche, puis ouvrez la poignée de came vers la droite.
4. A l'aide de deux mains et de la poignée de came, faites glisser le contrôleur hors de l'appareil.

Toujours utiliser deux mains pour soutenir le poids du contrôleur.

5. Placez le contrôleur sur une surface plane et sans électricité statique, le capot amovible orienté vers le haut.
6. Retirez le capot en appuyant sur le bouton et en le faisant glisser hors du capot.

Étape 4 : déplacer la batterie vers le nouveau contrôleur

Retirez la batterie du contrôleur défectueux et installez-la dans le contrôleur de remplacement.

Étapes

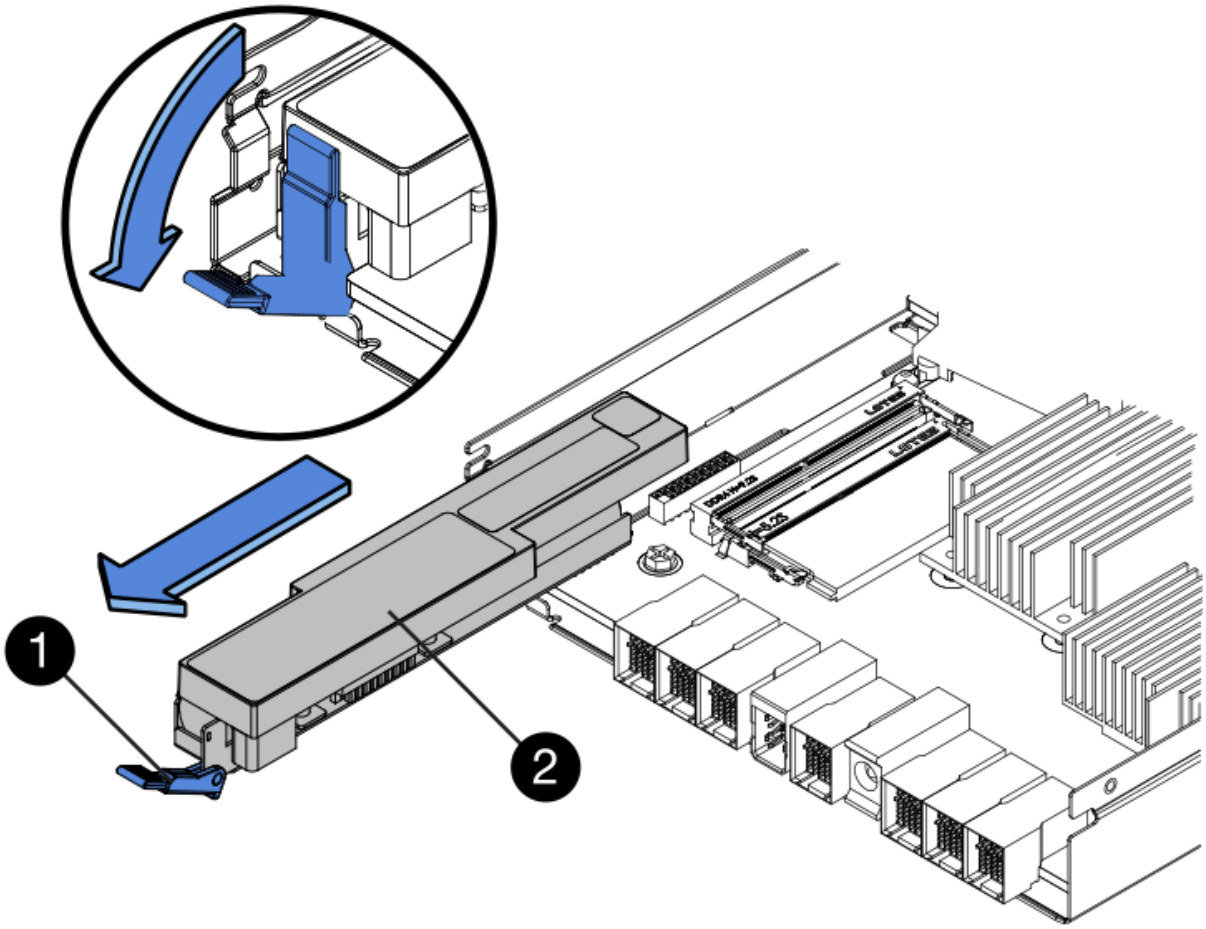
1. Vérifiez que le voyant vert à l'intérieur du contrôleur (entre la batterie et les modules DIMM) est éteint.

   Si ce voyant vert est allumé, le contrôleur utilise toujours l'alimentation de la batterie. Vous devez attendre que ce voyant s'éteigne avant de retirer des composants.

Élément	Description
1	LED active du cache interne

Élément	Description
2	Batterie

2. Repérez le loquet de dégagement bleu de la batterie.
3. Déverrouillez la batterie en appuyant sur le loquet de déverrouillage vers le bas et en l'éloignant du contrôleur.



Élément	Description
1	Loquet de déblocage de la batterie
2	Batterie

4. Soulevez la batterie et faites-la glisser hors du contrôleur.
5. Retirer le capot du contrôleur de remplacement.
6. Orientez le contrôleur de remplacement de manière à ce que le logement de la batterie soit orienté vers vous.
7. Insérez la batterie dans le contrôleur en l'inclinant légèrement vers le bas.

Vous devez insérer la bride métallique située à l'avant de la batterie dans le logement situé en bas du contrôleur et faire glisser le haut de la batterie sous la petite goupille d'alignement située sur le côté gauche du contrôleur.

8. Déplacez le loquet de la batterie vers le haut pour fixer la batterie.

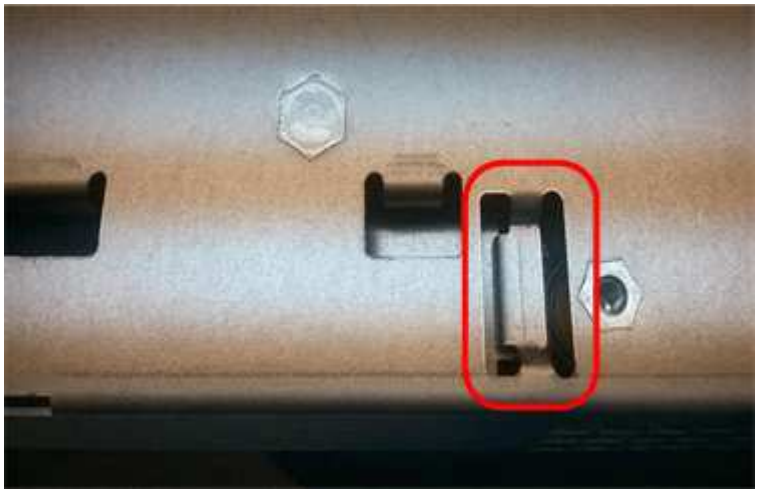
   Lorsque le loquet s'enclenche, le bas des crochets de verrouillage se trouve dans une fente métallique du châssis.

9. Retournez le contrôleur pour vérifier que la batterie est correctement installée.

   Dommages matériels possibles — la bride métallique à l'avant de la batterie doit être complètement insérée dans le logement du contrôleur (comme indiqué sur la première figure). Si la batterie n'est pas installée correctement (comme illustré sur la deuxième figure), la bride métallique peut entrer en contact avec la carte contrôleur, ce qui peut endommager la carte.

   - **Correct — la bride métallique de la batterie est complètement insérée dans le logement du contrôleur:**

   - **Incorrect — la bride métallique de la batterie n'est pas insérée dans le logement du contrôleur :**

10. Replacer le capot du contrôleur.

STEP5 : déplacer HIC vers le nouveau contrôleur, si nécessaire

Si le contrôleur défectueux est équipé d'une carte d'interface hôte (HIC), déplacez la carte HIC du contrôleur défectueux vers le contrôleur de remplacement.

Une HIC distincte est utilisée uniquement pour le contrôleur E2800B. La carte HIC est montée sur la carte contrôleur principale et comprend deux connecteurs SPF.

Les illustrations de cette procédure montrent une HIC 2 ports. La HIC de votre contrôleur peut avoir un nombre différent de ports.

E2800A

Un contrôleur E2800A ne possède pas de HIC.

Remettez le capot du contrôleur E2800A en place et passez à l'étape Étape 6 : remplacer le contrôleur

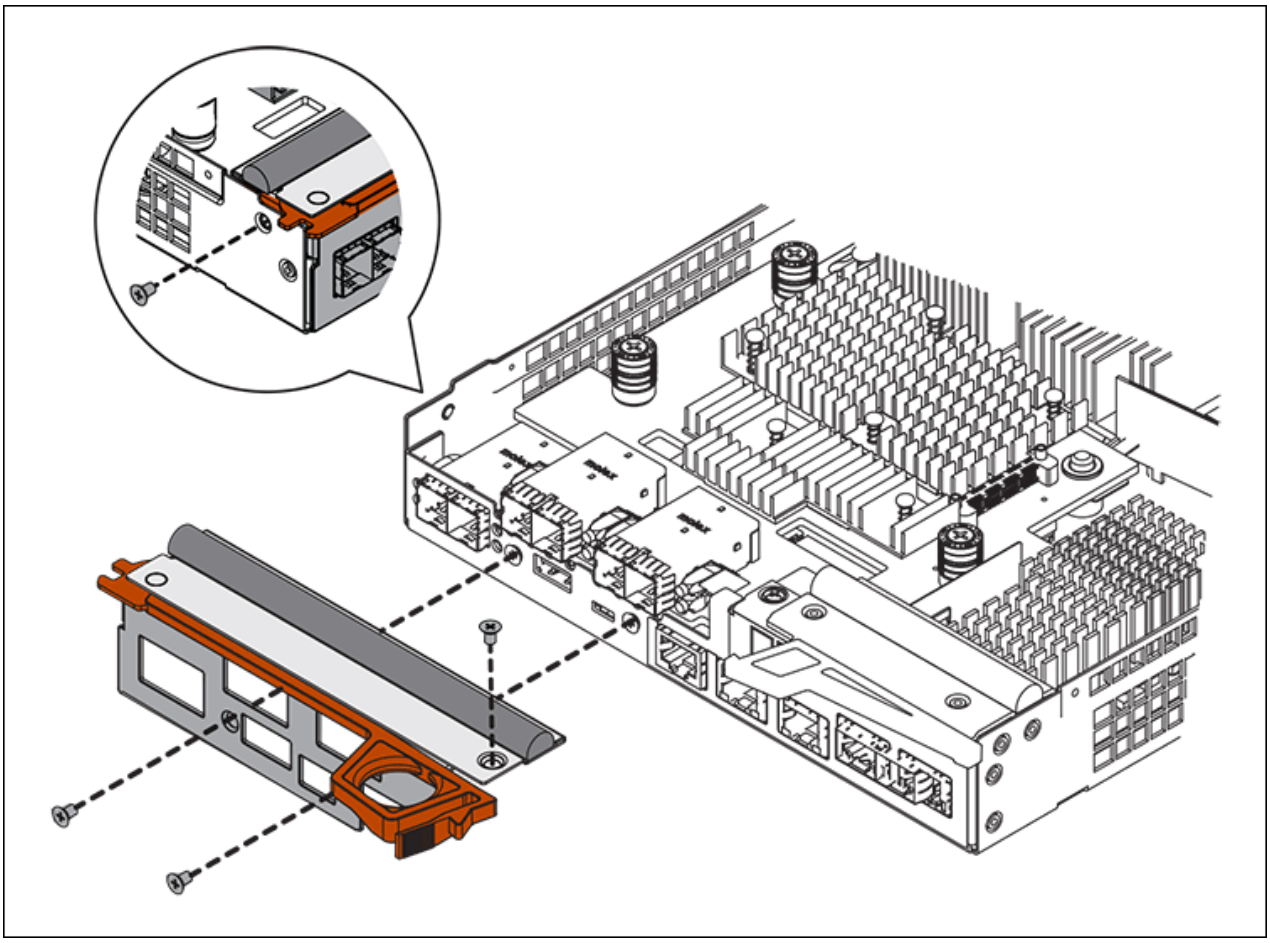
E2800B

Déplacez le HIC du contrôleur E2800B défectueux vers le contrôleur de remplacement.

Étapes

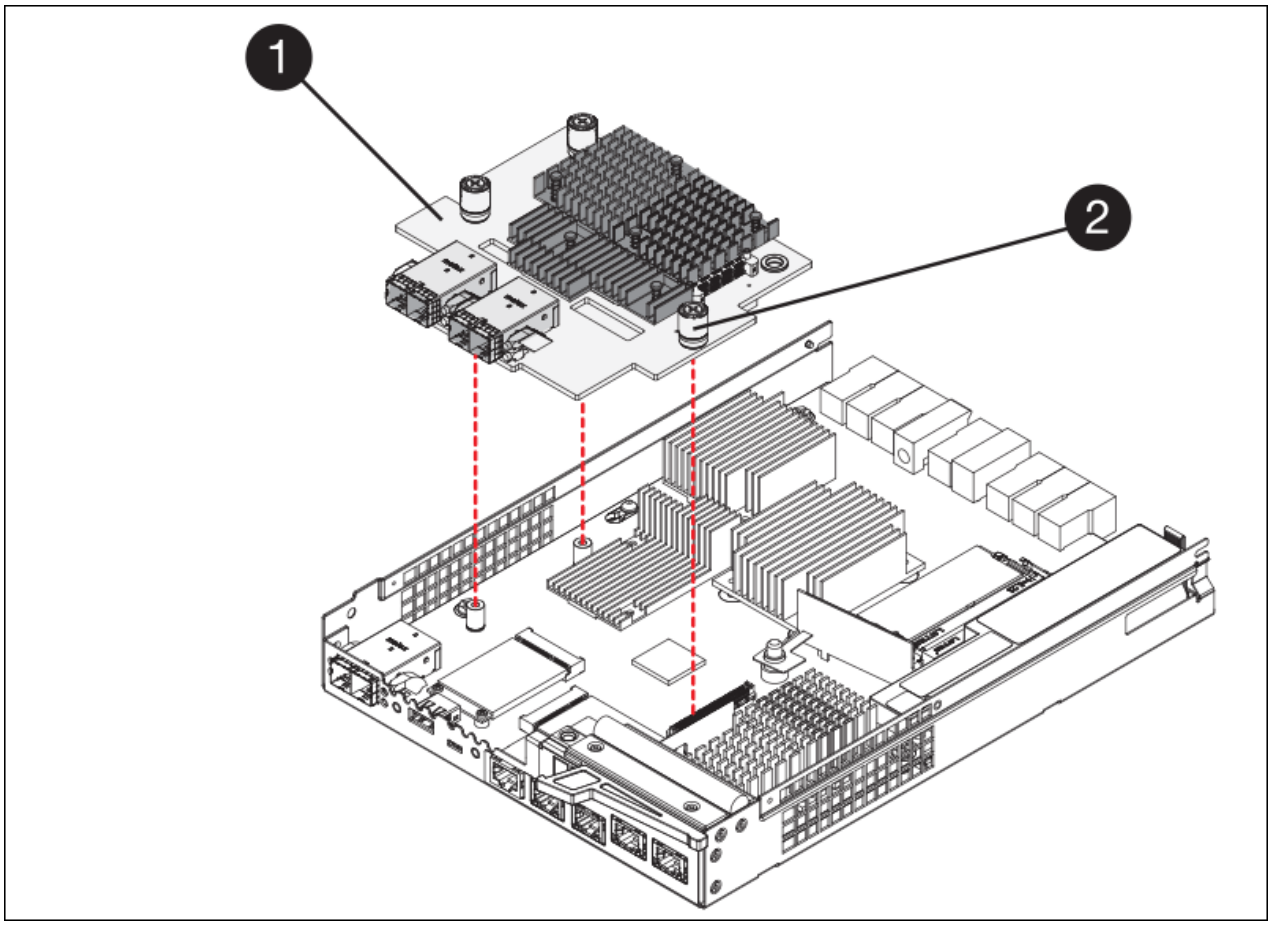
1. Supprimer tout SFP de la HIC.
2. À l'aide d'un tournevis cruciforme n° 1, retirez les vis qui fixent le cadran HIC au contrôleur.

   Il y a quatre vis : une sur le dessus, une sur le côté et deux sur l'avant.



3. Retirez la plaque HIC.
4. À l'aide de vos doigts ou d'un tournevis cruciforme, desserrez les trois vis à molette qui fixent le HIC à la carte contrôleur.
5. Détachez avec précaution la carte HIC de la carte contrôleur en la soulevant et en la faisant glisser vers l'arrière.

   Veillez à ne pas rayer ou heurter les composants au bas de la HIC ou au-dessus de la carte contrôleur.



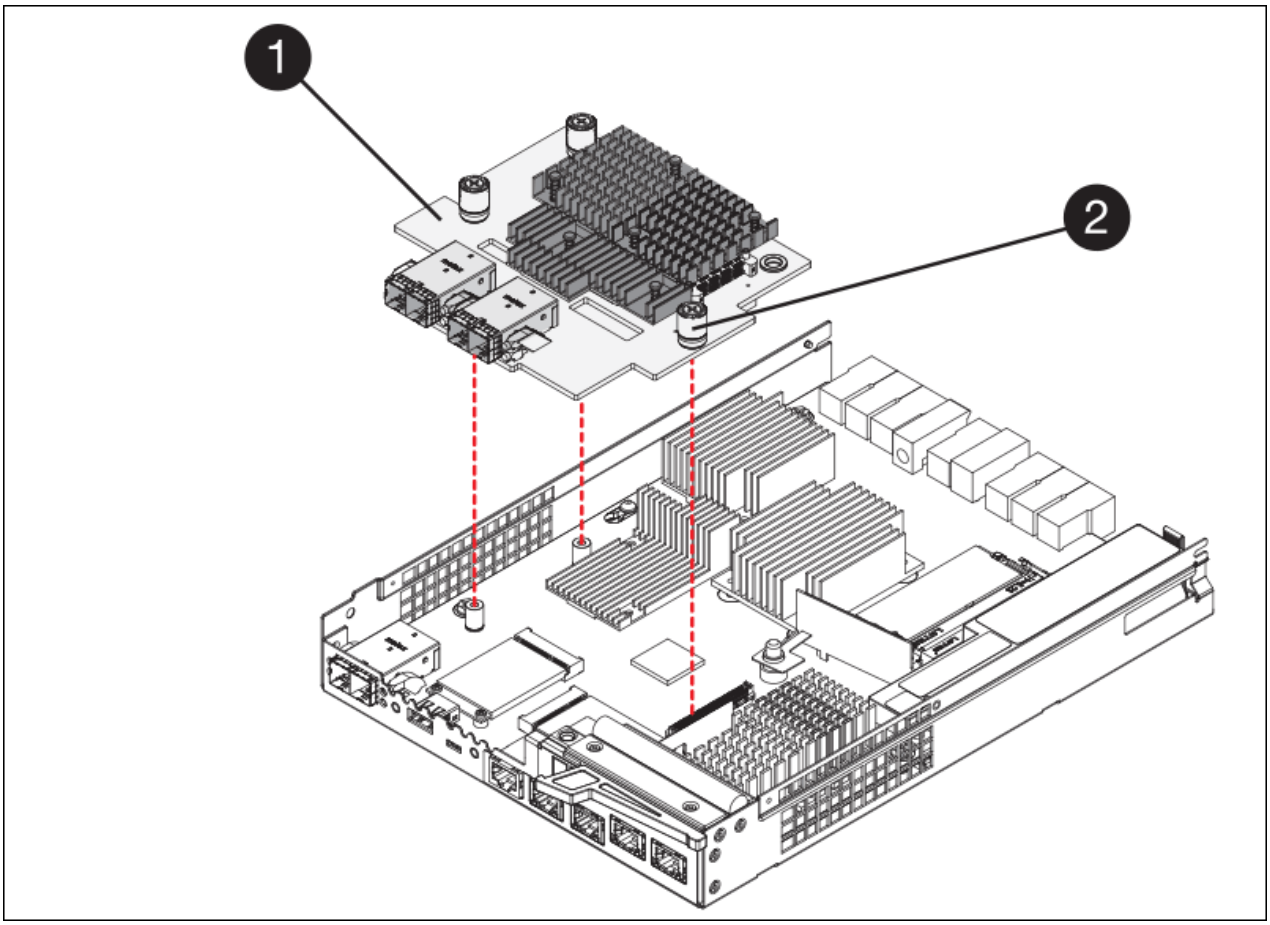
Étiquette	Description
1	Carte d'interface hôte
2	Vis moletées

6. Placez le HIC sur une surface antistatique.
7. À l'aide d'un tournevis cruciforme n° 1, retirez les quatre vis qui fixent le cache blanc au contrôleur de remplacement, puis retirez le cache.
8. Alignez les trois vis moletées de la HIC avec les trous correspondants du contrôleur de remplacement, puis alignez le connecteur situé au bas de la HIC avec le connecteur d'interface HIC de la carte contrôleur.

   Veillez à ne pas rayer ou heurter les composants au bas de la HIC ou au-dessus de la carte contrôleur.

9. Abaisser avec précaution la HIC et mettre le connecteur HIC en place en appuyant doucement sur la HIC.

Dommage possible de l'équipement — attention de ne pas pincer le connecteur ruban doré pour les voyants du contrôleur entre le HIC et les vis moletées.

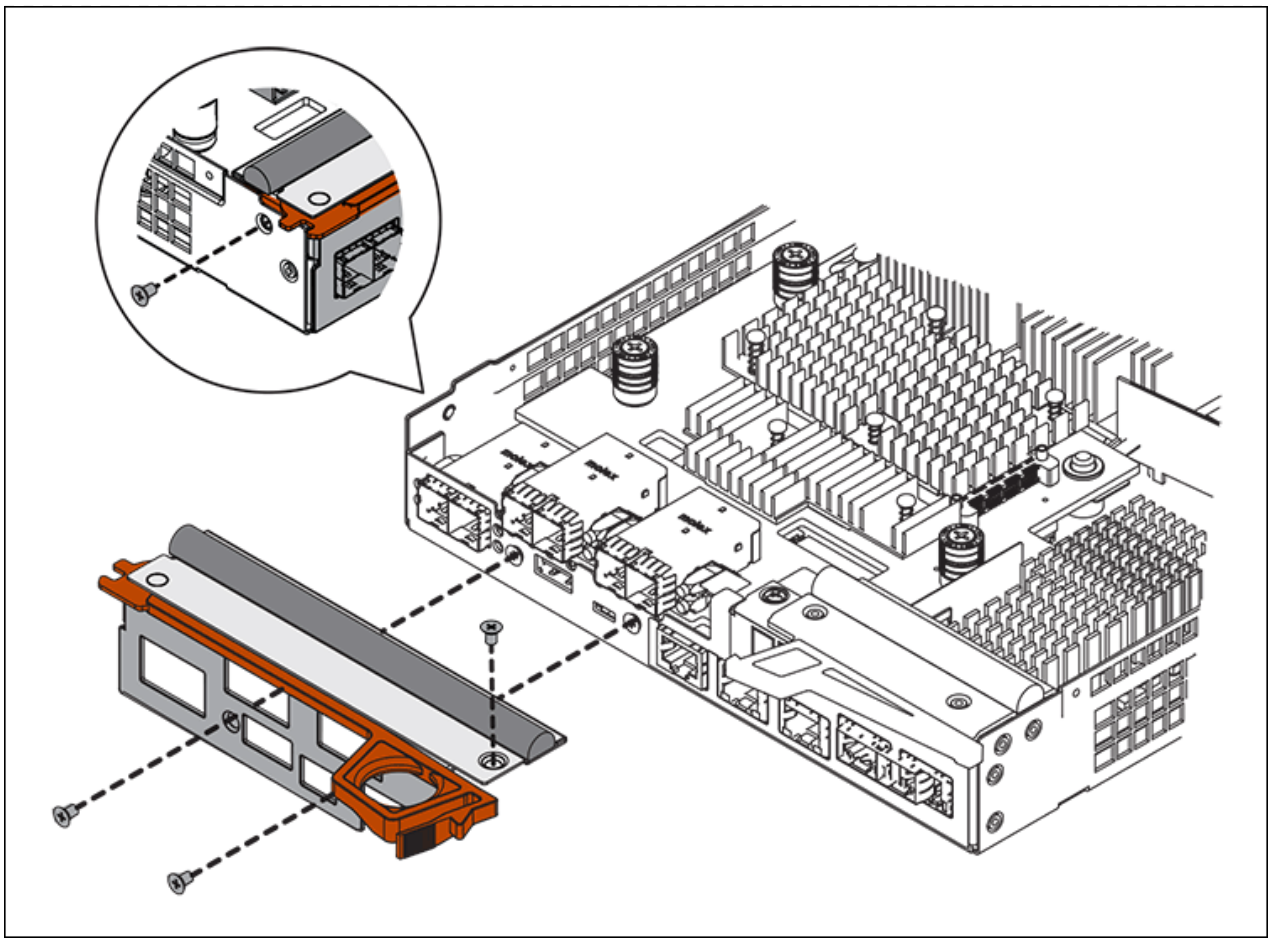


Étiquette	Description
1	Carte d'interface hôte
2	Vis moletées

10. Serrez les vis à molette HIC à la main.

    N'utilisez pas de tournevis, sinon vous risquez de trop serrer les vis.

11. À l'aide d'un tournevis cruciforme n° 1, fixez le cadran HIC retiré du contrôleur d'origine sur le nouveau contrôleur à l'aide de quatre vis.



12. Réinstallez tous les SFP retirés dans le HIC.

Étape 6 : remplacer le contrôleur

Installez le contrôleur de remplacement et vérifiez qu'il a rejoint la grille.

Étapes

1. Installez le contrôleur de remplacement sur l'appliance.
   a. Retournez le contrôleur pour que le capot amovible soit orienté vers le bas.
   b. Avec la poignée de came en position ouverte, faites glisser le contrôleur complètement dans l'appareil.
   c. Déplacez la poignée de came vers la gauche pour verrouiller le contrôleur en place.
   d. Remplacer les câbles et les SFP.
   e. Mettez le tiroir contrôleur sous tension.
   f. Si le contrôleur d'origine utilise DHCP pour l'adresse IP, localisez l'adresse MAC sur l'étiquette située à l'arrière du contrôleur de remplacement. Demandez à votre administrateur réseau d'associer le DNS/réseau et l'adresse IP du contrôleur que vous avez supprimé à l'adresse MAC du contrôleur de remplacement.

   > Si le contrôleur d'origine n'a pas utilisé DHCP pour l'adresse IP, le nouveau contrôleur adopte l'adresse IP du contrôleur que vous avez retiré.

2. Mettre le contrôleur en ligne à l'aide de SANtricity System Manager :

a. Sélectionnez **matériel**.
b. Si le graphique montre les lecteurs, sélectionnez **Afficher le verso du tiroir**.
c. Sélectionnez le contrôleur que vous souhaitez placer en ligne.
d. Sélectionnez **placer en ligne** dans le menu contextuel et confirmez que vous souhaitez effectuer l'opération.
e. Vérifiez que l'affichage à sept segments indique l'état de `99`.

3. Confirmer que le nouveau contrôleur est optimal et collecter les données de support.

Après le remplacement de la pièce, renvoyez la pièce défectueuse à NetApp, en suivant les instructions RMA (retour de matériel) livrées avec le kit. Voir la "Retour de pièce et amp ; remplacements" pour plus d'informations.

Informations associées

"Site de documentation sur les systèmes NetApp E-Series"

Remplacement des composants matériels dans le tiroir de contrôleur de stockage

En cas de problème matériel, vous devrez peut-être remplacer un composant du tiroir de contrôleur de stockage.

Avant de commencer

- Vous disposez de la procédure de remplacement du matériel E-Series.
- Vous avez physiquement situé l'appliance de stockage où vous remplacez des composants matériels de tiroirs de stockage dans le data Center.

