



Documentation du logiciel StorageGRID 11.9

StorageGRID software

NetApp
October 01, 2025

This PDF was generated from <https://docs.netapp.com/fr-fr/storagegrid-119/index.html> on October 01, 2025. Always check docs.netapp.com for the latest.

Sommaire

Documentation du logiciel StorageGRID 11.9	1
Appareils StorageGRID	2
Notes de version	3
Démarrer avec un système StorageGRID	4
En savoir plus sur StorageGRID	4
Qu'est-ce que StorageGRID?	4
Clouds hybrides avec StorageGRID	6
Architecture et topologie du réseau StorageGRID	7
Nœuds et services de grille	11
Comment StorageGRID gère les données	23
Découvrez StorageGRID	35
Directives de mise en réseau	43
Directives de mise en réseau	44
Types de réseaux StorageGRID	45
Exemples de topologie de réseau	49
Exigences de mise en réseau	55
Exigences spécifiques au réseau	57
Considérations relatives au réseau spécifiques au déploiement	59
Installation et provisionnement du réseau	62
Consignes post-installation	63
Référence du port réseau	64
Démarrage rapide pour StorageGRID	74
Installer, mettre à niveau et corriger StorageGRID	77
Appareils StorageGRID	77
Installer StorageGRID sur Red Hat Enterprise Linux	77
Démarrage rapide pour l'installation de StorageGRID sur Red Hat Enterprise Linux	77
Planifier et préparer l'installation sur Red Hat	78
Automatiser l'installation de StorageGRID sur Red Hat Enterprise Linux	105
Déployer des nœuds de grille virtuels (Red Hat)	108
Configurer la grille et terminer l'installation (Red Hat)	131
Installation de l'API REST	144
Où aller ensuite	145
Résoudre les problèmes d'installation	146
Exemple /etc/sysconfig/network-scripts	147
Installer StorageGRID sur Ubuntu ou Debian	149
Démarrage rapide pour l'installation de StorageGRID sur Ubuntu ou Debian	149
Planifier et préparer l'installation sur Ubuntu ou Debian	150
Automatiser l'installation (Ubuntu ou Debian)	178
Déployer des nœuds de grille virtuels (Ubuntu ou Debian)	180
Configurer la grille et terminer l'installation (Ubuntu ou Debian)	203
Installation de l'API REST	216
Où aller ensuite	217
Résoudre les problèmes d'installation	218

Exemple /etc/network/interfaces	219
Installer StorageGRID sur VMware	220
Démarrage rapide pour l'installation de StorageGRID sur VMware	220
Planifier et préparer l'installation sur VMware	221
Automatiser l'installation (VMware)	231
Déployer des nœuds de grille de machines virtuelles (VMware)	245
Configurer la grille et terminer l'installation (VMware)	254
Installation de l'API REST	268
Où aller ensuite	269
Résoudre les problèmes d'installation	270
Mettre à niveau le logiciel StorageGRID	271
Mettre à niveau le logiciel StorageGRID	271
Quoi de neuf dans StorageGRID 11.9	271
Fonctionnalités et capacités supprimées ou obsolètes	274
Modifications apportées à l'API de gestion de la grille	276
Modifications apportées à l'API de gestion des locataires	277
Planifier et préparer la mise à niveau	277
Mettre à niveau le logiciel	285
Résoudre les problèmes de mise à niveau	302
Appliquer le correctif StorageGRID	304
Procédure de correctif logiciel StorageGRID	304
Comment votre système est affecté lorsque vous appliquez un correctif	305
Obtenir le matériel nécessaire pour le correctif	306
Télécharger le fichier de correctif	307
Vérifiez l'état du système avant d'appliquer le correctif	308
Appliquer le correctif	308
Configurer et gérer un système StorageGRID	313
Administrer StorageGRID	313
Administrer StorageGRID	313
Démarrer avec Grid Manager	313
Contrôler l'accès à StorageGRID	345
Utiliser la fédération de grille	397
Gérer la sécurité	435
Gérer les locataires	504
Configurer les connexions client	524
Gérer les réseaux et les connexions	567
Utiliser AutoSupport	587
Gérer les nœuds de stockage	602
Gérer les nœuds d'administration	616
Gérer les objets avec ILM	619
Gérer les objets avec ILM	619
ILM et cycle de vie des objets	620
Créer et attribuer des niveaux de stockage	642
Utiliser des pools de stockage	645
Utiliser les pools de stockage cloud	653

Gérer les profils de codage d'effacement	674
Configurer les régions (facultatif et S3 uniquement)	677
Créer une règle ILM	679
Gérer les politiques ILM	696
Travailler avec les politiques et les règles ILM	713
Utiliser le verrouillage d'objet S3	717
Exemples de règles et de politiques ILM	726
Renforcement du système	748
Considérations générales pour le renforcement du système	748
Directives de renforcement pour les mises à niveau logicielles	749
Directives de renforcement pour les réseaux StorageGRID	750
Directives de renforcement pour les nœuds StorageGRID	751
Directives de renforcement pour TLS et SSH	754
Autres directives de durcissement	755
Configurer StorageGRID pour FabricPool	757
Configurer StorageGRID pour FabricPool	757
Informations nécessaires pour attacher StorageGRID en tant que niveau cloud	759
Utiliser l'assistant de configuration de FabricPool	760
Configurer StorageGRID manuellement	774
Configurer ONTAP System Manager	785
Configurer le serveur DNS	787
Bonnes pratiques StorageGRID pour FabricPool	787
Supprimer les données FabricPool de StorageGRID	791
Utiliser les locataires et les clients StorageGRID	793
Utiliser un compte locataire	793
Utiliser un compte locataire	793
Comment se connecter et se déconnecter	794
Comprendre le tableau de bord du Tenant Manager	799
API de gestion des locataires	802
Utiliser les connexions de la fédération de grille	807
Gérer les groupes et les utilisateurs	821
Gérer les clés d'accès S3	841
Gérer les buckets S3	846
Gérer les services de la plateforme S3	870
Utiliser l'API REST S3	903
Versions et mises à jour prises en charge par l'API REST S3	903
Référence rapide : requêtes API S3 prises en charge	906
Tester la configuration de l'API REST S3	925
Comment StorageGRID implémente l'API REST S3	926
Prise en charge de l'API REST Amazon S3	941
Opérations personnalisées StorageGRID	991
Politiques d'accès aux buckets et aux groupes	1013
Opérations S3 suivies dans les journaux d'audit	1041
Utiliser l'API REST Swift (fin de vie)	1042
Utiliser l'API REST Swift	1042

Surveiller et dépanner un système StorageGRID	1043
Surveiller le système StorageGRID	1043
Surveiller un système StorageGRID	1043
Afficher et gérer le tableau de bord	1043
Afficher la page Nœuds	1046
Informations à suivre régulièrement	1077
Gérer les alertes	1108
Référence des fichiers journaux	1146
Configurer les destinations des messages d'audit et des journaux	1165
Utiliser la surveillance SNMP	1180
Collecter des données StorageGRID supplémentaires	1192
Dépannage du système StorageGRID	1226
Dépanner un système StorageGRID	1226
Résoudre les problèmes d'objets et de stockage	1234
Résoudre les problèmes de métadonnées	1263
Résoudre les erreurs de certificat	1265
Résoudre les problèmes liés au nœud d'administration et à l'interface utilisateur	1266
Résoudre les problèmes de réseau, de matériel et de plate-forme	1270
Dépanner un serveur syslog externe	1278
Examiner les journaux d'audit	1280
Messages d'audit et journaux	1280
Auditer le flux et la rétention des messages	1281
Accéder au fichier journal d'audit	1284
Rotation du fichier journal d'audit	1285
Format du fichier journal d'audit	1285
Format du message d'audit	1298
Messages d'audit et cycle de vie des objets	1303
Messages d'audit	1310
Développer une grille	1361
Types d'extension	1361
Planifier l'extension de StorageGRID	1362
Ajouter de la capacité de stockage	1362
Ajouter une capacité de métadonnées	1370
Ajoutez des nœuds de grille pour ajouter des fonctionnalités à votre système	1372
Ajouter un nouveau site	1372
Rassembler le matériel nécessaire	1373
Téléchargez et extrayez les fichiers d'installation de StorageGRID	1374
Vérifier le matériel et le réseau	1380
Ajouter des volumes de stockage	1381
Ajouter des volumes de stockage aux nœuds de stockage	1381
VMware : ajouter des volumes de stockage au nœud de stockage	1384
Linux : ajouter des volumes à connexion directe ou SAN au nœud de stockage	1386
Ajouter des nœuds de grille ou un site	1389
Ajouter des nœuds de grille à un site existant ou ajouter un nouveau site	1389
Mettre à jour les sous-réseaux pour Grid Network	1390

Déployer de nouveaux nœuds de grille	1391
Effectuer une expansion	1397
Configurer le système étendu	1404
Étapes de configuration après l'extension	1404
Vérifiez que le nœud de stockage est actif	1406
Copier la base de données du nœud d'administration	1407
Copier les métriques Prometheus	1408
Copier les journaux d'audit	1409
Rééquilibrer les données codées par effacement après l'ajout de nœuds de stockage	1411
Dépannage de l'extension	1414
Maintenir un système StorageGRID	1416
Maintenance du réseau	1416
Avant de commencer	1416
Procédures d'entretien des appareils	1416
Télécharger le package de récupération	1416
Décommissionner les nœuds ou le site	1417
Décommissionner un nœud ou un site	1417
Décommissionner les nœuds	1417
Site de déclassement	1438
Renommer la grille, le site ou le nœud	1462
Utiliser la procédure de renommage	1462
Ajouter ou mettre à jour les noms d'affichage	1466
Procédures de nœud	1472
Procédures de maintenance des nœuds	1472
Procédures du gestionnaire de serveur	1473
Procédures de redémarrage, d'arrêt et d'alimentation	1483
Procédures de remappage des ports	1495
Procédures réseau	1499
Mettre à jour les sous-réseaux pour Grid Network	1499
Configurer les adresses IP	1501
Ajouter des interfaces au nœud existant	1519
Configurer les serveurs DNS	1523
Modifier la configuration DNS pour un nœud de grille unique	1524
Gérer les serveurs NTP	1526
Restaurer la connectivité réseau pour les nœuds isolés	1527
Procédures d'hôte et de middleware	1529
Linux : migrer le nœud de grille vers un nouvel hôte	1529
VMware : configurer la machine virtuelle pour un redémarrage automatique	1531
Récupérer ou remplacer les nœuds	1533
Avertissements et considérations pour la récupération des nœuds de grille	1533
Conditions préalables à la récupération des nœuds de grille	1533
Ordre de récupération des nœuds en cas de défaillance d'un serveur hébergeant plusieurs nœuds de grille	1534
Adresses IP des nœuds récupérés	1534
Rassembler les matériaux nécessaires à la récupération des nœuds du réseau	1534

Téléchargez et extrayez les fichiers d'installation de StorageGRID	1535
Sélectionnez la procédure de récupération du nœud	1541
Récupérer après une panne de nœud de stockage	1542
Récupérer après une panne de nœud de stockage	1542
Récupérer le nœud de stockage de l'appareil	1543
Récupérer après une panne de volume de stockage lorsque le lecteur système est intact	1566
Récupérer après une panne du lecteur système	1581
Restaurer les données d'objet à l'aide de Grid Manager	1599
Surveiller les tâches de réparation des données	1602
Récupérer après une panne du nœud d'administration	1604
Récupération du nœud d'administration principal ou non principal	1604
Récupérer après une panne du nœud d'administration principal	1604
Récupérer après une panne d'un nœud d'administration non principal	1613
Récupérer après une panne du nœud de passerelle	1621
Remplacer le nœud de passerelle	1621
Sélectionnez Démarrer la récupération pour configurer le nœud de passerelle	1622
Récupérer après une panne du nœud d'archivage	1624
Récupérer après une panne du nœud d'archivage	1624
Remplacer le nœud Linux	1624
Remplacer le nœud Linux	1624
Déployer de nouveaux hôtes Linux	1624
Restaurer les nœuds de la grille sur l'hôte	1625
Étapes suivantes : effectuez des étapes de récupération supplémentaires, si nécessaire.	1630
Remplacer le nœud VMware	1631
Remplacer le nœud défaillant par un dispositif de services	1632
Remplacer le nœud défaillant par un dispositif de services	1632
Installer l'appareil de services (changement de plateforme uniquement)	1633
Préparer l'appareil pour la réinstallation (remplacement de la plate-forme uniquement)	1634
Démarrer l'installation du logiciel sur l'appareil de services	1634
Surveillance de l'installation des appareils de services	1638
Comment le support technique récupère un site	1641
Comment activer StorageGRID dans votre environnement	1644
Comment gérer StorageGRID avec BlueXP	1645
Mentions légales	1646
Copyright	1646
Marques de commerce	1646
Brevets	1646
Politique de confidentialité	1646
Open source	1646

Documentation du logiciel StorageGRID 11.9

Appareils StorageGRID

Aller à "[Documentation de l'appliance StorageGRID](#)" pour apprendre à installer, configurer et entretenir les appliances de stockage et de services StorageGRID .

Notes de version

Obtenez des informations spécifiques à la version sur les problèmes résolus et les problèmes connus.

Connectez-vous au site de support NetApp pour "[afficher ou télécharger un fichier PDF](#)" contenant les notes de version de StorageGRID 11.9.

Démarrer avec un système StorageGRID

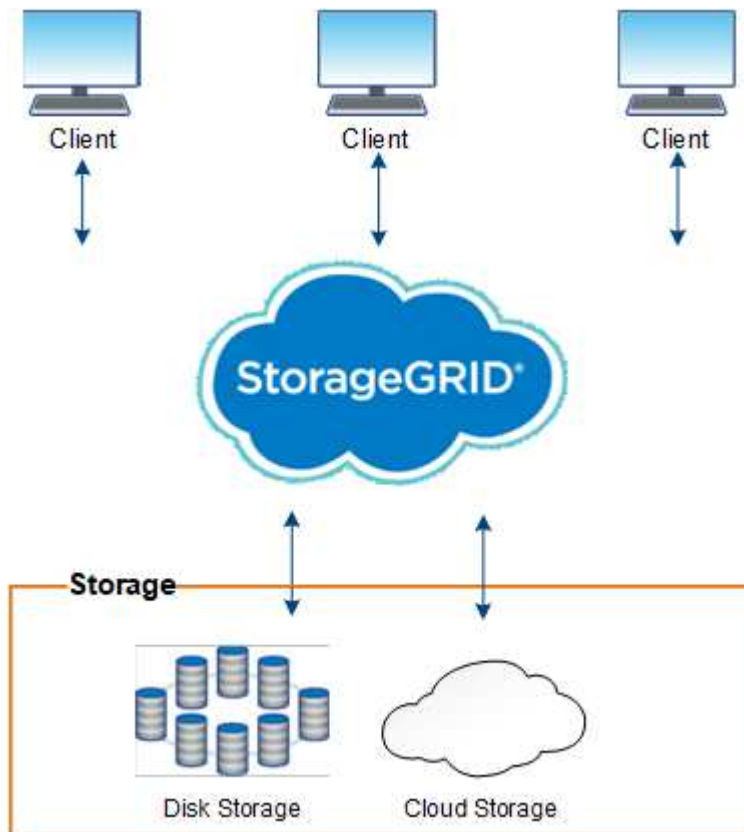
En savoir plus sur StorageGRID

Qu'est-ce que StorageGRID?

NetApp® StorageGRID® est une suite de stockage d'objets définie par logiciel qui prend en charge un large éventail de cas d'utilisation dans des environnements multicloud 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 préserver les données non structurées de manière rentable sur de longues périodes.

StorageGRID fournit un stockage sécurisé et durable pour les données non structurées à grande échelle. Les politiques de gestion du cycle de vie intégrées et basées sur les métadonnées optimisent l'emplacement de vos données tout au long de leur vie. Le contenu est placé au bon endroit, au bon moment et sur le bon niveau de stockage pour réduire les coûts.

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



La prise en charge des nœuds d'archive a été supprimée. Le déplacement d'objets d'un nœud d'archive vers un système de stockage d'archives externe via l'API S3 a été remplacé par "Pools de stockage cloud ILM", qui offrent plus de fonctionnalités.

Avantages de StorageGRID

Les avantages du système StorageGRID sont les suivants :

- Un référentiel de données distribué géographiquement, massivement évolutif et facile à utiliser pour les données non structurées.
- Protocoles de stockage d'objets standard :
 - Service de stockage simple Amazon Web Services (S3)
 - OpenStack Swift



La prise en charge des applications clientes Swift est obsolète et sera supprimée dans une prochaine version.

- Cloud hybride activé. La gestion du cycle de vie des informations basée sur des politiques (ILM) stocke les objets dans des clouds publics, notamment Amazon Web Services (AWS) et Microsoft Azure. Les services de la plateforme StorageGRID permettent la réplication de contenu, la notification d'événements et la recherche de métadonnées d'objets stockés dans des clouds publics.
- Protection flexible des données pour garantir la durabilité et la disponibilité. Les données peuvent être protégées à l'aide de la réplication et du codage d'effacement en couches. La vérification des données au repos et en vol garantit l'intégrité pour une conservation à long terme.
- Gestion dynamique du cycle de vie des données pour aider à gérer les coûts de stockage. Vous pouvez créer des règles ILM qui gèrent le cycle de vie des données au niveau de l'objet, en personnalisant la localité des données, la durabilité, les performances, le coût et le temps de conservation.
- Haute disponibilité du stockage de données et de certaines fonctions de gestion, avec équilibrage de charge intégré pour optimiser la charge de données sur les ressources StorageGRID .
- Prise en charge de plusieurs comptes de locataire de stockage pour séparer les objets stockés sur votre système par différentes entités.
- De nombreux outils pour surveiller la santé de votre système StorageGRID , notamment un système d'alerte complet, un tableau de bord graphique et des statuts détaillés pour tous les nœuds et sites.
- Prise en charge du déploiement logiciel ou matériel. Vous pouvez déployer StorageGRID sur l'un des éléments suivants :
 - Machines virtuelles exécutées dans VMware.
 - Moteurs de conteneurs sur les hôtes Linux.
 - Appareils conçus par StorageGRID .
 - Les appareils de stockage fournissent un stockage d'objets.
 - Les appareils de services fournissent des services d'administration du réseau et d'équilibrage de charge.
- Conforme aux exigences de stockage pertinentes de la présente réglementation :
 - Securities and Exchange Commission (SEC) dans 17 CFR § 240.17a-4(f), qui réglemente les membres de la bourse, les courtiers ou les négociants.
 - Règle 4511(c) de la Financial Industry Regulatory Authority (FINRA), qui s'en remet aux exigences de format et de support de la règle 17a-4(f) de la SEC.
 - Commodity Futures Trading Commission (CFTC) dans le règlement 17 CFR § 1.31(c)-(d), qui réglemente le trading à terme sur matières premières.
- Opérations de mise à niveau et de maintenance non perturbatrices. Maintenir l'accès au contenu pendant

les procédures de mise à niveau, d'extension, de mise hors service et de maintenance.

- Gestion des identités fédérées. S'intègre à Active Directory, OpenLDAP ou Oracle Directory Service pour l'authentification des utilisateurs. Prend en charge l'authentification unique (SSO) à l'aide de la norme Security Assertion Markup Language 2.0 (SAML 2.0) pour échanger des 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 mettant en œuvre une gestion des données basée sur des politiques pour stocker des objets dans des pools de stockage cloud, en exploitant les services de la plateforme StorageGRID et en hiérarchisant les données d'ONTAP vers StorageGRID avec NetApp FabricPool.

Pools de stockage cloud

Les pools de stockage cloud vous permettent de stocker des objets en dehors du système StorageGRID. Par exemple, vous souhaitez peut-être déplacer des objets rarement consultés vers un stockage cloud moins coûteux, tel qu'Amazon S3 Glacier, S3 Glacier Deep Archive, Google Cloud ou le niveau d'accès Archive dans le stockage Microsoft Azure Blob. Ou, vous souhaitez peut-être conserver une sauvegarde cloud des objets StorageGRID, qui peut être utilisée pour récupérer des données perdues en raison d'une défaillance d'un volume de stockage ou d'un 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 supplémentaire nécessaire pour récupérer un objet à partir de la cible du pool de stockage Cloud.

Services de la plateforme S3

Les services de la plateforme S3 vous offrent la possibilité d'utiliser des services distants comme points de terminaison pour la réplication d'objets, les notifications d'événements ou l'intégration de la recherche. Les services de plateforme fonctionnent indépendamment des règles ILM de la grille 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 deuxième système StorageGRID.
- Le service de notification d'événements envoie des messages sur les actions spécifiées à un point de terminaison externe qui prend en charge la réception d'événements Simple Notification Service (Amazon SNS).
- Le service d'intégration de recherche envoie des 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.

Par exemple, vous pouvez utiliser la réplication CloudMirror pour mettre en miroir des enregistrements clients spécifiques dans Amazon S3, puis exploiter les services AWS pour effectuer des analyses sur vos données.

Hiérarchisation des données ONTAP à l'aide de FabricPool

Vous pouvez réduire le coût du stockage ONTAP en hiérarchisant les données vers StorageGRID à l'aide de FabricPool. FabricPool permet la hiérarchisation automatisée des données vers des niveaux de stockage d'objets à faible coût, sur site ou hors site.

Contrairement aux solutions de hiérarchisation manuelle, FabricPool réduit le coût total de possession en automatisant la hiérarchisation des données pour réduire le coût de stockage. Il offre les avantages de l'économie du cloud en s'intégrant aux clouds publics et privés, y compris StorageGRID.

Informations connexes

- ["Qu'est-ce qu'un pool de stockage cloud ?"](#)
- ["Gérer les services de la plateforme"](#)
- ["Configurer StorageGRID pour FabricPool"](#)

Architecture et topologie du réseau StorageGRID

Un système StorageGRID se compose de plusieurs types de nœuds de grille sur un ou plusieurs sites de centre de données.

Voir le ["descriptions des types de nœuds de grille"](#) .

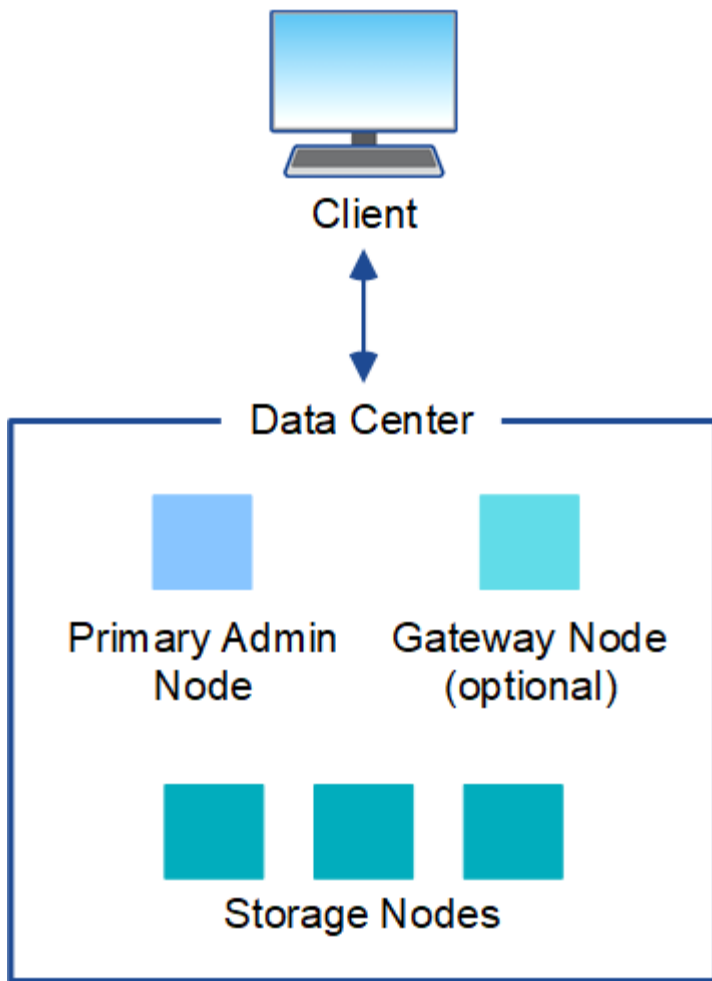
Pour plus d'informations sur la topologie du réseau StorageGRID , les exigences et les communications de grille, consultez le ["Directives de mise en réseau"](#) .

Topologies de déploiement

Le système StorageGRID peut être déployé sur un seul site de centre de données ou sur plusieurs sites de centre de données.

Site unique

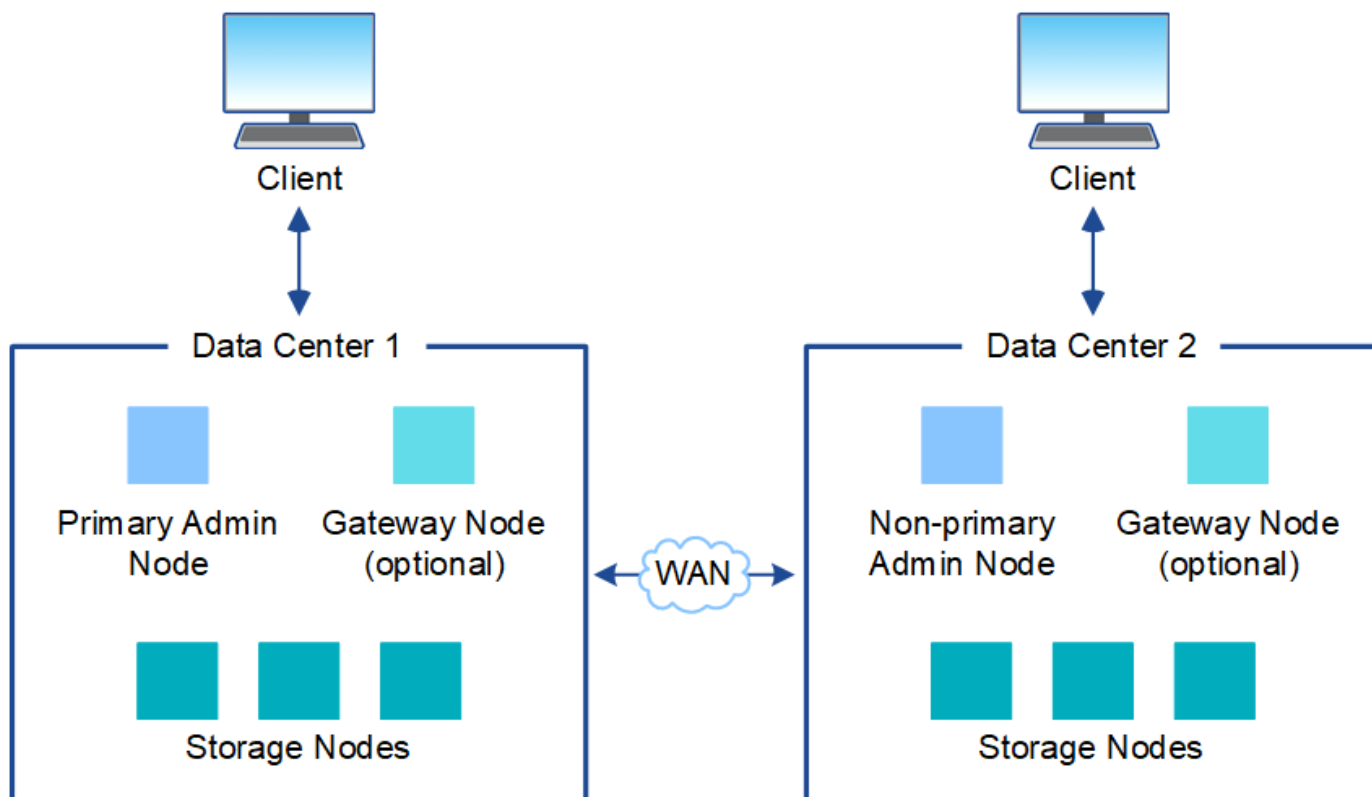
Dans un déploiement avec un seul site, l'infrastructure et les opérations du système StorageGRID sont centralisées.



Plusieurs sites

Dans un déploiement avec plusieurs sites, différents types et nombres de ressources StorageGRID peuvent être installés sur chaque site. Par exemple, il se peut qu'un centre de données nécessite davantage de stockage qu'un autre.

Différents sites sont souvent situés dans des emplacements géographiques différents dans différents domaines de défaillance, comme une ligne de faille sismique ou une plaine inondable. Le partage des données et la reprise après sinistre sont réalisés par la distribution automatisée des données vers d'autres sites.



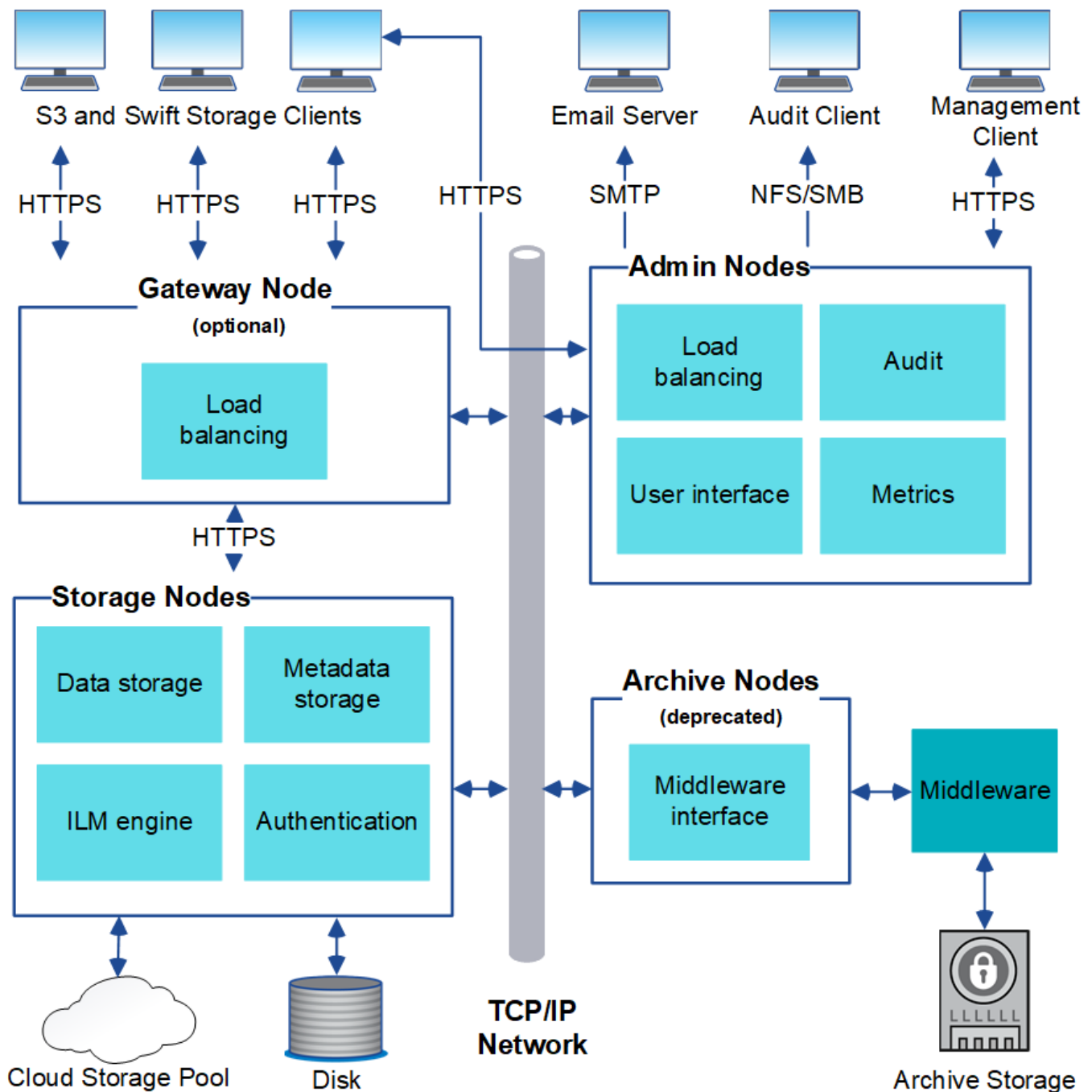
Plusieurs sites logiques peuvent également exister au sein d'un même centre de données pour permettre l'utilisation de la réplication distribuée et du codage d'effacement afin d'augmenter la disponibilité et la résilience.

Redondance des nœuds de grille

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

Architecture du système

Ce diagramme montre comment les nœuds de grille sont organisés dans un système StorageGRID .



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

Les clients S3 peuvent se connecter à un nœud de passerelle ou à un nœud d'administration pour utiliser l'interface d'équilibrage de charge vers les nœuds de stockage. Alternativement, les clients S3 peuvent 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, constitués de buckets S3 externes ou de conteneurs de stockage Azure Blob.

Nœuds et services de grille

Nœuds et services de grille

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

Types de nœuds de grille

Le système StorageGRID utilise quatre types de nœuds de grille :

Nœuds d'administration

Fournir des services de gestion tels que la configuration du système, la surveillance et la journalisation. Lorsque vous vous connectez au Grid Manager, vous vous connectez à un nœud d'administration. Chaque grille doit avoir un nœud d'administration principal et peut avoir des nœuds d'administration non principaux supplémentaires pour 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 client S3.

Voir "[Qu'est-ce qu'un nœud d'administration ?](#)"

Nœuds de stockage

Gérer et stocker les données et métadonnées des objets. Chaque site de votre système StorageGRID doit disposer d'au moins trois nœuds de stockage.

Voir "[Qu'est-ce qu'un nœud de stockage ?](#)"

Nœuds de passerelle (facultatif)

Fournissez 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 des nœuds ou même d'un site entier soit transparente.

Voir "[Qu'est-ce qu'un nœud de passerelle ?](#)"

Nœuds matériels et logiciels

Les nœuds StorageGRID peuvent être déployés en tant que nœuds d'appliance StorageGRID ou en tant que nœuds logiciels.

Nœuds d'appliance StorageGRID

Les appareils matériels StorageGRID sont spécialement conçus pour être utilisés dans un système StorageGRID . Certains appareils peuvent être utilisés comme nœuds de stockage. D'autres appareils peuvent être utilisés comme nœuds d'administration ou nœuds de passerelle. Vous pouvez combiner des nœuds d'appliance avec des nœuds logiciels ou déployer des grilles entièrement conçues et entièrement composées d'appliances qui ne dépendent pas d'hyperviseurs externes, de stockage ou de matériel de calcul.

Consultez les éléments suivants pour en savoir plus sur les appareils disponibles :

- ["Documentation de l'appliance StorageGRID"](#)
- ["Hardware Universe NetApp"](#)

Nœuds basés sur des logiciels

Les nœuds de grille basés sur des logiciels peuvent être déployés en tant que machines virtuelles VMware ou dans des moteurs de conteneurs sur un hôte Linux.

- Machine virtuelle (VM) dans VMware vSphere : voir ["Installer StorageGRID sur VMware"](#) .
- Dans un moteur de conteneur sur Red Hat Enterprise Linux : Voir ["Installer StorageGRID sur Red Hat Enterprise Linux"](#) .
- Au sein d'un moteur de conteneur sur Ubuntu ou Debian : Voir ["Installer StorageGRID sur Ubuntu ou Debian"](#) .

Utilisez le ["Outil de matrice d'interopérabilité NetApp \(IMT\)"](#) pour déterminer les versions prises en charge.

Lors de l'installation initiale d'un nouveau nœud de stockage basé sur un logiciel, vous pouvez spécifier qu'il soit utilisé uniquement pour ["stocker les métadonnées"](#) .

Services StorageGRID

Voici une liste complète des services StorageGRID .

Service	Description	Pays
Transitaire de service de compte	Fournit une interface permettant au service Load Balancer d'interroger le service de compte sur des hôtes distants et fournit des notifications des modifications de configuration du point de terminaison Load Balancer au service Load Balancer.	Service d'équilibrage de charge sur les nœuds d'administration et les nœuds de passerelle
ADC (contrôleur de domaine administratif)	Maintient les informations de topologie, fournit des services d'authentification et répond aux requêtes des services LDR et CMN.	Au moins trois nœuds de stockage contenant le service ADC sur chaque site
AMS (Système de gestion des audits)	Surveille et enregistre tous les événements et transactions système audités dans un fichier journal texte.	Nœuds d'administration
Cassandra Reaper	Effectue des réparations automatiques des métadonnées des objets.	Nœuds de stockage
Service de morceaux	Gère les données codées par effacement et les fragments de parité.	Nœuds de stockage
CMN (nœud de gestion de configuration)	Gère les configurations à l'échelle du système et les tâches de grille. Chaque grille dispose d'un service CMN.	Nœud d'administration principal

Service	Description	Pays
DDS (magasin de données distribué)	Interfaces avec la base de données Cassandra pour gérer les métadonnées des objets.	Nœuds de stockage
DMV (transporteur de données)	Déplace les données vers les points de terminaison cloud.	Nœuds de stockage
IP dynamique (dynip)	Surveille la grille pour les changements IP dynamiques et met à jour les configurations locales.	Tous les nœuds
Grafana	Utilisé pour la visualisation des métriques dans le gestionnaire de grille.	Nœuds d'administration
Haute disponibilité	Gère les adresses IP virtuelles haute disponibilité sur les nœuds configurés sur la page Groupes haute disponibilité. Ce service est également connu sous le nom de service keepalived.	Nœuds d'administration et de passerelle
Identité (idnt)	Fédère les identités des utilisateurs de LDAP et Active Directory.	Nœuds de stockage qui utilisent le service ADC
Arbitre Lambda	Gère les requêtes S3 Select SelectObjectContent.	Tous les nœuds
Équilibreur de charge (nginx-gw)	Fournit un équilibrage de charge du trafic S3 des clients vers les nœuds de stockage. Le service Load Balancer peut être configuré via la page de configuration des points de terminaison Load Balancer. Ce service est également connu sous le nom de service nginx-gw.	Nœuds d'administration et de passerelle
LDR (routeur de distribution local)	Gère le stockage et le transfert de contenu au sein de la grille.	Nœuds de stockage
Démon de contrôle du service d'information MISCd	Fournit une interface pour interroger et gérer les services sur d'autres nœuds et pour gérer les configurations environnementales sur le nœud, telles que l'interrogation de l'état des services exécutés sur d'autres nœuds.	Tous les nœuds

Service	Description	Pays
nginx	Agit comme un mécanisme d'authentification et de communication sécurisé pour divers services de grille (tels que Prometheus et Dynamic IP) pour pouvoir communiquer avec des services sur d'autres nœuds via des API HTTPS.	Tous les nœuds
nginx-gw	Alimente le service Load Balancer.	Nœuds d'administration et de passerelle
NMS (Système de gestion de réseau)	Alimente les options de surveillance, de création de rapports et de configuration affichées via le gestionnaire de grille.	Nœuds d'administration
Persistance	Gère les fichiers sur le disque racine qui doivent persister après un redémarrage.	Tous les nœuds
Prométhée	Collecte les métriques de séries chronologiques des services sur tous les nœuds.	Nœuds d'administration
RSM (machine à états répliquée)	Garantit que les demandes de service de la plateforme sont envoyées à leurs points de terminaison respectifs.	Nœuds de stockage qui utilisent le service ADC
SSM (moniteur d'état du serveur)	Surveille les conditions du matériel et les signale au service NMS.	Une instance est présente sur chaque nœud de grille
Collecteur de traces	Effectue une collecte de traces pour recueillir des informations à utiliser par le support technique. Le service de collecte de traces utilise le logiciel open source Jaeger.	Nœuds d'administration

Qu'est-ce qu'un nœud d'administration ?

Les nœuds d'administration fournissent des services de gestion tels que la configuration du système, la surveillance et la journalisation. Les nœuds d'administration peuvent également être utilisés pour équilibrer la charge du trafic client S3. Chaque grille doit avoir un nœud d'administration principal et peut avoir n'importe quel nombre de nœuds d'administration non principaux pour la redondance.

Différences entre les nœuds d'administration principaux et non principaux

Lorsque vous vous connectez au gestionnaire de grille ou au gestionnaire de locataires, vous vous connectez à un nœud 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, le nœud d'administration principal fournit plus de fonctionnalités que les nœuds d'administration non principaux. Par exemple, la plupart des procédures de maintenance doivent être effectuées à partir des nœuds

d'administration principaux.

Le tableau résume les capacités des nœuds d'administration principaux et non principaux.

Capacités	Nœud d'administration principal	Nœud d'administration non principal
Comprend leAMS service	Oui	Oui
Comprend leCMN service	Oui	Non
Comprend leNMS service	Oui	Oui
Comprend leProméthée service	Oui	Oui
Comprend leSSM service	Oui	Oui
Comprend leÉquilibreur de charge etHaute disponibilité services	Oui	Oui
Soutient leInterface de programmation d'application de gestion (API de gestion)	Oui	Oui
Peut être utilisé pour toutes les tâches de maintenance liées au réseau, par exemple le changement d'adresse IP et la mise à jour des serveurs NTP	Oui	Non
Peut effectuer un rééquilibrage EC après l'extension du nœud de stockage	Oui	Non
Peut être utilisé pour la procédure de restauration du volume	Oui	Oui
Peut collecter des fichiers journaux et des données système à partir d'un ou plusieurs nœuds	Oui	Non
Envoie des notifications d'alerte, des packages AutoSupport et des interruptions SNMP et informe	Oui. Agit comme leexpéditeur préféré .	Oui. Agit comme un expéditeur de secours.