  "Localiser le contrôleur dans le data Center"

Description de la tâche

Pour remplacer la batterie dans le contrôleur de stockage, reportez-vous aux étapes des instructions de "remplacement d'un contrôleur de stockage". Ces instructions décrivent le retrait d'un contrôleur de l'appareil, le retrait de la batterie du contrôleur, l'installation de la batterie et le remplacement du contrôleur.

Pour obtenir des instructions sur les autres unités remplaçables sur le terrain (FRU) des tiroirs disques, accédez aux procédures de maintenance du système E-Series.

FRU	Voir les instructions
Batterie	StorageGRID (ces instructions) : remplacement d'un contrôleur de stockage
Lecteur	Systèmes E-Series : • Remplacement du lecteur (60 disques) • Remplacement du lecteur (12 ou 24 disques)
Réservoir d'alimentation	E-Series • Remplacez le boîtier d'alimentation (60 disques) • Remplacement du bloc d'alimentation (12 disques ou 24 disques)

FRU	Voir les instructions
Boîtier du ventilateur (étagères à 60 disques uniquement)	E-Series : remplacement du boîtier du ventilateur (60 disques)
Tiroir disque (tiroirs de 60 disques uniquement)	E-Series : remplacement du tiroir disque (60 disques)

Après le remplacement de la pièce, renvoyez la pièce défectueuse à NetApp, en suivant les instructions RMA (retour de matériel) livrées avec le kit. Voir la "Retour de pièce et amp ; remplacements" pour plus d'informations.

Informations associées

"Site de documentation sur les systèmes NetApp E-Series"

"Remplacement du contrôleur de stockage"

Remplacement des composants matériels dans un tiroir d'extension de 60 disques en option

Vous devrez peut-être remplacer un module d'entrée/sortie, un bloc d'alimentation ou un ventilateur dans le tiroir d'extension.

Avant de commencer

- Vous disposez de la procédure de remplacement du matériel E-Series.
- Vous avez trouvé physiquement l'appliance de stockage où vous remplacez les composants matériels des tiroirs d'extension dans le data Center.

  "Localiser le contrôleur dans le data Center"

Description de la tâche

Pour remplacer un module d'entrée/sortie (IOM) dans un tiroir d'extension de 60 disques, reportez-vous aux étapes des instructions de "remplacement d'un contrôleur de stockage".

Pour remplacer un bloc d'alimentation ou un ventilateur dans un tiroir d'extension de 60 disques, accédez aux procédures E-Series pour entretenir le matériel de 60 disques.

FRU	Reportez-vous aux instructions relatives à la gamme E-Series pour
Module d'entrée/sortie (IOM)	Remplacement d'un module d'E/S.
Réservoir d'alimentation	Remplacez le boîtier d'alimentation (60 disques)
Boîtier de ventilateur	Remplacez le boîtier du ventilateur (60 disques)

Remplacer le contrôleur SG6000-CN

Vous devrez peut-être remplacer le contrôleur SG6000-CN s'il ne fonctionne pas de

manière optimale ou s'il est défectueux.

Avant de commencer

- Vous disposez d'un contrôleur de remplacement avec la même référence que le contrôleur que vous remplacez.
- Vous avez des étiquettes pour identifier chaque câble connecté au contrôleur.
- Vous avez trouvé le contrôleur à remplacer dans le data Center.

  "Localiser le contrôleur dans le data Center"

Description de la tâche

Le nœud de stockage de l'appliance ne sera pas accessible lors du remplacement du contrôleur SG6000-CN. Si le contrôleur SG6000-CN fonctionne suffisamment, vous pouvez effectuer un arrêt contrôlé au début de cette procédure.

> Si vous remplacez le contrôleur avant d'installer le logiciel StorageGRID, il se peut que vous ne puissiez pas accéder au programme d'installation de l'appliance StorageGRID immédiatement après avoir terminé cette procédure. Bien que vous puissiez accéder au programme d'installation de l'appliance StorageGRID à partir d'autres hôtes situés sur le même sous-réseau que l'appliance, vous ne pouvez pas y accéder à partir d'hôtes situés sur d'autres sous-réseaux. Cette condition doit se résoudre dans les 15 minutes (lorsque les entrées du cache ARP pour le contrôleur d'origine sont écoulées), ou vous pouvez effacer immédiatement la condition en éliminant manuellement les anciennes entrées du cache ARP à partir du routeur ou de la passerelle local.

Étapes

1. Affichez les configurations actuelles de l'appareil et enregistrez-les.
   a. Connectez-vous à l'appliance à remplacer :
      i. Saisissez la commande suivante : `ssh admin@grid_node_IP`
      ii. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
      iii. Entrez la commande suivante pour passer à la racine : `su -`
      iv. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

      Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

   b. Entrez : **`run-host-command ipmitool lan print`** Pour afficher les configurations BMC actuelles de l'appliance.
2. Si le contrôleur SG6000-CN fonctionne suffisamment pour permettre un arrêt contrôlé, arrêtez le contrôleur SG6000-CN.

   "Arrêtez le contrôleur SG6000-CN"

3. Si l'une des interfaces réseau de cette appliance StorageGRID est configurée pour DHCP, vous devrez peut-être mettre à jour les attributions de bail DHCP permanentes sur les serveurs DHCP pour référencer les adresses MAC de l'appliance de remplacement. Cette mise à jour garantit que l'appliance se voit attribuer les adresses IP attendues. Voir "Mettre à jour les références d'adresse MAC".
4. Retirez et remplacez le contrôleur SG6000-CN :

a. Etiqueter les câbles, puis débrancher les câbles et les émetteurs-récepteurs SFP+ ou SFP28.

> Pour éviter toute dégradation des performances, ne tordez pas, ne pliez pas, ne pincez pas ou ne montez pas sur les câbles.

b. Retirez le contrôleur défectueux de l'armoire ou du rack.

c. Installez le contrôleur de remplacement dans l'armoire ou le rack.

d. Remplacez les câbles et les émetteurs-récepteurs SFP+ ou SFP28.

e. Mettez le contrôleur sous tension et surveillez les LED du contrôleur et les codes de démarrage.

5. Si l'appliance sur laquelle vous avez remplacé le contrôleur a utilisé un serveur de gestion des clés (KMS) pour chiffrer les données, il est possible que vous ayez besoin d'une configuration supplémentaire avant que le nœud puisse rejoindre la grille. Si le nœud ne rejoint pas automatiquement la grille, assurez-vous que ces paramètres de configuration ont été transférés vers le nouveau contrôleur et configurez manuellement les paramètres qui ne possèdent pas la configuration attendue :
   - "Configurer les liaisons réseau"
   - "Configurez les adresses IP StorageGRID"
   - "Configurez le chiffrement des nœuds pour l'appliance"
6. Connectez-vous à l'appliance avec le contrôleur remplacé :
   a. Saisissez la commande suivante : `ssh admin@grid_node_IP`
   b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
   c. Entrez la commande suivante pour passer à la racine : `su -`
   d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
7. Restaurez la connectivité réseau du contrôleur BMC pour l'appliance. Deux options sont disponibles :
   - Utilisez une adresse IP statique, un masque de réseau et une passerelle
   - Utilisez DHCP pour obtenir une adresse IP, un masque de réseau et une passerelle

     i. Pour restaurer la configuration du contrôleur BMC afin d'utiliser une adresse IP statique, un masque de réseau et une passerelle, entrez les commandes suivantes :

     `run-host-command ipmitool lan set 1 ipsrc static`

     `run-host-command ipmitool lan set 1 ipaddr Appliance_IP`

     `run-host-command ipmitool lan set 1 netmask Netmask_IP`

     `run-host-command ipmitool lan set 1 defgw ipaddr Default_gateway`

     i. Pour restaurer la configuration du contrôleur BMC afin d'utiliser DHCP pour obtenir une adresse IP, un masque de réseau et une passerelle, entrez la commande suivante :

     `run-host-command ipmitool lan set 1 ipsrc dhcp`

8. Après avoir restauré la connectivité réseau du contrôleur BMC, connectez-vous à l'interface du contrôleur BMC pour vérifier et restaurer toute configuration BMC personnalisée supplémentaire que vous avez éventuellement appliquée. Par exemple, vous devez confirmer les paramètres des destinations d'interruption SNMP et des notifications par e-mail. Voir "Configurer l'interface BMC".

9. Vérifiez que le nœud de l'appliance s'affiche dans Grid Manager et qu'aucune alerte n'apparaît.

Après le remplacement de la pièce, renvoyez la pièce défectueuse à NetApp, en suivant les instructions RMA (retour de matériel) livrées avec le kit. Voir la "Retour de pièce et amp ; remplacements" pour plus d'informations.

Informations associées

"Installez le SG6000-CN dans l'armoire ou le rack"

"Afficher les indicateurs d'état"

"Afficher les codes de démarrage du contrôleur SG6000-CN"

Remplacez une ou les deux alimentations du contrôleur SG6000-CN

Le contrôleur SG6000-CN dispose de deux blocs d'alimentation pour la redondance. En cas de panne de l'un des blocs d'alimentation, vous devez le remplacer dès que possible afin de s'assurer que le contrôleur de calcul est alimenté en redondance. Les deux blocs d'alimentation qui fonctionnent au niveau du contrôleur doivent être du même modèle et de la même puissance.

Avant de commencer

- Vous avez déterminé l'emplacement physique dans le data Center du contrôleur avec l'alimentation à remplacer.

  "Localisation du contrôleur dans un data Center"

- Si vous remplacez une seule alimentation :
  - Vous avez déballé le bloc d'alimentation de remplacement et vous êtes assuré qu'il est le même modèle et la même puissance que l'unité d'alimentation que vous remplacez.
  - Vous avez confirmé que l'autre bloc d'alimentation est installé et en cours d'exécution.
- Si vous remplacez les deux alimentations en même temps :
  - Vous avez déballé les blocs d'alimentation de remplacement et vous êtes assuré qu'ils sont du même modèle et de la même puissance.

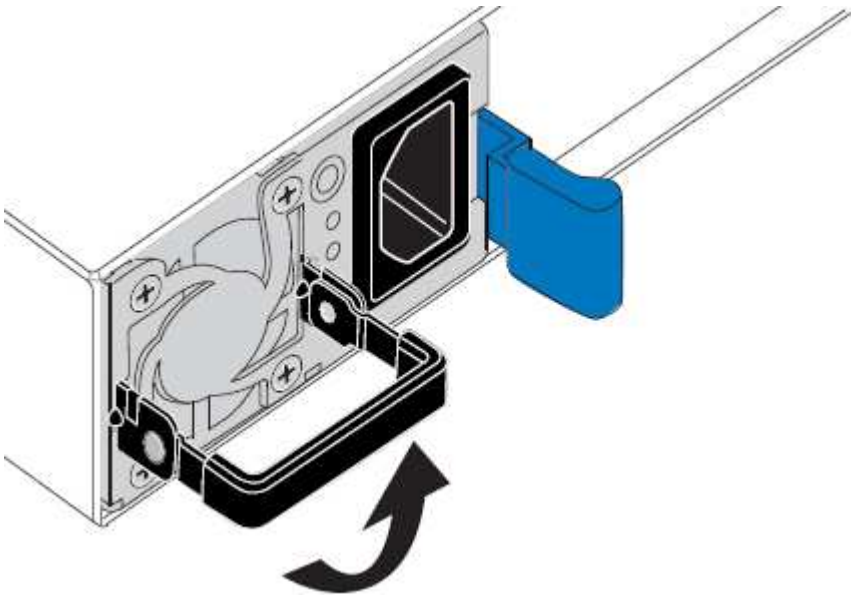
Description de la tâche

La figure montre les deux blocs d'alimentation du contrôleur SG6000-CN, accessibles à l'arrière du contrôleur. Utilisez cette procédure pour remplacer l'une des alimentations ou les deux. Si vous remplacez les deux blocs d'alimentation, vous devez d'abord effectuer un arrêt contrôlé de l'appareil.

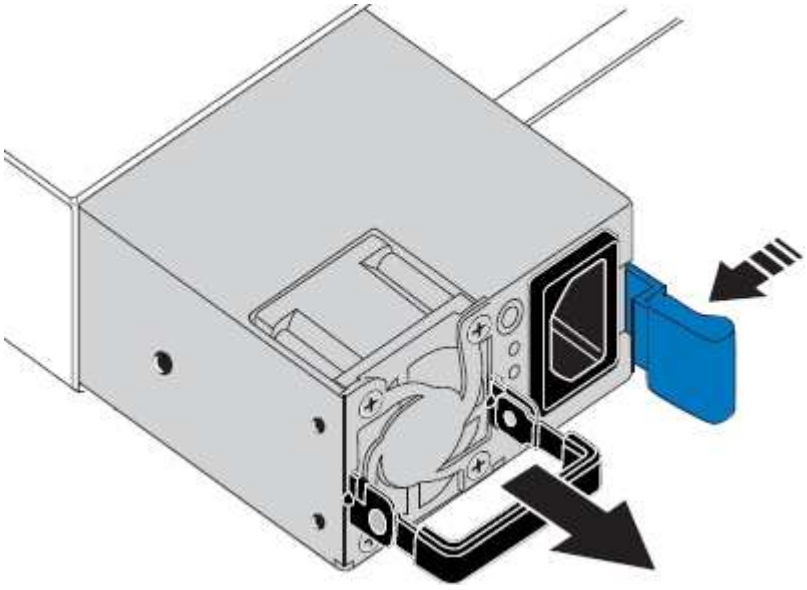
Étapes

1. Si vous ne remplacez qu'une seule alimentation, vous n'avez pas besoin d'éteindre l'appareil. Accédez au Débranchez le cordon d'alimentation étape. Si vous remplacez les deux blocs d'alimentation en même temps, procédez comme suit avant de débrancher les cordons d'alimentation :
   a. "Arrêtez l'appareil".

2. débranchez le cordon d’alimentation de chaque alimentation à remplacer.
3. Soulevez la poignée de came sur la première alimentation à remplacer.



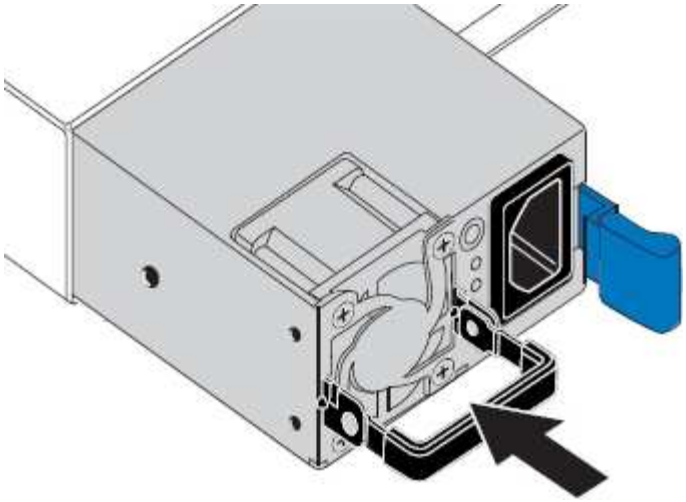
4. Appuyez sur le loquet bleu et retirez le bloc d’alimentation.



5. Avec le loquet bleu sur la droite, faites glisser le bloc d’alimentation de remplacement dans le châssis.

Les deux blocs d’alimentation doivent avoir le même modèle et la même puissance.

Assurez-vous que le loquet bleu se trouve sur le côté droit lorsque vous faites glisser l’unité de rechange.



6. Poussez la poignée de came vers le bas pour fixer le bloc d'alimentation de remplacement.
7. Si vous remplacez les deux blocs d'alimentation, répétez les étapes 2 à 6 pour remplacer la seconde.
8. "Branchez les câbles d'alimentation aux unités remplacées et mettez-les sous tension".

Après le remplacement de la pièce, renvoyez la pièce défectueuse à NetApp, en suivant les instructions RMA (retour de matériel) livrées avec le kit. Voir la "Retour de pièce et amp ; remplacements" pour plus d'informations.

Remplacez le contrôleur dans le rack

Retirez le contrôleur SG6000-CN de l'armoire ou du rack

Retirez le contrôleur SG6000-CN d'une armoire ou d'un rack pour accéder au capot supérieur ou pour déplacer le contrôleur à un autre emplacement.

Avant de commencer

- Vous disposez d'étiquettes pour identifier chaque câble connecté au contrôleur SG6000-CN.
- Vous avez installé physiquement le contrôleur SG6000-CN où vous effectuez des opérations de maintenance dans le centre de données.

  "Localiser le contrôleur dans le data Center"

- Vous avez arrêté le contrôleur SG6000-CN.

  "Arrêtez le contrôleur SG6000-CN"

  N'arrêtez pas le contrôleur à l'aide de l'interrupteur d'alimentation.

Étapes

1. Etiqueter puis débrancher les câbles d'alimentation du contrôleur.
2. Enroulez l'extrémité du bracelet antistatique autour de votre poignet et fixez l'extrémité du clip à une masse métallique afin d'éviter toute décharge statique.
3. Etiqueter puis débrancher les câbles de données du contrôleur et les émetteurs-récepteurs SFP+ ou SFP28.

Pour éviter toute dégradation des performances, ne tordez pas, ne pliez pas, ne pincez pas ou ne montez pas sur les câbles.

4. Desserrez les deux vis imperdables du panneau avant du contrôleur.

5. Faites glisser le contrôleur SG6000-CN vers l'avant pour le sortir du rack jusqu'à ce que les rails de montage soient complètement étendus et que vous entendiez les loquets des deux côtés cliquent.

   Le capot supérieur du contrôleur est accessible.

6. Facultatif : si vous retirez complètement le contrôleur de l'armoire ou du rack, suivez les instructions du kit de rails pour retirer le contrôleur des rails.

Après le remplacement de la pièce, renvoyez la pièce défectueuse à NetApp, en suivant les instructions RMA (retour de matériel) livrées avec le kit. Voir la "Retour de pièce et amp ; remplacements" pour plus d'informations.

Informations associées

"Déposer le couvercle du contrôleur SG6000-CN"

Réinstallez le contrôleur SG6000-CN dans l'armoire ou le rack

Une fois la maintenance matérielle terminée, réinstallez le contrôleur dans une armoire ou un rack.

Avant de commencer

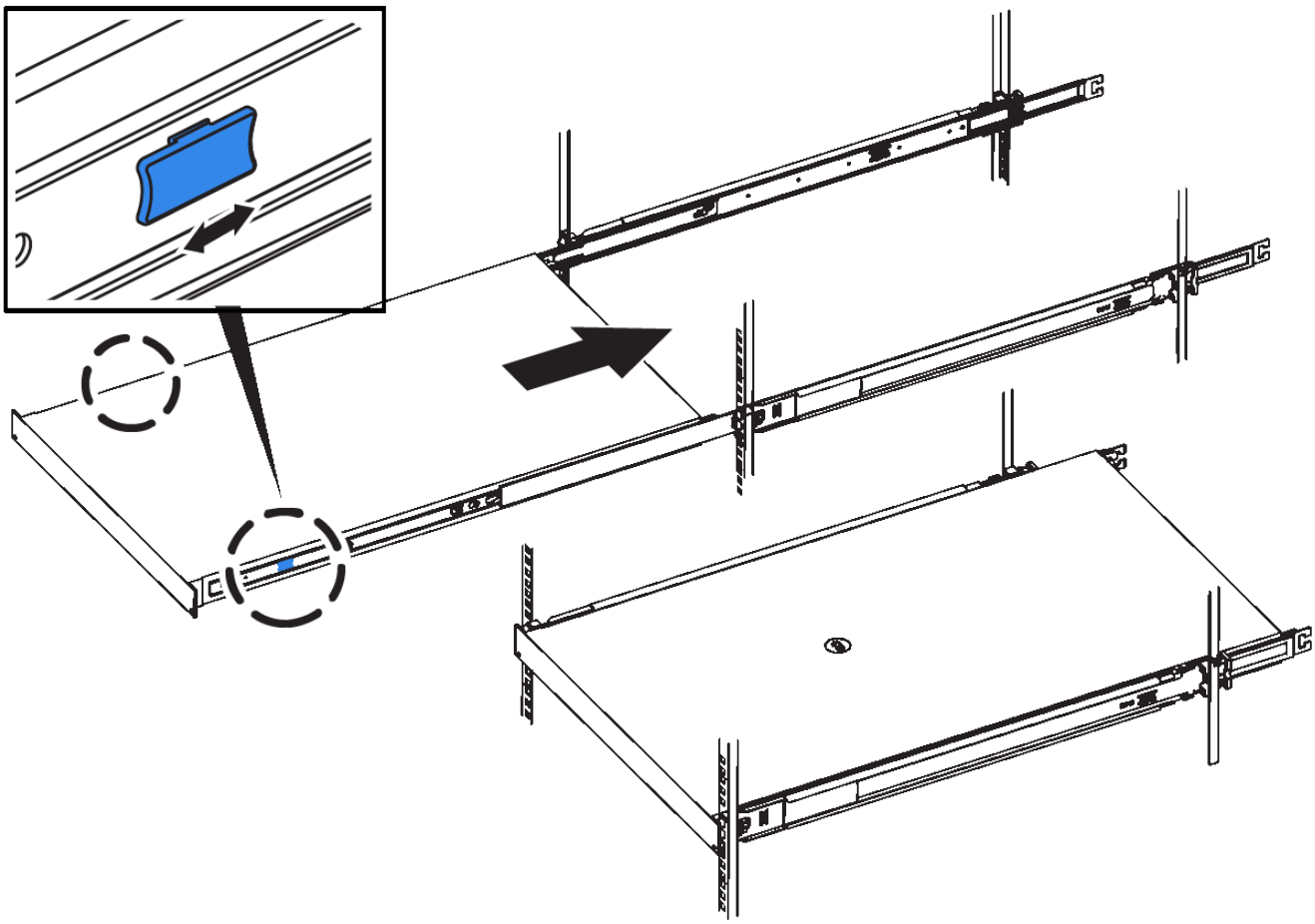
Vous avez réinstallé le capot du contrôleur.

"Réinstallez le couvercle du contrôleur SG6000-CN"

Étapes

1. Appuyez sur le rail bleu pour libérer les deux rails de rack en même temps et faites glisser le contrôleur SG6000-CN dans le rack jusqu'à ce qu'il soit bien en place.

   Lorsque vous ne pouvez plus déplacer le contrôleur, tirez sur les loquets bleus des deux côtés du châssis pour faire glisser le contrôleur complètement vers l'intérieur.



Ne fixez le panneau avant qu'après la mise sous tension du contrôleur.

2. Serrez les vis imperdables du panneau avant du contrôleur pour fixer le contrôleur dans le rack.

3. Enroulez l'extrémité du bracelet antistatique autour de votre poignet et fixez l'extrémité du clip à une masse métallique afin d'éviter toute décharge statique.
4. Reconnectez les câbles de données du contrôleur et les émetteurs-récepteurs SFP+ ou SFP28.

Pour éviter toute dégradation des performances, ne tordez pas, ne pliez pas, ne pincez pas ou ne montez pas sur les câbles.

"Cable appliance (SG6000)"

5. Reconnectez les câbles d'alimentation du contrôleur.

"Branchement des câbles d'alimentation et alimentation (SG6000)"

Une fois que vous avez terminé

Le contrôleur peut être redémarré.

"Mettez le contrôleur SG6000-CN sous tension et vérifiez son fonctionnement"

Remettez le capot du contrôleur en place

Déposer le couvercle du contrôleur SG6000-CN

Retirer le capot du contrôleur pour accéder aux composants internes en vue de leur maintenance.

Avant de commencer

Retirez le contrôleur de l'armoire ou du rack pour accéder au capot supérieur.

"Retirez le contrôleur SG6000-CN de l'armoire ou du rack"

Étapes

1. Assurez-vous que le loquet du capot du contrôleur SG6000-CN n'est pas verrouillé. Si nécessaire, tournez le verrou en plastique bleu d'un quart de tour dans le sens de déverrouillage, comme illustré sur le verrou.
2. Faites pivoter le loquet vers le haut et vers l'arrière du châssis du contrôleur SG6000-CN jusqu'à ce qu'il s'arrête, puis soulevez avec précaution le capot du châssis et mettez-le de côté.

Enroulez l'extrémité du bracelet antistatique autour de votre poignet et fixez l'extrémité du clip à une masse métallique pour éviter toute décharge statique lors du travail à l'intérieur du contrôleur SG6000-CN.

Après le remplacement de la pièce, renvoyez la pièce défectueuse à NetApp, en suivant les instructions RMA (retour de matériel) livrées avec le kit. Voir la "Retour de pièce et amp ; remplacements" pour plus d'informations.

Informations associées

"Retirez l'adaptateur HBA Fibre Channel"

Réinstallez le couvercle du contrôleur SG6000-CN

Réinstallez le capot du contrôleur une fois la maintenance matérielle interne terminée.

Avant de commencer

Vous avez effectué toutes les procédures de maintenance à l'intérieur du contrôleur.

Étapes

1. Avec le loquet du capot ouvert, tenez le capot au-dessus du châssis et alignez le trou du loquet du capot supérieur avec la broche du châssis. Lorsque le capot est aligné, abaissez-le sur le châssis.

2. Faites pivoter le loquet du capot vers l'avant et vers le bas jusqu'à ce qu'il s'arrête et que le capot s'insère complètement dans le châssis. Vérifier qu'il n'y a pas d'espace le long du bord avant du couvercle.

   Si le capot n'est pas bien en place, il se peut que vous ne puissiez pas faire glisser le contrôleur SG6000-CN dans le rack.

3. En option : tournez d'un quart de tour le verrou en plastique bleu dans le sens de verrouillage, comme illustré sur le verrou, pour le verrouiller.

Une fois que vous avez terminé

Réinstallez le contrôleur dans l'armoire ou le rack.

"Réinstallez le contrôleur SG6000-CN dans l'armoire ou le rack"

Remplacez la carte HBA Fibre Channel dans le contrôleur SG6000-CN

Vérifiez que la carte HBA Fibre Channel doit être remplacée

En cas de doute sur la carte HBA (Fibre Channel Host bus adapter) à remplacer, procédez comme suit pour l'identifier.

Avant de commencer

- Vous disposez du numéro de série de l'appliance de stockage ou du contrôleur SG6000-CN sur lequel l'adaptateur HBA Fibre Channel doit être remplacé.

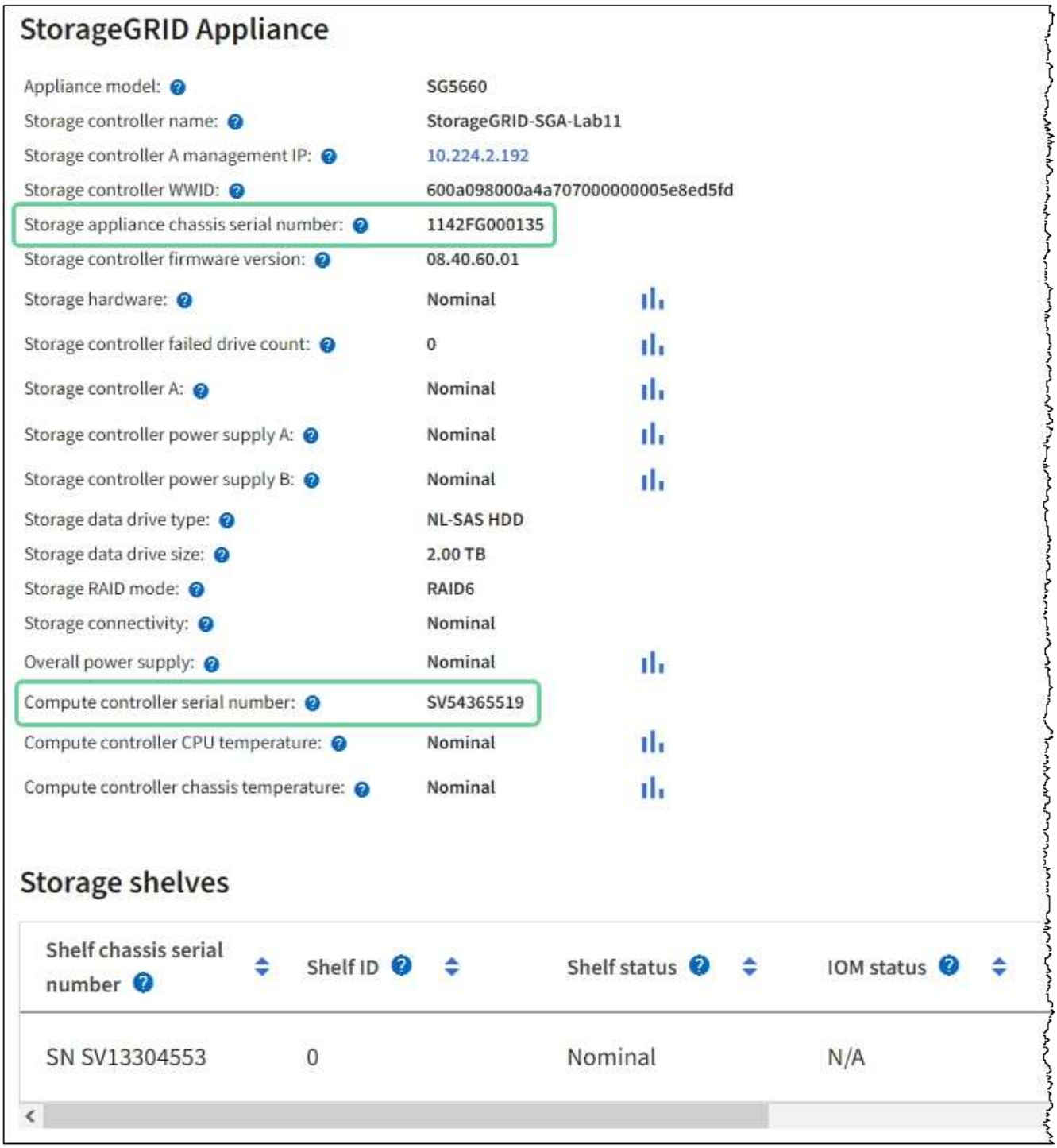
> Si le numéro de série du dispositif de stockage contenant l'adaptateur HBA Fibre Channel que vous remplacez commence par la lettre Q, il ne sera pas répertorié dans le gestionnaire de réseau. Vous devez vérifier les étiquettes fixées à l'avant de chaque contrôleur SG6000-CN du centre de données jusqu'à ce que vous trouviez la correspondance.

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".

Étapes

1. Dans Grid Manager, sélectionnez **NODES**.
2. Dans le tableau de la page nœuds, sélectionnez un nœud de stockage d'appliance.
3. Sélectionnez l'onglet **matériel**.

   Vérifiez le **numéro de série du châssis de l'appliance de stockage** et le **numéro de série du contrôleur de calcul** dans la section serveur StorageGRID. Voyez si l'un de ces numéros de série correspond au numéro de série de l'appliance de stockage où vous remplacez l'adaptateur HBA Fibre Channel. Si l'un ou l'autre des numéros de série correspond, vous avez trouvé l'appliance appropriée.



- Si la section appliance StorageGRID ne s'affiche pas, le nœud sélectionné n'est pas une appliance StorageGRID. Sélectionnez un nœud différent dans l'arborescence.
- Si le modèle d'appliance n'est pas SG6060 ou SG6060X, sélectionnez un nœud différent dans l'arborescence.
- Si les numéros de série ne correspondent pas, sélectionnez un autre nœud dans l'arborescence.

4. Une fois que vous avez trouvé le nœud sur lequel l'adaptateur HBA Fibre Channel doit être remplacé, notez l'adresse IP du contrôleur de calcul dans la section Appliance StorageGRID.

   Vous pouvez utiliser cette adresse IP pour activer la LED d'identification du contrôleur de calcul, afin de vous aider à localiser l'appliance dans le data Center.

   "Allumer et éteindre la LED d'identification du contrôleur"

Informations associées

"Retirez l'adaptateur HBA Fibre Channel"

Retirez l'adaptateur HBA Fibre Channel

Vous devrez peut-être remplacer l'adaptateur de bus hôte Fibre Channel (HBA) dans le contrôleur SG6000-CN s'il ne fonctionne pas de manière optimale ou s'il est défectueux.

Avant de commencer

- Vous disposez de l'adaptateur HBA Fibre Channel de remplacement approprié.
- Vous avez "Déterminez quel contrôleur SG6000-CN contient l'adaptateur HBA Fibre Channel à remplacer - effectué".
- Vous avez "Emplacement physique du contrôleur SG6000-CN" dans le data center.
- Vous avez "Arrêtez le contrôleur SG6000-CN".

  Un arrêt contrôlé est nécessaire avant de retirer le contrôleur du rack.

- Vous avez "retirez le contrôleur de l'armoire ou du rack - effectué".
- Vous avez "retirez le capot du contrôleur - effectué".

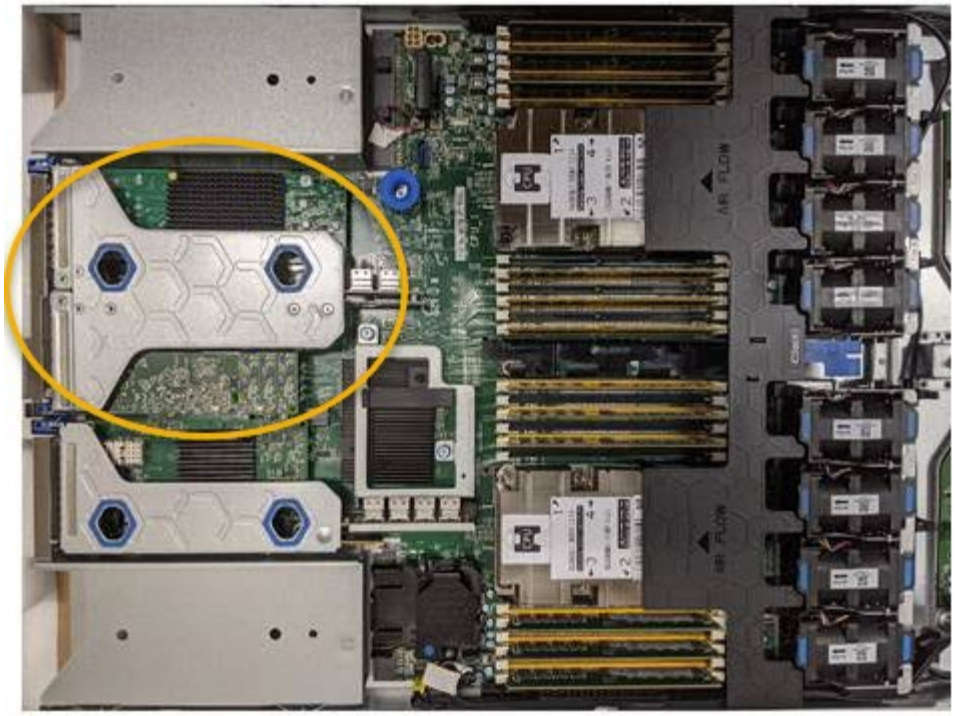
Description de la tâche

Pour éviter toute interruption de service, vérifiez que tous les autres nœuds de stockage sont connectés à la grille avant de démarrer le remplacement de HBA Fibre Channel ou de remplacer l'adaptateur lors d'une fenêtre de maintenance planifiée en cas d'interruption de service. Voir les informations sur "contrôle de l'état de connexion du nœud".

Si vous avez déjà utilisé une règle ILM pour créer une seule copie d'un objet, vous devez remplacer l'adaptateur HBA Fibre Channel lors d'une fenêtre de maintenance planifiée. Sinon, vous risquez de perdre temporairement l'accès à ces objets au cours de cette procédure. + Voir les informations sur "pourquoi ne pas utiliser la réplication à copie unique".

Étapes

1. Enroulez l'extrémité du bracelet antistatique autour de votre poignet et fixez l'extrémité du clip à une masse métallique afin d'éviter toute décharge statique.
2. Repérez l'ensemble de montage à l'arrière du contrôleur contenant le HBA Fibre Channel.



3. Saisissez l'ensemble de montage dans les trous marqués de couleur bleue et soulevez-le avec précaution vers le haut. Déplacez l'ensemble de montage vers l'avant du châssis tout en le soulevant pour permettre aux connecteurs externes des adaptateurs installés de dégager le châssis.
4. Placez la carte de montage sur une surface antistatique plane, face en métal vers le bas pour accéder aux adaptateurs.

L'ensemble carte de montage comprend deux adaptateurs : un adaptateur HBA Fibre Channel et un adaptateur réseau Ethernet. Le HBA Fibre Channel est indiqué sur l'illustration.

5. Ouvrez le loquet bleu de l'adaptateur (encerclé) et retirez avec précaution le HBA Fibre Channel de l'ensemble de montage. Secouez légèrement l'adaptateur pour retirer l'adaptateur de son connecteur. N'utilisez pas de force excessive.
6. Placez l'adaptateur sur une surface antistatique plane.

Une fois que vous avez terminé

"Installez la carte HBA Fibre Channel de remplacement".

Après le remplacement de la pièce, renvoyez la pièce défectueuse à NetApp, en suivant les instructions RMA

(retour de matériel) livrées avec le kit. Voir la "Retour de pièce et amp ; remplacements" pour plus d'informations.

Réinstallez l'adaptateur HBA Fibre Channel

L'adaptateur HBA Fibre Channel de remplacement est installé au même emplacement que celui qui a été retiré.

Avant de commencer

- Vous disposez de l'adaptateur HBA Fibre Channel de remplacement approprié.
- Vous avez supprimé l'adaptateur HBA Fibre Channel existant.

  "Retirez l'adaptateur HBA Fibre Channel"

Étapes

1. Enroulez l'extrémité du bracelet antistatique autour de votre poignet et fixez l'extrémité du clip à une masse métallique afin d'éviter toute décharge statique.
2. Retirer le HBA Fibre Channel de remplacement de son emballage.
3. Avec le loquet bleu de l'adaptateur en position ouverte, alignez l'adaptateur HBA Fibre Channel avec son connecteur sur le dispositif de montage. Appuyez ensuite avec précaution sur l'adaptateur pour l'insérer dans le connecteur jusqu'à ce qu'il soit bien en place.

   L'ensemble carte de montage comprend deux adaptateurs : un adaptateur HBA Fibre Channel et un adaptateur réseau Ethernet. Le HBA Fibre Channel est indiqué sur l'illustration.

4. Repérez le trou d'alignement de l'ensemble de montage (entouré de cercles) qui s'aligne sur une goupille de guidage de la carte système pour assurer le positionnement correct de l'ensemble de montage.

5. Positionnez l’ensemble de montage dans le châssis, en vous assurant qu’il est aligné avec le connecteur et la broche de guidage de la carte système, puis insérez l’ensemble de montage.
6. Appuyez avec précaution sur l’ensemble de montage pour le mettre en place le long de sa ligne centrale, à côté des trous marqués en bleu, jusqu’à ce qu’il soit bien en place.
7. Retirez les capuchons de protection des ports HBA Fibre Channel sur lesquels vous devez réinstaller les câbles.

Une fois que vous avez terminé

Si vous ne disposez d’aucune autre procédure de maintenance à effectuer dans le contrôleur, réinstallez le capot du contrôleur.

"Réinstallez le couvercle du contrôleur SG6000-CN"

Maintenance du matériel SG5700

Conservez l’appliance SG5700

Il peut être nécessaire de mettre à niveau le logiciel SANtricity OS du contrôleur E2800, de modifier la configuration de la liaison Ethernet du contrôleur E5700SG ou de remplacer le contrôleur E2800 ou le contrôleur E5700SG ou de remplacer des composants spécifiques. Les procédures décrites dans cette section supposent que l’appliance a déjà été déployée en tant que nœud de stockage dans un système StorageGRID.

Cette section décrit les procédures spécifiques à la maintenance de votre appliance SG5700.

Voir "Procédures courantes" pour les procédures de maintenance utilisées par tous les appareils.

Voir "Configurer le matériel" pour les procédures de maintenance qui sont également effectuées lors de l’installation et de la configuration initiales de l’appliance.

Procédures de configuration de la maintenance

Mettre à niveau le système d’exploitation SANtricity sur le contrôleur de stockage

Pour optimiser le fonctionnement du contrôleur de stockage, vous devez effectuer une mise à niveau vers la dernière version de maintenance du système d’exploitation

SANtricity compatible avec votre appliance StorageGRID.

Consulter le "Matrice d'interopérabilité NetApp (IMT)" pour déterminer la version que vous devez utiliser.

Téléchargez le nouveau fichier du logiciel SANtricity OS sur "Téléchargement NetApp : appliance StorageGRID".

Utilisez l'une des procédures suivantes basées sur la version de SANtricity OS actuellement installée :

- Si le contrôleur de stockage utilise SANtricity OS 08.42.20.00 (11.42) ou une version ultérieure, utilisez Grid Manager pour effectuer la mise à niveau.

  "Mettez à niveau le système d'exploitation SANtricity sur les contrôleurs de stockage à l'aide de Grid Manager"

- Si le contrôleur de stockage utilise une version de SANtricity OS antérieure à 08.42.20.00 (11.42), utilisez le mode de maintenance pour effectuer la mise à niveau.

  "Mettez à niveau SANtricity OS sur le contrôleur E2800 à l'aide du mode de maintenance"

Mettez à niveau le système d'exploitation SANtricity sur les contrôleurs de stockage à l'aide de Grid Manager

Pour les contrôleurs de stockage qui utilisent actuellement SANtricity OS 08.42.20.00 (11.42) ou version ultérieure, vous devez utiliser le gestionnaire grid pour appliquer une mise à niveau.

Avant de commencer

- Vous avez consulté le "Matrice d'interopérabilité NetApp (IMT)" Pour vérifier que la version de SANtricity OS utilisée pour la mise à niveau est compatible avec votre appliance.
- Vous avez le "Maintenance ou autorisation d'accès racine".
- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous avez la phrase secrète pour le provisionnement.
- Vous avez accès à "Téléchargement NetApp : appliance StorageGRID".

Description de la tâche

Vous ne pouvez pas effectuer d'autres mises à jour logicielles (mise à niveau du logiciel StorageGRID ou correctif) tant que vous n'avez pas terminé le processus de mise à niveau du système d'exploitation SANtricity. Si vous tentez de lancer un correctif ou une mise à niveau du logiciel StorageGRID avant la fin du processus de mise à niveau de SANtricity OS, vous êtes redirigé vers la page de mise à niveau de SANtricity OS.

La procédure ne sera terminée qu'une fois la mise à niveau de SANtricity OS appliquée avec succès à tous les nœuds applicables sélectionnés pour la mise à niveau. Cela peut prendre plus de 30 minutes pour charger le système d'exploitation SANtricity sur chaque nœud (de façon séquentielle) et jusqu'à 90 minutes pour redémarrer chaque appliance de stockage StorageGRID. Les nœuds de votre grille qui n'utilisent pas SANtricity OS ne seront pas affectés par cette procédure.

Les étapes suivantes s'appliquent uniquement lorsque vous utilisez le gestionnaire de grille pour effectuer la mise à niveau. Les contrôleurs de stockage de l'appliance ne peuvent pas être mis à niveau à l'aide du gestionnaire de grid lorsque les contrôleurs utilisent un système d'exploitation SANtricity antérieur à 08.42.20.00 (11.42).

Cette procédure met automatiquement à niveau la NVSRAM vers la version la plus récente associée à la mise à niveau du système d'exploitation SANtricity. Vous n'avez pas besoin d'appliquer un fichier de mise à niveau NVSRAM distinct.

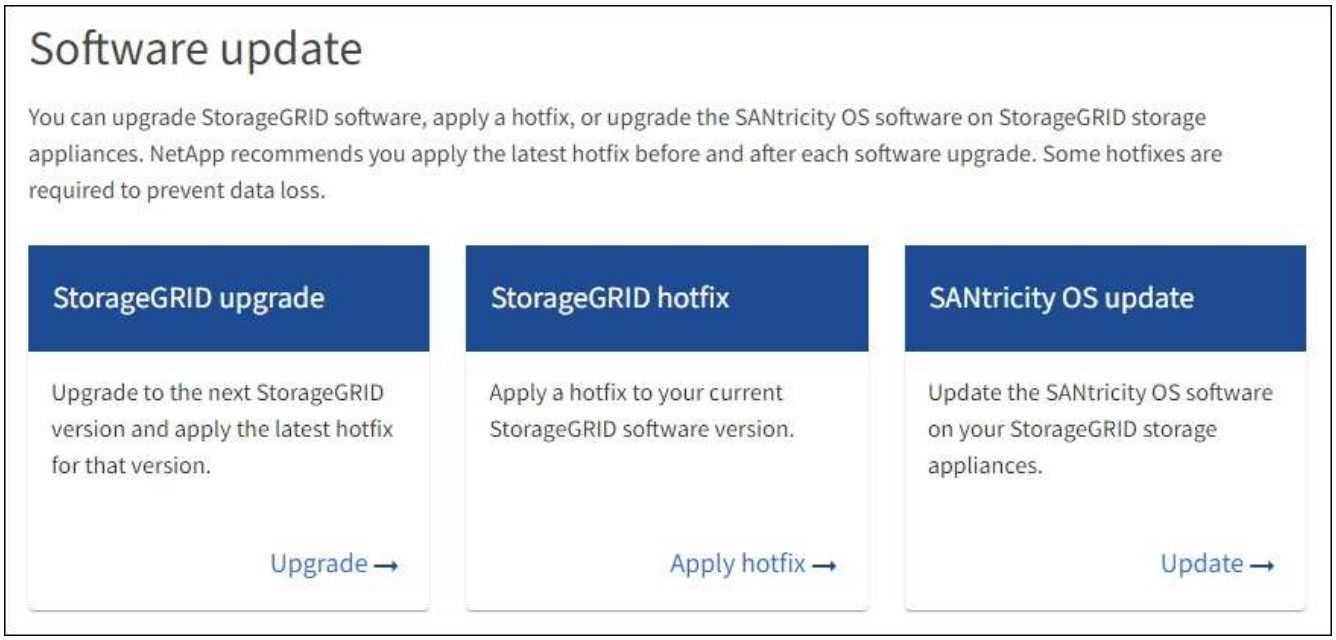
Veillez à appliquer le dernier correctif StorageGRID avant de commencer cette procédure. Voir "Procédure de correctif StorageGRID" pour plus d'informations.

Étapes

1. Téléchargez le nouveau fichier du logiciel SANtricity OS depuis le site "Téléchargement NetApp : appliance StorageGRID".

   Veillez à choisir la version de système d'exploitation SANtricity pour vos contrôleurs de stockage.

2. Sélectionnez **MAINTENANCE** > **système** > **mise à jour logicielle**.



3. Dans la section mise à jour de SANtricity OS, sélectionnez **mise à jour**.

   La page de mise à niveau de SANtricity OS s'affiche et répertorie les détails de chaque nœud d'appliance, notamment :

   - Nom du nœud
   - Le site
   - Modèle de type appliance
   - Version du système d'exploitation SANtricity
   - État
   - État de la dernière mise à niveau

4. Consultez les informations du tableau pour tous vos appareils pouvant être mis à niveau. Vérifiez que tous les contrôleurs de stockage ont l'état **nominal**. Si l'état d'un contrôleur est **Inconnu**, passez à **nœuds** > ***appliance node*** > **matériel** pour rechercher et résoudre le problème.

5. Sélectionnez le fichier de mise à niveau du système d'exploitation SANtricity que vous avez téléchargé depuis le site du support NetApp.

a. Sélectionnez **Parcourir**.

b. Localisez et sélectionnez le fichier.

c. Sélectionnez **Ouvrir**.

Le fichier est téléchargé et validé. Une fois le processus de validation terminé, le nom du fichier est affiché avec une coche verte à côté du bouton **Browse**. Ne modifiez pas le nom du fichier car il fait partie du processus de vérification.

6. Entrez la phrase de passe de provisionnement et sélectionnez **Continuer**.

   Un message d'avertissement s'affiche indiquant que la connexion de votre navigateur peut être perdue temporairement car les services sur les nœuds mis à niveau sont redémarrés.

7. Sélectionnez **Oui** pour placer le fichier de mise à niveau de SANtricity OS sur le nœud d'administration principal.

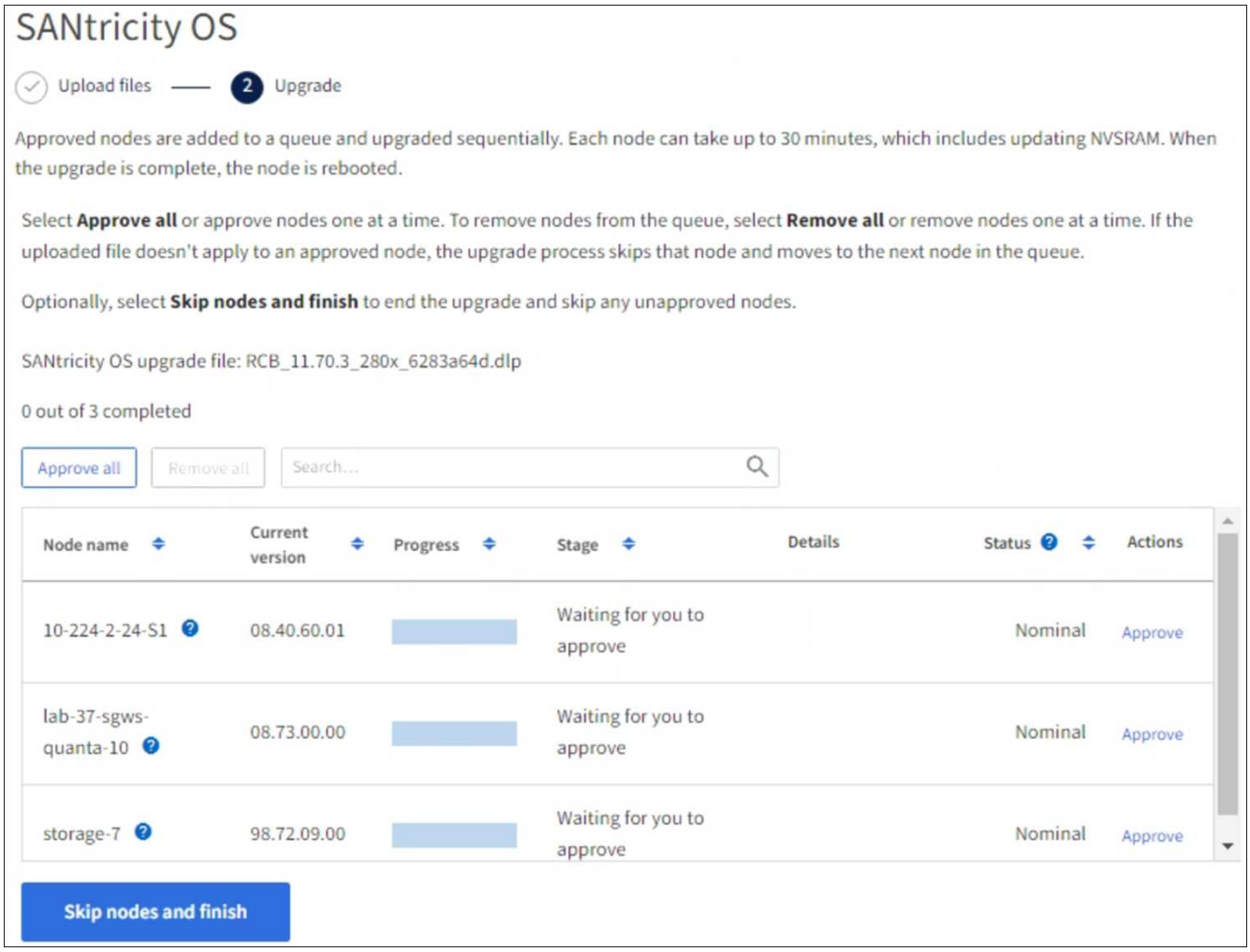
   Lorsque la mise à niveau de SANtricity OS démarre :

   a. Le contrôle de l'état est exécuté. Ce processus vérifie qu'aucun nœud ne présente l'état nécessite une intervention.

      Si des erreurs sont signalées, résolvez-les et sélectionnez à nouveau **Démarrer**.

   b. Le tableau de progression de la mise à niveau de SANtricity OS s'affiche. Ce tableau affiche tous les nœuds de stockage de votre grille ainsi que l'étape actuelle de la mise à niveau de chaque nœud.

      Le tableau indique tous les nœuds de stockage de l'appliance. Les nœuds de stockage logiciels ne sont pas affichés. Sélectionnez **Approve** pour tous les nœuds nécessitant la mise à niveau.



8. Vous pouvez également trier la liste des nœuds par ordre croissant ou décroissant :
   - Nom du nœud
   - Version actuelle
   - Progression
   - Étape
   - État

   Vous pouvez également saisir un terme dans la zone de recherche pour rechercher des nœuds spécifiques.

9. Approuver les nœuds de grille que vous êtes prêt à ajouter à la file d'attente de mise à niveau. Les nœuds approuvés sont mis à niveau un par un.

   > N'approuvez pas la mise à niveau de SANtricity OS pour un nœud de stockage d'appliance, sauf si vous êtes sûr que le nœud est prêt à être arrêté et redémarré. Lorsque la mise à niveau de SANtricity OS est approuvée sur un nœud, les services qui y sont arrêtés et le processus de mise à niveau commence. Plus tard, lorsque la mise à niveau du nœud est terminée, le nœud d'appliance est redémarré. Ces opérations peuvent entraîner des interruptions de service pour les clients qui communiquent avec le nœud.

   - Sélectionnez le bouton **Approve All** pour ajouter tous les nœuds de stockage à la file d'attente de mise à niveau de SANtricity OS.

Si l'ordre dans lequel les nœuds sont mis à niveau est important, approuvez les nœuds ou les groupes de nœuds un par un et attendez que la mise à niveau soit terminée sur chaque nœud avant d'approuver le nœud suivant.

- Sélectionnez un ou plusieurs boutons **Approve** pour ajouter un ou plusieurs nœuds à la file d'attente de mise à niveau de SANtricity OS. Le bouton **Approve** est désactivé si l'état n'est pas nominal.

  Après avoir sélectionné **Approve**, le processus de mise à niveau détermine si le noeud peut être mis à niveau. Si un nœud peut être mis à niveau, il est ajouté à la file d'attente de mise à niveau.

Pour certains noeuds, le fichier de mise à niveau sélectionné n'est pas appliqué intentionnellement et vous pouvez terminer le processus de mise à niveau sans mettre à niveau ces noeuds spécifiques. Les nœuds volontairement non mis à niveau affichent une étape terminée (tentative de mise à niveau) et indiquent la raison pour laquelle le nœud n'a pas été mis à niveau dans la colonne Détails.

10. Si vous devez supprimer un nœud ou tous les nœuds de la file d'attente de mise à niveau de SANtricity OS, sélectionnez **Supprimer** ou **tout supprimer**.

    Lorsque l'étape dépasse la mise en file d'attente, le bouton **Supprimer** est masqué et vous ne pouvez plus supprimer le nœud du processus de mise à niveau de SANtricity OS.

11. Attendez que la mise à niveau de SANtricity OS soit appliquée à chaque nœud de grid approuvé.

    - Si un nœud affiche une étape d'erreur alors que la mise à niveau de SANtricity OS est appliquée, la mise à niveau a échoué pour le nœud. Avec l'aide du support technique, vous devrez peut-être placer l'appliance en mode maintenance pour la restaurer.
    - Si le firmware du nœud est trop ancien pour être mis à niveau avec le Gestionnaire de grille, le nœud affiche un stade d'erreur avec les détails que vous devez utiliser le mode de maintenance pour mettre à niveau SANtricity OS sur le nœud. Pour résoudre l'erreur, procédez comme suit :
      i. Utilisez le mode de maintenance pour mettre à niveau SANtricity OS sur le nœud qui affiche une étape d'erreur.
      ii. Utilisez Grid Manager pour redémarrer et terminer la mise à niveau de SANtricity OS.