Nœud d'administration de 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 packages AutoSupport et les interruptions et informations SNMP.

Dans le cadre du fonctionnement normal du système, seul l'expéditeur préféré envoie des notifications. Cependant, tous les autres nœuds d'administration surveillent l'expéditeur préféré. Si un problème est détecté, d'autres nœuds d'administration agissent comme des *expéditeurs de secours*.

Plusieurs notifications peuvent être envoyées dans ces cas :

- Si les nœuds d'administration deviennent « isolés » les uns des autres, l'expéditeur préféré et les expéditeurs de secours tenteront d'envoyer des notifications, et plusieurs copies des notifications pourraient être reçues.
- Si l'expéditeur de secours détecte des problèmes avec l'expéditeur préféré et commence à envoyer des notifications, l'expéditeur préféré peut retrouver sa capacité à envoyer des notifications. Si cela se produit, des notifications en double peuvent être envoyées. L'expéditeur de secours cessera d'envoyer des notifications lorsqu'il ne détectera plus d'erreurs sur l'expéditeur préféré.



Lorsque vous testez les packages AutoSupport, tous les nœuds d'administration envoient le test. Lorsque vous testez les notifications d'alerte, vous devez vous connecter à chaque nœud d'administration pour vérifier la connectivité.

Services principaux pour les nœuds d'administration

Le tableau suivant présente les principaux services des nœuds d'administration ; cependant, ce tableau ne répertorie pas tous les services de nœud.

Service	Fonction clé
Système de gestion des audits (AMS)	Suivi de l'activité et des événements du système.
Nœud de gestion de configuration (CMN)	Gère la configuration à l'échelle du système.
Haute disponibilité	Gère les adresses IP virtuelles haute disponibilité pour les groupes de nœuds d'administration et de nœuds de passerelle. Remarque : ce service est également disponible sur les nœuds de passerelle.
Équilibreur de charge	Fournit un équilibrage de charge du trafic S3 des clients vers les nœuds de stockage. Remarque : ce service est également disponible sur les nœuds de passerelle.
Interface de programmation d'application de gestion (mgmt-api)	Traite les demandes de l'API Grid Management et de l'API Tenant Management.
Système de gestion de réseau (NMS)	Fournit des fonctionnalités pour le gestionnaire de grille.
Prométhée	Collecte et stocke les métriques 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.

Qu'est-ce qu'un nœud de stockage ?

Les nœuds de stockage gèrent et stockent les données et les métadonnées des objets. Les nœuds de stockage incluent les services et processus requis pour stocker, déplacer, vérifier et récupérer les données et métadonnées des objets sur le disque.

Chaque site de votre système StorageGRID doit disposer d'au moins trois nœuds de stockage.

Types de nœuds de stockage

Lors de l'installation, vous pouvez sélectionner le type de nœud de stockage que vous souhaitez installer. Ces types sont disponibles pour les nœuds de stockage basés sur des logiciels et pour les nœuds de stockage basés sur des appliances qui prennent en charge la fonctionnalité :

- Nœud de stockage combiné de données et de métadonnées
- Nœud de stockage de métadonnées uniquement
- Nœud de stockage de données uniquement

Vous pouvez sélectionner le type de nœud de stockage dans ces situations :

- Lors de l'installation initiale d'un nœud de stockage
- Lorsque vous ajoutez un nœud de stockage lors de l'extension du système StorageGRID



Vous ne pouvez pas modifier le type une fois l'installation du nœud de stockage terminée.

Nœud de stockage de données et de métadonnées (combiné)

Par défaut, tous les nouveaux nœuds de stockage stockeront à la fois les données d'objet et les métadonnées. Ce type de nœud de stockage est appelé nœud de stockage *combiné*.

Nœud de stockage de métadonnées uniquement

L'utilisation d'un nœud de stockage exclusivement pour les métadonnées peut être judicieuse si votre grille stocke un très grand nombre de petits objets. L'installation d'une capacité de métadonnées dédiée offre un meilleur équilibre entre l'espace nécessaire à un très grand nombre de petits objets et l'espace nécessaire aux métadonnées de ces objets. De plus, les nœuds de stockage contenant uniquement des métadonnées hébergés sur des appliances hautes performances peuvent augmenter les performances.

Les nœuds de stockage de métadonnées uniquement ont des exigences matérielles spécifiques :

- Lors de l'utilisation d'appliances StorageGRID, les nœuds de métadonnées uniquement peuvent être configurés uniquement sur les appliances SGF6112 avec douze disques de 1,9 To ou douze disques de 3,8 To.
- Lors de l'utilisation de nœuds basés sur des logiciels, les ressources de nœuds contenant uniquement des métadonnées doivent correspondre aux ressources de nœuds de stockage existantes. Par exemple:
 - Si le site StorageGRID existant utilise des appliances SG6000 ou SG6100, les nœuds de métadonnées uniquement basés sur des logiciels doivent répondre aux exigences minimales suivantes :
 - 128 Go de RAM
 - processeur à 8 cœurs
 - SSD de 8 To ou stockage équivalent pour la base de données Cassandra (rangedb/0)

- Si le site StorageGRID existant utilise des nœuds de stockage virtuels avec 24 Go de RAM, un processeur à 8 cœurs et 3 To ou 4 To de stockage de métadonnées, les nœuds de métadonnées uniquement basés sur un logiciel doivent utiliser des ressources similaires (24 Go de RAM, un processeur à 8 cœurs et 4 To de stockage de métadonnées (rangedb/0)).
- Lors de l'ajout d'un nouveau site StorageGRID, la capacité totale des métadonnées du nouveau site doit, au minimum, correspondre aux sites StorageGRID existants et les nouvelles ressources du site doivent correspondre aux nœuds de stockage des sites StorageGRID existants.

Lors de l'installation de nœuds contenant uniquement des métadonnées, la grille doit également contenir un nombre minimum de nœuds pour le stockage des données :

- Pour une grille à site unique, configurez au moins deux nœuds de stockage combinés ou de données uniquement.
- Pour une grille multisite, configurez au moins un nœud de stockage combiné ou de données uniquement *par site*.



Bien que les nœuds de stockage contenant uniquement des métadonnées contiennent les [Service LDR](#) et peut traiter les demandes des clients S3, les performances de StorageGRID peuvent ne pas augmenter.

Nœud de stockage de données uniquement

L'utilisation d'un nœud de stockage exclusivement pour les données peut être judicieuse si vos nœuds de stockage présentent des caractéristiques de performances différentes. Par exemple, pour potentiellement augmenter les performances, vous pouvez disposer de nœuds de stockage à disque rotatif haute capacité uniquement pour les données, accompagnés de nœuds de stockage hautes performances uniquement pour les métadonnées.

Lors de l'installation de nœuds de données uniquement, la grille doit contenir les éléments suivants :

- Un minimum de deux nœuds de stockage combinés ou de données uniquement *par grille*
- Au moins un nœud de stockage combiné ou de données uniquement *par site*
- Un minimum de trois nœuds de stockage combinés ou de métadonnées uniquement *par site*

Services principaux pour les nœuds de stockage

Le tableau suivant présente les principaux services des nœuds de stockage ; toutefois, ce tableau ne répertorie pas tous les services de nœud.



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

Service	Fonction clé
Compte (acct)	Gère les comptes des locataires.

Service	Fonction clé
Contrôleur de domaine administratif (ADC)	Maintient la topologie et la configuration à l'échelle du réseau. Remarque : les nœuds de stockage de données uniquement n'hébergent pas le service ADC. Détails Le service Contrôleur de domaine administratif (ADC) authentifie les nœuds de grille et leurs connexions entre eux. Le service ADC est hébergé sur un minimum de trois nœuds de stockage sur 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 d'un autre nœud de grille ou une action à effectuer par un autre nœud de grille, il contacte un service ADC pour trouver le meilleur nœud de grille pour traiter sa demande. De plus, le service ADC conserve une copie des bundles de configuration du déploiement StorageGRID , permettant à n'importe quel nœud de grille de récupérer les informations de configuration actuelles. Pour faciliter les opérations distribuées et isolées, chaque service ADC synchronise les certificats, les ensembles 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 grille maintiennent une connexion à au moins un service ADC. Cela garantit que les nœuds de la grille accèdent toujours aux informations les plus récentes. Lorsque les nœuds de grille se connectent, ils mettent en cache les certificats des autres nœuds de grille, permettant aux systèmes de continuer à fonctionner avec les nœuds de grille connus même lorsqu'un service ADC n'est pas disponible. Les nouveaux nœuds de grille ne peuvent établir des connexions qu'en utilisant un service ADC. La connexion de chaque nœud de grille permet au service ADC de collecter des informations sur la topologie. Ces informations sur le nœud de grille incluent la charge du processeur, l'espace disque disponible (s'il dispose d'un stockage), les services pris en charge et l'ID du site du nœud de grille. D'autres services demandent au service ADC des informations de topologie via des requêtes de topologie. Le service ADC répond à chaque requête avec les dernières informations reçues du système StorageGRID .
Cassandra	Stocke et protège les métadonnées des objets. Remarque : les nœuds de stockage de données uniquement n'hébergent pas le service Cassandra.

Service	Fonction clé
Cassandra Reaper	Effectue des réparations automatiques des métadonnées des objets. Remarque : les nœuds de stockage de données uniquement n'hébergent pas le service Cassandra Reaper.
Gros morceau	Gère les données codées par effacement et les fragments de parité.
Déplaceur de données (DMV)	Déplace les données vers les pools de stockage cloud.
Magasin de données distribué (DDS)	Surveille le stockage des métadonnées des objets. Détails Chaque nœud de stockage inclut le service de magasin de données distribuées (DDS). Ce service 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 . Le service DDS suit le nombre total d'objets ingérés dans le système StorageGRID ainsi que le nombre total d'objets ingérés via chacune des interfaces prises en charge du système (S3).
Identité (idnt)	Fédère les identités des utilisateurs de LDAP et Active Directory.

Service	Fonction clé
Routeur de distribution local (LDR)	Traite les demandes du protocole de stockage d'objets et gère les données d'objets sur le disque.

Service	Fonction clé
Machine à états répliquée (RSM)	Garantit que les demandes de services de la plateforme S3 sont envoyées à leurs points de terminaison respectifs.
Moniteur d'état du serveur (SSM)	Surveille le système d'exploitation et le matériel sous-jacent.

Qu'est-ce qu'un nœud de passerelle ?

Le service LDR gère les tâches suivantes :

Les nœuds de passerelle fournissent une interface d'équilibrage de charge dédiée que les applications clientes S3 peuvent utiliser pour se connecter à StorageGRID.

L'équilibrage de charge maximise la vitesse et la capacité de connexion en répartissant la charge de travail sur plusieurs nœuds de stockage. Les nœuds de passerelle sont facultatifs.

Le service d'équilibrage de charge StorageGRID est fourni sur tous les nœuds d'administration et tous les nœuds de passerelle. Il effectue la terminaison TLS (Transport Layer Security) des demandes client, inspecte les demandes et établit de nouvelles connexions sécurisées aux nœuds de stockage. Le service Load Balancer dirige de manière transparente les clients vers un nœud de stockage optimal, de sorte que la défaillance des nœuds ou même d'un site entier soit transparente.

Vous configurez un ou plusieurs points de terminaison d'équilibrage de charge sur défini le port unique protocole réseau (HTTPS ou HTTP) que les demandes client entrantes et sortantes utiliseront pour accéder aux services d'équilibrage de charge. Le service LDR mappe également chaque objet S3 à son ID unique.

Si nécessaire, vous pouvez regrouper les interfaces réseau de plusieurs nœuds de passerelle et nœuds d'administration dans un groupe haute disponibilité (HA). Si l'interface active du groupe HA échoue, une interface de sauvegarde peut gérer la charge de travail de l'application cliente. Voir "Gérer les groupes de haute disponibilité (HA)".

Services principaux pour les nœuds de passerelle

Le tableau suivant présente les principaux services des nœuds de passerelle ; toutefois, ce tableau ne répertorie pas tous les services de nœud.

Service	Fonction clé
Haute disponibilité	Gère les adresses IP virtuelles haute disponibilité pour les groupes de nœuds d'administration et de nœuds de passerelle. Remarque : ce service est également disponible sur les nœuds d'administration.

Protection des métadonnées

StorageGRID stocke les métadonnées des objets dans une base de données Cassandra, qui s'interface avec le service LDR.

Pour assurer la redondance et donc la protection contre les pertes, trois copies des métadonnées des objets sont conservées sur chaque site. Cette réplication n'est pas configurable et est effectuée automatiquement. Pour plus de détails, consultez la section "Gérer le stockage des métadonnées des objets".

Service	Fonction clé
Équilibreur de charge	Fournit un équilibrage de charge de couche 7 du trafic S3 des clients vers les nœuds de stockage. Il s'agit du mécanisme d'équilibrage de charge recommandé. Remarque : ce service est également disponible sur les nœuds d'administration.
Moniteur d'état du serveur (SSM)	Surveille le système d'exploitation et le matériel sous-jacent.

Qu'est-ce qu'un nœud d'archive ?

La prise en charge des nœuds d'archive a été supprimée.

Pour plus d'informations sur les nœuds d'archives, voir ["Qu'est-ce qu'un nœud d'archive \(site de documentation StorageGRID 11.8\)"](#) .

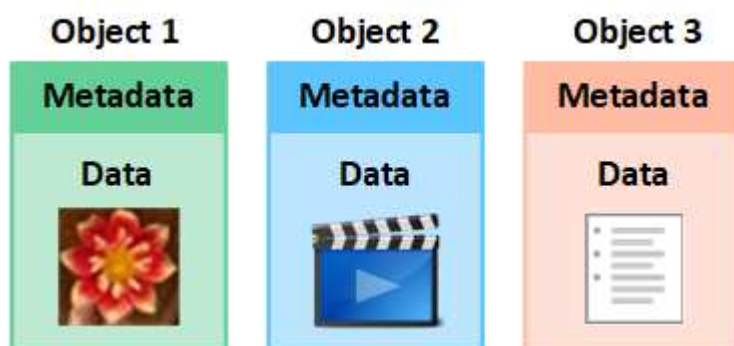
Comment StorageGRID gère les données

Qu'est-ce qu'un objet

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

Le stockage d'objets dissocie l'emplacement physique des données de la méthode utilisée pour stocker et récupérer ces données.

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



Que sont les données d'objet ?

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

Que sont les métadonnées d'objet ?

Les métadonnées d'objet sont toutes les informations qui décrivent un objet. StorageGRID utilise les métadonnées des objets pour suivre les emplacements de tous les objets sur la grille et pour gérer le cycle de vie de chaque objet au fil du temps.

Les métadonnées d'objet incluent des informations telles que les suivantes :

- Métadonnées système, y compris un identifiant 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 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.
- L'emplacement de stockage actuel de chaque copie d'objet ou fragment codé par effacement.
- Toutes les métadonnées utilisateur associées à l'objet.

Les métadonnées des objets sont personnalisables et extensibles, ce qui les rend flexibles à utiliser pour les applications.

Pour des informations détaillées sur la manière et l'endroit où StorageGRID stocke les métadonnées des objets, accédez à ["Gérer le stockage des métadonnées des objets"](#) .

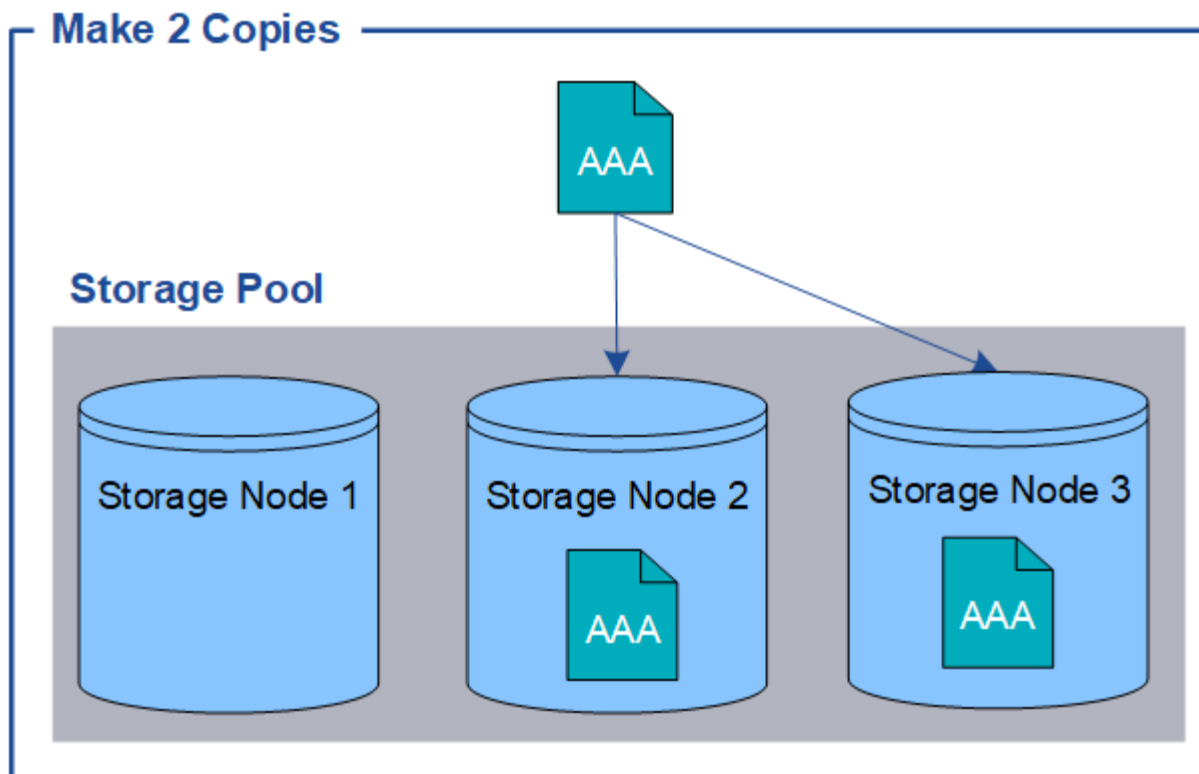
Comment les données des objets sont-elles protégées ?

Le système StorageGRID vous fournit deux mécanismes pour protéger les données des objets contre la perte : la réplication et le codage d'effacement.

Réplication

Lorsque StorageGRID fait correspondre des objets à 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 ou des pools de stockage cloud. Les règles ILM dictent le nombre de copies effectuées, l'endroit où ces copies sont stockées et la durée pendant laquelle elles sont conservées par le système. Si une copie est perdue, par exemple suite à la perte d'un nœud de stockage, l'objet est toujours disponible si une copie existe ailleurs dans le système StorageGRID .

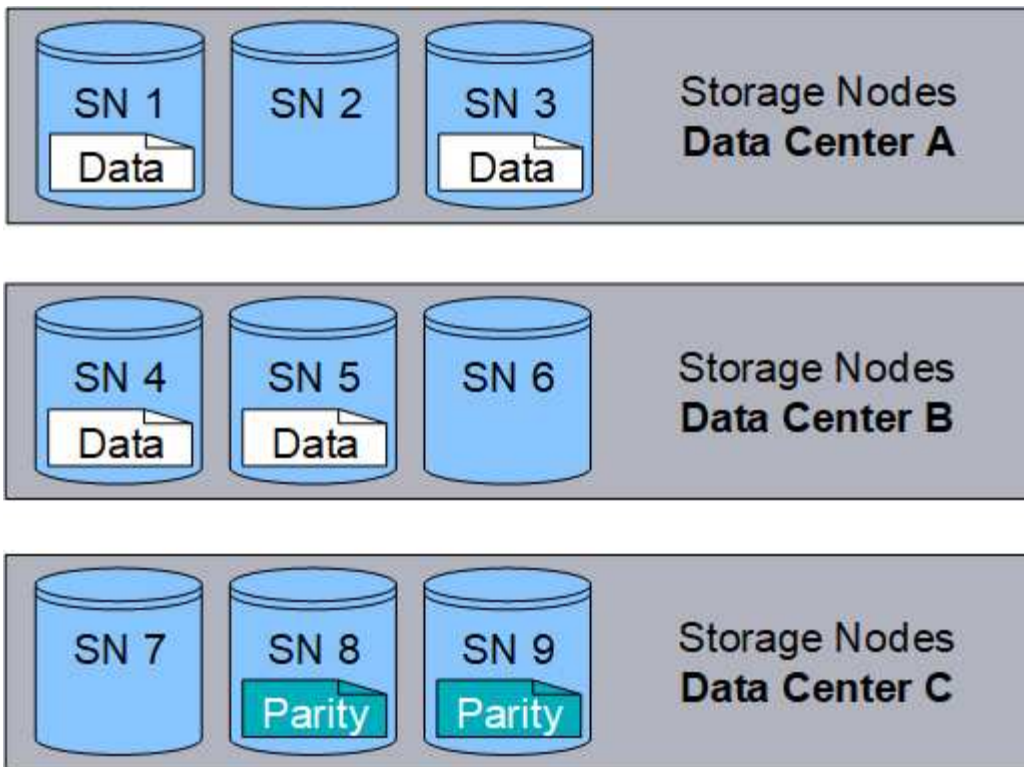
Dans l'exemple suivant, la règle Créer 2 copies spécifie que deux copies répliquées de chaque objet doivent être placées dans un pool de stockage contenant trois nœuds de stockage.