    Une fois la mise à niveau du système d'exploitation SANtricity terminée sur tous les nœuds approuvés, le tableau de progression de la mise à niveau du système d'exploitation SANtricity se ferme et une bannière verte indique le nombre de nœuds mis à niveau, ainsi que la date et l'heure de fin de la mise à niveau.

12. Si un nœud ne peut pas être mis à niveau, notez la raison indiquée dans la colonne Détails et prenez l'action appropriée.

    La mise à niveau de SANtricity OS n'est terminée qu'une fois la mise à niveau de SANtricity OS approuvée sur tous les nœuds de stockage répertoriés.

Raison	Action recommandée
Le nœud de stockage a déjà été mis à niveau.	Aucune autre action n'est requise.
La mise à niveau de SANtricity OS n'est pas applicable à ce nœud.	Le nœud ne dispose d'aucun contrôleur de stockage qui peut être géré par le système StorageGRID. Terminez le processus de mise à niveau sans mettre à niveau le nœud affichant ce message.

Raison	Action recommandée
SANtricity OS fichier n'est pas compatible avec ce nœud.	Le nœud nécessite un fichier SANtricity OS différent de celui que vous avez sélectionné. Une fois la mise à niveau actuelle terminée, téléchargez le fichier SANtricity OS approprié pour le nœud et répétez le processus de mise à niveau.

13. Si vous souhaitez mettre fin à l'approbation des nœuds et revenir à la page SANtricity OS pour permettre le téléchargement d'un nouveau fichier SANtricity OS, procédez comme suit :
    a. Sélectionnez **Ignorer les nœuds et Terminer**.

       Un avertissement s'affiche vous demandant si vous êtes sûr de vouloir terminer le processus de mise à niveau sans mettre à niveau tous les nœuds applicables.

    b. Sélectionnez **OK** pour revenir à la page **SANtricity OS**.
    c. Lorsque vous êtes prêt à poursuivre l'approbation des nœuds, Téléchargez SANtricity OS pour redémarrer le processus de mise à niveau.

       Les nœuds déjà approuvés et mis à niveau sans erreur restent mis à niveau.

14. Répétez cette procédure de mise à niveau pour tous les nœuds dont la procédure de fin nécessite un fichier de mise à niveau SANtricity OS différent.

    Pour les nœuds avec un état de nécessite une intervention, utilisez le mode maintenance pour effectuer la mise à niveau.

Informations associées

"Matrice d'interopérabilité NetApp"

"Mettez à niveau SANtricity OS sur le contrôleur E2800 à l'aide du mode de maintenance"

Mettez à niveau SANtricity OS sur le contrôleur E2800 à l'aide du mode de maintenance

Pour les contrôleurs de stockage qui utilisent actuellement SANtricity OS antérieurs à la version 08.42.20.00 (11.42), vous devez utiliser la procédure du mode de maintenance pour appliquer une mise à niveau.

Avant de commencer

- Vous avez consulté le "Matrice d'interopérabilité NetApp (IMT)" Pour vérifier que la version de SANtricity OS utilisée pour la mise à niveau est compatible avec votre appliance.
- Vous devez placer le contrôleur E5700SG dans "mode maintenance", Qui interrompt la connexion au contrôleur E2800.

  Dans de rares cas, le fait de placer une appliance StorageGRID en mode de maintenance peut rendre l'appliance indisponible pour l'accès à distance.

Description de la tâche

Ne mettez pas à niveau le système d'exploitation SANtricity ou la NVSRAM du contrôleur E-Series sur plusieurs appliances StorageGRID à la fois.

La mise à niveau de plusieurs appliances StorageGRID peut entraîner une indisponibilité des données, en fonction du modèle de déploiement et des règles ILM.

Étapes

1. Vérifiez que l'appareil est dans "mode maintenance".
2. Depuis un ordinateur portable de service, accédez à SANtricity System Manager et connectez-vous.
3. Téléchargez le nouveau fichier du logiciel SANtricity OS et le fichier NVSRAM sur le client de gestion.

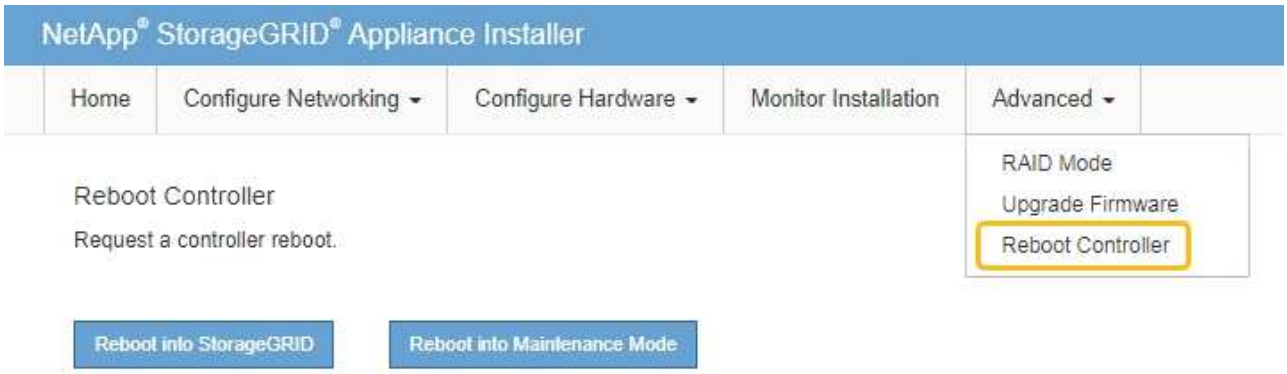
   La NVSRAM est spécifique à l'appliance StorageGRID. N'utilisez pas le téléchargement standard de NVSRAM.

4. Suivez les instructions du Guide de mise à niveau du firmware et du logiciel SANtricity _E2800 et E5700 ou de l'aide en ligne de SANtricity System Manager pour mettre à niveau le firmware et la NVSRAM du contrôleur E2800.

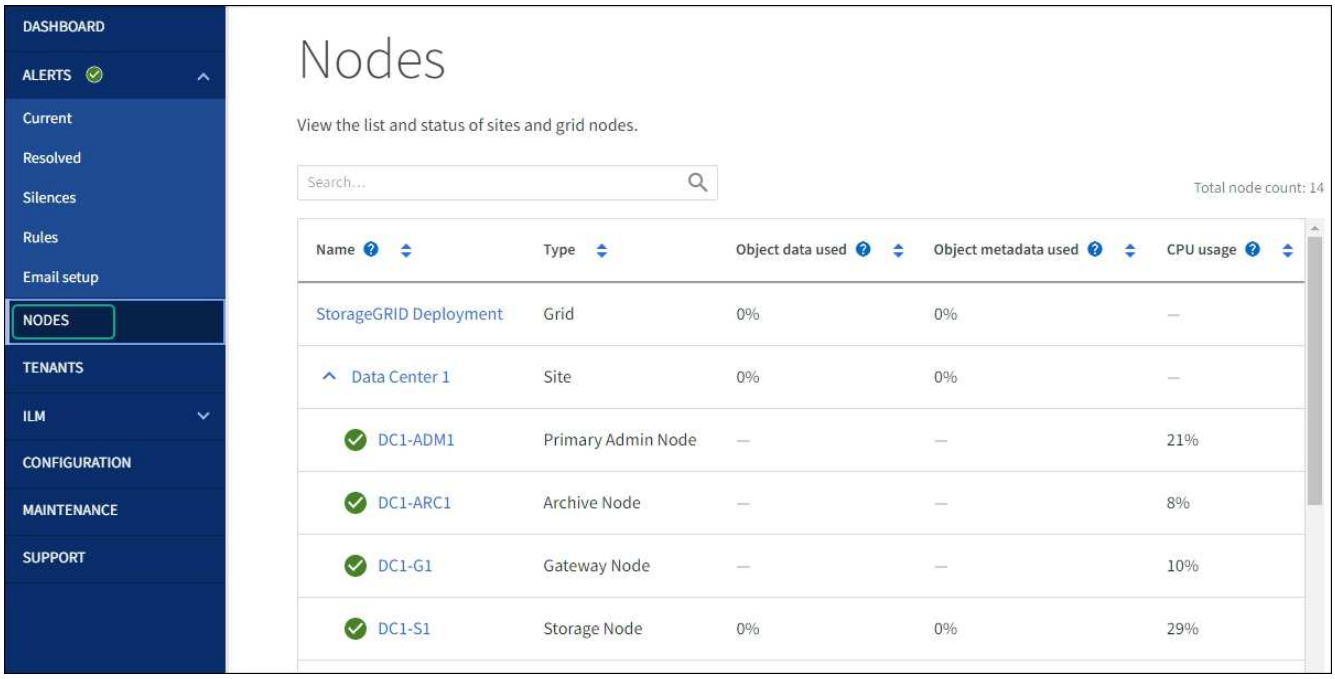
   Activez immédiatement les fichiers de mise à niveau. Ne différez pas l'activation.

5. Si cette procédure s'est terminée avec succès et que vous disposez de procédures supplémentaires pour effectuer cette opération pendant que le nœud est en mode de maintenance, effectuez-les maintenant. Lorsque vous avez terminé, ou si vous avez rencontré des échecs et souhaitez recommencer, sélectionnez **Avancé** > **redémarrer le contrôleur**, puis sélectionnez l'une des options suivantes :

   - Sélectionnez **redémarrer dans StorageGRID**
   - Sélectionnez **redémarrer en mode maintenance** pour redémarrer le contrôleur avec le nœud restant en mode de maintenance. Sélectionnez cette option si vous avez rencontré des échecs au cours de la procédure et souhaitez recommencer. Une fois le redémarrage du nœud en mode maintenance terminé, redémarrez à partir de l'étape appropriée de la procédure ayant échoué.



   L'appliance peut redémarrer et rejoindre la grille en 20 minutes. Pour confirmer que le redémarrage est terminé et que le nœud a rejoint la grille, retournez à la grille Manager. La page nœuds doit afficher un état normal (icône en forme de coche verte) à gauche du nom du nœud) pour le nœud de l'appliance, indiquant qu'aucune alerte n'est active et que le nœud est connecté à la grille.



Informations associées

"Mettez à niveau le système d'exploitation SANtricity sur les contrôleurs de stockage à l'aide de Grid Manager"

Mise à niveau du firmware des disques à l'aide de SANtricity System Manager

Mise à niveau du firmware du disque SG5700 avec la méthode en ligne de SANtricity System Manager

Utilisez la méthode en ligne du Gestionnaire système SANtricity pour mettre à niveau le firmware des disques de votre appliance et vous assurer que vous disposez des dernières fonctionnalités et des derniers correctifs.

Avant de commencer

- Le dispositif de stockage est à l'état optimal.
- Tous les disques ont un état optimal.

> Ne mettez pas à niveau le firmware du disque sur plusieurs appliances StorageGRID à la fois. Cela pourrait entraîner une indisponibilité des données, selon votre modèle de déploiement et votre politique ILM.

Description de la tâche

Les disques sont mis à niveau un par un pendant que l'appliance effectue des E/S. Cette méthode ne nécessite pas le passage de l'appareil en mode de maintenance. Cependant, les performances du système peuvent être affectées et la mise à niveau peut prendre plusieurs heures de plus que la méthode hors ligne.

> Les disques appartenant à des volumes qui ne sont pas redondants doivent être mis à jour à l'aide du "méthode hors ligne". La méthode offline doit être utilisée pour tout disque associé au cache de lecture Flash ou tout pool ou groupe de volumes actuellement dégradé.
> Vous devez utiliser le "méthode hors ligne" Lors de la mise à niveau des disques SSD.

Étapes

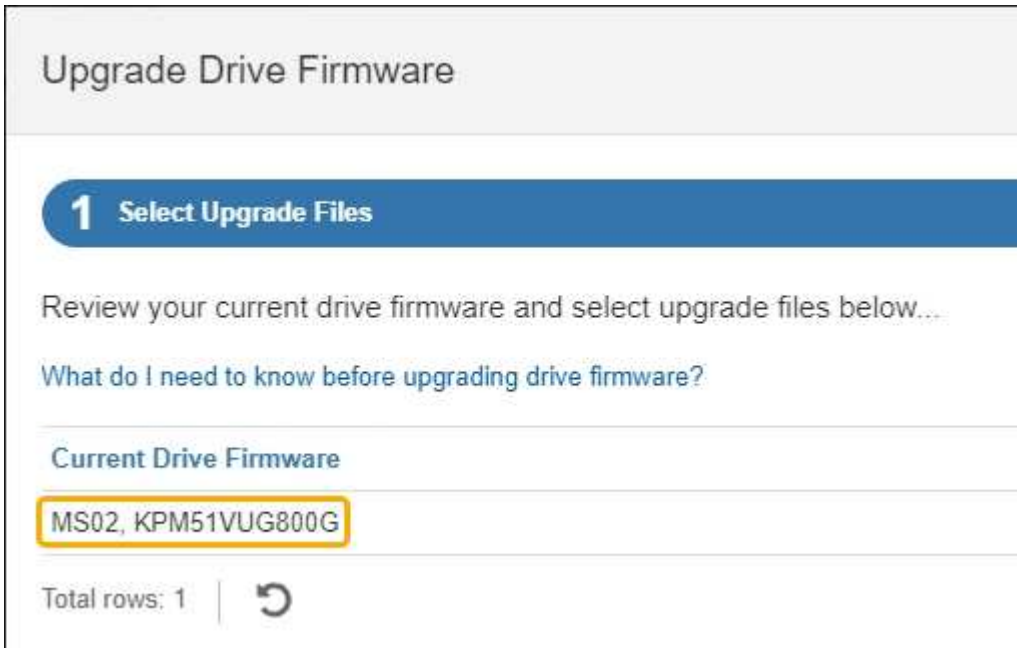
1. Pour accéder à SANtricity System Manager, utilisez l'une des méthodes suivantes :
   - Utilisez le programme d'installation de l'appliance StorageGRID et sélectionnez **Avancé** > **Gestionnaire système SANtricity**
   - Utilisez le Gestionnaire de grille et sélectionnez **NODES** > ***noeud de stockage*** > **Gestionnaire système SANtricity**
   - Pour utiliser SANtricity System Manager, accédez à l'adresse IP du contrôleur de stockage :

     `https://Storage_Controller_IP`

2. Entrez le nom d'utilisateur et le mot de passe de l'administrateur SANtricity System Manager si nécessaire.
3. Vérifiez la version du micrologiciel du lecteur actuellement installé sur l'appliance de stockage :
   a. Dans le Gestionnaire système SANtricity, sélectionnez **SUPPORT** > **Centre de mise à niveau**.
   b. Sous mise à niveau du micrologiciel du lecteur, sélectionnez **commencer la mise à niveau**.

      La page mettre à niveau le micrologiciel du lecteur affiche les fichiers du micrologiciel du lecteur actuellement installés.

   c. Notez les révisions actuelles du micrologiciel du lecteur et les identificateurs de lecteur dans la colonne micrologiciel du lecteur en cours.

      Dans cet exemple :

      - La version du micrologiciel du lecteur est **MS02**.
      - L'identifiant du lecteur est **KPM51VUG800G**.

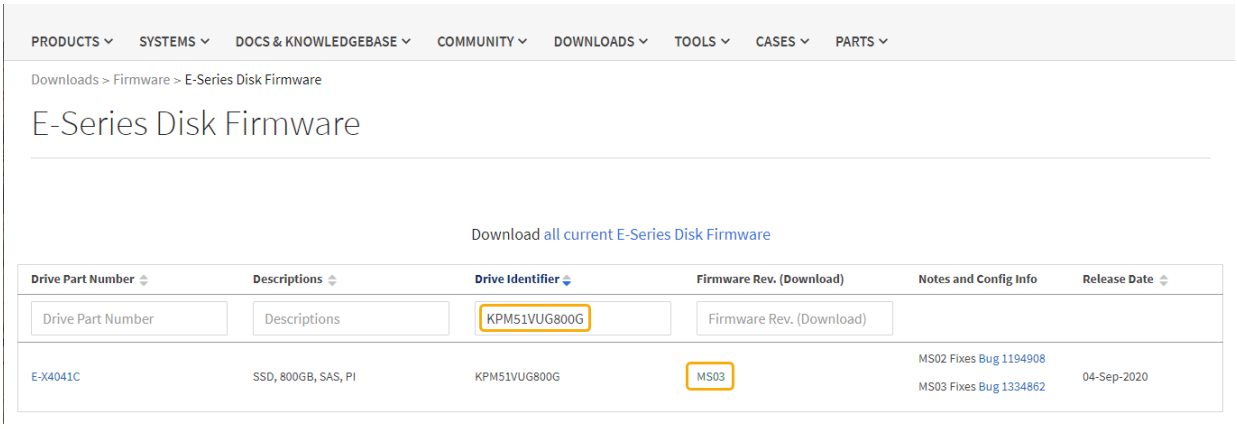
   d. Sélectionnez **Afficher les lecteurs** dans la colonne lecteurs associés pour afficher l'emplacement d'installation de ces lecteurs dans votre appliance de stockage.
   e. Fermez la fenêtre mise à niveau du micrologiciel du lecteur.
4. Téléchargez et préparez la mise à niveau disponible du firmware des disques :
   a. Sous mise à niveau du micrologiciel des disques, sélectionnez **NetApp support**.

b. Sur le site de support NetApp, sélectionnez l'onglet **Téléchargements**, puis sélectionnez **micrologiciel de lecteur de disque E-Series**.

   La page firmware des disques E-Series s'affiche.

c. Recherchez chaque **Drive identifier** installé dans votre appliance de stockage et vérifiez que chaque identificateur de lecteur dispose de la dernière révision du micrologiciel.

   - Si la révision du micrologiciel n'est pas un lien, cet identificateur de lecteur a la dernière révision du micrologiciel.
   - Si un ou plusieurs numéros de référence de lecteur sont répertoriés pour un identificateur de lecteur, une mise à niveau du micrologiciel est disponible pour ces lecteurs. Vous pouvez sélectionner n'importe quel lien pour télécharger le fichier de micrologiciel.



d. Si une version ultérieure du micrologiciel est répertoriée, sélectionnez le lien dans la révision du micrologiciel (Télécharger) pour télécharger un `.zip` archive contenant le fichier du micrologiciel.

e. Extrayez (décompressez le fichier d'archive du micrologiciel du lecteur que vous avez téléchargé sur le site de support.

5. Installez la mise à niveau du micrologiciel du lecteur :

   a. Dans le Gestionnaire système SANtricity, sous mise à niveau du micrologiciel du lecteur, sélectionnez **commencer la mise à niveau**.

   b. Sélectionnez **Browse**, puis sélectionnez les nouveaux fichiers de micrologiciel de lecteur que vous avez téléchargés à partir du site de support.

      Les fichiers du micrologiciel du lecteur ont un nom de fichier similaire à `D_HUC101212CSS600_30602291_MS01_2800_0002.dlp`.

      Vous pouvez sélectionner jusqu'à quatre fichiers de micrologiciel de lecteur, un par un. Si plusieurs fichiers de micrologiciel de lecteur sont compatibles avec le même lecteur, vous obtenez une erreur de conflit de fichier. Choisissez le fichier de micrologiciel de lecteur que vous souhaitez utiliser pour la mise à niveau et supprimez l'autre.

   c. Sélectionnez **Suivant**.

      Sélectionner les lecteurs répertorie les lecteurs que vous pouvez mettre à niveau avec les fichiers de micrologiciel sélectionnés.

      Seuls les lecteurs compatibles apparaissent.

Le micrologiciel sélectionné pour le lecteur apparaît dans la colonne **micrologiciel proposé**. Si vous devez modifier ce micrologiciel, sélectionnez **Retour**.

d. Sélectionnez **mettre à niveau tous les lecteurs en ligne** — met à niveau les lecteurs qui peuvent prendre en charge le téléchargement du micrologiciel pendant que la matrice de stockage traite les E/S. Lorsque vous sélectionnez cette méthode de mise à niveau, vous n'avez pas besoin d'arrêter les E/S sur les volumes associés utilisant ces disques.

> Une mise à niveau en ligne peut prendre plusieurs heures de plus qu'une mise à niveau hors ligne.

e. Dans la première colonne du tableau, sélectionnez le ou les lecteurs que vous souhaitez mettre à niveau.

La meilleure pratique consiste à mettre à niveau tous les lecteurs du même modèle vers la même révision du micrologiciel.

f. Sélectionnez **Démarrer** et confirmez que vous souhaitez effectuer la mise à niveau.

Si vous devez arrêter la mise à niveau, sélectionnez **Stop**. Tous les téléchargements de micrologiciel en cours sont terminés. Tous les téléchargements de micrologiciel qui n'ont pas démarré sont annulés.

> L'arrêt de la mise à niveau du micrologiciel du lecteur peut entraîner une perte de données ou l'indisponibilité des disques.

g. (Facultatif) pour afficher la liste des mises à niveau, sélectionnez **Enregistrer le journal**.

Le fichier journal est enregistré dans le dossier des téléchargements de votre navigateur portant le nom `latest-upgrade-log-timestamp.txt`.

"Si nécessaire, dépannez les erreurs de mise à niveau du micrologiciel du pilote".

Mise à niveau du firmware du disque SG5700 à l'aide de SANtricity System Manager via la méthode hors ligne

Utilisez la méthode en ligne du Gestionnaire système SANtricity pour mettre à niveau le firmware des disques de votre appliance et vous assurer que vous disposez des dernières fonctionnalités et des derniers correctifs.

Avant de commencer

- Le dispositif de stockage est à l'état optimal.
- Tous les disques ont un état optimal.
- Vous avez "Mettez l'appliance StorageGRID en mode de maintenance - effectué".

> Lorsque l'appliance est en mode de maintenance, les opérations d'E/S (entrée/sortie) vers le contrôleur de stockage sont arrêtées pour la sécurité des interruptions.

Ne mettez pas à niveau le firmware du disque sur plusieurs appliances StorageGRID à la fois. Cela pourrait entraîner une indisponibilité des données, selon votre modèle de déploiement et votre politique ILM.

Description de la tâche

Les disques sont mis à niveau en parallèle lorsque l'appliance est en mode de maintenance. Si le pool ou le groupe de volumes ne prend pas en charge la redondance ou est dégradé, vous devez utiliser la méthode hors ligne pour mettre à niveau le micrologiciel du lecteur. Vous devez également utiliser la méthode offline pour tout disque associé au cache de lecture Flash ou tout pool ou groupe de volumes actuellement dégradé. La méthode hors ligne met à niveau le micrologiciel uniquement lorsque toutes les activités d'E/S sont arrêtées sur les disques à mettre à niveau. Pour arrêter les E/S, placez le nœud en mode de maintenance.

La méthode hors ligne est plus rapide que la méthode en ligne et sera beaucoup plus rapide lorsque de nombreux lecteurs d'une seule appliance auront besoin de mises à niveau. Cependant, il requiert la mise hors service des nœuds. Cela peut nécessiter la planification d'une fenêtre de maintenance et le suivi de l'avancement. Choisissez la méthode la mieux adaptée à vos procédures opérationnelles et le nombre de lecteurs à mettre à niveau.

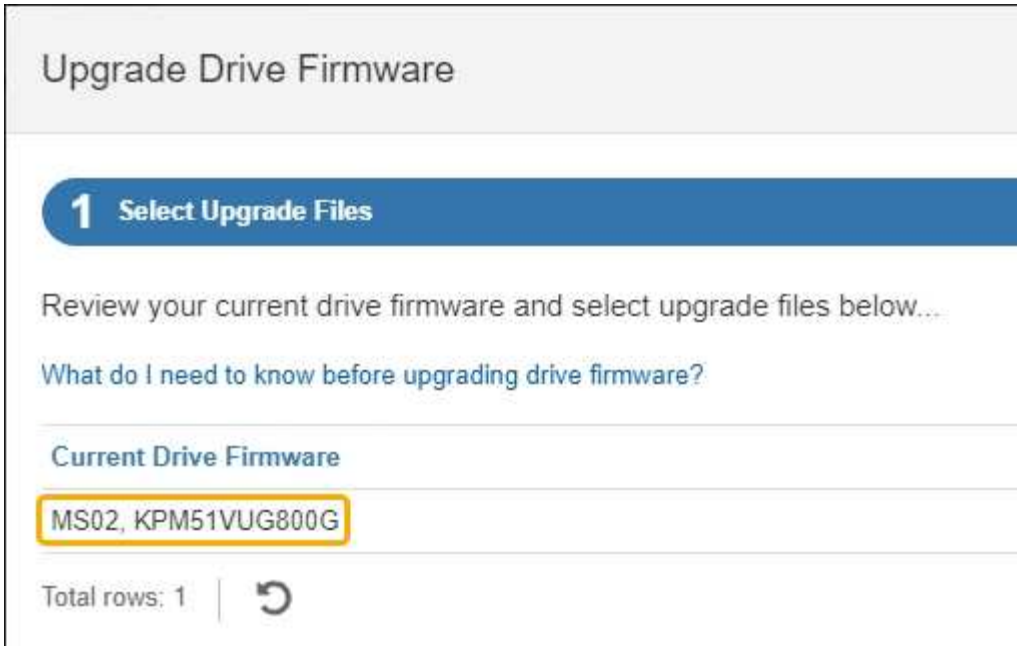
Étapes

1. Vérifiez que l'appareil est dans "mode maintenance".
2. Pour accéder à SANtricity System Manager, utilisez l'une des méthodes suivantes :
   - Utilisez le programme d'installation de l'appliance StorageGRID et sélectionnez **Avancé** > **Gestionnaire système SANtricity**
   - Utilisez le Gestionnaire de grille et sélectionnez **NODES** > ***noeud de stockage*** > **Gestionnaire système SANtricity**
   - Pour utiliser SANtricity System Manager, accédez à l'adresse IP du contrôleur de stockage :

     `https://Storage_Controller_IP`
3. Entrez le nom d'utilisateur et le mot de passe de l'administrateur SANtricity System Manager si nécessaire.
4. Vérifiez la version du micrologiciel du lecteur actuellement installé sur l'appliance de stockage :
   a. Dans le Gestionnaire système SANtricity, sélectionnez **SUPPORT** > **Centre de mise à niveau**.
   b. Sous mise à niveau du micrologiciel du lecteur, sélectionnez **commencer la mise à niveau**.

      La page mettre à niveau le micrologiciel du lecteur affiche les fichiers du micrologiciel du lecteur actuellement installés.

   c. Notez les révisions actuelles du micrologiciel du lecteur et les identificateurs de lecteur dans la colonne micrologiciel du lecteur en cours.



Dans cet exemple :

- La version du micrologiciel du lecteur est **MS02**.
- L'identifiant du lecteur est **KPM51VUG800G**.

d. Sélectionnez **Afficher les lecteurs** dans la colonne lecteurs associés pour afficher l'emplacement d'installation de ces lecteurs dans votre appliance de stockage.

e. Fermez la fenêtre mise à niveau du micrologiciel du lecteur.