Codage d'effacement

Lorsque StorageGRID fait correspondre des objets à une règle ILM configurée pour créer des copies à code d'effacement, il découpe les données d'objet en fragments de données, calcule des fragments de parité supplémentaires et stocke chaque fragment sur un nœud de stockage différent. Lorsqu'un objet est consulté, il est réassemblé à l'aide des fragments stockés. Si des données ou un fragment de parité sont corrompus ou perdus, l'algorithme de codage d'effacement peut recréer ce fragment en utilisant un sous-ensemble des données et des fragments de parité restants. Les règles ILM et les profils de codage d'effacement déterminent le schéma de codage d'effacement utilisé.

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



Informations connexes

- ["Gérer les objets avec ILM"](#)
- ["Utiliser la gestion du cycle de vie des informations"](#)

La vie d'un objet

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

La vie d'un objet comprend les opérations d'ingestion, de gestion de copie, de récupération et de suppression.

- **Ingest** : Le processus par lequel une application client S3 enregistre un objet via HTTP sur le système StorageGRID . À ce stade, le système StorageGRID commence à gérer l'objet.
- **Gestion des copies** : processus de gestion des copies répliquées et codées par effacement dans StorageGRID, comme décrit par les règles ILM dans les politiques ILM actives. Au cours de l'étape de gestion des copies, StorageGRID protège les données d'objet contre la perte en créant et en conservant le nombre et le type spécifiés de copies d'objet sur les nœuds de stockage ou dans un pool de stockage cloud.
- **Récupérer** : Le processus d'une application cliente accédant à un objet stocké par le système StorageGRID . Le client lit l'objet, qui est récupéré à partir d'un nœud de stockage ou d'un pool de stockage cloud.
- **Supprimer** : Le processus de suppression de toutes les copies d'objets de la grille. Les objets peuvent être supprimés soit à la suite de l'envoi par l'application cliente d'une demande de suppression au système StorageGRID , soit à la suite d'un processus automatique exécuté par StorageGRID lorsque la durée de vie de l'objet expire.



Informations connexes

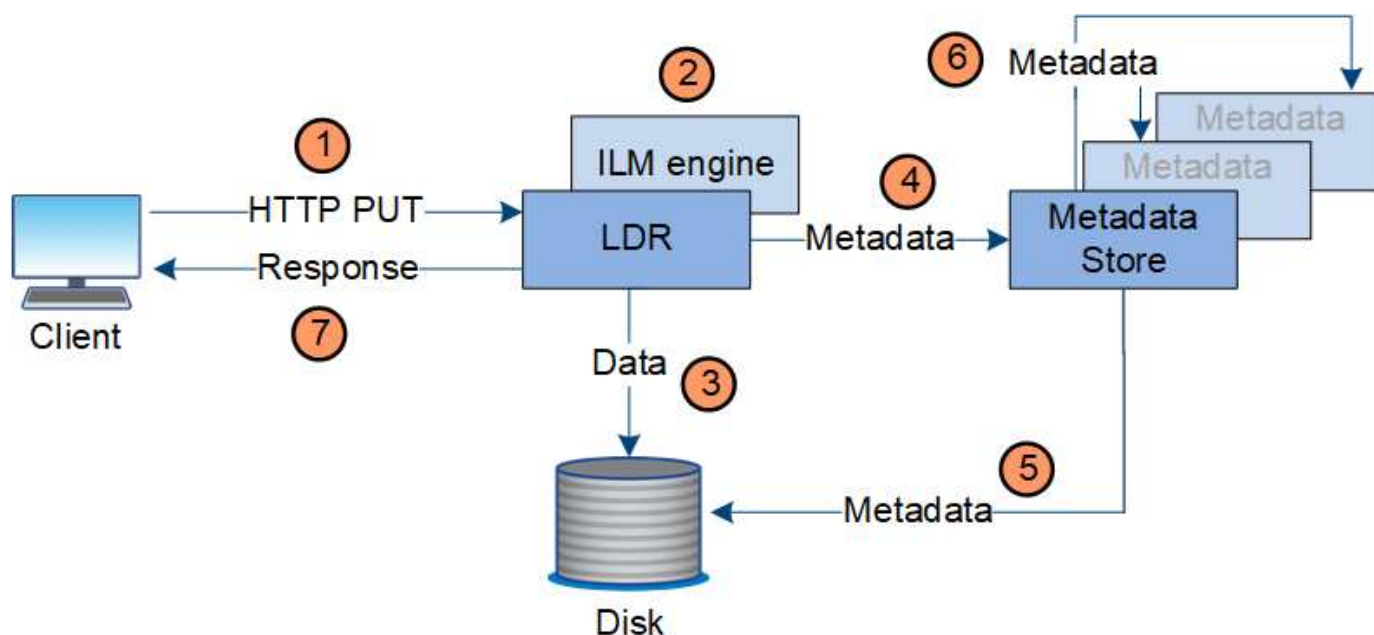
- ["Gérer les objets avec ILM"](#)
- ["Utiliser la gestion du cycle de vie des informations"](#)

Ingérer le flux de données

Une opération d'ingestion ou de sauvegarde consiste en 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 les nœuds de stockage traite la demande et stocke les métadonnées et les données sur le disque.



1. L'application cliente crée l'objet et l'envoie au système StorageGRID via une requête HTTP PUT.
2. L'objet est évalué par rapport à la politique ILM du système.
3. Le service LDR enregistre les données de l'objet sous forme de copie répliquée ou de copie à code d'effacement. (Le diagramme montre une version simplifiée du stockage d'une copie répliquée sur le disque.)
4. Le service LDR envoie les métadonnées de l'objet au magasin de métadonnées.
5. Le magasin de métadonnées enregistre les métadonnées de l'objet sur le disque.
6. Le magasin de métadonnées propage des copies des métadonnées d'objet vers 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 confirmer que l'objet a été ingéré.

Gestion des copies

Les données d'objet sont gérées par les politiques ILM actives et les règles ILM associées. Les règles ILM créent des copies répliquées ou codées par effacement pour protéger les données des objets contre la perte.

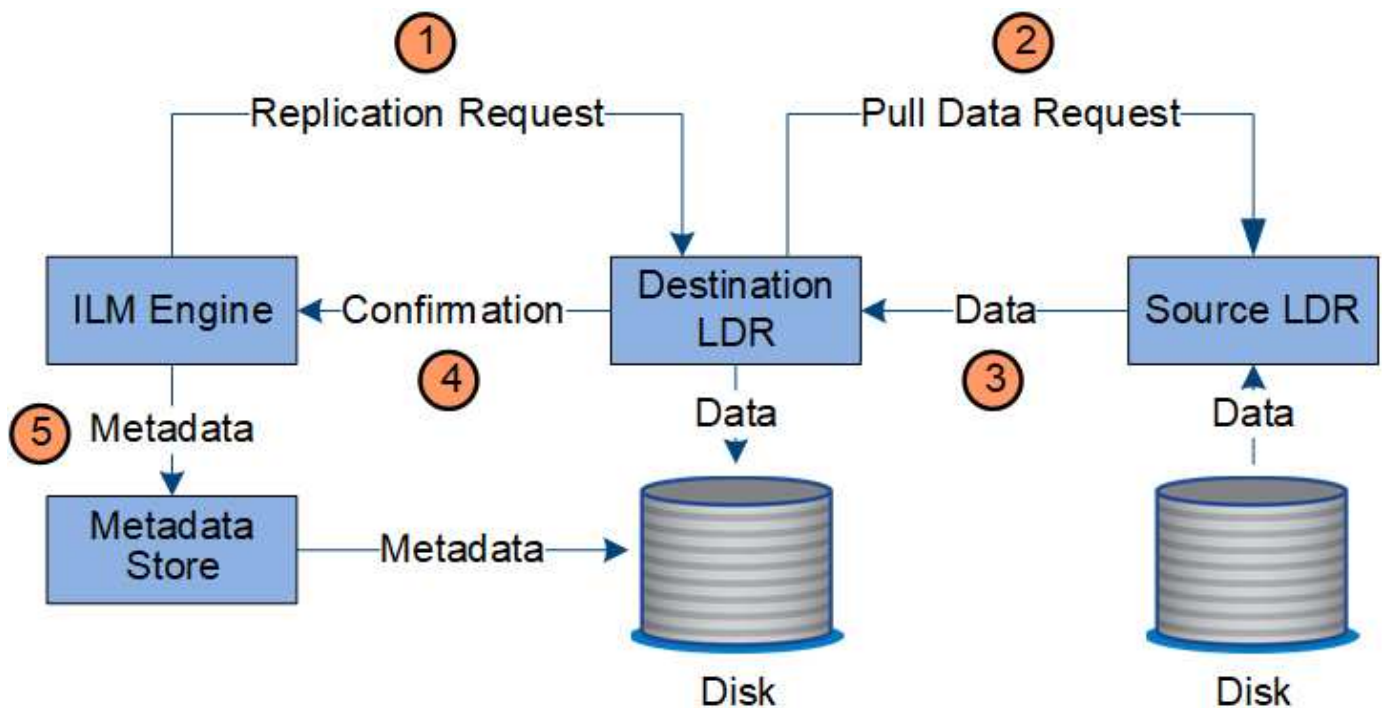
Différents types ou emplacements de copies d'objets peuvent être nécessaires à différents moments de la vie de l'objet. Les règles ILM sont évaluées périodiquement pour garantir que les objets sont placés comme requis.

Les données des objets 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 effectuées et stockées sur le disque par les nœuds de stockage qui composent le pool de stockage configuré.

Le moteur ILM du service LDR contrôle la réplication et garantit que le nombre correct de copies est stocké aux bons emplacements et pendant la durée correcte.



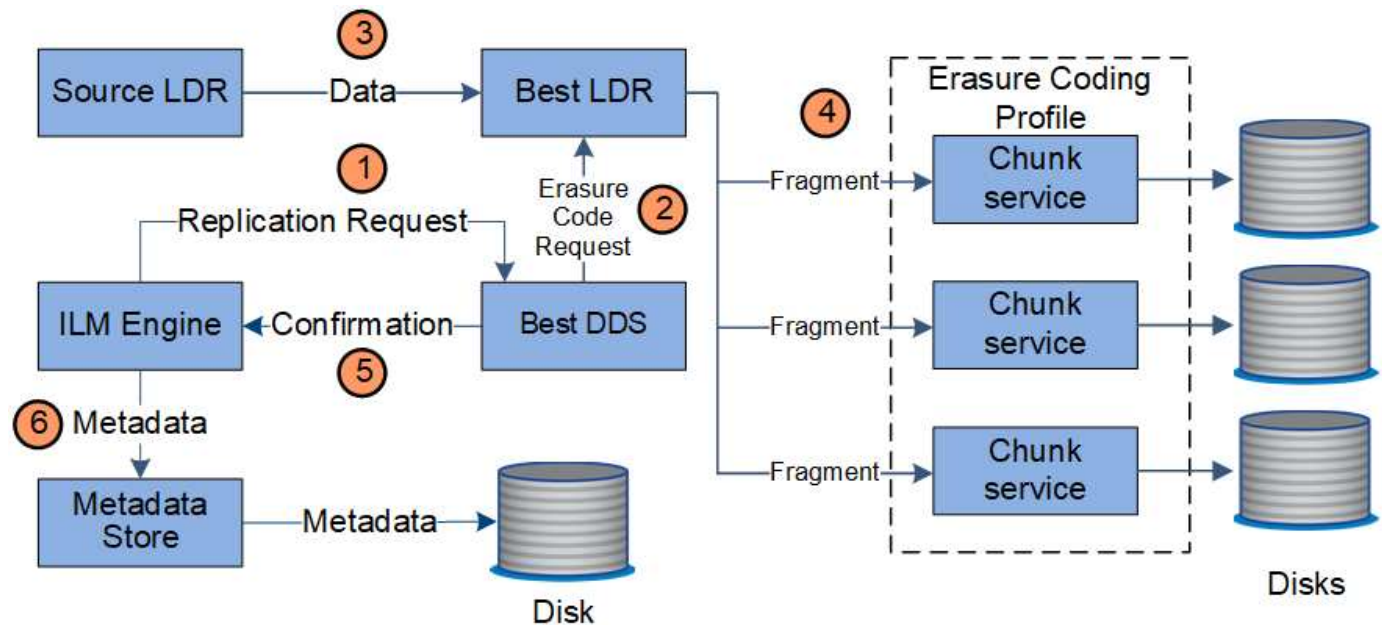
1. Le moteur ILM interroge le service ADC pour déterminer le meilleur service LDR de destination au sein du pool de stockage spécifié par la règle ILM. Il envoie ensuite à ce service LDR une commande pour lancer la réplication.
2. Le service LDR de destination interroge le service ADC pour connaître le meilleur emplacement source. Il envoie ensuite une demande de réplication au service LDR source.
3. Le service LDR source envoie une copie au service LDR de destination.
4. Le service LDR de destination informe le moteur ILM que les données de l'objet ont été stockées.

5. Le moteur ILM met à jour le magasin de métadonnées avec les métadonnées d'emplacement des objets.

Protection du contenu : codage d'effacement

Si une règle ILM inclut des instructions pour créer des copies codées par effacement des données d'objet, le schéma de codage par effacement applicable divise les données d'objet en fragments de données et de parité et distribue ces fragments sur les nœuds de stockage configurés dans le profil de codage par effacement.

Le moteur ILM, qui est un composant du service LDR, contrôle le codage d'effacement et garantit que le profil de codage d'effacement est appliqué aux données de l'objet.

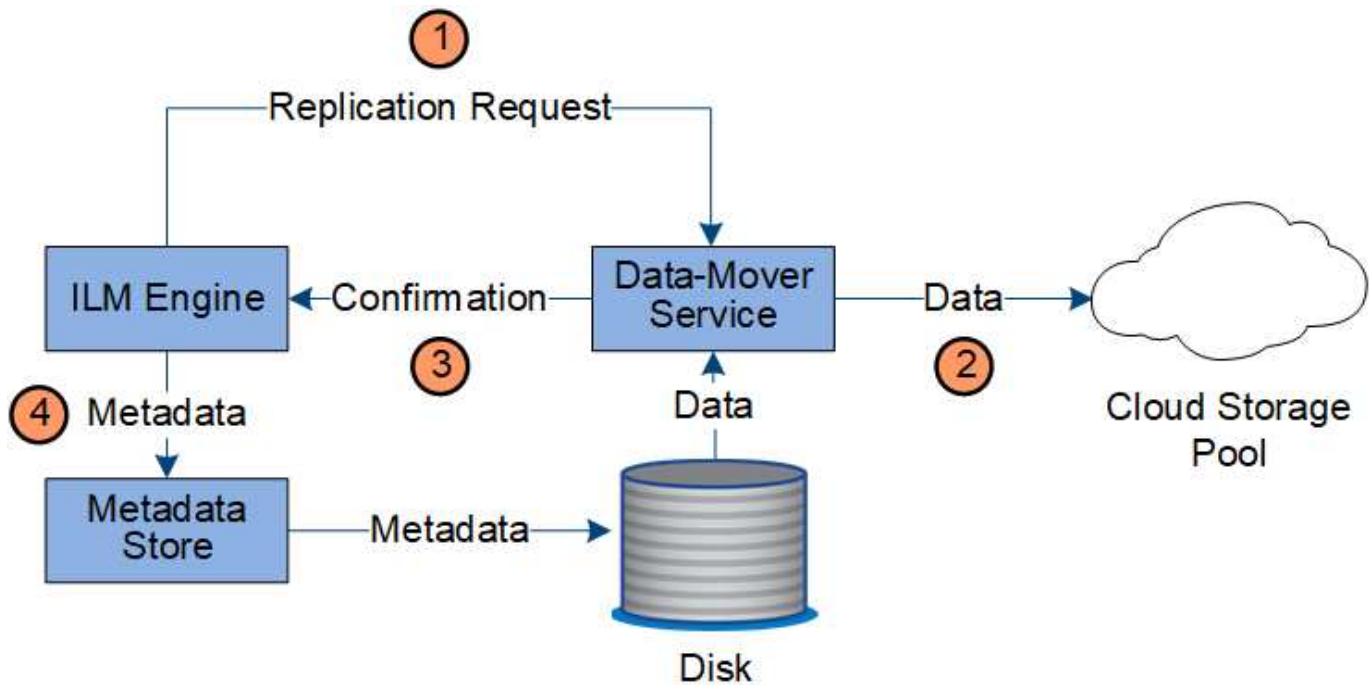


1. Le moteur ILM interroge le service ADC pour déterminer quel service DDS peut le mieux effectuer l'opération de codage d'effacement. Une fois déterminé, le moteur ILM envoie une demande « d'initiation » à ce service.
2. Le service DDS demande à un LDR d'effacer le code des données de l'objet.
3. Le service LDR source envoie une copie au service LDR sélectionné pour le codage d'effacement.
4. Après avoir créé le nombre approprié de fragments de parité et de données, le service LDR distribue ces fragments sur les nœuds de stockage (services de blocs) qui constituent le pool de stockage du profil de codage d'effacement.
5. Le service LDR notifie le moteur ILM, confirmant que les données de l'objet sont distribuées avec succès.
6. Le moteur ILM met à jour le magasin de métadonnées avec les métadonnées d'emplacement des objets.

Protection du contenu : pool de stockage cloud

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

Le moteur ILM, qui est un composant du service LDR, et le service Data Mover contrôlent le mouvement des objets vers le pool de stockage cloud.



1. Le moteur ILM sélectionne un service Data Mover à répliquer vers le pool de stockage cloud.
2. Le service Data Mover envoie les données de l'objet au pool de stockage cloud.
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 des objets.

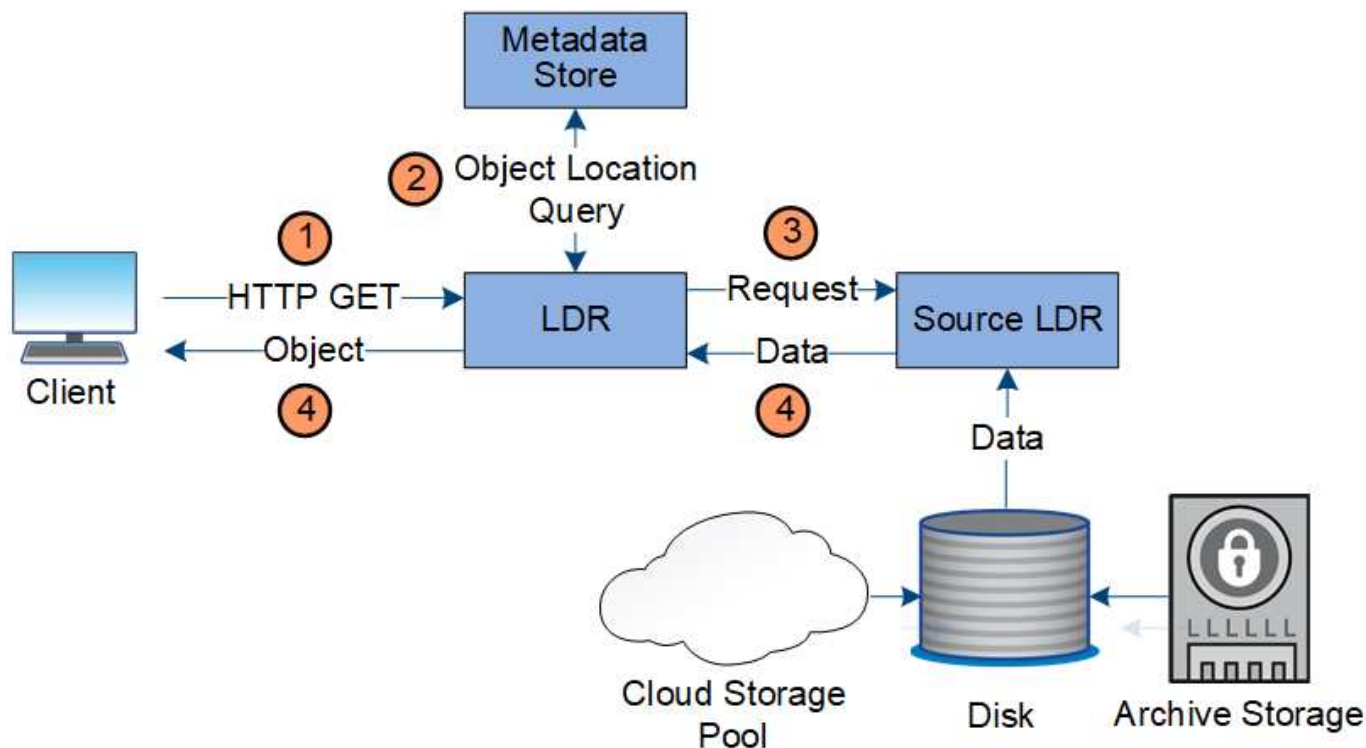
Récupérer le flux de données

Une opération de récupération consiste en 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.

Le service LDR du nœud de stockage interroge le magasin de métadonnées pour connaître l'emplacement des données de l'objet et les récupère à partir du service LDR source. De préférence, la récupération s'effectue 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.



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



1. Le service LDR reçoit une demande de récupération de l'application cliente.
2. Le service LDR interroge le magasin de métadonnées pour connaître l'emplacement des données de l'objet et les métadonnées.
3. Le service LDR transmet la demande 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 cliente.

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 la durée de vie de l'objet expire, déclenchant sa suppression automatique. Il existe un flux de données défini pour la suppression d'objets.

Hiérarchie de suppression

StorageGRID fournit plusieurs méthodes pour contrôler le moment où les objets sont conservés ou supprimés. Les objets peuvent être supprimés à la demande du client ou automatiquement. StorageGRID donne toujours la priorité aux paramètres de verrouillage d'objet S3 par rapport aux demandes de suppression des clients, qui sont prioritaires par rapport aux instructions de cycle de vie du compartiment S3 et de placement ILM.

- **Verrouillage d'objet S3** : si le paramètre global de verrouillage d'objet S3 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 jusqu'à la date et de conservation légale pour chaque version d'objet ajoutée à ce compartiment.
 - Une version d'objet soumise à une suspension légale ne peut être supprimée par aucune méthode.
 - Avant que la date de conservation d'une version d'objet ne soit atteinte, cette version ne peut être supprimée par aucune méthode.

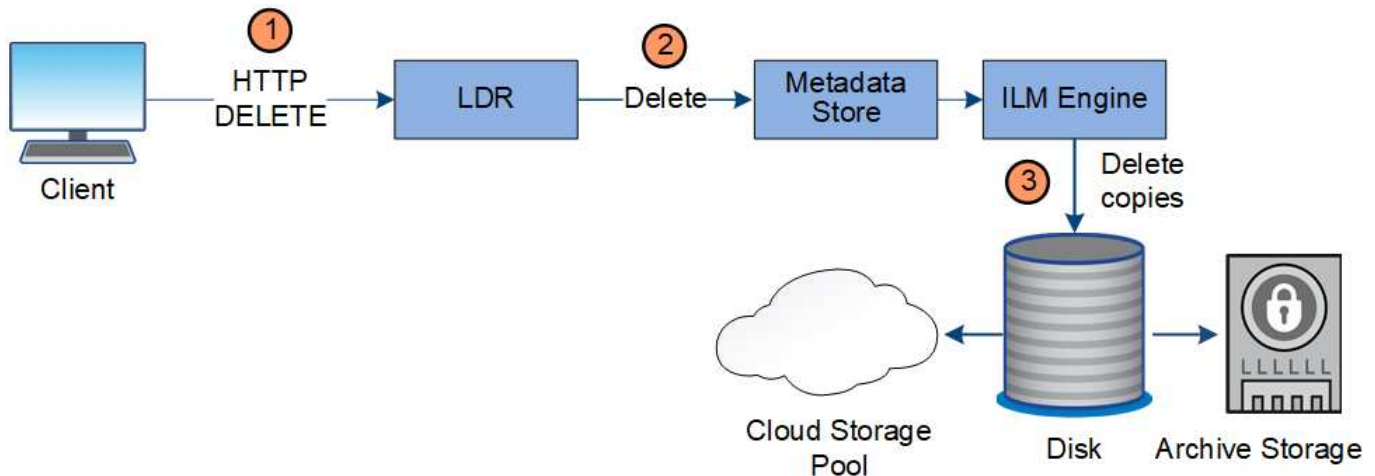
- Les objets dans les buckets avec le verrouillage d'objet S3 activé sont conservés par ILM « pour toujours ». Cependant, une fois sa date de conservation atteinte, une version d'objet peut être supprimée par une demande client ou par l'expiration du cycle de vie du bucket.
- Si les clients S3 appliquent une date de conservation par défaut au bucket, ils n'ont pas besoin de spécifier une date de conservation pour chaque objet.
- **Demande de suppression du client** : Un client S3 peut émettre une demande de suppression d'objet. Lorsqu'un client supprime un objet, toutes les copies de l'objet sont supprimées du système StorageGRID .
- **Supprimer les objets dans le bucket** : les utilisateurs de Tenant Manager peuvent utiliser cette option pour supprimer définitivement toutes les copies des objets et des versions d'objet dans les buckets sélectionnés du système StorageGRID .
- **Cycle de vie du bucket S3** : les clients S3 peuvent ajouter une configuration de cycle de vie à leurs buckets qui spécifie une action d'expiration. Si un cycle de vie de compartiment existe, StorageGRID supprime automatiquement toutes les copies d'un objet lorsque la date ou le nombre de jours spécifiés dans l'action Expiration est atteint, sauf si le client supprime d'abord l'objet.
- **Instructions de placement ILM** : En supposant que le verrouillage d'objet S3 n'est pas activé pour le bucket et qu'il n'y a pas de cycle de vie de bucket, 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.



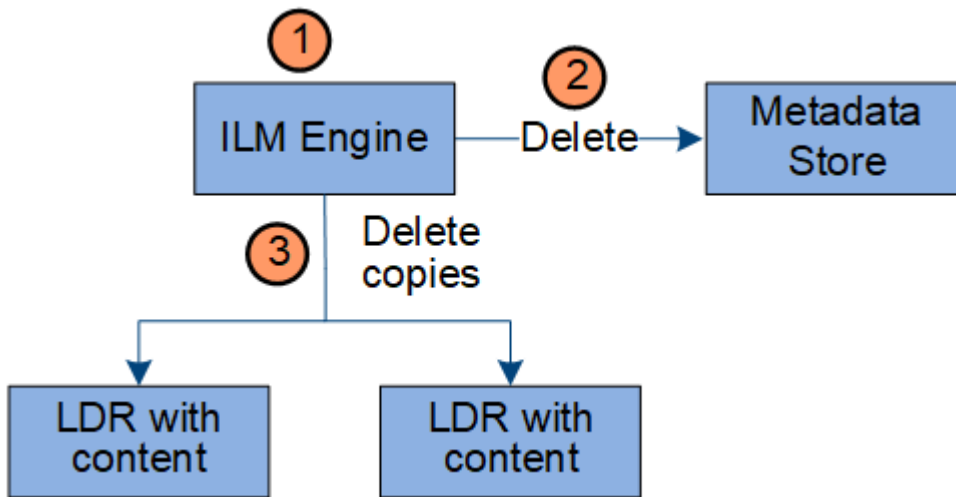
Lorsqu'un cycle de vie de compartiment S3 est configuré, les actions d'expiration du cycle de vie remplacent la stratégie ILM pour les objets qui correspondent au filtre de cycle de vie. Par conséquent, un objet peut être conservé sur la grille même après l'expiration des instructions ILM de placement de l'objet.

Voir "[Comment les objets sont supprimés](#)" pour plus d'informations.

Flux de données pour les suppressions de clients



1. Le service LDR reçoit une demande de suppression de l'application cliente.
2. Le service LDR met à jour le magasin de métadonnées afin que l'objet semble supprimé aux demandes des clients et demande au moteur ILM de supprimer toutes les copies des données de l'objet.
3. L'objet est supprimé du système. Le magasin de métadonnées est mis à jour pour supprimer les métadonnées de l'objet.



1. Le moteur ILM détermine que l'objet doit être supprimé.
2. Le moteur ILM notifie le magasin de métadonnées. Le magasin de métadonnées met à jour les métadonnées de l'objet afin que l'objet semble supprimé aux demandes des clients.
3. Le moteur ILM supprime toutes les copies de l'objet. Le magasin de métadonnées est mis à jour pour supprimer les métadonnées de l'objet.

Gestion du cycle de vie de l'information

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

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

Les règles ILM définissent :

- Quels objets doivent être stockés. 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 peut s'appliquer uniquement aux objets associés à certains comptes de locataire, à des buckets S3 ou conteneurs Swift spécifiques, ou à des valeurs de métadonnées spécifiques.
- Le type et l'emplacement de stockage. Les objets peuvent être stockés sur des nœuds de stockage ou dans des pools de stockage cloud.
- Le type de copies d'objets réalisées. Les copies peuvent être répliquées ou codées par effacement.
- Pour les copies répliquées, le nombre de copies réalisées.
- Pour les copies à codage d'effacement, le schéma de codage d'effacement utilisé.
- Les modifications apportées au fil du temps à l'emplacement de stockage d'un objet et au type de copies.
- Comment les données d'objet sont protégées lorsque les objets sont ingérés dans la grille (placement synchrone ou double validation).

Notez que les métadonnées des objets ne sont pas gérées par les règles ILM. Au lieu de cela, les métadonnées des objets sont stockées dans une base de données Cassandra dans ce que l'on appelle un

magasin de métadonnées. Trois copies des métadonnées de l'objet sont automatiquement conservées sur chaque site pour protéger les données contre toute perte.

Exemple de règle ILM

À titre d'exemple, une règle ILM pourrait spécifier ce qui suit :

- S'applique uniquement aux objets appartenant au locataire A.
- Créez deux copies répliquées de ces objets et stockez chaque copie dans un site différent.
- Conservez les deux copies « pour toujours », ce qui signifie que StorageGRID ne les supprimera pas automatiquement. Au lieu de cela, StorageGRID conservera ces objets jusqu'à ce qu'ils soient supprimés par une demande de suppression du client ou par l'expiration d'un cycle de vie de bucket.
- Utilisez l'option Équilibré pour le comportement d'ingestion : l'instruction de placement sur deux sites est appliquée dès que le locataire A enregistre un objet dans StorageGRID, sauf s'il n'est pas possible de créer immédiatement les deux copies requises.

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

Comment une politique ILM évalue les objets

Les stratégies ILM actives pour votre système StorageGRID contrôlent le placement, la durée et le comportement d'ingestion de tous les objets.

Lorsque les clients enregistrent des objets dans StorageGRID, les objets sont évalués par rapport à l'ensemble ordonné de règles ILM dans la politique active, comme suit :

1. Si les filtres de la première règle de la politique correspondent à un objet, l'objet est ingéré selon le comportement d'ingestion de cette règle et stocké selon les 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 suivante de la politique jusqu'à ce qu'une correspondance soit établie.
3. Si aucune règle ne correspond à un objet, le comportement d'ingestion et les instructions de placement de la règle par défaut dans la politique sont appliqués. La règle par défaut est la dernière règle d'une politique et ne peut utiliser aucun filtre. Cela doit s'appliquer à tous les locataires, à tous les buckets et à toutes les versions d'objet.

Exemple de politique ILM

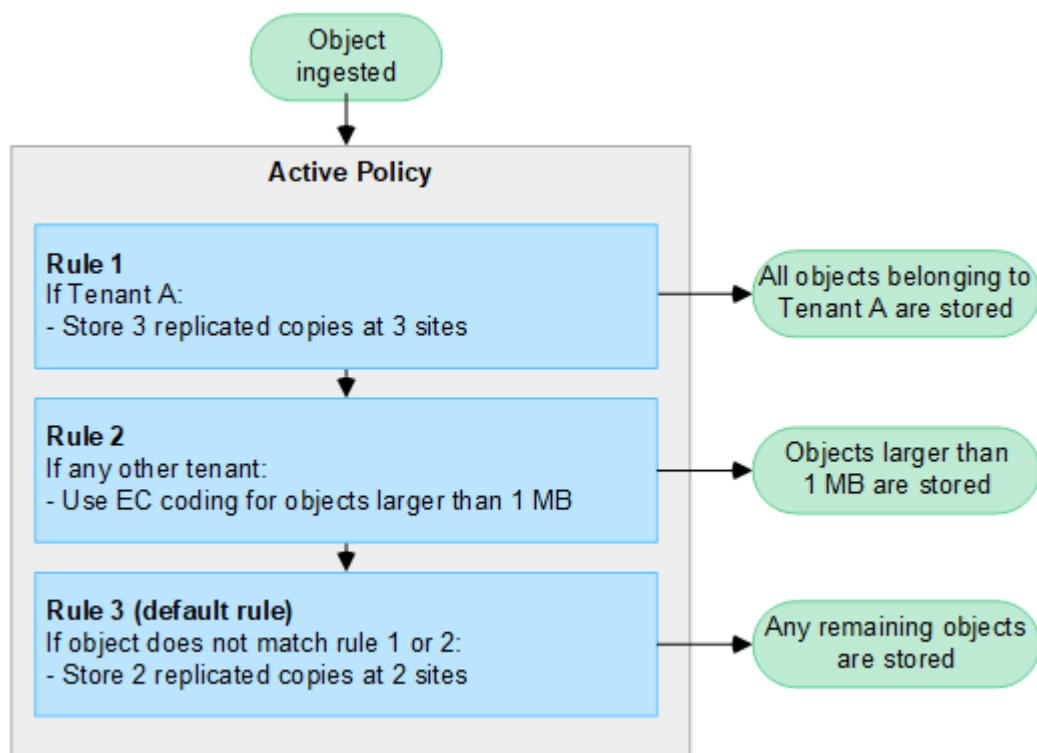
À titre d'exemple, une politique ILM pourrait contenir trois règles ILM qui spécifient les éléments suivants :

- **Règle 1 : Copies dupliquées 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 : Codage d'effacement pour les objets supérieurs à 1 Mo**
 - Faites correspondre tous les objets des autres locataires, mais uniquement s'ils sont supérieurs à 1 Mo. Ces objets plus grands sont stockés à l'aide du codage d'effacement 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)

- Il s'agit de la dernière règle par défaut de la politique. N'utilise pas de filtres.
- Créez deux copies répliquées de tous les objets ne correspondant pas à la règle 1 ou à la règle 2 (objets n'appartenant pas au locataire A et dont la taille est de 1 Mo ou moins).



Informations connexes

- ["Gérer les objets avec ILM"](#)

Découvrez StorageGRID

Explorez le gestionnaire de grille

Grid Manager est l'interface graphique basée sur un navigateur qui vous permet de configurer, de gérer et de surveiller votre système StorageGRID .



Le gestionnaire de grille est mis à jour à chaque version et peut ne pas correspondre aux exemples de captures d'écran sur cette page.

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

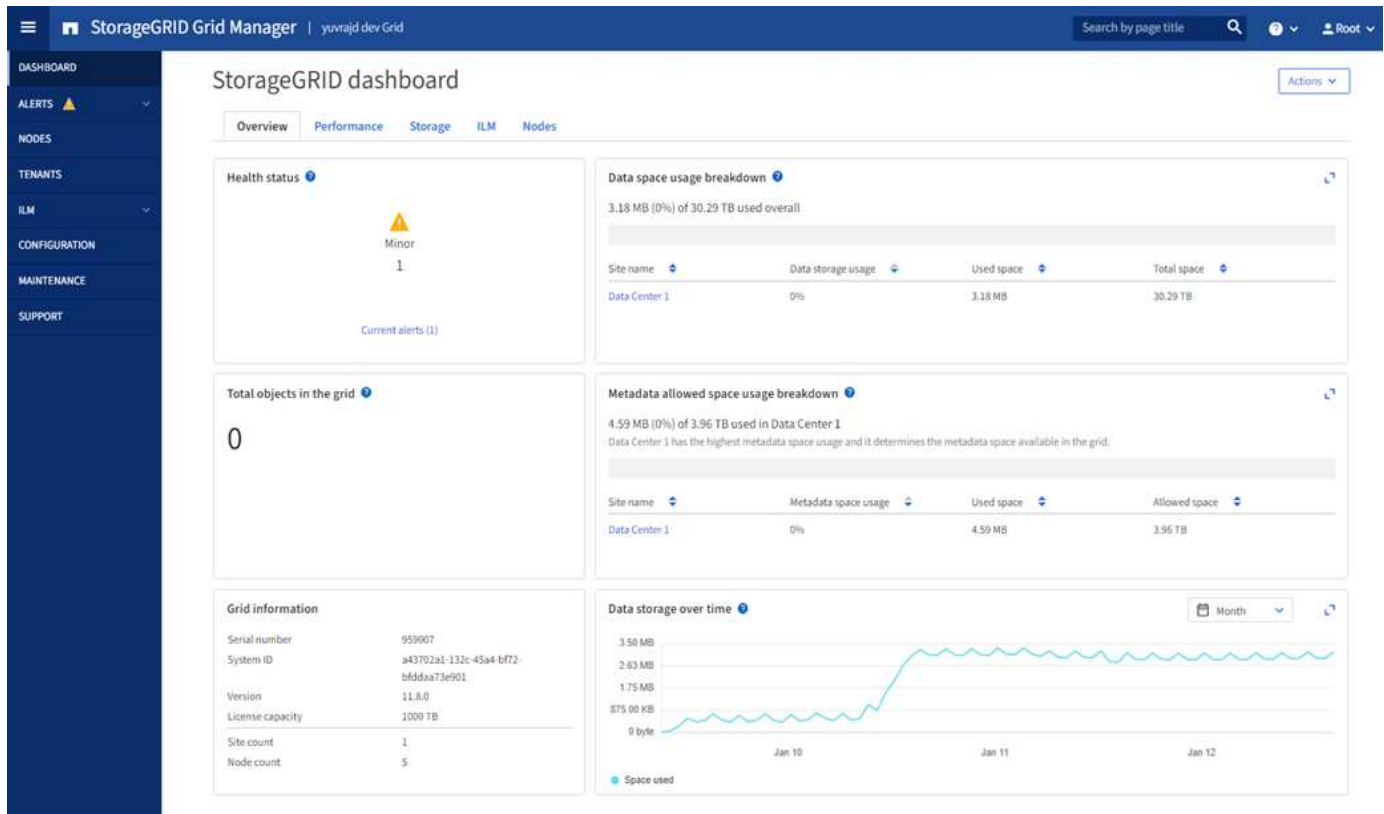
Vous pouvez accéder au gestionnaire de grille à l'aide d'un ["navigateur Web pris en charge"](#) .

Tableau de bord du gestionnaire de grille

Lorsque vous vous connectez pour la première fois au Grid Manager, 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 les nœuds de la grille. Tu peux "configurer le tableau de bord" en sélectionnant parmi une collection 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.

Champ de recherche

Le champ **Rechercher** dans la barre d'en-tête vous permet de naviguer rapidement vers une page spécifique dans Grid Manager. Par exemple, vous pouvez saisir **km** pour accéder à la page du serveur de gestion des clés (KMS).

Vous pouvez utiliser **Rechercher** pour rechercher des entrées dans la barre latérale du gestionnaire de grille et dans les menus Configuration, Maintenance et Support. Vous pouvez également rechercher par nom des éléments tels que des nœuds de grille et des comptes locataires.

Menu d'aide

Le menu d'aide ? donne accès à :

- Le "FabricPool" et "Configuration S3" magicien
- Le centre de documentation StorageGRID pour la version actuelle
- "Documentation API"
- Informations sur la version de StorageGRID actuellement installée

Menu des alertes

Le menu Alertes fournit une interface facile à utiliser pour détecter, évaluer et résoudre les problèmes pouvant survenir pendant le fonctionnement de StorageGRID .

Depuis le menu Alertes, vous pouvez effectuer les opérations suivantes pour ["gérer les alertes"](#) :

- Consultez les alertes actuelles
- Examiner les alertes résolues
- Configurer les silences pour supprimer les notifications d'alerte
- Définir des règles d'alerte pour les conditions qui déclenchent des alertes
- Configurer le serveur de messagerie pour les notifications d'alerte

Page des nœuds

Le ["Page des nœuds"](#) affiche des informations sur l'ensemble de la grille, chaque site de la grille et chaque nœud d'un site.

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

Nodes

View the list and status of sites and grid nodes.