5. Téléchargez et préparez la mise à niveau disponible du firmware des disques :

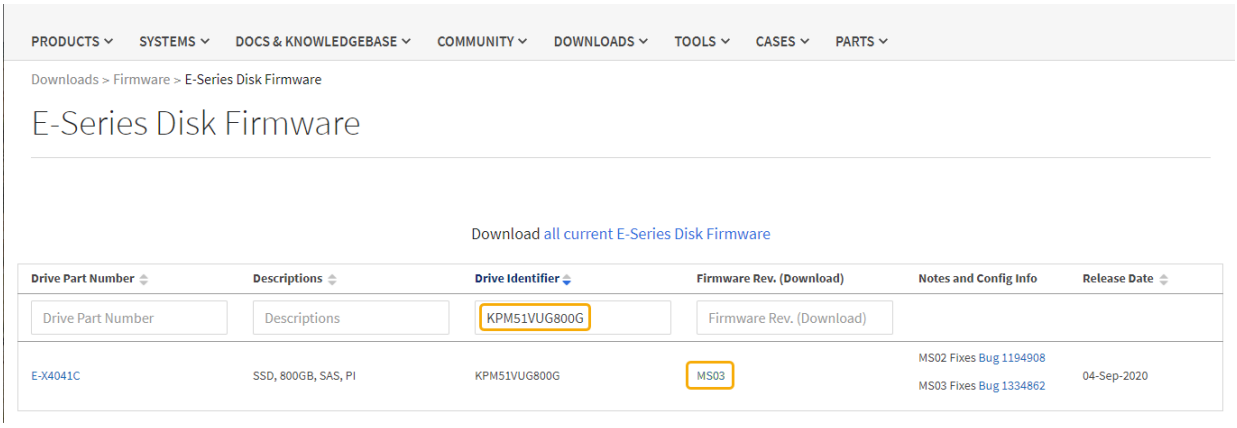
a. Sous mise à niveau du micrologiciel des disques, sélectionnez **NetApp support**.

b. Sur le site de support NetApp, sélectionnez l'onglet **Téléchargements**, puis sélectionnez **micrologiciel de lecteur de disque E-Series**.

La page firmware des disques E-Series s'affiche.

c. Recherchez chaque **Drive identifier** installé dans votre appliance de stockage et vérifiez que chaque identificateur de lecteur dispose de la dernière révision du micrologiciel.

- Si la révision du micrologiciel n'est pas un lien, cet identificateur de lecteur a la dernière révision du micrologiciel.
- Si un ou plusieurs numéros de référence de lecteur sont répertoriés pour un identificateur de lecteur, une mise à niveau du micrologiciel est disponible pour ces lecteurs. Vous pouvez sélectionner n'importe quel lien pour télécharger le fichier de micrologiciel.



d. Si une version ultérieure du micrologiciel est répertoriée, sélectionnez le lien dans la révision du micrologiciel (Télécharger) pour télécharger un `.zip` archive contenant le fichier du micrologiciel.

e. Extrayez (décompressez le fichier d'archive du micrologiciel du lecteur que vous avez téléchargé sur le site de support.

6. Installez la mise à niveau du micrologiciel du lecteur :

a. Dans le Gestionnaire système SANtricity, sous mise à niveau du micrologiciel du lecteur, sélectionnez **commencer la mise à niveau**.

b. Sélectionnez **Browse**, puis sélectionnez les nouveaux fichiers de micrologiciel de lecteur que vous avez téléchargés à partir du site de support.

Les fichiers du micrologiciel du lecteur ont un nom de fichier similaire à `D_HUC101212CSS600_30602291_MS01_2800_0002.dlp`.

Vous pouvez sélectionner jusqu'à quatre fichiers de micrologiciel de lecteur, un par un. Si plusieurs fichiers de micrologiciel de lecteur sont compatibles avec le même lecteur, vous obtenez une erreur de conflit de fichier. Choisissez le fichier de micrologiciel de lecteur que vous souhaitez utiliser pour la mise à niveau et supprimez l'autre.

c. Sélectionnez **Suivant**.

Sélectionner les lecteurs répertorie les lecteurs que vous pouvez mettre à niveau avec les fichiers de micrologiciel sélectionnés.

Seuls les lecteurs compatibles apparaissent.

Le micrologiciel sélectionné pour le lecteur apparaît dans la colonne **micrologiciel proposé**. Si vous devez modifier ce micrologiciel, sélectionnez **Retour**.

d. Sélectionnez **mettre à niveau tous les lecteurs hors ligne (parallèle)** — met à niveau les lecteurs qui peuvent prendre en charge un téléchargement de micrologiciel uniquement lorsque toutes les activités d'E/S sont arrêtées sur tous les volumes qui utilisent les lecteurs.

Vous devez mettre l'appareil en mode maintenance avant d'utiliser cette méthode. Vous devez utiliser la méthode **Offline** pour mettre à niveau le micrologiciel du lecteur.

Si vous souhaitez utiliser la mise à niveau hors ligne (parallèle), ne continuez pas, sauf si vous êtes certain que l'appliance est en mode de maintenance. Si vous ne mettez pas l'appliance en mode de maintenance avant d'effectuer une mise à jour hors ligne du firmware des disques, vous risquez de perdre des données.

e. Dans la première colonne du tableau, sélectionnez le ou les lecteurs que vous souhaitez mettre à niveau.

   La meilleure pratique consiste à mettre à niveau tous les lecteurs du même modèle vers la même révision du micrologiciel.

f. Sélectionnez **Démarrer** et confirmez que vous souhaitez effectuer la mise à niveau.

   Si vous devez arrêter la mise à niveau, sélectionnez **Stop**. Tous les téléchargements de micrologiciel en cours sont terminés. Tous les téléchargements de micrologiciel qui n'ont pas démarré sont annulés.

   L'arrêt de la mise à niveau du micrologiciel du lecteur peut entraîner une perte de données ou l'indisponibilité des disques.

g. (Facultatif) pour afficher la liste des mises à niveau, sélectionnez **Enregistrer le journal**.

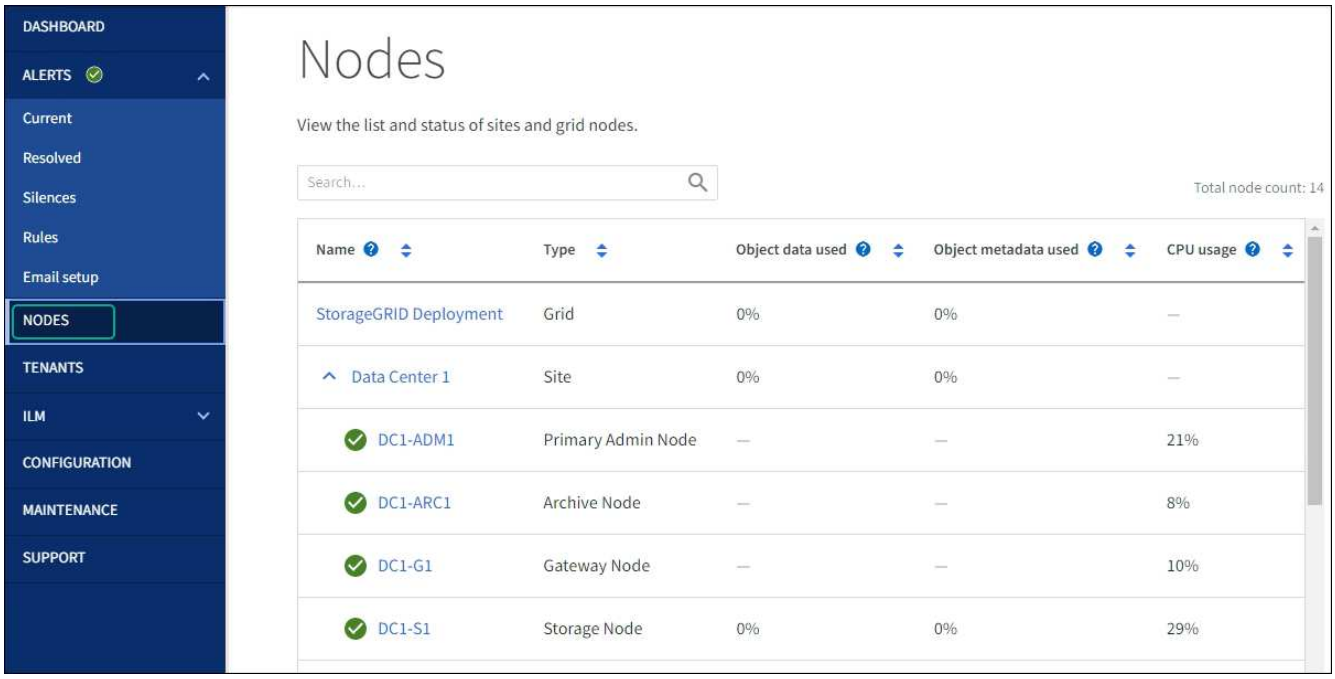
   Le fichier journal est enregistré dans le dossier des téléchargements de votre navigateur portant le nom `latest-upgrade-log-timestamp.txt`.

"Si nécessaire, dépannez les erreurs de mise à niveau du micrologiciel du pilote".

7. Une fois la procédure terminée, effectuez les éventuelles procédures de maintenance supplémentaires lorsque le nœud est en mode maintenance. Lorsque vous avez terminé, ou si vous avez rencontré des défaillances et que vous souhaitez recommencer, accédez au programme d'installation de l'appliance StorageGRID et sélectionnez **Avancé** > **redémarrer le contrôleur**. Sélectionnez ensuite l'une des options suivantes :

   - **Redémarrer dans StorageGRID**.
   - **Redémarrer en mode Maintenance**. Redémarrez le contrôleur et laissez le nœud en mode de maintenance. Sélectionnez cette option si des échecs se sont produits au cours de la procédure et que vous souhaitez recommencer. Une fois le redémarrage du nœud en mode maintenance terminé, redémarrez à partir de l'étape appropriée de la procédure ayant échoué.

     L'appliance peut redémarrer et rejoindre la grille en 20 minutes. Pour confirmer que le redémarrage est terminé et que le nœud a rejoint la grille, retournez à la grille Manager. La page nœuds doit afficher un état normal (icône en forme de coche verte) à gauche du nom du nœud) pour le nœud de l'appliance, indiquant qu'aucune alerte n'est active et que le nœud est connecté à la grille.



Dépannez les erreurs de mise à niveau du firmware des disques

Résolvez les erreurs qui peuvent se produire lorsque vous utilisez SANtricity System Manager pour mettre à niveau le firmware des disques de votre appliance.

- **Disques affectés en échec**
  - L'une des raisons de la défaillance est que le lecteur ne possède pas la signature appropriée. Assurez-vous que le disque concerné est un disque autorisé. Contactez le support technique pour plus d'informations.
  - Lorsque vous remplacez un lecteur, assurez-vous que sa capacité est supérieure ou égale à celle du lecteur défectueux que vous remplacez.
  - Vous pouvez remplacer le disque défectueux alors que la matrice de stockage reçoit des E/S.
- **Vérifier la matrice de stockage**
  - Assurez-vous qu'une adresse IP a été attribuée à chaque contrôleur.
  - Assurez-vous que tous les câbles connectés au contrôleur ne sont pas endommagés.
  - Assurez-vous que tous les câbles sont bien connectés.
- **Disques de secours intégrés**

  Ce problème d'erreur doit être corrigé avant de pouvoir mettre à niveau le micrologiciel.
- **Groupes de volumes incomplets**

  Si un ou plusieurs groupes de volumes ou pools de disques sont incomplets, vous devez corriger cette condition d'erreur avant de pouvoir mettre à niveau le micrologiciel.
- **Opérations exclusives (autres que l'analyse des supports/parité en arrière-plan) actuellement en cours d'exécution sur n'importe quel groupe de volumes**

  Si une ou plusieurs opérations exclusives sont en cours, les opérations doivent être effectuées avant la mise à niveau du micrologiciel. Utilisez System Manager pour surveiller la progression des opérations.

- **Volumes manquants**

  Vous devez corriger la condition de volume manquant avant de pouvoir mettre à niveau le micrologiciel.

- **L'un ou l'autre des contrôleurs dans un état autre que optimal**

  L'un des contrôleurs de la baie de stockage doit faire attention. Ce problème doit être résolu avant la mise à niveau du firmware.

- **Discordance des informations de partition de stockage entre les graphiques d'objet du contrôleur**

  Une erreur s'est produite lors de la validation des données sur les contrôleurs. Contactez le support technique pour résoudre ce problème.

- **Échec de la vérification du contrôleur de base de données SPM**

  Une erreur de mappage de la base de données de mappage des partitions de stockage s'est produite sur un contrôleur. Contactez le support technique pour résoudre ce problème.

- **Validation de la base de données de configuration (si prise en charge par la version du contrôleur de la matrice de stockage)**

  Une erreur de base de données de configuration s'est produite sur un contrôleur. Contactez le support technique pour résoudre ce problème.

- **Vérifications liées au MEL**

  Contactez le support technique pour résoudre ce problème.

- **Plus de 10 événements MEL informationnels ou critiques de la DDE ont été rapportés au cours des 7 derniers jours**

  Contactez le support technique pour résoudre ce problème.

- **Plus de 2 pages 2C des événements MEL critiques ont été rapportés au cours des 7 derniers jours**

  Contactez le support technique pour résoudre ce problème.

- **Plus de 2 événements MEL critiques de canal d'entraînement dégradés ont été signalés au cours des 7 derniers jours**

  Contactez le support technique pour résoudre ce problème.

- **Plus de 4 entrées MEL critiques au cours des 7 derniers jours**

  Contactez le support technique pour résoudre ce problème.

Modifier la configuration de liaison du contrôleur E5700SG

Vous pouvez modifier la configuration de la liaison Ethernet du contrôleur E5700SG. Vous pouvez modifier le mode de liaison du port, le mode de liaison réseau et la vitesse de liaison.

Avant de commencer

"Placez le contrôleur E5700SG en mode de maintenance".

> Dans de rares cas, le fait de placer une appliance StorageGRID en mode de maintenance peut rendre l'appliance indisponible pour l'accès à distance.

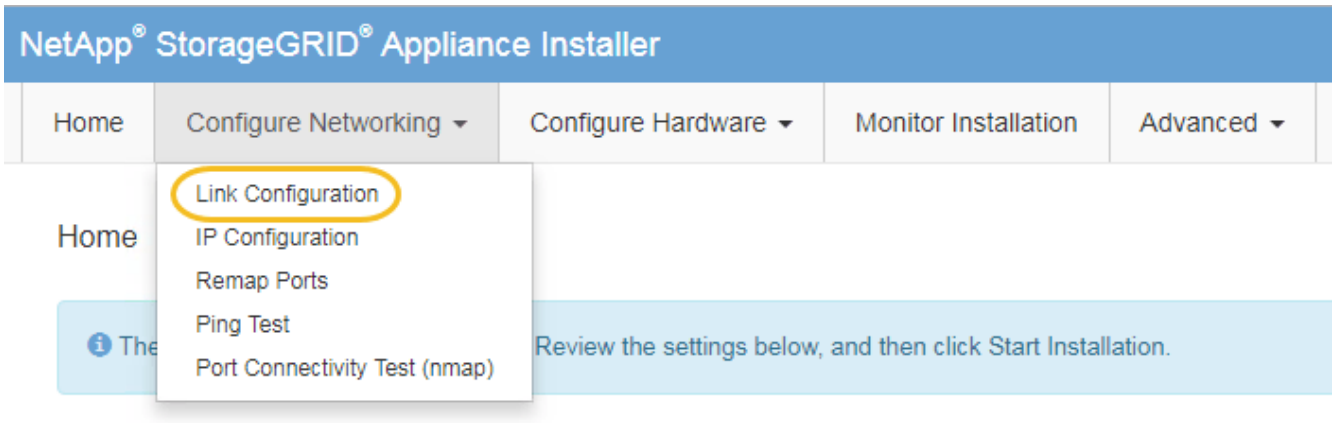
Description de la tâche

Les options permettant de modifier la configuration de la liaison Ethernet du contrôleur E5700SG sont les suivantes :

- Changement du mode **Port bond** de fixe à agrégé, ou d'agrégat à fixe
- Passage du mode de liaison réseau * d'Active-Backup à LACP, ou de LACP à Active-Backup
- Activation ou désactivation du balisage VLAN ou modification de la valeur d'une balise VLAN
- Modification de la vitesse de liaison de 10-GbE à 25-GbE, ou de 25-GbE à 10-GbE

Étapes

1. Sélectionnez **configurer réseau** > **Configuration lien** dans le menu.



2. apportez les modifications souhaitées à la configuration de liaison.

   Pour plus d'informations sur les options, reportez-vous à la section "Configurer les liaisons réseau".

3. Lorsque vous êtes satisfait de vos sélections, cliquez sur **Enregistrer**.

   > Vous risquez de perdre votre connexion si vous avez apporté des modifications au réseau ou au lien auquel vous êtes connecté. Si vous n'êtes pas reconnecté dans un délai d'une minute, saisissez à nouveau l'URL du programme d'installation de l'appliance StorageGRID à l'aide de l'une des autres adresses IP attribuées à l'appliance : `https://E5700SG_Controller_IP:8443`

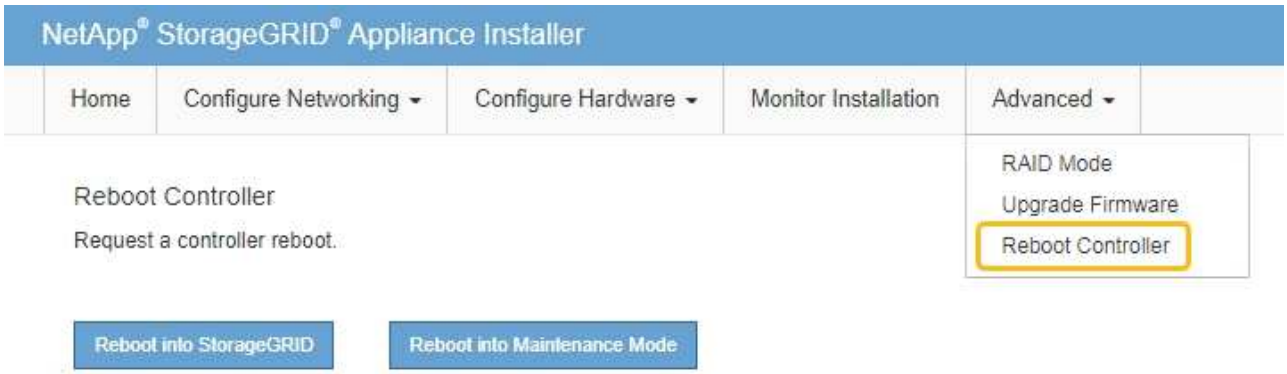
   Si vous avez modifié les paramètres VLAN, le sous-réseau de l'appliance a peut-être changé. Si vous devez modifier les adresses IP de l'appareil, suivez la "Configurez les adresses IP StorageGRID" instructions.

4. Dans le programme d'installation de l'appliance StorageGRID, sélectionnez **configurer le réseau** > **Test Ping**.
5. Utilisez l'outil Test Ping pour vérifier la connectivité aux adresses IP sur tous les réseaux susceptibles d'avoir été affectés par les modifications de configuration de liaison que vous avez effectuées dans Modifier la configuration du lien étape.

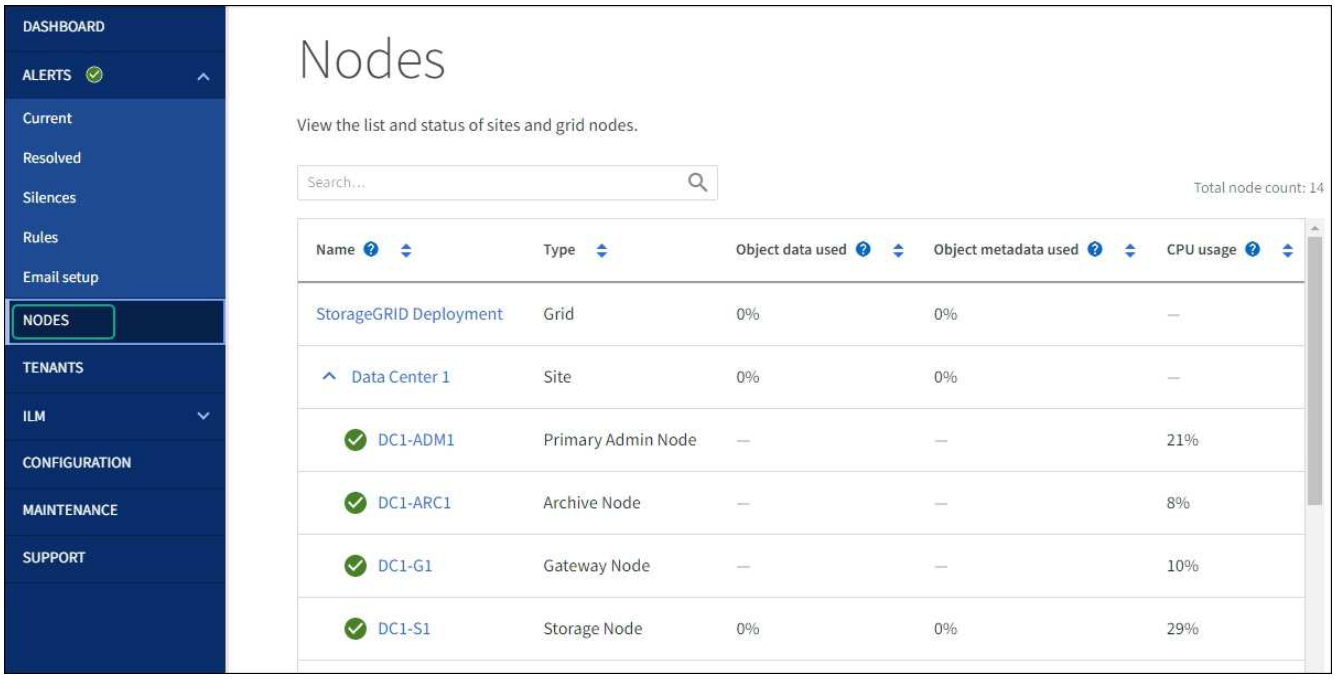
En plus des autres tests que vous choisissez d'effectuer, vérifiez que vous pouvez envoyer une commande ping à l'adresse IP de la grille du nœud d'administration principal et à l'adresse IP de la grille d'au moins un autre nœud de stockage. Si nécessaire, corrigez tout problème de configuration de liaison.

6. Une fois que vous êtes satisfait du fait que les modifications de configuration du lien fonctionnent, redémarrez le nœud. Dans le programme d'installation de l'appliance StorageGRID, sélectionnez **Avancé** > **redémarrer le contrôleur**, puis sélectionnez l'une des options suivantes :

   - Sélectionnez **Reboot dans StorageGRID** pour redémarrer le contrôleur avec le noeud qui rejoint la grille. Sélectionnez cette option si vous avez terminé de travailler en mode maintenance et que vous êtes prêt à rétablir le fonctionnement normal du nœud.
   - Sélectionnez **redémarrer en mode maintenance** pour redémarrer le contrôleur avec le nœud restant en mode de maintenance. (Cette option n'est disponible que lorsque le contrôleur est en mode de maintenance.) Sélectionnez cette option si des opérations de maintenance supplémentaires doivent être effectuées sur le nœud avant de rejoindre la grille.



L'appliance peut redémarrer et rejoindre la grille en 20 minutes. Pour confirmer que le redémarrage est terminé et que le nœud a rejoint la grille, retournez à la grille Manager. La page **NODES** doit afficher un état normal (icône de coche verte à gauche du nom du nœud) pour le nœud de l'appliance, indiquant qu'aucune alerte n'est active et que le nœud est connecté à la grille.



Procédures matérielles

Remplacement du contrôleur de stockage E2800 Series dans l'appliance SG5700

Vous devrez peut-être remplacer le contrôleur E2800 Series si ce dernier ne fonctionne pas de manière optimale ou en cas de défaillance.

Description de la tâche

- Vous disposez d'un contrôleur de remplacement avec la même référence que le contrôleur que vous remplacez.

> Ne vous fiez pas aux instructions E-Series pour remplacer un contrôleur de l'appliance StorageGRID, car les procédures ne sont pas identiques.

- Vous avez des étiquettes pour identifier chaque câble connecté au contrôleur.
- Si tous les lecteurs sont sécurisés, vous avez passé en revue les étapes de la section "Procédure de remplacement du contrôleur E2800 simplex", Ce qui inclut le téléchargement et l'installation de E-Series SANtricity System Manager à partir du site de support NetApp, puis l'utilisation de la fenêtre de gestion d'entreprise (EMW) pour déverrouiller les disques sécurisés après le remplacement du contrôleur.

> Vous ne pourrez pas utiliser l'appareil avant de déverrouiller les lecteurs à l'aide de la touche enregistrée.

- Vous devez disposer d'autorisations d'accès spécifiques.
- Vous devez être connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".

Description de la tâche

Vous pouvez déterminer si le boîtier de contrôleur est défectueux de deux façons :

- Il vous est alors dirigé vers le remplacement du contrôleur dans SANtricity System Manager.

- La LED d’avertissement orange située sur le contrôleur est allumée, ce qui indique que le contrôleur est en panne.

L’appliance Storage Node ne sera pas accessible lors du remplacement du contrôleur. Si le contrôleur E2800 fonctionne suffisamment, vous pouvez "Placez le contrôleur E5700SG en mode de maintenance".

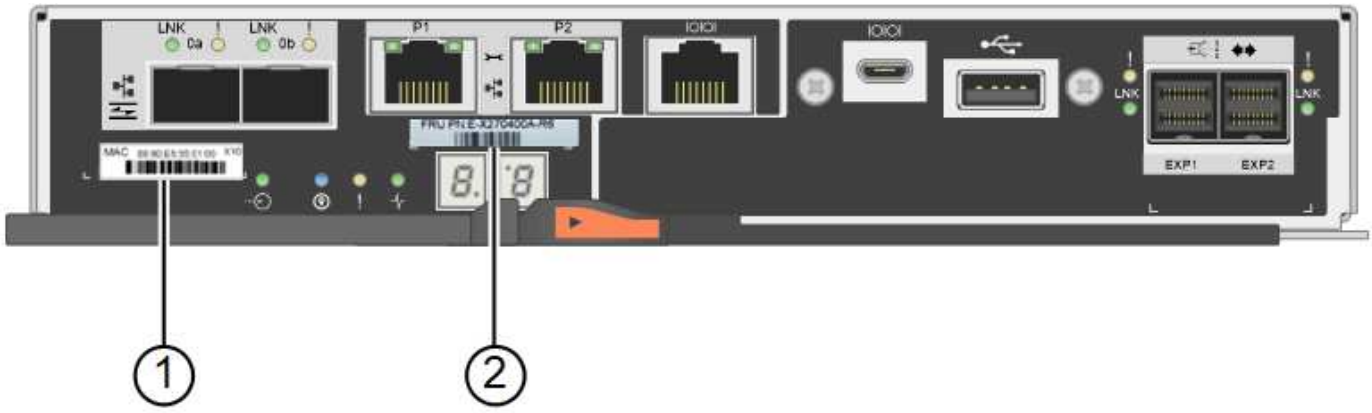
Lorsque vous remplacez un contrôleur, vous devez retirer la batterie du contrôleur d’origine et l’installer dans le contrôleur de remplacement. Dans certains cas, vous devrez également retirer la carte d’interface hôte du contrôleur d’origine et l’installer dans le contrôleur de remplacement.

Dans la plupart des modèles d’appliance, les contrôleurs de stockage n’incluent pas de cartes d’interface hôte (HIC).

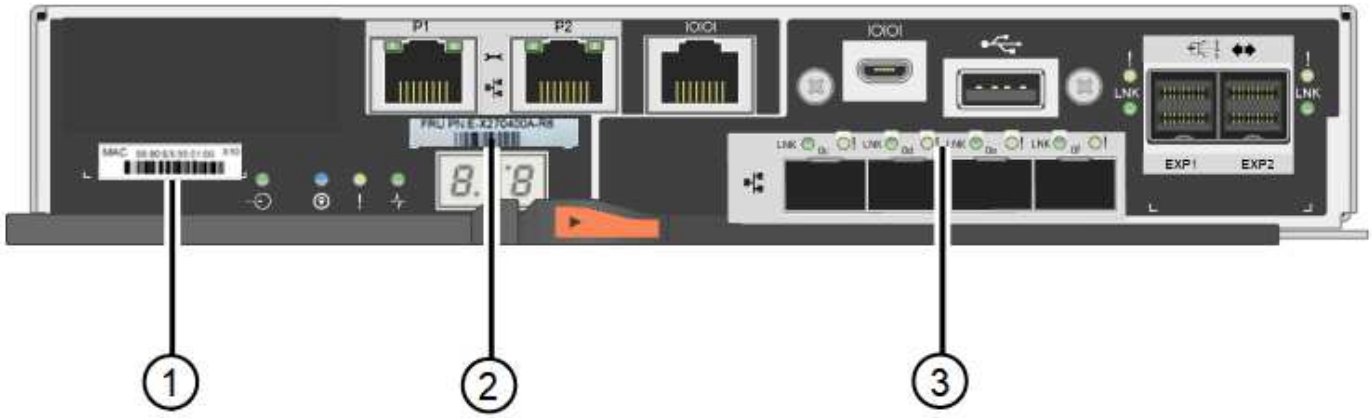
Étape 1 : préparation du retrait du contrôleur

Ces figures illustrent le contrôleur E2800A et le contrôleur E2800B. La procédure de remplacement des contrôleurs E2800 Series et du contrôleur EF570 est identique.