Total node count: 14

Name ?	Type	Object data used ?	Object metadata used ?	CPU usage ?
StorageGRID Deployment	Grid	0%	0%	—
^ Data Center 1	Site	0%	0%	—
✓ DC1-ADM1	Primary Admin Node	—	—	21%
✓ DC1-ARC1	Archive Node	—	—	8%
✓ DC1-G1	Gateway Node	—	—	10%
✓ DC1-S1	Storage Node	0%	0%	29%

Page des locataires

Le ["Page des locataires"](#) vous permet de ["créer et surveiller les comptes des locataires de stockage"](#) pour votre système StorageGRID . Vous devez créer au moins un compte locataire pour spécifier qui peut stocker et récupérer des objets et quelles fonctionnalités leur sont disponibles.

La page Locataires fournit également des détails d'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 quelle partie de ce quota a été utilisée.

Tenants

View information for each tenant account. Depending on the timing of ingests, network connectivity, and node status, the usage data shown might be out of date. To view more recent values, select the tenant name.

CreateExport to CSVActions

Search tenants by name or ID

Displaying 2 results

☐	Name	Logical space used	Quota utilization	Quota	Object count	Sign in/Copy URL
☐	S3 Tenant	0 bytes	0%	100.00 GB	0	→ 📄
☐	Swift Tenant	0 bytes	0%	100.00 GB	0	→ 📄

← Previous1Next →

Menu ILM

Le "Menu ILM" vous permet de "configurer les règles et politiques de gestion du cycle de vie de l'information (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.

Depuis le menu ILM, vous pouvez afficher et gérer ILM :

- Règles
- Politiques
- Balises de politique
- Piscines de stockage
- Niveaux de stockage
- Régions
- Recherche de métadonnées d'objet

Menu de 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 du réseau comprennent :

- "Gestion des groupes de haute disponibilité"
- "Gestion des points de terminaison de l'équilibreur de charge"
- "Configuration des noms de domaine des points de terminaison S3"
- "Gestion des politiques 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 de clés"
- Configuration des paramètres de sécurité, y compris le "Politique TLS et SSH" , "options de sécurité du réseau et des objets" , et "paramètres de sécurité de l'interface" .
- Configuration des paramètres d'un "proxy de stockage" ou un "proxy d'administration"

Tâches système

Les tâches du système incluent :

- En utilisant "fédération de réseau" pour cloner les informations du compte locataire et répliquer les données d'objet entre deux systèmes StorageGRID .
- En option, activer le "Compresser les objets stockés" option.
- "Gestion du verrouillage des objets S3"
- Comprendre les options de stockage telles que "segmentation d'objets" et "filigranes de volume de stockage" .
- "Gérer les profils de codage d'effacement" .

Tâches de surveillance

Les tâches de surveillance comprennent :

- "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'administrateurs"
- "Gestion des utilisateurs administrateurs"
- Changer le "phrase de passe d'approvisionnement" ou "mots de passe de la console du nœud"
- "Utilisation de la fédération d'identité"
- "Configuration de SSO"

Menu de 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 comprennent :

- ["Opérations de démantèlement"](#) pour supprimer les nœuds de grille et les sites inutilisés
- ["Opérations d'expansion"](#) pour ajouter de nouveaux nœuds de grille et sites
- ["Procédures de récupération des nœuds de 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 (mais pas l'exactitude) des données de l'objet
- Effectuer une ["redémarrage progressif"](#) pour redémarrer plusieurs nœuds de grille
- ["Opérations de restauration de volume"](#)

Système

Les tâches de maintenance du système que vous pouvez effectuer incluent :

- ["Affichage des informations de licence StorageGRID"](#) ou ["mise à jour des informations de licence"](#)
- Génération et téléchargement du ["Paquet de relance"](#)
- Exécution des mises à jour du logiciel StorageGRID , y compris les mises à niveau logicielles, les correctifs et les mises à jour du logiciel SANtricity OS sur les appareils sélectionnés
 - ["Procédure de mise à niveau"](#)
 - ["Procédure de correctif"](#)
 - ["Mettre à niveau le système d'exploitation SANtricity sur les contrôleurs de stockage SG6000 à l'aide de Grid Manager"](#)
 - ["Mettre à niveau le système d'exploitation SANtricity sur les contrôleurs de stockage SG5700 à l'aide de Grid Manager"](#)

Réseau

Les tâches de maintenance du réseau que vous pouvez effectuer incluent :

- ["Configuration des serveurs DNS"](#)
- ["Mise à jour des sous-réseaux du réseau Grid"](#)
- ["Gestion des serveurs NTP"](#)

Menu d'assistance

Le menu Assistance fournit des options qui aident le support technique à analyser et à dépanner votre système.

Outils

Depuis la section Outils du menu Support, vous pouvez :

- ["Configurer AutoSupport"](#)
- ["Exécuter les diagnostics"](#) sur l'état actuel du réseau
- ["Accéder à l'arborescence de la topologie de la grille"](#) pour afficher des informations détaillées sur les nœuds de grille, les services et les attributs

- ["Collecter les fichiers journaux et les données système"](#)
- ["Examiner les mesures de support"](#)



Les outils disponibles à partir de l'option **Metrics** sont destinés à être utilisés par le support technique. Certaines fonctionnalités et éléments de menu de ces outils sont intentionnellement non fonctionnels.

Alarmes (héritage)

Les informations sur les alarmes héritées ont été supprimées de cette version de la documentation. Se référer à ["Gérer les alertes et les alarmes \(documentation StorageGRID 11.8\)"](#).

Autre

Depuis la section Autre du menu Support, vous pouvez :

- Gérer ["coût du lien"](#)
- Voir ["Système de gestion de réseau \(NMS\)"](#) entrées
- Gérer ["filigranes de stockage"](#)

Découvrez le gestionnaire de locataires

Le ["Gestionnaire de locataires"](#) est l'interface graphique basée sur un navigateur à laquelle les utilisateurs locataires accèdent pour configurer, gérer et surveiller leurs comptes de stockage.



Le gestionnaire de locataires est mis à jour à chaque version et peut ne pas correspondre aux exemples de captures d'écran sur cette page.

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

Tableau de bord du gestionnaire de locataires

Une fois qu'un administrateur de grille a créé un compte locataire à l'aide du gestionnaire de grille ou de l'API de gestion de grille, les utilisateurs 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 d'utilisation du stockage contient une liste des plus grands buckets (S3) ou conteneurs (Swift) pour le locataire. La valeur de l'espace utilisé correspond à la quantité totale de données d'objet dans le bucket ou le conteneur. Le graphique à barres représente les tailles relatives de ces seaux ou conteneurs.

La valeur affichée au-dessus du graphique à barres est la 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, la quantité de quota utilisée et restante est également affichée.

Dashboard

16**Buckets**[View buckets](#)**2****Platform services****endpoints**[View endpoints](#)**0****Groups**[View groups](#)**1****User**[View users](#)

Storage usage ?

6.5 TB of 7.2 TB used

0.7 TB (10.1%) remaining



Bucket name	Space used	Number of objects
Bucket-15	969.2 GB	913,425
Bucket-04	937.2 GB	576,806
Bucket-13	815.2 GB	957,389
Bucket-06	812.5 GB	193,843
Bucket-10	473.9 GB	583,245
Bucket-03	403.2 GB	981,226
Bucket-07	362.5 GB	420,726
Bucket-05	294.4 GB	785,190
8 other buckets	1.4 TB	3,007,036

Top buckets by capacity limit usage ?

Bucket name	Usage
Bucket-10	82%
Bucket-03	57%
Bucket-15	20%

Tenant details ?

Name: Tenant02

ID: 3341 1240 0546 8283 2208

- ✓ Platform services enabled
- ✓ Can use own identity source
- ✓ S3 Select enabled

Menu de stockage (S3)

Le menu Stockage est fourni uniquement pour les comptes locataires S3. Ce menu permet aux utilisateurs S3 de gérer les clés d'accès, de créer, de gérer et de supprimer des buckets, de gérer les points de terminaison des services de la plateforme et d'afficher toutes les connexions de fédération de grille qu'ils sont autorisés à utiliser.

Mes clés d'accès

Les utilisateurs du locataire S3 peuvent gérer les clés d'accès comme suit :

- 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 d'accès root peuvent gérer les clés d'accès pour le compte root S3, leur propre compte et tous les autres utilisateurs. Les clés d'accès racine fournissent également un accès complet aux compartiments et aux objets du locataire, sauf si elles sont explicitement désactivées par une stratégie de compartiment.



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

Seaux

Les utilisateurs locataires S3 disposant des autorisations appropriées peuvent effectuer les tâches suivantes

pour leurs compartiments :

- Créer des buckets
- Activer le verrouillage d'objet S3 pour un nouveau compartiment (en supposant que le verrouillage d'objet S3 est activé pour le système StorageGRID)
- Mettre à jour les valeurs de cohérence
- Activer et désactiver les mises à jour de l'heure du dernier accès
- Activer ou suspendre le contrôle de version des objets
- Mettre à jour la conservation par défaut du verrouillage des objets S3
- Configurer le partage de ressources inter-origines (CORS)
- Supprimer tous les objets d'un bucket
- Supprimer les compartiments vides
- Utilisez le ["Console S3"](#) pour gérer les objets du bucket

Si un administrateur de grille a activé l'utilisation des services de plateforme pour le compte locataire, un utilisateur locataire S3 disposant des autorisations appropriées peut également effectuer ces tâches :

- Configurez les notifications d'événements S3, qui peuvent être envoyées à un service de destination prenant en charge Amazon Simple Notification Service.
- Configurez la réplication CloudMirror, qui permet au locataire de répliquer automatiquement des objets vers un bucket S3 externe.
- Configurez l'intégration de recherche, qui envoie les métadonnées d'objet à un index de recherche de destination chaque fois qu'un objet est créé, supprimé ou que ses métadonnées ou balises sont mises à jour.

Points de terminaison des services de plateforme

Si un administrateur de grille a activé l'utilisation des services de plateforme pour le compte locataire, un utilisateur locataire S3 disposant de l'autorisation Gérer les points de terminaison peut configurer un point de terminaison de destination pour chaque service de plateforme.

Connexions de la fédération de réseau

Si un administrateur de grille a activé l'utilisation d'une connexion de fédération de grille pour le compte de locataire, un utilisateur de locataire S3 disposant de l'autorisation d'accès racine peut afficher le nom de la connexion, accéder à la page des détails du bucket pour chaque bucket dont la réplication inter-grille est activée et afficher l'erreur la plus récente survenue lors de la réplication des données du bucket vers l'autre grille de la connexion. Voir ["Afficher les connexions de la fédération de grille"](#) .

Menu de gestion des accès

Le menu Gestion des accès permet aux locataires StorageGRID d'importer des groupes d'utilisateurs à partir d'une source d'identité fédérée et d'attribuer des autorisations de gestion. Les locataires peuvent également gérer les groupes de locataires et les utilisateurs locaux, sauf si l'authentification unique (SSO) est en vigueur pour l'ensemble du système StorageGRID .

Directives de mise en réseau

Directives de mise en réseau

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

À propos de ces instructions

Ces instructions fournissent des informations que vous pouvez utiliser pour créer l'infrastructure réseau StorageGRID avant de déployer et de configurer les nœuds StorageGRID . Utilisez ces directives pour garantir que la communication peut avoir lieu 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 des fonctions telles que les suivantes :

- Stocker et récupérer des données d'objet
- Recevoir des notifications par e-mail
- Accéder à l'interface de gestion StorageGRID (le Grid Manager et le Tenant Manager)
- Accéder au partage d'audit (facultatif)
- Fournir des services tels que :
 - Protocole de temps réseau (NTP)
 - 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 plus encore.

Avant de commencer

La configuration du réseau pour un système StorageGRID nécessite un niveau élevé d'expérience en matière de commutation Ethernet, de 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 ["En savoir plus sur StorageGRID"](#) .

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

Installer des nœuds d'appareils

- ["Installer le matériel de l'appareil"](#)

Installer des nœuds basés sur des logiciels

- ["Installer StorageGRID sur Red Hat Enterprise Linux"](#)
- ["Installer StorageGRID sur Ubuntu ou Debian"](#)
- ["Installer StorageGRID sur VMware"](#)

Configurer et administrer le logiciel StorageGRID

- ["Administrer StorageGRID"](#)
- ["Notes de version"](#)

Types de réseaux StorageGRID

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

Types de trafic

Type de trafic	Description	Type de réseau
Trafic sur le réseau	Le trafic StorageGRID interne qui circule entre tous les nœuds de la grille. Tous les nœuds du réseau doivent pouvoir communiquer avec tous les autres nœuds du réseau sur ce réseau.	Réseau de grille (obligatoire)
Trafic administratif	Le 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 clientes externes et la grille, y compris toutes les demandes de stockage d'objets provenant des clients S3.	Réseau client (facultatif), Réseau VLAN (facultatif)

Vous pouvez configurer la mise en réseau des manières suivantes :

- Réseau de grille uniquement
- Réseaux de grille et d'administration
- Réseaux de grille et de clients
- Réseaux de grille, d'administration et de clients

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

Les ports internes ne sont accessibles que via le réseau Grid. Les ports externes sont accessibles depuis tous les types de réseaux. Cette flexibilité offre plusieurs options pour la conception d'un déploiement StorageGRID et la configuration du filtrage IP et des ports externes dans les commutateurs et les pare-feu.

Voir ["communications internes des nœuds de grille"](#) et ["communications externes"](#) .

Interfaces réseau

Les nœuds StorageGRID sont connectés à chaque réseau à l'aide des interfaces spécifiques suivantes :

Réseau	Nom de l'interface
Réseau de grille (obligatoire)	eth0
Réseau d'administration (facultatif)	eth1
Réseau client (facultatif)	eth2

Pour plus de détails sur le mappage des ports virtuels ou physiques aux interfaces réseau des nœuds, consultez les instructions d'installation :

Nœuds basés sur des logiciels

- ["Installer StorageGRID sur Red Hat Enterprise Linux"](#)
- ["Installer StorageGRID sur Ubuntu ou Debian"](#)
- ["Installer StorageGRID sur VMware"](#)

Nœuds d'appareils

- ["Appareil de stockage SG6160"](#)
- ["Appareil de stockage SGF6112"](#)
- ["Appareil de stockage SG6000"](#)
- ["Appareil de stockage SG5800"](#)
- ["Appareil de stockage SG5700"](#)
- ["Appareils de service SG110 et SG1100"](#)
- ["Appareils de service SG100 et SG1000"](#)

Informations réseau pour chaque nœud

Vous devez configurer les éléments suivants pour chaque réseau que vous activez 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 sur chaque nœud de grille. Si vous ne souhaitez pas configurer de passerelle pour un réseau, vous devez utiliser l'adresse IP comme adresse de passerelle.

Groupes de haute disponibilité

Les groupes haute disponibilité (HA) offrent la possibilité d'ajouter des adresses IP virtuelles (VIP) à l'interface réseau de grille ou de client. Pour plus d'informations, consultez la section ["Gérer les groupes de haute disponibilité"](#) .

Réseau de grille

Le réseau Grid est requis. Il est utilisé pour tout le trafic interne de StorageGRID . Le réseau Grid fournit une connectivité entre tous les nœuds du réseau, 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 constitué 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 peut être utilisé pour tout le trafic administrateur et tout le trafic client, même si le réseau administrateur et le réseau client sont configurés. La passerelle du 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 contre les clients non approuvés, tels que ceux présents sur Internet ouvert.

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

- La passerelle du réseau de grille doit être configurée s'il existe plusieurs sous-réseaux de grille.
- La passerelle du réseau Grid est la passerelle par défaut du nœud jusqu'à ce que la configuration du réseau soit terminée.
- Les itinéraires statiques sont générés automatiquement pour tous les nœuds vers tous les sous-réseaux configurés dans la liste globale des sous-réseaux du réseau Grid.
- Si un réseau client est ajouté, la passerelle par défaut passe de la passerelle du réseau de grille à la passerelle du réseau client une fois la configuration de la grille 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 d'administration est généralement un réseau privé et n'a pas besoin d'être routable entre les nœuds.

Vous pouvez choisir sur quels nœuds de grille le réseau d'administration doit être activé.

Lorsque vous utilisez le réseau d'administration, le trafic administratif et de maintenance n'a pas besoin de transiter par le réseau Grid. Les utilisations typiques du réseau d'administration incluent les suivantes :

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

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

Notez les exigences et les détails suivants pour la passerelle du réseau d'administration :

- La passerelle du réseau d'administration est requise si les connexions doivent être établies depuis l'extérieur du sous-réseau du réseau d'administration ou si plusieurs sous-réseaux du réseau d'administration sont configurés.
- Des itinéraires statiques sont créés pour chaque sous-réseau configuré dans la liste des sous-réseaux du réseau d'administration du nœud.

Réseau de clients

Le réseau client est facultatif. Une fois configuré, il est utilisé pour fournir l'accès aux services de grille pour les applications clientes telles que S3. Si vous prévoyez de rendre les données StorageGRID accessibles 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 grille peuvent communiquer avec n'importe quel sous-réseau accessible via la passerelle du réseau client.

Vous pouvez choisir sur quels nœuds de grille le réseau client doit être activé. Tous les nœuds ne doivent pas nécessairement se trouver sur le même réseau client et les nœuds ne communiqueront jamais entre eux via le réseau client. Le réseau client ne devient opérationnel qu'une fois l'installation du réseau terminée.

Pour plus de sécurité, vous pouvez spécifier que l'interface réseau client d'un nœud ne soit pas approuvée afin que le réseau client soit plus restrictif quant aux connexions autorisées. Si l'interface réseau client d'un nœud n'est pas approuvée, 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 points de terminaison d'équilibrage de charge. Voir ["Gérer les contrôles du pare-feu"](#) et ["Configurer les points de terminaison de l'équilibreur de charge"](#).

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

- Nœuds de passerelle, car ces nœuds fournissent l'accès au service d'équilibrage de charge StorageGRID et l'accès client S3 à la grille.
- Nœuds de stockage, car ces nœuds fournissent un accès au protocole S3, aux pools de stockage Cloud et au service de réplication CloudMirror.
- Nœuds d'administration, pour garantir que les utilisateurs locataires peuvent se connecter au gestionnaire de locataires sans avoir besoin d'utiliser le réseau d'administration.

Notez les points suivants pour la passerelle réseau client :

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

Réseaux VLAN optionnels

Si nécessaire, vous pouvez éventuellement utiliser des réseaux LAN virtuels (VLAN) pour le trafic client et pour certains types de trafic administrateur. Le trafic réseau ne peut cependant pas utiliser une 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) pour qu'elle soit une jonction, ou vous pouvez ajouter des interfaces de jonction au nœud.

Si eth0 est configuré comme une liaison, le trafic du réseau Grid circule sur l'interface native de la liaison, telle que configurée sur le commutateur. De même, si eth2 est configuré en tant que trunk et que le réseau client est également configuré sur le même nœud, le réseau client utilise le VLAN natif du port trunk tel que configuré sur le commutateur.

Seul le trafic d'administration entrant, tel que celui utilisé pour le trafic SSH, Grid Manager ou Tenant Manager, est pris en charge sur les réseaux VLAN. Le trafic sortant, tel que celui utilisé pour NTP, DNS, LDAP, KMS et

les pools de stockage cloud, n'est pas pris en charge sur les réseaux VLAN.



Les interfaces VLAN peuvent être ajoutées uniquement aux nœuds d'administration et aux nœuds de passerelle. Vous ne pouvez pas utiliser une interface VLAN pour l'accès client ou administrateur aux nœuds de stockage.

Voir "[Configurer les interfaces VLAN](#)" pour obtenir des instructions et des directives.

Les interfaces VLAN ne sont utilisées que dans les groupes HA et se voient attribuer des adresses VIP sur le nœud actif. Voir "[Gérer les groupes de haute disponibilité](#)" pour obtenir des instructions et des directives.

Exemples de topologie de réseau

Topologie du réseau en grille

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

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

Lors de la configuration, vous devez ajouter tous les sous-réseaux du réseau Grid à la liste des 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 qui fournissent un accès à des services critiques tels que NTP, DNS ou LDAP.

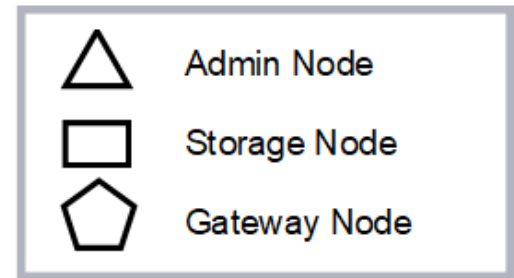
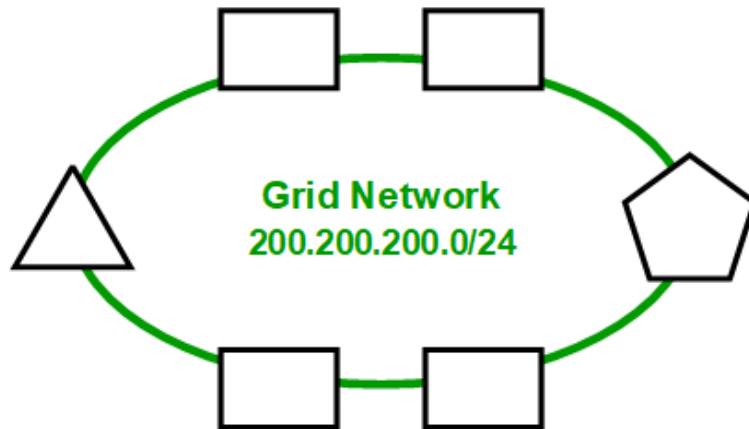
Lors de l'installation, l'interface Grid Network applique des itinéraires statiques pour tous les sous-réseaux du GNSL et définit l'itinéraire par défaut du nœud sur la passerelle Grid Network si elle est configurée. Le GNSL n'est pas requis s'il n'y a pas de réseau client et que la passerelle du réseau de grille est la route par défaut du nœud. Les routes hôtes 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 aux fonctions administratives et de maintenance.