Contrôleur de stockage E2800A :



Contrôleur de stockage E2800B :



Étiquette	composant	Description
1	Adresse MAC	L'adresse MAC du port de gestion 1 (« P1 sur le E2800A et 0a sur le E2800B »). Si vous avez utilisé DHCP pour obtenir l'adresse IP du contrôleur d'origine, vous devez disposer de cette adresse pour vous connecter au nouveau contrôleur.
2	Référence de l'unité remplaçable sur site	Numéro de référence de l'unité remplaçable sur site. Ce numéro doit correspondre au numéro de référence de remplacement du contrôleur actuellement installé.
3	HIC 4 ports	La carte d'interface hôte 4 ports (HIC). Cette carte doit être déplacée vers le nouveau contrôleur lors du remplacement. **Remarque** : le contrôleur E2800A n'a pas de HIC.

Suivez les instructions de la procédure de remplacement du contrôleur E2800 pour préparer le retrait du contrôleur.

Ces étapes sont réalisées à l'aide de SANtricity System Manager.

Étapes

1. Notez la version du logiciel SANtricity OS actuellement installée sur le contrôleur.
2. Notez quelle version de NVSRAM est actuellement installée.
3. Si la fonction de sécurité du lecteur est activée, assurez-vous qu'une clé enregistrée existe et que vous connaissez la phrase de passe requise pour l'installer.

> **Perte possible de l'accès aux données et#8212;** si tous les lecteurs du dispositif sont activés pour la sécurité, le nouveau contrôleur ne pourra pas accéder au dispositif tant que vous ne pourrez pas déverrouiller les lecteurs sécurisés à l'aide de la fenêtre de gestion d'entreprise dans le Gestionnaire système SANtricity.

4. Sauvegardez la base de données de configuration.

   Si un problème survient lorsque vous supprimez un contrôleur, vous pouvez utiliser le fichier enregistré pour restaurer votre configuration.

5. Collecte des données d'assistance pour l'appareil.

> La collecte des données de support avant et après le remplacement d'un composant vous permet d'envoyer un ensemble complet de journaux au support technique si le remplacement ne résout pas le problème.

Étape 2 : mettre le contrôleur hors ligne

Mettre le contrôleur hors ligne et vérifier que toutes les opérations sont terminées.

Étapes

1. Si l'appliance StorageGRID s'exécute sur un système StorageGRID, "Placez le contrôleur E5700SG en mode de maintenance".

2. Si le contrôleur E2800 fonctionne suffisamment pour permettre un arrêt contrôlé, vérifiez que toutes les opérations sont terminées.
3. Dans la page d'accueil de SANtricity System Manager, sélectionnez **Afficher les opérations en cours**.
4. Confirmez que toutes les opérations ont été effectuées.
5. Met le tiroir contrôleur hors tension.

Étape 3 : retirez le contrôleur

Retirez le contrôleur de l'appareil.

Étapes

1. Placez un bracelet antistatique ou prenez d'autres précautions antistatiques.
2. Etiqueter les câbles puis débrancher les câbles et les SFP.

   Pour éviter toute dégradation des performances, ne tordez pas, ne pliez pas, ne pincez pas ou ne montez pas sur les câbles.

3. Libérez le contrôleur de l'appareil en appuyant sur le loquet de la poignée de came jusqu'à ce qu'il se relâche, puis ouvrez la poignée de came vers la droite.
4. A l'aide de deux mains et de la poignée de came, faites glisser le contrôleur hors de l'appareil.

   Toujours utiliser deux mains pour soutenir le poids du contrôleur.

5. Placez le contrôleur sur une surface plane et sans électricité statique, le capot amovible orienté vers le haut.
6. Retirez le capot en appuyant sur le bouton et en le faisant glisser hors du capot.

Étape 4 : déplacer la batterie vers le nouveau contrôleur

Retirez la batterie du contrôleur défectueux et installez-la dans le contrôleur de remplacement.

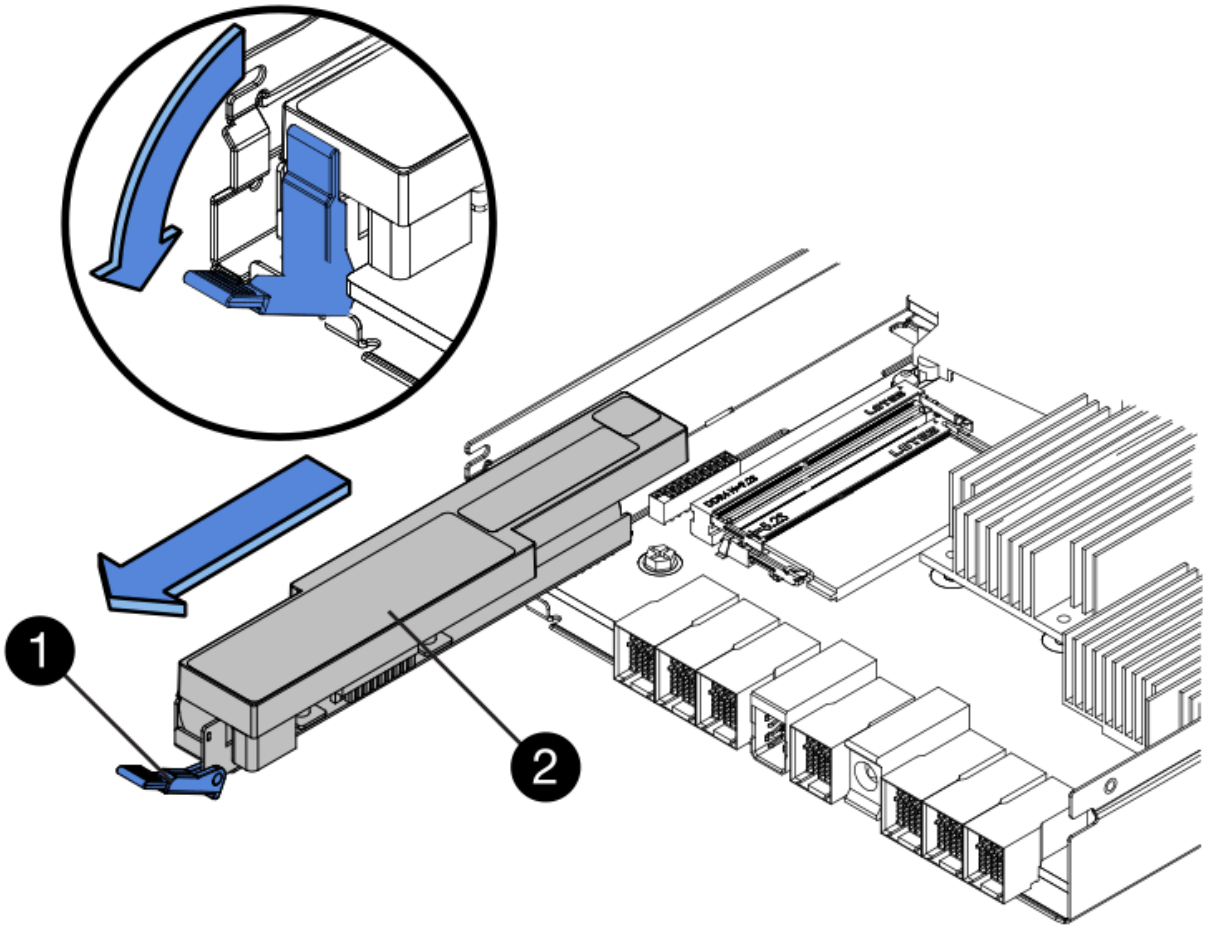
Étapes

1. Vérifiez que le voyant vert à l'intérieur du contrôleur (entre la batterie et les modules DIMM) est éteint.

   Si ce voyant vert est allumé, le contrôleur utilise toujours l'alimentation de la batterie. Vous devez attendre que ce voyant s'éteigne avant de retirer des composants.

Élément	Description
1	LED active du cache interne
2	Batterie

2. Repérez le loquet de dégagement bleu de la batterie.
3. Déverrouillez la batterie en appuyant sur le loquet de déverrouillage vers le bas et en l'éloignant du contrôleur.



Élément	Description
1	Loquet de déblocage de la batterie
2	Batterie

4. Soulevez la batterie et faites-la glisser hors du contrôleur.
5. Retirer le capot du contrôleur de remplacement.
6. Orientez le contrôleur de remplacement de manière à ce que le logement de la batterie soit orienté vers vous.
7. Insérez la batterie dans le contrôleur en l'inclinant légèrement vers le bas.

   Vous devez insérer la bride métallique située à l'avant de la batterie dans le logement situé en bas du contrôleur et faire glisser le haut de la batterie sous la petite goupille d'alignement située sur le côté gauche du contrôleur.

8. Déplacez le loquet de la batterie vers le haut pour fixer la batterie.

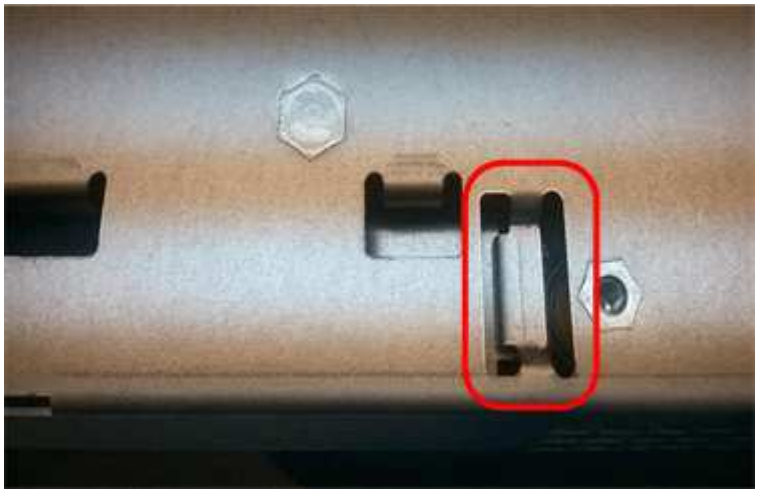
   Lorsque le loquet s'enclenche, le bas des crochets de verrouillage se trouve dans une fente métallique du châssis.

9. Retournez le contrôleur pour vérifier que la batterie est correctement installée.

> **Dommages matériels possibles** — la bride métallique à l'avant de la batterie doit être complètement insérée dans le logement du contrôleur (comme indiqué sur la première figure). Si la batterie n'est pas installée correctement (comme illustré sur la deuxième figure), la bride métallique peut entrer en contact avec la carte contrôleur, ce qui peut endommager la carte.

- **Correct — la bride métallique de la batterie est complètement insérée dans le logement du contrôleur:**

- **Incorrect — la bride métallique de la batterie n'est pas insérée dans le logement du contrôleur :**



10. Replacer le capot du contrôleur.

STEP5 : déplacer HIC vers le nouveau contrôleur, si nécessaire

Si le contrôleur défectueux est équipé d'une carte d'interface hôte (HIC), déplacez la carte HIC du contrôleur défectueux vers le contrôleur de remplacement.

Une HIC distincte est utilisée uniquement pour le contrôleur E2800B. La carte HIC est montée sur la carte contrôleur principale et comprend deux connecteurs SPF.

Les illustrations de cette procédure montrent une HIC 2 ports. La HIC de votre contrôleur peut avoir un nombre différent de ports.

E2800A

Un contrôleur E2800A ne possède pas de HIC.

Remettez le capot du contrôleur E2800A en place et passez à l'étape Étape 6 : remplacer le contrôleur

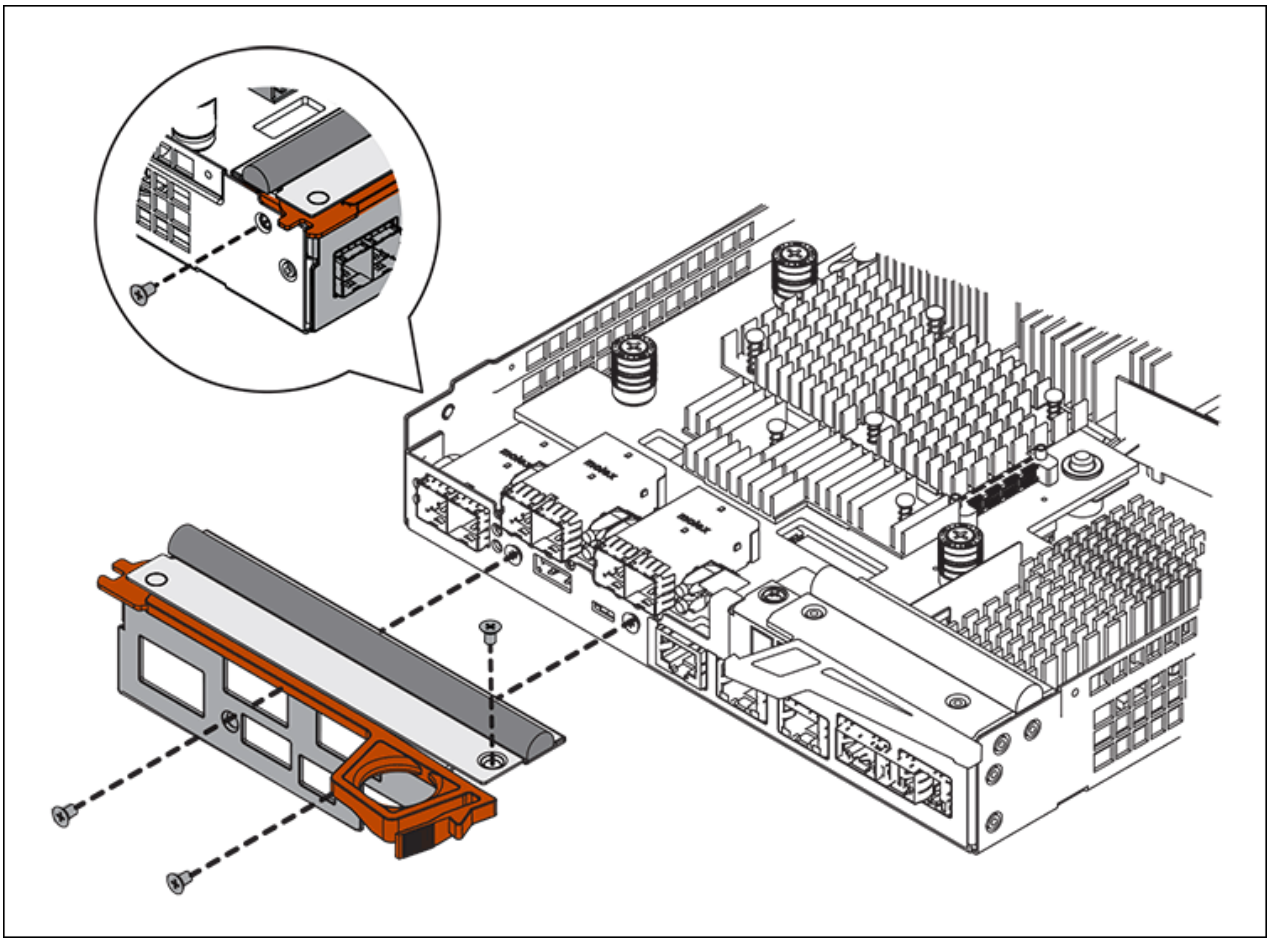
E2800B

Déplacez le HIC du contrôleur E2800B défectueux vers le contrôleur de remplacement.

Étapes

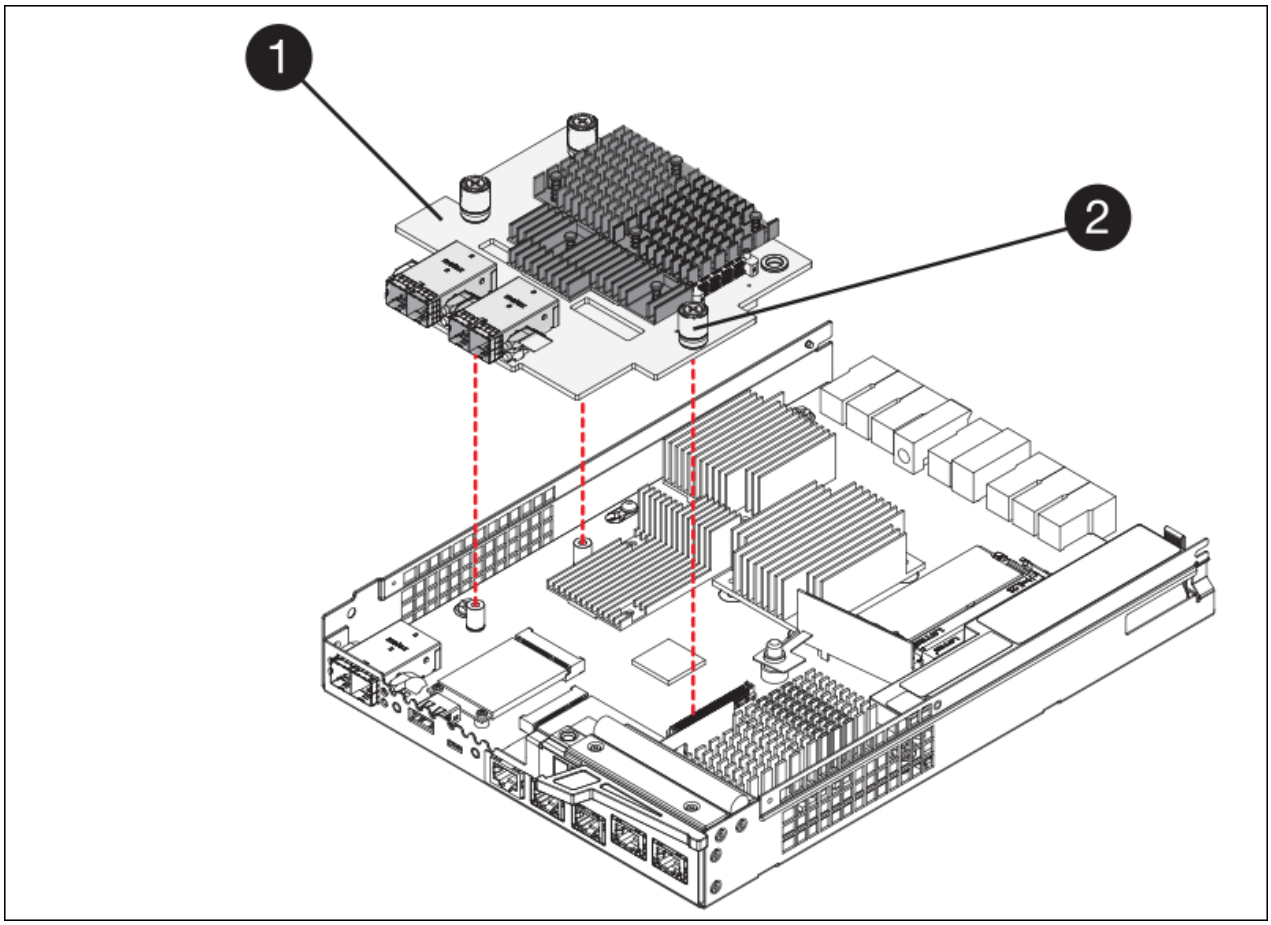
1. Supprimer tout SFP de la HIC.
2. À l'aide d'un tournevis cruciforme n° 1, retirez les vis qui fixent le cadran HIC au contrôleur.

   Il y a quatre vis : une sur le dessus, une sur le côté et deux sur l'avant.



3. Retirez la plaque HIC.
4. À l'aide de vos doigts ou d'un tournevis cruciforme, desserrez les trois vis à molette qui fixent le HIC à la carte contrôleur.
5. Détachez avec précaution la carte HIC de la carte contrôleur en la soulevant et en la faisant glisser vers l'arrière.

> Veillez à ne pas rayer ou heurter les composants au bas de la HIC ou au-dessus de la carte contrôleur.



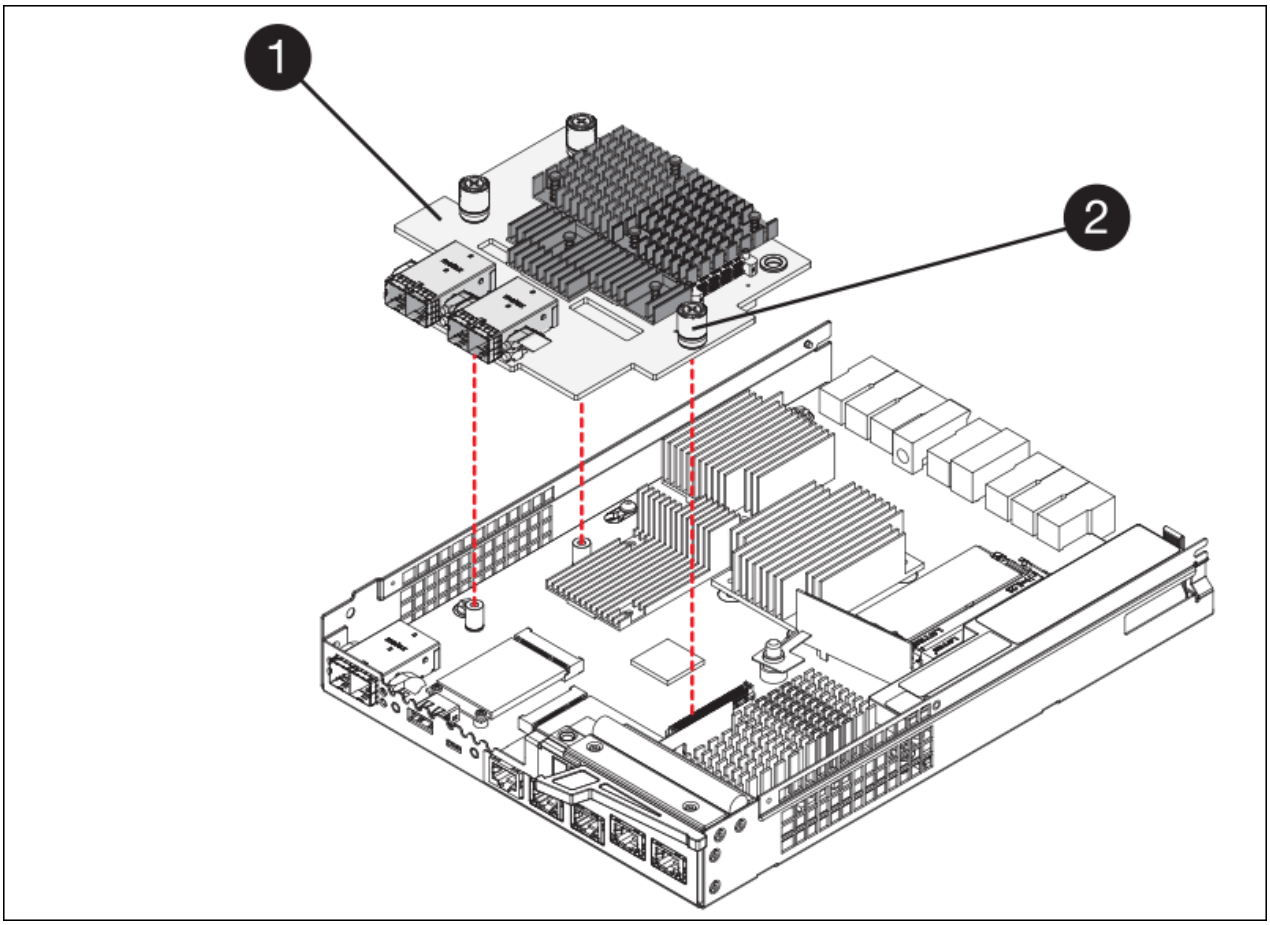
Étiquette	Description
1	Carte d'interface hôte
2	Vis moletées

6. Placez le HIC sur une surface antistatique.
7. À l'aide d'un tournevis cruciforme n° 1, retirez les quatre vis qui fixent le cache blanc au contrôleur de remplacement, puis retirez le cache.
8. Alignez les trois vis moletées de la HIC avec les trous correspondants du contrôleur de remplacement, puis alignez le connecteur situé au bas de la HIC avec le connecteur d'interface HIC de la carte contrôleur.

   Veillez à ne pas rayer ou heurter les composants au bas de la HIC ou au-dessus de la carte contrôleur.

9. Abaisser avec précaution la HIC et mettre le connecteur HIC en place en appuyant doucement sur la HIC.

Dommage possible de l'équipement — attention de ne pas pincer le connecteur ruban doré pour les voyants du contrôleur entre le HIC et les vis moletées.

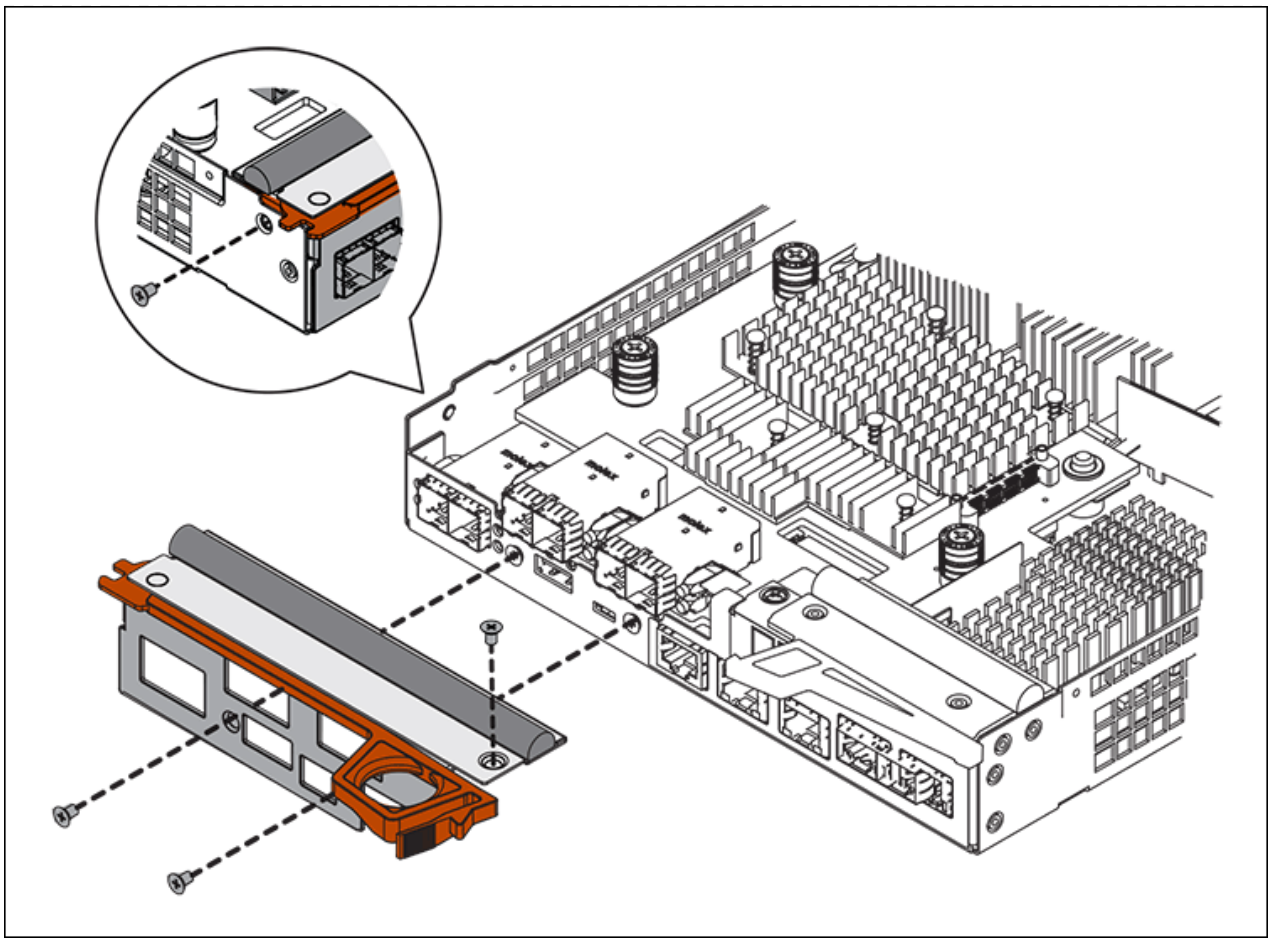


Étiquette	Description
1	Carte d'interface hôte
2	Vis moletées

10. Serrez les vis à molette HIC à la main.

    N'utilisez pas de tournevis, sinon vous risquez de trop serrer les vis.