Cette topologie est adaptée aux déploiements sur site unique qui ne sont pas disponibles en externe, aux déploiements de preuve de concept ou de test, ou lorsqu'un équilibreur de charge tiers agit comme limite d'accès client. Dans la mesure du possible, le réseau Grid doit être utilisé exclusivement pour le trafic interne. Le réseau d'administration et le réseau client disposent tous deux de restrictions de pare-feu supplémentaires 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.

Topology example: Grid Network only



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

Avoir un réseau d'administration est facultatif. Une façon d'utiliser un réseau d'administration et un réseau de grille consiste à configurer un réseau de grille routable et un réseau d'administration délimité pour chaque nœud.

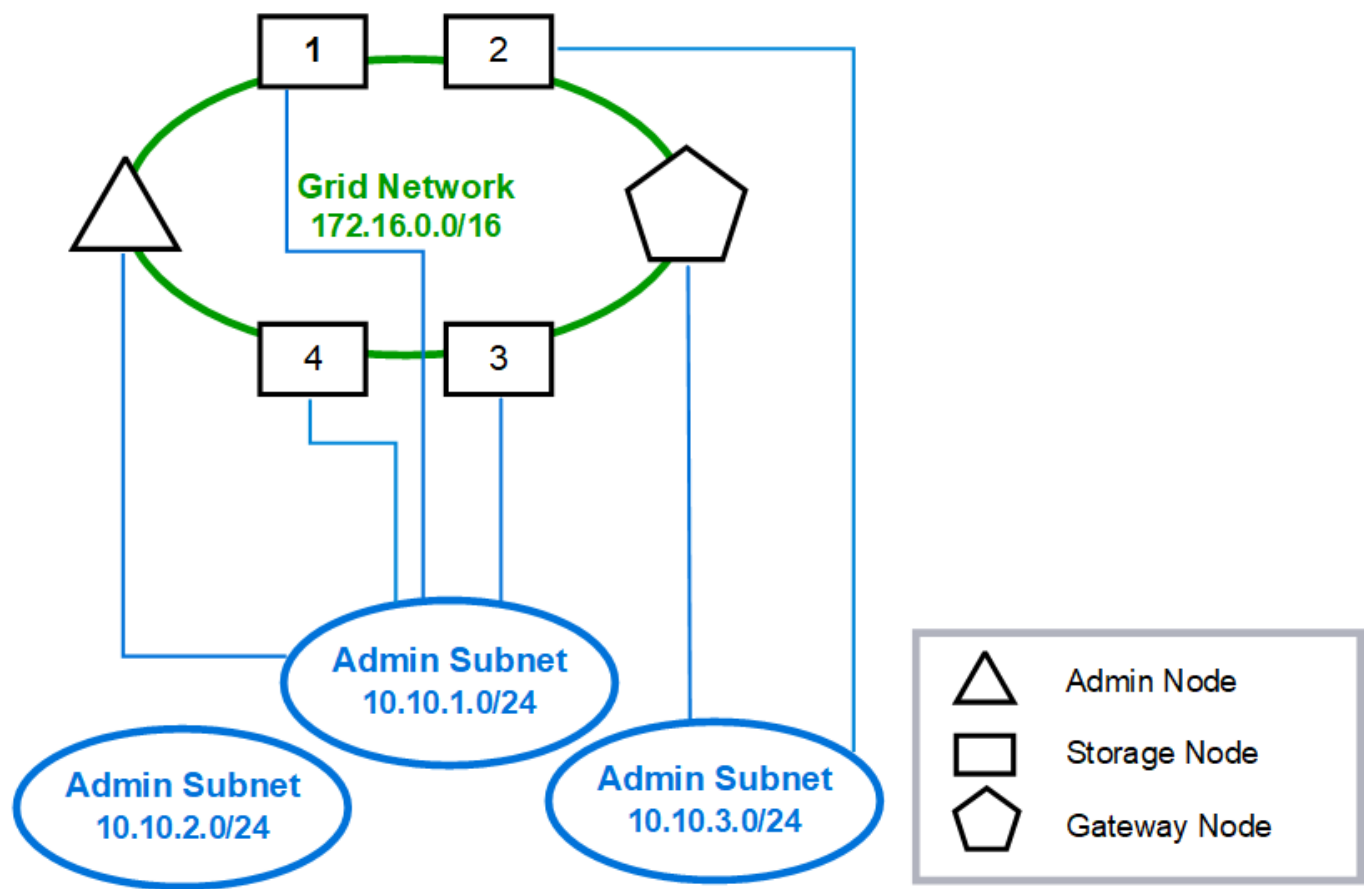
Lorsque vous configurez le réseau d'administration, vous établissez l'adresse IP de l'hôte, le masque de sous-réseau et l'adresse IP de la passerelle pour l'interface eth1 pour chaque nœud de grille.

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-réseaux externes d'administration (AESL). L'AESL répertorie les sous-réseaux accessibles via le réseau d'administration pour chaque nœud. L'AESL doit également inclure les sous-réseaux de tous les services auxquels la grille accédera via le réseau d'administration, tels que NTP, DNS, KMS et LDAP. Des itinéraires statiques sont appliqués pour chaque sous-

réseau de l'AESL.

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

Topology example: Grid and Admin Networks



GNSL → 172.16.0.0/16

AESL (all) → 10.10.1.0/24 10.10.2.0/24 10.10.3.0/24

Nodes	Grid Network		Admin Network	
	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

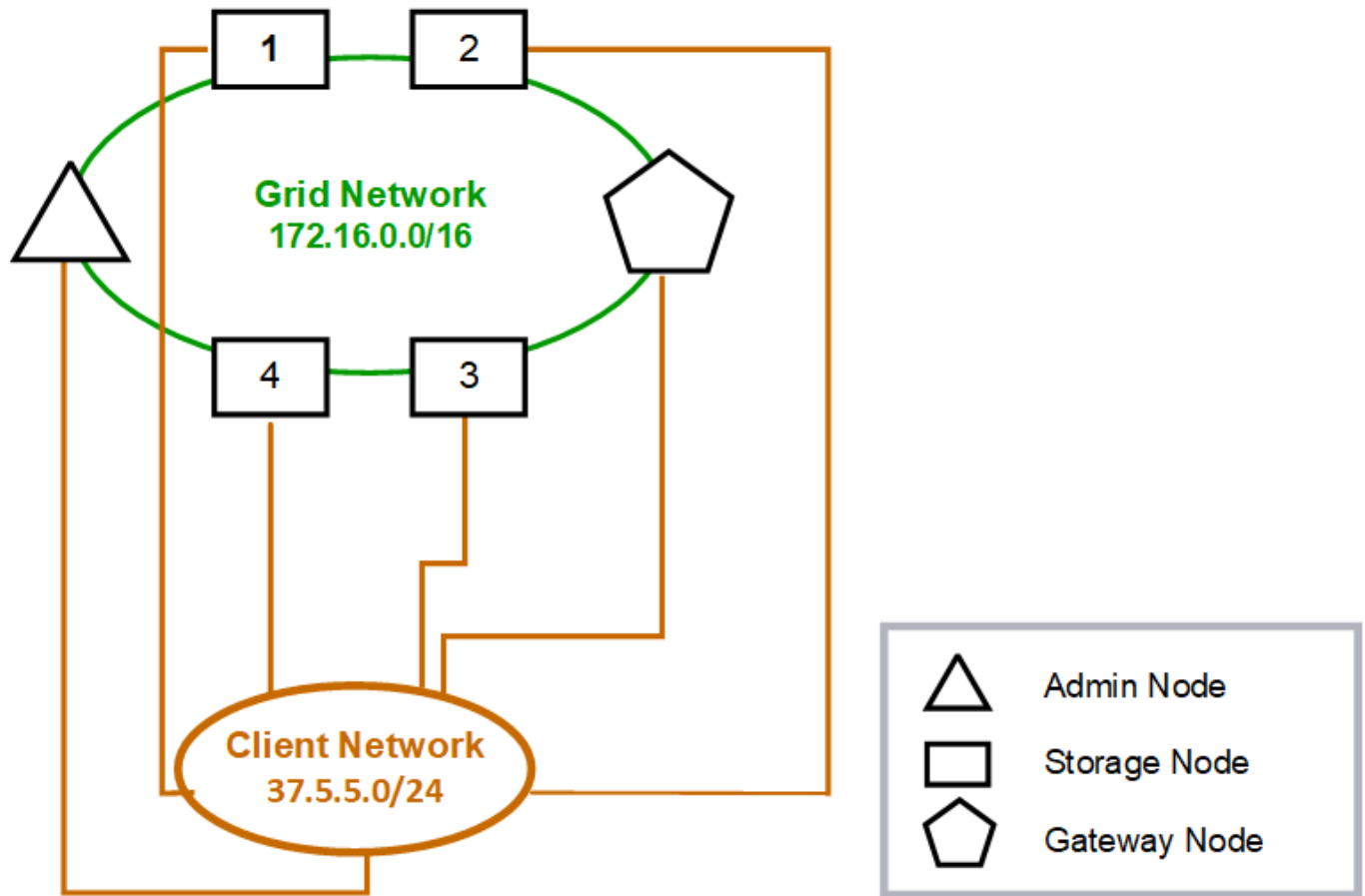
Avoir un réseau de clients est facultatif. L'utilisation d'un réseau client permet de séparer le trafic réseau client (par exemple, S3) du trafic interne du réseau, ce qui permet de sécuriser davantage le réseau du réseau. Le trafic administratif peut être géré par le client ou par le réseau de grille lorsque le réseau d'administration n'est pas configuré.

Lorsque vous configurez le réseau client, vous établissez 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 de tout autre nœud.

Si vous configurez un réseau client pour un nœud pendant l'installation, la passerelle par défaut du nœud passe de la passerelle du réseau de grille à la passerelle du 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 client S3 et pour les fonctions administratives, tandis que le réseau grille est dédié aux opérations de gestion d'objets internes.

Topology example: Grid and Client Networks



GNSL → 172.16.0.0/16

Nodes	Grid Network	Client Network	
	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

Informations connexes

["Modifier la configuration du réseau de nœuds"](#)

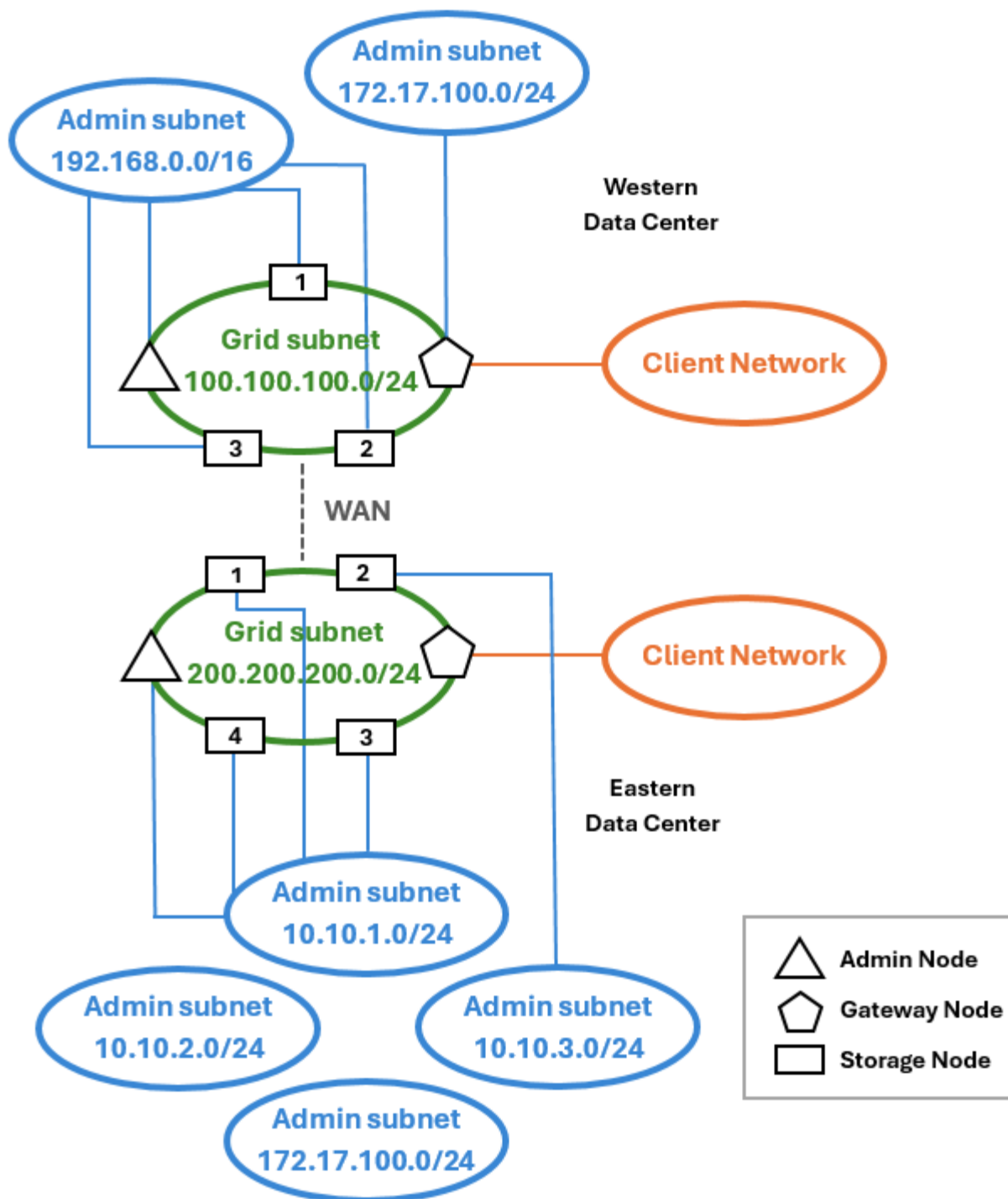
Topologie des trois réseaux

Vous pouvez configurer les trois réseaux dans une topologie de réseau composée d'un réseau de grille privé, de réseaux d'administration spécifiques au site délimités et de réseaux clients ouverts. L'utilisation de points de terminaison d'équilibrage de charge et de réseaux clients non approuvés peut fournir une sécurité supplémentaire si nécessaire.

Dans cet exemple :

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

Exemple de topologie : réseaux grille, administrateur et client



Exigences de mise en réseau

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

Exigences générales de mise en réseau

Tous les déploiements StorageGRID doivent pouvoir prendre en charge les connexions suivantes.

Ces connexions peuvent se produire via les réseaux Grid, Admin ou Client, ou les combinaisons de ces réseaux, comme illustré dans les exemples de topologie de réseau.

- **Connexions de gestion** : connexions entrantes d'un administrateur vers le nœud, généralement via SSH. Accès par navigateur Web au Grid Manager, au Tenant Manager et au programme d'installation de l'appliance StorageGRID .
- **Connexions au 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 au serveur DNS** : connexion UDP sortante qui reçoit une réponse UDP entrante.
- **Connexions au serveur LDAP/Active Directory** : connexion TCP sortante depuis le service d'identité sur les nœuds de stockage.
- * AutoSupport*: Connexion TCP sortante des nœuds d'administration vers `support.netapp.com` ou un proxy configuré par le client.
- **Serveur de gestion de clés externe** : connexion TCP sortante depuis chaque nœud d'appliance avec chiffrement de nœud activé.
- Connexions TCP entrantes provenant de clients S3.
- Requêtes sortantes provenant des services de la plateforme StorageGRID tels que la réplication CloudMirror ou des pools de stockage Cloud.

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 tentera automatiquement de contacter tous les réseaux (Grille, Admin et Client) tant que les adresses IP des serveurs DNS et NTP sont spécifiées. Si les serveurs NTP ou DNS sont accessibles sur n'importe quel réseau, StorageGRID créera automatiquement des règles de routage supplémentaires pour garantir que le réseau est utilisé pour toutes les tentatives futures de connexion.



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

Si vous n'êtes pas prêt à configurer les réseaux administrateur et client facultatifs lors du déploiement, vous pouvez configurer ces réseaux lorsque vous approuvez les nœuds de grille pendant les étapes de configuration. De plus, vous pouvez configurer ces réseaux après l'installation, à l'aide de l'outil Modifier l'IP (voir "[Configurer les adresses IP](#)").

Seules les connexions client S3 et les connexions administratives SSH, Grid Manager et Tenant Manager sont prises en charge sur les interfaces VLAN. Les connexions sortantes, telles que celles vers les serveurs NTP, DNS, LDAP, AutoSupport et KMS, doivent passer directement par les interfaces client, administrateur ou réseau Grid. Si l'interface est configurée en tant que trunk pour prendre en charge les interfaces VLAN, ce trafic circulera sur le VLAN natif de l'interface, tel que 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 les sites doit avoir une bande passante minimale de 25 Mbit/seconde dans chaque direction avant de prendre en compte le trafic client. La réplication des données ou le codage d'effacement entre les sites, l'extension de nœud ou de site, la récupération de nœud et d'autres opérations ou configurations nécessiteront une bande passante supplémentaire.

Les exigences réelles en matière de bande passante WAN minimale dépendent de l'activité du client et du schéma de protection ILM. Pour obtenir de l'aide sur l'estimation des exigences minimales en matière de

bande passante WAN, contactez votre consultant NetApp Professional Services.

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

Les nœuds d'administration doivent toujours être protégés contre les clients non fiables, tels que ceux présents sur Internet ouvert. Vous devez vous assurer qu'aucun client non approuvé ne peut accéder à un nœud d'administration sur le réseau de grille, le réseau d'administration ou le réseau client.

Les nœuds d'administration et les nœuds de passerelle que vous prévoyez d'ajouter aux groupes de haute disponibilité doivent être configurés avec une adresse IP statique. Pour plus d'informations, consultez la section "[Gérer les groupes de haute disponibilité](#)".

Utilisation de la traduction d'adresses réseau (NAT)

N'utilisez pas la traduction d'adresses réseau (NAT) sur le réseau Grid 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 grille sur chaque site. Toutefois, si nécessaire, vous pouvez utiliser NAT entre les clients externes et les nœuds de grille, par exemple pour fournir une adresse IP publique pour un nœud de passerelle. L'utilisation de 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

Suivez les exigences pour chaque type de réseau StorageGRID.

Passerelles et routeurs réseau

- Si cette option 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 n'avez pas de passerelle, la meilleure pratique consiste à définir l'adresse de la passerelle comme étant l'adresse IP de l'interface réseau.

Sous-réseaux



Chaque réseau doit être connecté à son propre sous-réseau qui ne chevauche aucun autre réseau sur le nœud.

Les restrictions suivantes sont appliquées par le gestionnaire de grille lors du déploiement. Ils sont fournis ici pour aider à la planification du réseau avant le déploiement.

- Le masque de sous-réseau pour toute 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.
- N'utilisez pas de sous-réseaux contenant les adresses IPv4 suivantes pour le réseau de grille, le réseau d'administration ou le réseau client d'un nœud :
 - 192 168 130 101

- 192.168.131.101
- 192.168.130.102
- 192.168.131.102
- 198.51.100.2
- 198.51.100.4

Par exemple, n'utilisez pas les plages de sous-réseaux suivantes pour le réseau de grille, le réseau d'administration ou le réseau client d'un nœud :

- 192.168.130.0/24 car cette plage de sous-réseaux contient les adresses IP 192.168.130.101 et 192.168.130.102
- 192.168.131.0/24 car cette plage de sous-réseaux contient les adresses IP 192.168.131.101 et 192.168.131.102
- 198.51.100.0/24 car cette plage de sous-réseaux contient les adresses IP 198.51.100.2 et 198.51.100.4
- Le sous-réseau Grid Network de chaque nœud doit être inclus dans le GNSL.
- Le sous-réseau du réseau d'administration ne peut pas chevaucher le sous-réseau du réseau de grille, le sous-réseau du réseau client ou tout autre sous-réseau du GNSL.
- Les sous-réseaux de l'AESL ne peuvent chevaucher aucun sous-réseau du GNSL.
- Le sous-réseau du réseau client ne peut pas chevaucher le sous-réseau du réseau de grille, le sous-réseau du réseau d'administration, aucun sous-réseau du GNSL ou aucun sous-réseau de l'AESL.