11. À l'aide d'un tournevis cruciforme n° 1, fixez le cadran HIC retiré du contrôleur d'origine sur le nouveau contrôleur à l'aide de quatre vis.



12. Réinstallez tous les SFP retirés dans le HIC.

Étape 6 : remplacer le contrôleur

Installez le contrôleur de remplacement et vérifiez qu'il a rejoint la grille.

Étapes

1. Installez le contrôleur de remplacement sur l'appliance.
   a. Retournez le contrôleur pour que le capot amovible soit orienté vers le bas.
   b. Avec la poignée de came en position ouverte, faites glisser le contrôleur complètement dans l'appareil.
   c. Déplacez la poignée de came vers la gauche pour verrouiller le contrôleur en place.
   d. Remplacer les câbles et les SFP.
   e. Mettez le tiroir contrôleur sous tension.
   f. Attendez le redémarrage du contrôleur E2800. Vérifiez que l'affichage à sept segments indique l'état de `99`.
   g. Déterminez la manière dont vous allez attribuer une adresse IP au contrôleur de remplacement.

> Les étapes d'attribution d'une adresse IP au contrôleur de remplacement dépendent de la connexion du port de gestion 1 à un réseau avec un serveur DHCP et de la sécurité de tous les lecteurs.

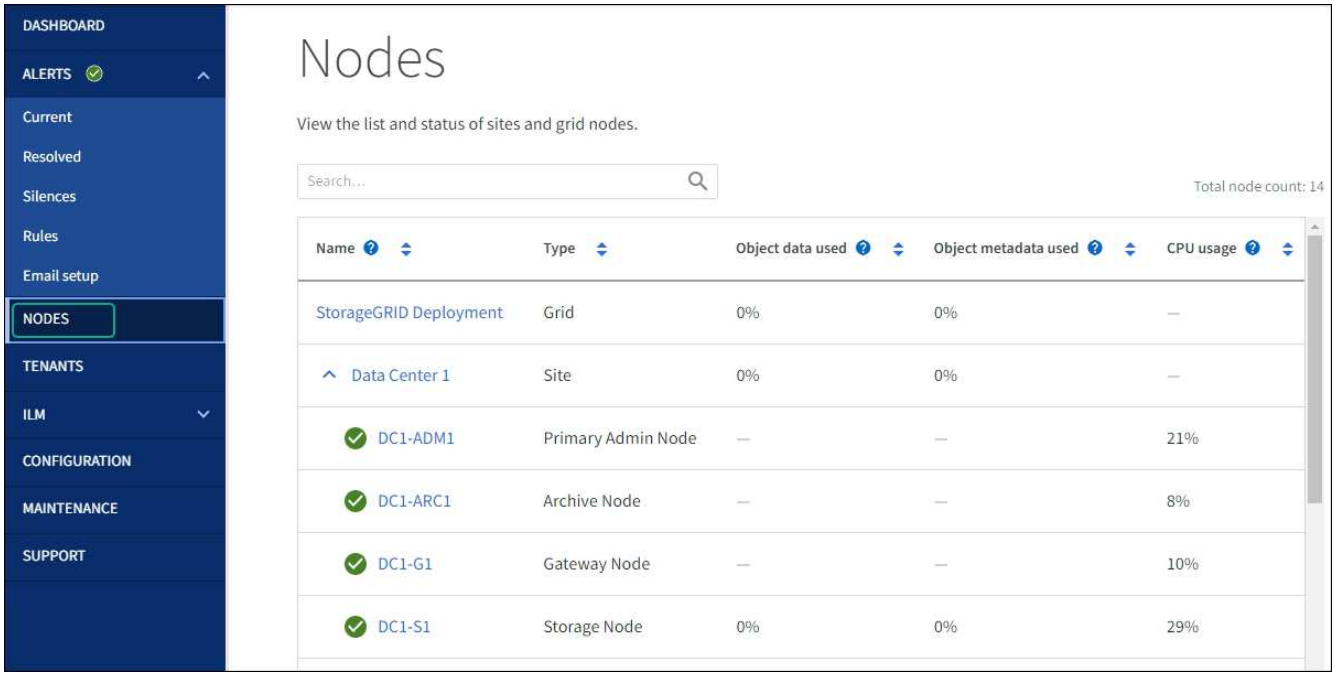
Si le port de gestion 1 est connecté à un réseau avec un serveur DHCP, le nouveau contrôleur obtient son adresse IP auprès du serveur DHCP. Cette valeur peut être différente de l'adresse IP du contrôleur d'origine.

2. Si l'appliance utilise des disques sécurisés, suivez les instructions de la procédure de remplacement du contrôleur E2800 pour importer la clé de sécurité du disque.
3. Ramenez l'appareil en mode de fonctionnement normal. Dans le programme d'installation de l'appliance StorageGRID, sélectionnez **Avancé** > **redémarrer le contrôleur**, puis sélectionnez **redémarrer dans StorageGRID**.

4. Durant le redémarrage, surveillez l'état du nœud pour déterminer quand il a rejoint la grille.

   L'appareil redémarre et rejoint la grille. Ce processus peut prendre jusqu'à 20 minutes.

5. Vérifiez que le redémarrage est terminé et que le nœud a rejoint à nouveau la grille. Dans le Gestionnaire de grille, vérifiez que la page nœuds affiche un état normal (icône avec une coche verte) à gauche du nom du nœud) pour le nœud de l'appliance, indiquant qu'aucune alerte n'est active et que le nœud est connecté à la grille.



6. Depuis SANtricity System Manager, confirmer que le nouveau contrôleur est optimal et collecter les données de support

Après le remplacement de la pièce, renvoyez la pièce défectueuse à NetApp, en suivant les instructions RMA (retour de matériel) livrées avec le kit. Voir la "Retour de pièce et amp ; remplacements" pour plus d'informations.

Informations associées

"Site de documentation sur les systèmes NetApp E-Series"

Remplacez le contrôleur de calcul E5700SG

Vous devrez peut-être remplacer le contrôleur E5700SG s'il ne fonctionne pas de manière optimale ou s'il est défectueux.

Avant de commencer

- Vous disposez d'un contrôleur de remplacement avec la même référence que le contrôleur que vous remplacez.
- Vous avez téléchargé les instructions du système E-Series pour remplacer un contrôleur E5700 défectueux.

> Utilisez les instructions E-Series à titre de référence uniquement si vous avez besoin de plus de détails pour effectuer une étape spécifique. Ne vous fiez pas aux instructions E-Series pour remplacer un contrôleur de l'appliance StorageGRID, car les procédures ne sont pas identiques. Par exemple, les instructions relatives à E-Series pour le contrôleur E5700 décrivent le retrait de la batterie et la carte d'interface hôte (HIC) d'un contrôleur défectueux et leur installation dans un contrôleur de remplacement. Ces étapes ne s'appliquent pas au contrôleur E5700SG.

- Vous avez des étiquettes pour identifier chaque câble connecté au contrôleur.

Description de la tâche

L'appliance Storage Node ne sera pas accessible lors du remplacement du contrôleur. Si le contrôleur E5700SG fonctionne suffisamment, vous pouvez effectuer un arrêt contrôlé au début de cette procédure.

> Si vous remplacez le contrôleur avant d'installer le logiciel StorageGRID, il se peut que vous ne puissiez pas accéder au programme d'installation de l'appliance StorageGRID immédiatement après avoir terminé cette procédure. Bien que vous puissiez accéder au programme d'installation de l'appliance StorageGRID à partir d'autres hôtes situés sur le même sous-réseau que l'appliance, vous ne pouvez pas y accéder à partir d'hôtes situés sur d'autres sous-réseaux. Cette condition doit se résoudre dans les 15 minutes (lorsque les entrées du cache ARP pour le contrôleur d'origine sont écoulées), ou vous pouvez effacer immédiatement la condition en éliminant manuellement les anciennes entrées du cache ARP à partir du routeur ou de la passerelle local.

Étapes

1. Arrêtez le contrôleur E5700SG.
   a. Connectez-vous au nœud grid :
      i. Saisissez la commande suivante : `ssh admin@grid_node_IP`
      ii. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

iii. Entrez la commande suivante pour passer à la racine : `su -`

iv. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

b. Arrêtez le contrôleur E5700SG :
`shutdown -h now`

c. Attendez que les données de la mémoire cache soient écrites sur les disques.

La LED verte cache actif située à l'arrière du contrôleur E2800 est allumée lorsque les données en cache ont besoin d'être écrites sur les disques. Vous devez attendre que ce voyant s'éteigne.

2. Eteindre l'alimentation en panne.
   a. Dans la page d'accueil de SANtricity System Manager, sélectionnez **Afficher les opérations en cours**.
   b. Confirmez que toutes les opérations ont été effectuées.
   c. Éteignez les deux interrupteurs de l'appareil.
   d. Attendez que tous les voyants s'éteignent.
3. Si les réseaux StorageGRID connectés au contrôleur utilisent des serveurs DHCP :
   a. Notez les adresses MAC des ports du contrôleur de remplacement (situées sur les étiquettes du contrôleur).
   b. Demandez à votre administrateur réseau de mettre à jour les paramètres d'adresse IP du contrôleur d'origine afin qu'ils reflètent les adresses MAC du contrôleur de remplacement.

> Vous devez vous assurer que les adresses IP du contrôleur d'origine ont été mises à jour avant d'appliquer la mise sous tension au contrôleur de remplacement. Dans le cas contraire, le contrôleur obtiendra de nouvelles adresses IP DHCP lors de son démarrage et risque de ne pas pouvoir se reconnecter à StorageGRID. Cette étape s'applique à tous les réseaux StorageGRID reliés au contrôleur.

4. Retirer le contrôleur de l'appliance :
   a. Placez un bracelet antistatique ou prenez d'autres précautions antistatiques.
   b. Etiqueter les câbles puis débrancher les câbles et les SFP.

> Pour éviter toute dégradation des performances, ne tordez pas, ne pliez pas, ne pincez pas ou ne montez pas sur les câbles.

   c. Libérez le contrôleur de l'appareil en appuyant sur le loquet de la poignée de came jusqu'à ce qu'il se relâche, puis ouvrez la poignée de came vers la droite.
   d. A l'aide de deux mains et de la poignée de came, faites glisser le contrôleur hors de l'appareil.

> Toujours utiliser deux mains pour soutenir le poids du contrôleur.

5. Installez le contrôleur de remplacement sur l'appliance.
   a. Retournez le contrôleur pour que le capot amovible soit orienté vers le bas.
   b. Avec la poignée de came en position ouverte, faites glisser le contrôleur complètement dans l'appareil.

c. Déplacez la poignée de came vers la gauche pour verrouiller le contrôleur en place.
d. Remplacer les câbles et les SFP.

6. Mettez l'appareil sous tension et surveillez les LED du contrôleur et les affichages à sept segments.

   Une fois les contrôleurs démarrés, les affichages à sept segments doivent indiquer les éléments suivants :

   - Contrôleur E2800 Series :

     L'état final est `99`.

   - Contrôleur E5700SG :

     L'état final est `HA`.

7. Vérifiez que le nœud de stockage de l'appliance apparaît dans Grid Manager et qu'aucune alarme ne s'affiche.

Après le remplacement de la pièce, renvoyez la pièce défectueuse à NetApp, en suivant les instructions RMA (retour de matériel) livrées avec le kit. Voir la "Retour de pièce et amp ; remplacements" pour plus d'informations.

Informations associées

"Site de documentation sur les systèmes NetApp E-Series"

Remplacer les autres composants matériels

Vous devrez peut-être remplacer la batterie du contrôleur, le lecteur, le ventilateur ou le bloc d'alimentation de l'appliance StorageGRID.

Avant de commencer

- Vous disposez de la procédure de remplacement du matériel E-Series.
- L'appareil a été "passe en mode maintenance" si la procédure de remplacement des composants requiert l'arrêt de l'appareil.

Description de la tâche

Pour remplacer la batterie du contrôleur E2800, reportez-vous aux instructions décrites dans ces instructions pour remplacer le contrôleur E2800. Ces instructions décrivent le retrait du contrôleur de l'appareil, le retrait de la batterie du contrôleur, l'installation de la batterie et le remplacement du contrôleur.

Pour remplacer un lecteur, une cartouche de ventilateur, une cartouche de ventilateur, une cartouche d'alimentation ou un tiroir disque dans l'appliance, accédez aux procédures de maintenance du matériel E2800.

Instructions de remplacement des composants SG5712

FRU	Reportez-vous aux instructions relatives à la gamme E-Series pour
Lecteur	Remplacement d'un disque dans des tiroirs E2800 de 12 ou 24 disques
Absorbeur de ventilateur d'alimentation	Réinstallation d'une cartouche de ventilateur à commande électrique dans les tiroirs E2800

Instructions de remplacement des composants SG5760

FRU	Reportez-vous aux instructions relatives à la gamme E-Series pour
Lecteur	Remplacement d'un disque dans les tiroirs E2860
Réservoir d'alimentation	Remplacement d'un boîtier électrique dans les tiroirs E2860
Boîtier de ventilateur	Remplacement d'un boîtier de ventilateur dans les tiroirs E2860
Tiroir d'entraînement	Remplacement d'un tiroir disque dans les tiroirs E2860

Informations associées

"Remplacement du contrôleur E2800"

"Site de documentation sur les systèmes NetApp E-Series"

Conservez l'appliance SG5600

L'appliance SG5600 n'est plus prise en charge. Contactez votre ingénieur commercial NetApp pour connaître les options de mise à jour du matériel.

Si vous devez effectuer des procédures de maintenance sur du matériel SG5600, utilisez le "Instructions pour StorageGRID 11.6".

Maintenance du matériel SG100 et SG1000

Maintenance des appliances SG100 et SG1000

Vous devrez peut-être effectuer des procédures de maintenance sur l'appareil. Les procédures de cette section supposent que l'appliance a déjà été déployée en tant que nœud de passerelle ou nœud d'administration dans un système StorageGRID.

Cette section présente les procédures spécifiques à la maintenance de votre système SG100 ou SG1000.

Voir "Procédures courantes" pour les procédures de maintenance utilisées par tous les appareils.

Voir "Configurer le matériel" pour les procédures de maintenance qui sont également effectuées lors de l'installation et de la configuration initiales de l'appliance.

Procédures de configuration de la maintenance

Allumer et éteindre la LED d'identification du contrôleur

Il est possible d'allumer la LED d'identification bleue à l'avant et à l'arrière du contrôleur pour localiser l'appliance dans un data Center.

Avant de commencer

Vous disposez de l'adresse IP du contrôleur BMC que vous souhaitez identifier.

Étapes

1. Accédez à l'interface BMC de l'appliance.
2. Sélectionnez **identification du serveur**.

   L'état actuel de la LED Identify est sélectionné.

3. Sélectionnez **ON** ou **OFF**, puis sélectionnez **Exécuter l'action**.

   Lorsque vous sélectionnez **ACTIVÉ**, les voyants d'identification bleus s'allument à l'avant (illustré) et à l'arrière de l'appareil.

> Si un panneau est installé sur le contrôleur, il peut être difficile de voir le voyant d'identification avant.

4. Allumer et éteindre le voyant selon les besoins.

Informations associées

"Localiser le contrôleur dans le data Center"

"Accéder à l'interface BMC"

Localiser le contrôleur dans le data Center

Identifiez le contrôleur pour effectuer des opérations de maintenance ou de mise à niveau du matériel.

Avant de commencer

- Vous avez déterminé quel contrôleur doit être entretenu.
- (Facultatif) pour localiser le contrôleur dans votre data Center, "Activez le voyant d'identification bleu".

Étapes

1. Trouver le contrôleur qui nécessite une maintenance dans le data Center.
   - Recherchez une LED d'identification bleue allumée à l'avant ou à l'arrière du contrôleur.

     Le voyant d'identification avant se trouve derrière le panneau avant du contrôleur et il peut être difficile de voir si le panneau est installé.

- Vérifiez que les étiquettes fixées à l'avant de chaque contrôleur correspondent à un numéro de pièce.

2. Retirez le cadre avant du contrôleur, le cas échéant, pour accéder aux commandes et aux indicateurs du panneau avant.
3. Facultatif : si vous l'utilisez pour localiser le contrôleur, désactivez le voyant d'identification bleu.
   - Appuyez sur le commutateur LED identifier sur le panneau avant du contrôleur.
   - Utilisez l'interface du contrôleur BMC.

Arrêtez l'appliance de services

Arrêtez l'appareil de services pour effectuer la maintenance du matériel.

Avant de commencer

- Vous avez situé physiquement l'appliance de services qui nécessite une maintenance dans le data Center.

  "Localisation du contrôleur dans un data Center".

Description de la tâche

Pour éviter toute interruption de service, arrêtez l'appliance de services pendant une fenêtre de maintenance planifiée en cas d'interruption de service.

Étapes

1. Éteignez l'appareil :

   > Vous devez effectuer un arrêt contrôlé de l'appliance en entrant les commandes indiquées ci-dessous. Il est recommandé d'effectuer un arrêt contrôlé lorsque cela est possible pour éviter les alertes inutiles, vérifier que les journaux complets sont disponibles et éviter toute interruption de service.

   a. Si vous n'avez pas encore ouvert de session sur le nœud grid, connectez-vous à l'aide de PuTTY ou d'un autre client ssh :
      i. Saisissez la commande suivante : `ssh admin@grid_node_IP`
      ii. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
      iii. Entrez la commande suivante pour passer à la racine : `su -`
      iv. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

b. Arrêtez l'appareil de services :
`shutdown -h now`

Cette commande peut prendre jusqu'à 10 minutes.

2. Utilisez l'une des méthodes suivantes pour vérifier que l'appareil est hors tension :
   - Vérifiez que le voyant d'alimentation situé à l'avant de l'appareil est éteint.
   - Consultez la page Power Control de l'interface BMC pour vérifier que l'appliance est éteinte.

Modifier la configuration de liaison de l'appliance de services

Vous pouvez modifier la configuration de la liaison Ethernet de l'appliance de services. Vous pouvez modifier le mode de liaison du port, le mode de liaison réseau et la vitesse de liaison.

Avant de commencer

- Vous avez "placez l'appareil en mode maintenance".

> Dans de rares cas, le fait de placer une appliance StorageGRID en mode de maintenance peut rendre l'appliance indisponible pour l'accès à distance.

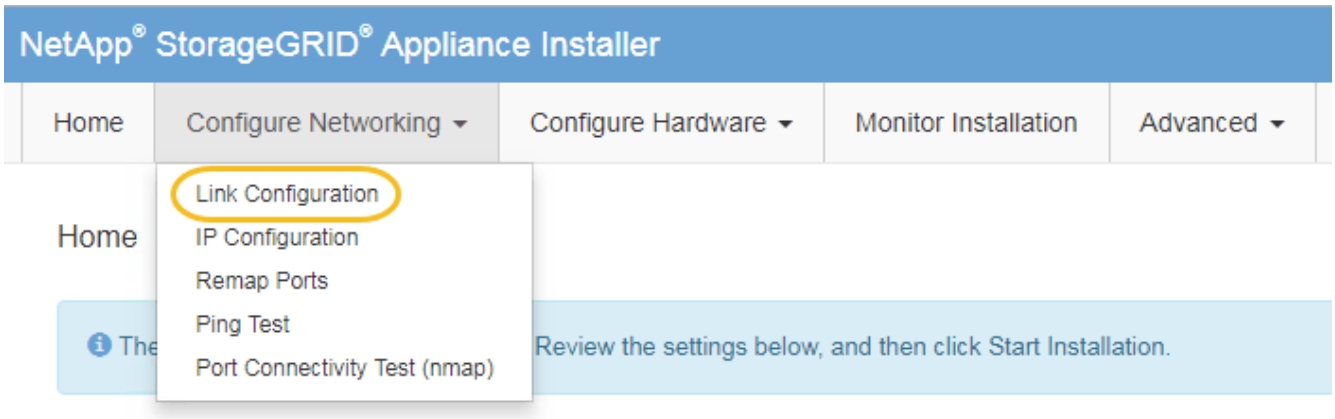
Description de la tâche

Les options permettant de modifier la configuration de la liaison Ethernet de l'appliance de services sont les suivantes :

- Changement du mode **Port bond** de fixe à agrégé, ou d'agrégat à fixe
- Passage du mode de liaison réseau * d'Active-Backup à LACP, ou de LACP à Active-Backup
- Activation ou désactivation du balisage VLAN ou modification de la valeur d'une balise VLAN
- Modification de la vitesse de liaison

Étapes

1. Dans le programme d'installation de l'appliance StorageGRID, sélectionnez **configurer réseau** > **Configuration lien**.



2. Apportez les modifications souhaitées à la configuration de liaison.

Pour plus d'informations sur les options, reportez-vous à la section "Configurer les liaisons réseau".

3. Lorsque vous êtes satisfait de vos sélections, cliquez sur **Enregistrer**.

> Vous risquez de perdre votre connexion si vous avez apporté des modifications au réseau ou au lien auquel vous êtes connecté. Si vous n'êtes pas reconnecté dans un délai d'une minute, saisissez à nouveau l'URL du programme d'installation de l'appliance StorageGRID à l'aide de l'une des autres adresses IP attribuées à l'appliance : `https://services_appliance_IP:8443`

4. Apportez les modifications nécessaires aux adresses IP de l'appliance.

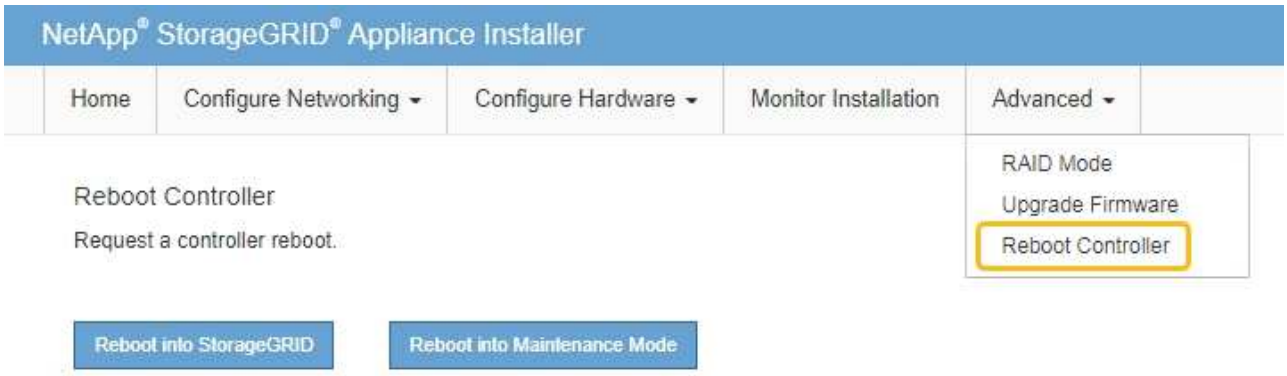
   Si vous avez modifié les paramètres VLAN, le sous-réseau de l'appliance a peut-être changé. Si vous devez modifier les adresses IP de l'appliance, reportez-vous à la section "Configurez les adresses IP StorageGRID".

5. Sélectionnez **configurer réseau** > **Test Ping** dans le menu.
6. Utilisez l'outil de test Ping pour vérifier la connectivité aux adresses IP sur tous les réseaux susceptibles d'avoir été affectés par les modifications de configuration de liaison effectuées lors de la configuration de l'appliance.

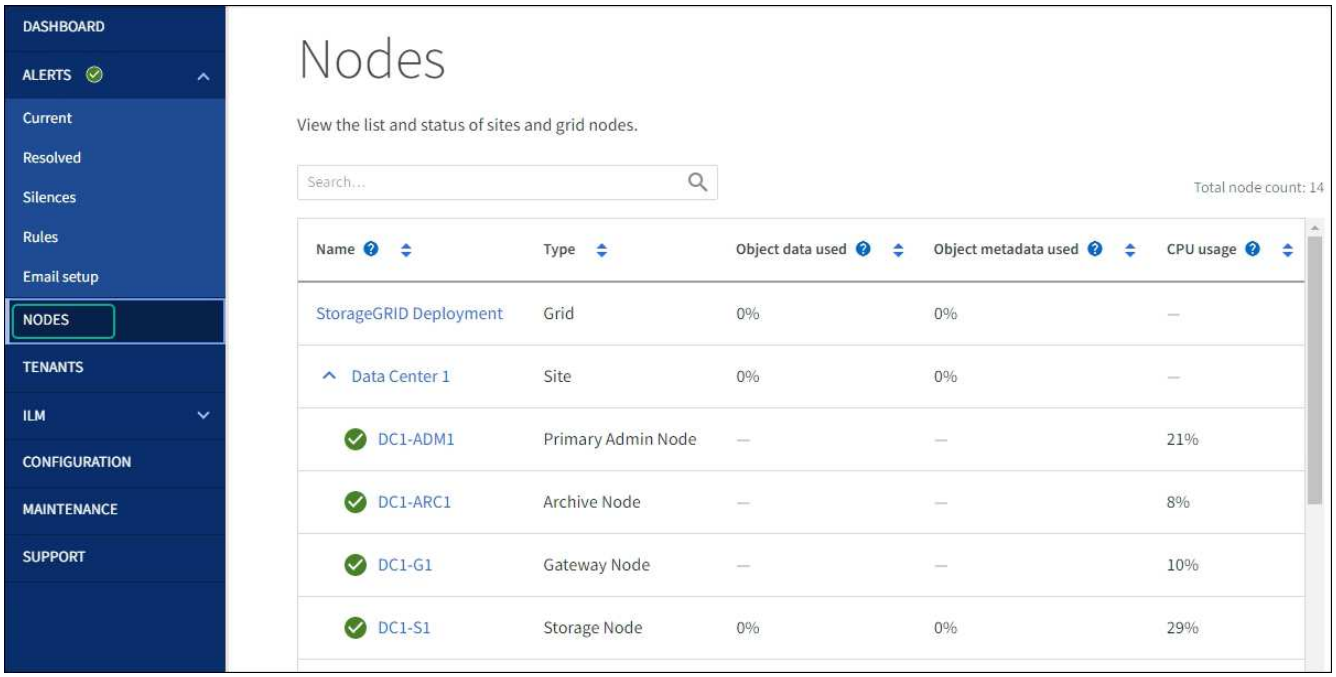
   En plus des autres tests que vous choisissez d'effectuer, confirmez que vous pouvez envoyer une commande ping à l'adresse IP du réseau de la grille du nœud d'administration principal et à l'adresse IP du réseau de la grille d'au moins un autre nœud. Si nécessaire, revenez aux instructions de configuration des liaisons réseau et corrigez tout problème.

7. Une fois que vous êtes satisfait du fait que les modifications de configuration du lien fonctionnent, redémarrez le nœud. Dans le programme d'installation de l'appliance StorageGRID, sélectionnez **Avancé** > **redémarrer le contrôleur**, puis sélectionnez l'une des options suivantes :

   - Sélectionnez **Reboot dans StorageGRID** pour redémarrer le contrôleur avec le noeud qui rejoint la grille. Sélectionnez cette option si vous avez terminé de travailler en mode maintenance et que vous êtes prêt à rétablir le fonctionnement normal du nœud.
   - Sélectionnez **redémarrer en mode maintenance** pour redémarrer le contrôleur avec le nœud restant en mode de maintenance. (Cette option n'est disponible que lorsque le contrôleur est en mode de maintenance.) Sélectionnez cette option si des opérations de maintenance supplémentaires doivent être effectuées sur le nœud avant de rejoindre la grille.



L’appliance peut redémarrer et rejoindre la grille en 20 minutes. Pour confirmer que le redémarrage est terminé et que le nœud a rejoint la grille, retournez à la grille Manager. La page **NODES** doit afficher un état normal (icône de coche verte à gauche du nom du nœud) pour le nœud de l’appliance, indiquant qu’aucune alerte n’est active et que le nœud est connecté à la grille.



Procédures matérielles

Remplacez l’un des blocs d’alimentation de l’appliance de services, ou les deux

L’appareil de services dispose de deux blocs d’alimentation pour assurer la redondance. En cas de panne de l’un des blocs d’alimentation, vous devez le remplacer dès que possible afin de s’assurer que le contrôleur de calcul est alimenté en redondance. Les deux blocs d’alimentation qui fonctionnent au niveau du contrôleur doivent être du même modèle et de la même puissance.

Avant de commencer

- Vous avez "situé physiquement le contrôleur" avec l’alimentation à remplacer.
- Si vous remplacez une seule alimentation :
  - Vous avez déballé le bloc d’alimentation de remplacement et vous êtes assuré qu’il est le même modèle et la même puissance que l’unité d’alimentation que vous remplacez.
  - Vous avez confirmé que l’autre bloc d’alimentation est installé et en cours d’exécution.
- Si vous remplacez les deux alimentations en même temps :
  - Vous avez déballé les blocs d’alimentation de remplacement et vous êtes assuré qu’ils sont du même modèle et de la même puissance.

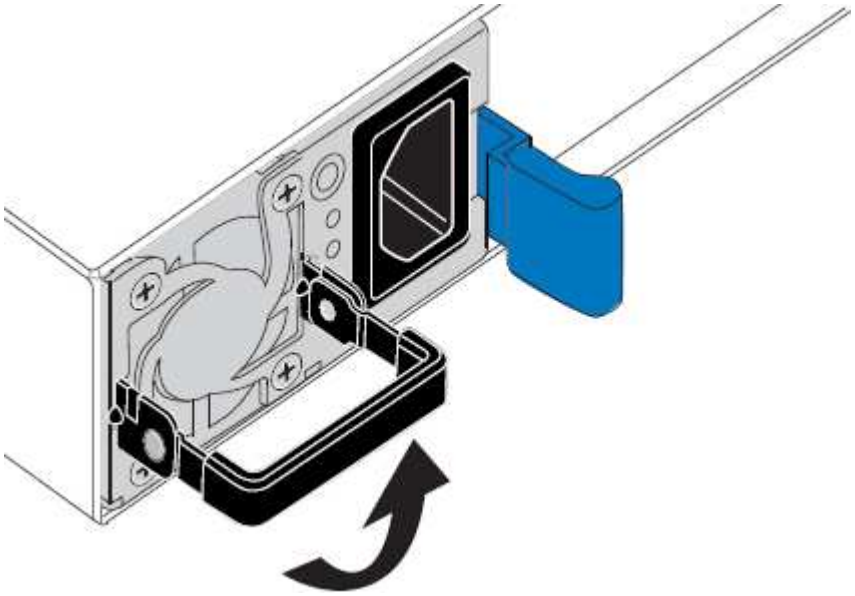
Description de la tâche

La figure montre les deux blocs d’alimentation du SG100, accessibles à l’arrière de l’appareil.

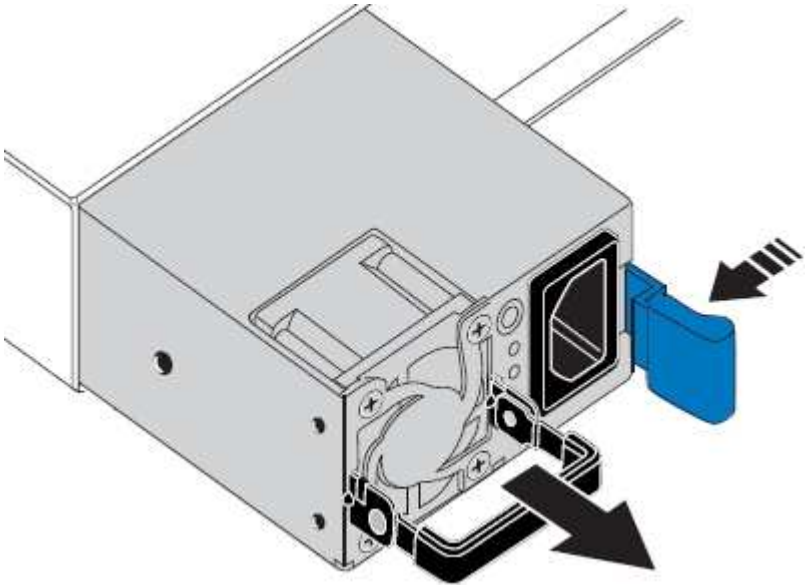
Les alimentations du SG1000 sont identiques.

Étapes

1. Si vous ne remplacez qu'une seule alimentation, vous n'avez pas besoin d'éteindre l'appareil. Accédez au Débranchez le cordon d'alimentation étape. Si vous remplacez les deux blocs d'alimentation en même temps, procédez comme suit avant de débrancher les cordons d'alimentation :
   a. "Arrêtez l'appareil".
2. débranchez le cordon d'alimentation de chaque alimentation à remplacer.
3. Soulevez la poignée de came sur la première alimentation à remplacer.



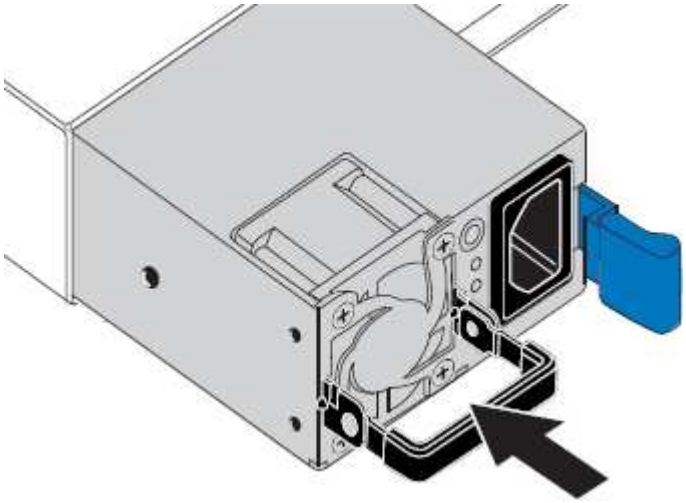
4. Appuyez sur le loquet bleu et retirez le bloc d'alimentation.



5. Avec le loquet bleu sur la droite, faites glisser le bloc d'alimentation de remplacement dans le châssis.

   Les deux blocs d'alimentation doivent avoir le même modèle et la même puissance.

   Assurez-vous que le loquet bleu se trouve sur le côté droit lorsque vous faites glisser l'unité de rechange.



6. Poussez la poignée de came vers le bas pour fixer le bloc d'alimentation de remplacement.
7. Si vous remplacez les deux blocs d'alimentation, répétez les étapes 2 à 6 pour remplacer la seconde.
8. "Branchez les câbles d'alimentation aux unités remplacées et mettez-les sous tension".

Après le remplacement de la pièce, renvoyez la pièce défectueuse à NetApp, en suivant les instructions RMA (retour de matériel) livrées avec le kit. Voir la "Retour de pièce et amp ; remplacements" pour plus d'informations.

Remplacez le ventilateur de l'appliance de services

L'appareil de service dispose de huit ventilateurs. Si l'un des ventilateurs tombe en panne, vous devez le remplacer dès que possible pour vous assurer que l'appareil est bien refroidi.

Avant de commencer

- Vous avez déballé le ventilateur de remplacement.
- Vous avez "l'appareil se trouve physiquement".
- Vous avez confirmé que les autres ventilateurs sont installés et en cours d'exécution.

Description de la tâche

Le nœud d'appliance ne sera pas accessible pendant le remplacement du ventilateur.

La photo montre un ventilateur pour l'appareil de services. Les ventilateurs de refroidissement sont accessibles lorsque vous retirez le couvercle supérieur de l'appareil.

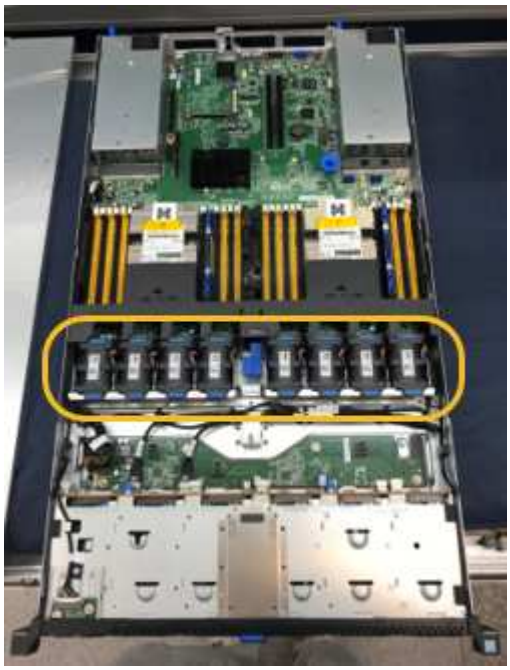
Chacun des deux blocs d'alimentation contient également un ventilateur. Ces ventilateurs ne sont pas inclus dans cette procédure.

Étapes

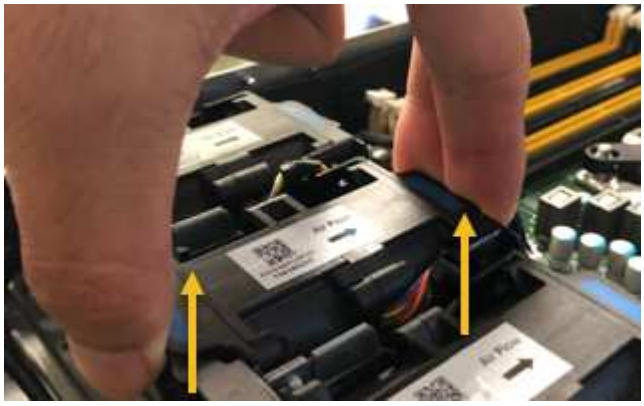
1. Éteignez l'appareil.
   a. Connectez-vous au nœud grid :
      i. Saisissez la commande suivante : `ssh admin@grid_node_IP`
      ii. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
      iii. Entrez la commande suivante pour passer à la racine : `su -`
      iv. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

      Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

   b. Arrêtez l'appareil de services :
      `shutdown -h now`
2. Utilisez l'une des deux méthodes pour vérifier que l'appareil de services est hors tension :
   - Le voyant d'alimentation situé à l'avant de l'appareil est éteint.
   - La page Power Control de l'interface BMC indique que l'appliance est éteinte.
3. Retirez l'appliance du rack.
4. Soulevez le loquet du capot supérieur et retirez le capot de l'appareil.
5. Localisez le ventilateur défectueux.

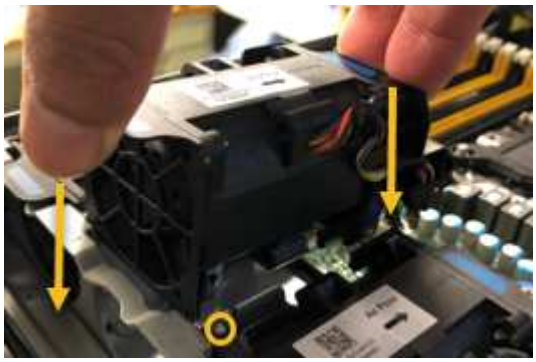


6. Soulevez le ventilateur défectueux pour le sortir du châssis.

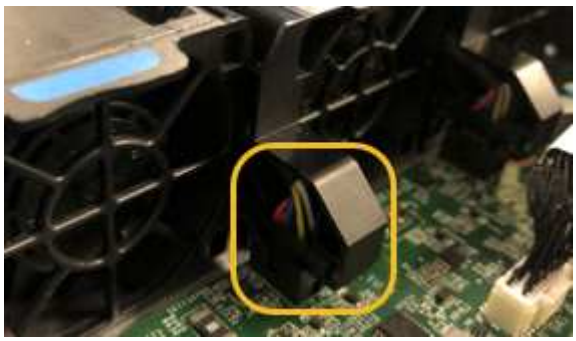


7. Faites glisser le ventilateur de remplacement dans le logement ouvert du châssis.

   Alignez le bord du ventilateur avec la goupille de guidage. La goupille est entourée dans la photo.



8. Enfoncer fermement le connecteur du ventilateur dans la carte de circuit imprimé.



9. Replacez le capot supérieur sur l'appareil et appuyez sur le loquet pour fixer le capot en place.
10. Mettez l'appareil sous tension et surveillez les voyants du contrôleur et les codes de démarrage.

    Utilisez l'interface BMC pour surveiller l'état de démarrage.

11. Vérifiez que le nœud de l'appliance s'affiche dans Grid Manager et qu'aucune alerte n'apparaît.

Après le remplacement de la pièce, renvoyez la pièce défectueuse à NetApp, en suivant les instructions RMA (retour de matériel) livrées avec le kit. Voir la "Retour de pièce et amp ; remplacements" pour plus d'informations.

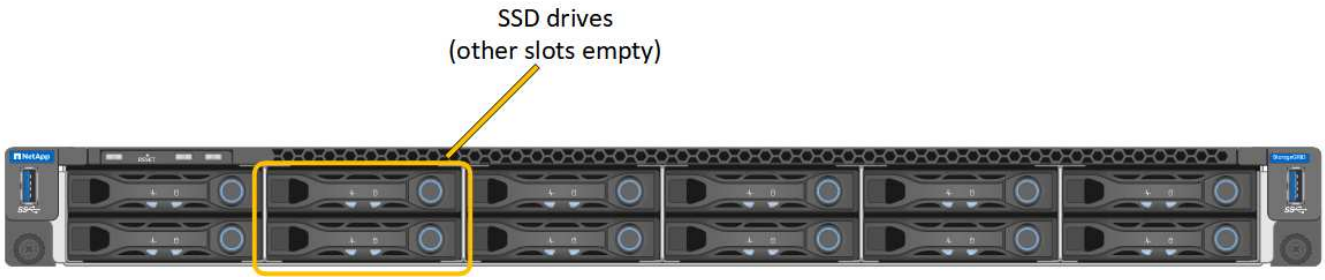
Remplacez le disque de l'appliance de services

Les disques SSD de l'appliance de services contiennent le système d'exploitation StorageGRID. En outre, lorsque l'appliance est configurée en tant que nœud d'administration, les disques SSD contiennent également des journaux d'audit, des mesures et des tables de base de données. Les disques sont mis en miroir à l'aide de RAID1 pour la redondance. Si l'un des lecteurs tombe en panne, vous devez le remplacer dès que possible pour assurer la redondance.

Avant de commencer

- Vous avez "l'appareil se trouve physiquement".
- Vous avez vérifié quel lecteur est défectueux en notant que le voyant de gauche est orange clignotant.

  Les deux disques SSD sont placés dans les emplacements comme illustré dans le schéma ci-dessous :



> Si vous retirez le disque en fonctionnement, le nœud de l'appliance est arrêté. Reportez-vous aux informations sur l'affichage des indicateurs d'état pour vérifier l'échec.

- Vous avez obtenu le disque de remplacement.
- Vous avez obtenu une protection ESD appropriée.

Étapes

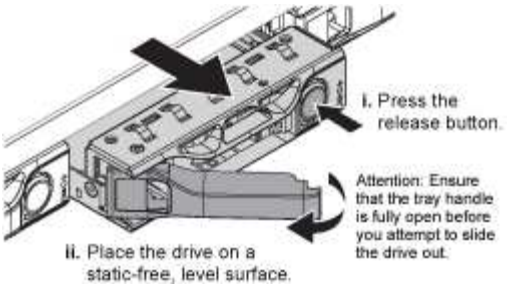
1. Vérifiez que le voyant de gauche du lecteur à remplacer clignote en orange. Si un problème de lecteur a été signalé dans les interfaces utilisateur Grid Manager ou BMC, HDD02 ou HDD2, reportez-vous au lecteur dans le logement supérieur et HDD03 ou HDD3, reportez-vous au lecteur dans le logement inférieur.

   Vous pouvez également utiliser Grid Manager pour contrôler l'état des disques SSD. Sélectionnez **NOEUDS**. Puis faire **`Appliance Node`** > **matériel**. Si un lecteur est défectueux, le champ Storage RAID mode contient un message indiquant quel lecteur est défectueux.

2. Enroulez l'extrémité du bracelet antistatique autour de votre poignet et fixez l'extrémité du clip à une masse métallique afin d'éviter toute décharge statique.
3. Déballez le lecteur de remplacement et placez-le sur une surface plane et sans électricité statique près de l'appareil.

   Conservez tous les matériaux d'emballage.

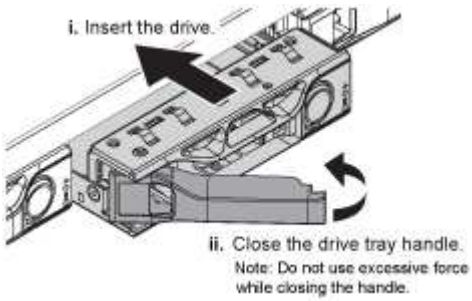
4. Appuyez sur le bouton de déverrouillage du disque défectueux.



La poignée des ressorts d'entraînement s'ouvre partiellement et l'entraînement se relâche de la fente.

5. Ouvrez la poignée, faites glisser l'entraînement vers l'extérieur et placez-le sur une surface plane et non statique.
6. Appuyez sur le bouton de dégagement du disque de remplacement avant de l'insérer dans le slot.

   Les ressorts de verrouillage s'ouvrent.



7. Insérez le lecteur de remplacement dans son logement, puis fermez la poignée du lecteur.

   Ne forcez pas trop lorsque vous fermez la poignée.

   Lorsque le lecteur est complètement inséré, vous entendez un clic.

   Le lecteur est automatiquement reconstruit à l'aide de données en miroir provenant du disque de travail. Vous pouvez vérifier l'état de la reconstruction à l'aide du Gestionnaire de grille. Sélectionnez **NOEUDS**. Puis faire **`Appliance Node`** > **matériel**. Le champ Storage RAID mode contient un message de « reconstitution » jusqu'à ce que le disque soit entièrement reconstruit.

Après le remplacement de la pièce, renvoyez la pièce défectueuse à NetApp, en suivant les instructions RMA (retour de matériel) livrées avec le kit. Voir la "Retour de pièce et amp ; remplacements" pour plus d'informations.

Remplacer l'appliance de services

Vous devrez peut-être remplacer l'appareil s'il ne fonctionne pas de manière optimale ou s'il est défectueux.

Avant de commencer

- Vous disposez d'un appareil de remplacement avec le même numéro de pièce que l'appareil que vous remplacez.
- Vous disposez d'étiquettes pour identifier chaque câble connecté à l'appareil.
- Vous avez "l'appareil se trouve physiquement".

Description de la tâche

Le nœud StorageGRID ne sera pas accessible lors du remplacement de l'appliance. Si l'appareil fonctionne correctement, vous pouvez procéder à un arrêt contrôlé au début de cette procédure.

> Si vous remplacez l'appliance avant d'installer le logiciel StorageGRID, il se peut que vous ne puissiez pas accéder immédiatement au programme d'installation de l'appliance StorageGRID après avoir terminé cette procédure. Bien que vous puissiez accéder au programme d'installation de l'appliance StorageGRID à partir d'autres hôtes situés sur le même sous-réseau que l'appliance, vous ne pouvez pas y accéder à partir d'hôtes situés sur d'autres sous-réseaux. Cette condition doit se résoudre dans les 15 minutes (lorsque les entrées du cache ARP pour l'appliance d'origine sont écoulées), ou vous pouvez effacer immédiatement la condition en éliminant manuellement les anciennes entrées du cache ARP à partir du routeur ou de la passerelle local.

Étapes

1. Affichez les configurations actuelles de l'appareil et enregistrez-les.
   a. Connectez-vous à l'appliance à remplacer :
      i. Saisissez la commande suivante : `ssh admin@grid_node_IP`
      ii. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
      iii. Entrez la commande suivante pour passer à la racine : `su -`
      iv. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

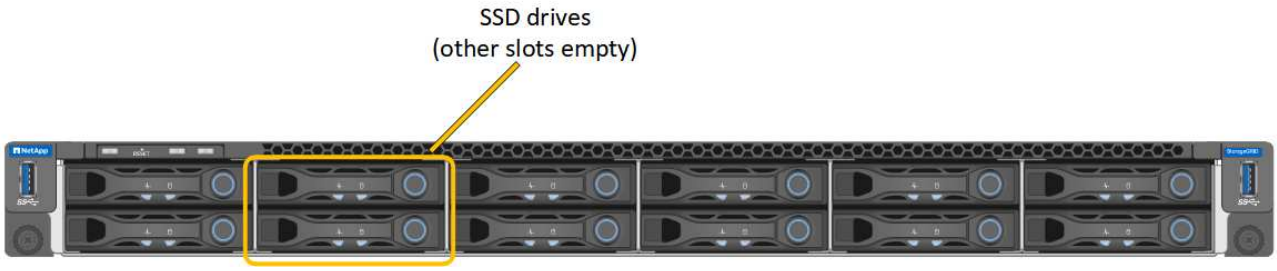
      Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

   b. Entrez : **`run-host-command ipmitool lan print`** Pour afficher les configurations BMC actuelles de l'appliance.
2. Éteignez l'appareil : `shutdown -h now`
3. Si l'une des interfaces réseau de cette appliance StorageGRID est configurée pour DHCP, vous devrez peut-être mettre à jour les attributions de bail DHCP permanentes sur les serveurs DHCP pour référencer les adresses MAC de l'appliance de remplacement. Cette mise à jour garantit que l'appliance se voit attribuer les adresses IP attendues. Voir "Mettre à jour les références d'adresse MAC".
4. Retirez et remplacez l'appareil :
   a. Etiqueter les câbles, puis débrancher les câbles et les émetteurs-récepteurs réseau.

      > Pour éviter toute dégradation des performances, ne tordez pas, ne pliez pas, ne pincez pas ou ne montez pas sur les câbles.

   b. Retirez l'appliance défectueuse de l'armoire ou du rack.
   c. Transférez les deux blocs d'alimentation, les huit ventilateurs et les deux disques SSD de l'appliance défectueuse vers l'appliance de remplacement.

      Les deux disques SSD sont placés dans les emplacements comme illustré dans le schéma ci-dessous :



HDD02 ou HDD2 désigne le lecteur dans le logement supérieur et HDD03 ou HDD3 désigne le lecteur dans le logement inférieur.

Suivez les instructions fournies pour le remplacement de ces composants.

a. Installez l'appliance de remplacement dans l'armoire ou le rack.
b. Remplacez les câbles et les émetteurs-récepteurs optiques.
c. Mettez l'appareil sous tension et attendez qu'il rejoigne à nouveau la grille.
d. Vérifiez que le nœud de l'appliance s'affiche dans Grid Manager et qu'aucune alerte n'apparaît.

5. Connectez-vous à l'appliance remplacée :
   a. Saisissez la commande suivante : `ssh admin@grid_node_IP`
   b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
   c. Entrez la commande suivante pour passer à la racine : `su -`
   d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
6. Restaurez la connectivité réseau du contrôleur BMC pour l'appliance remplacée. Deux options sont disponibles :
   - Utilisez une adresse IP statique, un masque de réseau et une passerelle
   - Utilisez DHCP pour obtenir une adresse IP, un masque de réseau et une passerelle

     i. Pour restaurer la configuration du contrôleur BMC afin d'utiliser une adresse IP statique, un masque de réseau et une passerelle, entrez les commandes suivantes :

     `run-host-command ipmitool lan set 1 ipsrc static`

     `run-host-command ipmitool lan set 1 ipaddr *Appliance_IP*`

     `run-host-command ipmitool lan set 1 netmask *Netmask_IP*`

     `run-host-command ipmitool lan set 1 defgw ipaddr *Default_gateway*`

     i. Pour restaurer la configuration du contrôleur BMC afin d'utiliser DHCP pour obtenir une adresse IP, un masque de réseau et une passerelle, entrez la commande suivante :

     `run-host-command ipmitool lan set 1 ipsrc dhcp`

7. Après avoir restauré la connectivité réseau du contrôleur BMC, connectez-vous à l'interface du contrôleur BMC pour vérifier et restaurer toute configuration BMC personnalisée supplémentaire que vous avez éventuellement appliquée. Par exemple, vous devez confirmer les paramètres des destinations d'interruption SNMP et des notifications par e-mail. Voir "Configurer l'interface BMC".

8. Vérifiez que le nœud de l’appliance s’affiche dans Grid Manager et qu’aucune alerte n’apparaît.

Après le remplacement de la pièce, renvoyez la pièce défectueuse à NetApp, en suivant les instructions RMA (retour de matériel) livrées avec le kit. Voir la "Retour de pièce et amp ; remplacements" pour plus d’informations.

Informations associées

"Afficher les indicateurs d’état"

"Afficher les codes de démarrage de l’appareil"

Activation de StorageGRID dans votre environnement

Accédez à "Activation de StorageGRID dans votre environnement" Pour savoir comment tester et activer les applications dans votre environnement StorageGRID.

Le site de documentation **storagegrid-enable** fournit des exemples et des livres de cuisine qui s'étendent sur la documentation produit de ce site, et il décrit quelques étapes suivantes dans l'évaluation et l'intégration avec StorageGRID.

Voici quelques-unes des informations incluses :

- Liste des solutions tierces validées pour les versions StorageGRID passées et actuelles.
- Guides des fonctionnalités des produits. Par exemple, ces guides fournissent toutes les informations dont vous avez besoin pour créer des pools de stockage cloud.
- Guides d'utilisation et d'outils.
- Exemples d'API pour l'utilisation de fonctionnalités StorageGRID telles que le chiffrement S3 et le verrouillage d'objet S3.

Mentions légales

Les mentions légales donnent accès aux déclarations de copyright, aux marques, aux brevets, etc.

Droits d’auteur

"https://www.netapp.com/company/legal/copyright/"

Marques déposées

NetApp, le logo NETAPP et les marques mentionnées sur la page des marques commerciales NetApp sont des marques commerciales de NetApp, Inc. Les autres noms de sociétés et de produits peuvent être des marques commerciales de leurs propriétaires respectifs.

"https://www.netapp.com/company/legal/trademarks/"

Brevets

Vous trouverez une liste actuelle des brevets appartenant à NetApp à l’adresse suivante :

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Politique de confidentialité

"https://www.netapp.com/company/legal/privacy-policy/"

Source ouverte

Les fichiers de notification fournissent des informations sur les droits d’auteur et les licences de tiers utilisés dans le logiciel NetApp.

https://library.netapp.com/ecm/ecm_download_file/ECMLP2885794

Informations sur le copyright

Copyright © 2025 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTUELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site http://www.netapp.com/TM sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.