Réseau de grille

- Au moment du déploiement, chaque nœud de grille doit être connecté au réseau de 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.
- Lors du fonctionnement normal du réseau, chaque nœud du réseau doit pouvoir communiquer avec tous les autres nœuds du réseau via le réseau.



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

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

Réseau d'administration

Le réseau d'administration est facultatif. Si vous envisagez de configurer un réseau d'administration, suivez ces exigences et directives.

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 d'administration et l'AESL peuvent être uniques à chaque nœud, à condition que les services réseau et les clients souhaités soient 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. Les routes statiques sont générées automatiquement sur chaque nœud pour chaque sous-réseau de l'AESL.

Réseau de clients

Le réseau client est facultatif. Si vous envisagez de configurer un réseau client, tenez compte des considérations suivantes.

- Le réseau client est conçu pour prendre en charge le trafic des clients S3. Si elle est configurée, la passerelle réseau client devient la passerelle par défaut du nœud.
- Si vous utilisez un réseau client, vous pouvez contribuer à sécuriser StorageGRID contre les attaques hostiles en acceptant le trafic client entrant uniquement sur les points de terminaison d'équilibrage de charge explicitement configurés. Voir "[Configurer les points de terminaison de l'équilibreur de charge](#)".
- Si l'interface réseau client est configurée en tant que jonction pour prendre en charge les interfaces VLAN, déterminez si la configuration de l'interface réseau client (eth2) est nécessaire. Si configuré, le trafic réseau client circulera sur le VLAN natif du trunk, tel que configuré dans le commutateur.

Informations connexes

["Modifier la configuration du réseau de nœuds"](#)

Considérations relatives au réseau spécifiques au déploiement

Déploiements Linux

Pour des raisons d'efficacité, de fiabilité et de sécurité, le système StorageGRID fonctionne sous Linux en tant qu'ensemble de moteurs de conteneurs. La configuration réseau liée au moteur de conteneur n'est pas requise dans un système StorageGRID.

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



N'utilisez pas de périphériques 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 avec l'utilisation de macvlan avec les périphériques bond et bridge dans l'espace de noms du conteneur.

Consultez les instructions d'installation pour "[Red Hat Enterprise Linux](#)" ou "[Ubuntu ou Debian](#)" déploiements.

Configuration du réseau hôte pour les déploiements de moteurs de conteneurs

Avant de démarrer votre déploiement StorageGRID sur une plateforme de moteur de conteneur, 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 virtuelle ou physique correcte et que chaque réseau dispose d'une bande passante suffisante.

Hôtes physiques

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

- Assurez-vous 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 future des nœuds.
- Obtenez 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 sur l'hôte.
- Si vous envisagez 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 nœuds sous la forme eth0, eth2 ou sous la forme d'interfaces supplémentaires. Pour ajouter des interfaces de jonction ou d'accès, consultez les éléments suivants :
 - **RHEL (avant l'installation du nœud) :** ["Créer des fichiers de configuration de nœud"](#)
 - **Ubuntu ou Debian (avant d'installer le nœud) :** ["Créer des fichiers de configuration de nœud"](#)
 - **RHEL, Ubuntu ou Debian (après l'installation du nœud) :** ["Linux : ajouter des interfaces trunk ou d'accès à un nœud"](#)

Recommandations de bande passante minimale

Le tableau suivant fournit les recommandations de bande passante LAN minimale 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 exigences de bande passante minimale globale pour le nombre total et le type de nœuds StorageGRID que vous prévoyez d'exécuter sur cet hôte.

Type de nœud	Type de réseau		
	Grille	Administrateur	Client
	Bande passante LAN minimale	Administrateur	10 Gbit/s
1 Gbit/s	1 Gbit/s	Porte	10 Gbit/s
1 Gbit/s	10 Gbit/s	Stockage	10 Gbit/s
1 Gbit/s	10 Gbit/s	Archive	10 Gbit/s



Ce tableau n'inclut pas la bande passante SAN, qui est 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 une bande passante SAN suffisante. Pour éviter d'introduire un goulot d'étranglement, la bande passante SAN pour un hôte donné doit correspondre approximativement à la bande passante réseau globale du nœud de stockage pour tous les nœuds de stockage exécutés sur cet hôte.

Utilisez le tableau pour déterminer le nombre minimum 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 seul hôte :

- Connectez le réseau et les réseaux d'administration sur le nœud d'administration (nécessite $10 + 1 = 11$ Gbit/s)
- Connectez le réseau et les réseaux clients sur le nœud de passerelle (nécessite $10 + 10 = 20$ Gbit/s)
- Connectez le réseau Grid sur le nœud de stockage (nécessite 10 Gbit/s)

Dans ce scénario, vous devez fournir un minimum de $11 + 20 + 10 = 41$ Gbit/s de bande passante réseau, qui pourrait être satisfaite par deux interfaces de 40 Gbit/s ou cinq interfaces de 10 Gbit/s, potentiellement agrégées en trunks 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 certaines méthodes recommandées de configuration des ressources physiques et réseau sur les hôtes de votre cluster StorageGRID afin de préparer votre déploiement StorageGRID , consultez les éléments suivants :

- ["Configurer le réseau hôte \(Red Hat Enterprise Linux\)"](#)
- ["Configurer le réseau hôte \(Ubuntu ou Debian\)"](#)

Réseaux et ports pour les services de plateforme et les pools de stockage cloud

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

Mise en réseau des services de plateforme

Comme décrit dans ["Gérer les services de la plateforme pour les locataires"](#) et ["Gérer les services de la plateforme"](#) , les services de plateforme incluent des services externes qui fournissent l'intégration de la recherche, la notification d'événements et la réplication CloudMirror.

Les services de plateforme nécessitent un accès depuis les nœuds de stockage qui hébergent le service StorageGRID ADC aux points de terminaison de service externes. Voici quelques exemples de mesures d'accès :

- Sur les nœuds de stockage avec services ADC, configurez des réseaux d'administration uniques avec des entrées AESL qui acheminent vers les points de terminaison cibles.
- Fiez-vous à l'itinéraire par défaut fourni par un réseau client. Si vous utilisez l'itinéraire par défaut, vous pouvez utiliser le ["fonctionnalité de réseau client non fiable"](#) pour restreindre les connexions entrantes.

Mise en réseau pour les pools de stockage cloud

Les pools de stockage cloud nécessitent également un accès depuis les nœuds de stockage aux points de terminaison fournis par le service externe utilisé, tel qu'Amazon S3 Glacier ou le stockage Microsoft Azure Blob. Pour plus d'informations, voir ["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 du Cloud Storage Pool utilisent les ports suivants :

- **80** : pour les URI de point de terminaison qui commencent par `http`
- **443** : pour les URI de point de terminaison qui commencent par `https`

Un port différent peut être spécifié lors de la création ou de la modification du point de terminaison. Voir ["Référence du port réseau"](#) .

Si vous utilisez un serveur proxy non transparent, vous devez également ["configurer les paramètres du proxy de stockage"](#) pour permettre l'envoi de messages à des points de terminaison externes, tels qu'un point de terminaison sur Internet.

VLAN et services de plateforme et pools de stockage cloud

Vous ne pouvez pas utiliser les réseaux VLAN pour les services de plateforme ou les pools de stockage cloud. Les points de terminaison de destination doivent être accessibles via le réseau Grid, Admin ou Client.

Nœuds d'appareils

Vous pouvez configurer les ports réseau sur les appliances StorageGRID pour utiliser les modes de liaison de port 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 du réseau d'administration 1 GbE peuvent être configurés en mode indépendant ou de sauvegarde active pour les connexions au réseau d'administration.

Consultez les informations sur les modes de liaison de port pour votre appareil :

- ["Modes de liaison des ports \(SG6160\)"](#)
- ["Modes de liaison des ports \(SGF6112\)"](#)
- ["Modes de liaison de port \(contrôleur SG6000-CN\)"](#)
- ["Modes de liaison de port \(contrôleur SG5800\)"](#)
- ["Modes de liaison de port \(contrôleur E5700SG\)"](#)
- ["Modes de liaison des ports \(SG110 et SG1100\)"](#)
- ["Modes de liaison des ports \(SG100 et SG1000\)"](#)

Installation et provisionnement du réseau

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

Déploiement initial d'un nœud

Lorsque vous déployez un nœud pour la première fois, vous devez attacher le nœud au réseau de grille 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 de grille avec une passerelle configurée devient la passerelle par défaut pour un nœud pendant le déploiement. La passerelle par défaut permet aux nœuds de grille sur des sous-réseaux distincts 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 au Grid Manager ou à l'API peuvent également être configurés comme sous-réseaux de grille.

Enregistrement automatique des nœuds avec le nœud administrateur principal

Une fois les nœuds déployés, ils s'enregistrent auprès du nœud d'administration principal à l'aide du réseau Grid. Vous pouvez ensuite utiliser le Grid Manager, le `configure-storagegrid.py` Script Python ou API d'installation pour configurer la grille et approuver les nœuds enregistrés. Lors de la configuration du réseau, vous pouvez configurer plusieurs sous-réseaux de réseau. Des itinéraires statiques vers ces sous-réseaux via la passerelle Grid Network seront créés sur chaque nœud lorsque vous aurez terminé la configuration de la grille.

Désactivation du réseau administrateur ou du réseau client

Si vous souhaitez désactiver le réseau administrateur ou le réseau client, vous pouvez supprimer leur configuration pendant le processus d'approbation du nœud, ou vous pouvez utiliser l'outil Modifier l'IP une fois l'installation terminée (voir ["Configurer les adresses IP"](#)).

Consignes post-installation

Une fois le déploiement et la configuration du nœud de grille terminés, suivez ces instructions pour l'adressage DHCP et les modifications de configuration réseau.

- Si DHCP a été 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 lorsque la configuration du réseau de grille est modifiée par DHCP, ce qui peut provoquer des pannes si une modification DHCP affecte plusieurs nœuds en même temps.

- Vous devez utiliser les procédures de modification d'IP si vous souhaitez modifier les adresses IP, les masques de sous-réseau et les passerelles par défaut d'un nœud de grille. Voir ["Configurer les adresses IP"](#) .
- Si vous apportez des modifications à la configuration du réseau, notamment au routage et à la passerelle, la connectivité client au nœud d'administration principal et aux autres nœuds de grille peut être perdue. En fonction des modifications réseau appliquées, vous devrez peut-être rétablir ces connexions.

Référence du port réseau

Communications internes des nœuds de réseau

Le pare-feu interne StorageGRID autorise les connexions entrantes vers des ports spécifiques du réseau Grid. Les connexions sont également acceptées sur les ports définis par les points de terminaison de l'équilibreur de charge.



NetApp vous recommande d'activer le trafic ICMP (Internet Control Message Protocol) entre les nœuds de grille. Autoriser le trafic ICMP peut améliorer les performances de basculement lorsqu'un nœud de grille n'est pas accessible.

En plus de l'ICMP et des ports répertoriés dans le tableau, StorageGRID utilise le protocole VRRP (Virtual Router Redundancy Protocol). VRRP est un protocole Internet qui utilise le numéro de protocole IP 112. StorageGRID utilise VRRP en mode monodiffusion uniquement. VRRP n'est requis que si "[groupes de haute disponibilité](#)" sont configurés.

Directives pour les nœuds basés sur Linux

Si les stratégies de réseau d'entreprise restreignent l'accès à l'un de ces ports, vous pouvez remapper 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, consultez :

- "[Installer StorageGRID sur Red Hat Enterprise Linux](#)"
- "[Installer StorageGRID sur Ubuntu ou Debian](#)"

Directives pour les nœuds basés sur VMware

Configurez les ports suivants uniquement si vous devez définir des restrictions de pare-feu externes au réseau VMware.

Si les stratégies de réseau d'entreprise restreignent l'accès à l'un de ces ports, vous pouvez remapper les ports lorsque vous déployez des nœuds à l'aide de VMware vSphere Web Client ou en utilisant un paramètre de fichier de configuration lors de l'automatisation du déploiement des nœuds de grille. Pour plus d'informations sur le remappage des ports et les paramètres de configuration de déploiement, consultez "[Installer StorageGRID sur VMware](#)".

Directives pour les nœuds d'appareils

Si les politiques de réseau d'entreprise restreignent l'accès à l'un de ces ports, vous pouvez remapper les ports à l'aide du programme d'installation de l'appliance StorageGRID. Voir "[Facultatif : Remapper les ports réseau de l'appareil](#)".

Ports internes StorageGRID

Port	TCP ou UDP	Depuis	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 à l'aide de SSH sur le port 22. Autoriser le trafic SSH provenant d'autres nœuds est facultatif.
80	TCP	appareils électroménagers	Nœud d'administration principal	Utilisé par les appliances StorageGRID pour communiquer avec le nœud d'administration principal pour démarrer l'installation.
123	UDP	Tous les nœuds	Tous les nœuds	Service de protocole de temps réseau. Chaque nœud synchronise son heure avec tous les autres nœuds à l'aide de NTP.
443	TCP	Tous les nœuds	Nœud d'administration principal	Utilisé pour communiquer l'état au nœud d'administration principal pendant l'installation et d'autres procédures de maintenance.
1055	TCP	Tous les nœuds	Nœud d'administration principal	Trafic interne pour les procédures d'installation, d'extension, de récupération et autres procédures de maintenance.
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	Rapports, audits et configuration du trafic interne.
1502	TCP	Tous les nœuds	Nœuds de stockage	Trafic interne lié à S3 et Swift.
1504	TCP	Tous les nœuds	Nœuds d'administration	Rapport de service NMS et configuration du trafic interne.
1505	TCP	Tous les nœuds	Nœuds d'administration	Trafic interne du service AMS.
1506	TCP	Tous les nœuds	Tous les nœuds	État du serveur trafic interne.

Port	TCP ou UDP	Depuis	À	Détails
1507	TCP	Tous les nœuds	Nœuds de passerelle	Trafic interne de l'équilibreur de charge.
1508	TCP	Tous les nœuds	Nœud d'administration principal	Gestion de la configuration du trafic interne.
1511	TCP	Tous les nœuds	Nœuds de stockage	Trafic interne des métadonnées.
7001	TCP	Nœuds de stockage	Nœuds de stockage	Communication inter-nœuds du cluster Cassandra TLS.
7443	TCP	Tous les nœuds	Nœud d'administration principal	Trafic interne pour l'installation, l'extension, la récupération, d'autres procédures de maintenance et les rapports d'erreurs.
8011	TCP	Tous les nœuds	Nœud d'administration principal	Trafic interne pour les procédures d'installation, d'extension, de récupération et autres procédures de maintenance.
8443	TCP	Nœud d'administration principal	Nœuds d'appareils	Trafic interne lié à la procédure de mode 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. Comprend les procédures de maintenance, les mesures et les mises à jour du réseau.
10226	TCP	Nœuds de stockage	Nœud d'administration principal	Utilisé par les appliances StorageGRID pour transférer les packages AutoSupport du gestionnaire système SANtricity E-Series vers le nœud d'administration principal.
10342	TCP	Tous les nœuds	Nœud d'administration principal	Trafic interne pour les procédures d'installation, d'extension, de récupération et autres procédures de maintenance.

Port	TCP ou UDP	Depuis	À	Détails
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 d'identité.
18002	TCP	Nœuds d'administration/de stockage	Nœuds de stockage	Trafic API interne lié aux protocoles d'objet.
18003	TCP	Nœuds d'administration/de stockage	Nœuds de stockage avec ADC	La plateforme gère le trafic interne.
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 du service Chunk pour le codage 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 de la grille	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 des clients.

Port	TCP ou UDP	Depuis	À	Détails
19000	TCP	Nœuds d'administration/de stockage	Nœuds de stockage avec ADC	Trafic interne du service Keystone .

Informations connexes

["Communications externes"](#)

Communications externes

Les clients doivent communiquer avec les nœuds de la grille pour ingérer et récupérer du contenu. Les ports utilisés dépendent des protocoles de stockage d'objets choisis. Ces ports doivent être accessibles au client.

Accès restreint aux ports

Si les politiques de réseau d'entreprise restreignent l'accès à l'un des ports, vous pouvez effectuer l'une des opérations suivantes :

- Utiliser ["points de terminaison de l'équilibreur de charge"](#) pour permettre l'accès sur les ports définis par l'utilisateur.
- Remappez les ports lors du déploiement des nœuds. Cependant, vous ne devez pas remapper les points de terminaison de l'équilibreur de charge. Consultez les informations sur le remappage des ports pour votre nœud StorageGRID :
 - ["Clés de remappage de port pour StorageGRID sur Red Hat Enterprise Linux"](#)
 - ["Clés de remappage de port pour StorageGRID sur Ubuntu ou Debian"](#)
 - ["Remapper les ports pour StorageGRID sur VMware"](#)
 - ["Facultatif : Remapper les ports réseau de l'appareil"](#)

Ports utilisés pour les communications externes

Le tableau suivant montre les ports utilisés pour le trafic vers les nœuds.



Cette liste n'inclut pas les ports qui pourraient être configurés comme ["points de terminaison de l'équilibreur de charge"](#) .

Port	TCP ou UDP	Protocole	Depuis	À	Détails
22	TCP	SSH	Ordinateur portable de service	Tous les nœuds	L'accès SSH ou à la console est requis pour les procédures comportant des étapes de console. En option, vous pouvez utiliser le port 2022 au lieu du 22.

Port	TCP ou UDP	Protocole	Depuis	À	Détails
25	TCP	SMTP	Nœuds d'administration	Serveur de messagerie	Utilisé pour les alertes et AutoSupport par e-mail. 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 le DNS.
67	UDP	DHCP	Tous les nœuds	Service DHCP	Utilisé en option pour prendre en charge la configuration réseau basée sur DHCP. Le service dhclient ne fonctionne pas pour les grilles configurées de manière statique.
68	UDP	DHCP	Service DHCP	Tous les nœuds	Utilisé en option pour prendre en charge la configuration réseau basée sur DHCP. Le service dhclient ne fonctionne 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	appareils électroménagers	Le port 80 redirige vers le port 8443 pour le 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 qui utilisent HTTP. Les locataires peuvent remplacer le paramètre de port HTTP par défaut de 80 lors de la création d'un point de terminaison.
80	TCP	HTTP	Nœuds de stockage	AWS	Les requêtes Cloud Storage Pools sont envoyées aux cibles AWS qui utilisent HTTP. Les administrateurs de grille peuvent remplacer le paramètre de port HTTP par défaut de 80 lors de la configuration d'un pool de stockage cloud.

Port	TCP ou UDP	Protocole	Depuis	À	Détails
111	TCP/UDP	RPCBind	Client NFS	Nœuds d'administration	Utilisé par l'exportation d'audit basée sur NFS (portmap). Remarque : ce port est requis uniquement si l'exportation d'audit basée sur NFS est activée. Remarque : la prise en charge de NFS est obsolète et sera supprimée dans une prochaine version.
123	UDP	NTP	Nœuds NTP primaires	NTP externe	Service de protocole de temps réseau. Les nœuds sélectionnés comme sources NTP principales synchronisent également les heures d'horloge avec les sources de temps NTP externes.
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. La valeur par défaut est le port UDP 161 lors de la configuration. Remarque : ce port n'est requis et n'est ouvert sur le pare-feu du nœud que si SNMP est configuré. Si vous prévoyez d'utiliser SNMP, vous pouvez configurer des ports alternatifs. Remarque : pour plus d'informations sur l'utilisation de SNMP avec StorageGRID, contactez votre représentant de compte NetApp .
162	TCP/UDP	Notifications SNMP	Tous les nœuds	Destinations de notification	Les notifications et interruptions SNMP sortantes sont par défaut sur le 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 des ports alternatifs. Remarque : pour plus d'informations sur l'utilisation de SNMP avec StorageGRID, contactez votre représentant de compte NetApp .

Port	TCP ou UDP	Protocole	Depuis	À	Détails
389	TCP/UDP	LDAP	Nœuds de stockage avec ADC	Active Directory/LDAP	Utilisé pour se connecter à un serveur Active Directory ou LDAP pour la fédération d'identité.
443	TCP	HTTPS	Navigateur	Nœuds d'administration	Utilisé par les navigateurs Web et les clients API de gestion pour accéder au Grid Manager et au Tenant Manager. Remarque : si vous fermez les ports 443 ou 8443 de Grid Manager, 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. Voir "Configurer les contrôles du 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 de stockage avec ADC	AWS	Utilisé pour les messages de services de plateforme envoyés à AWS ou à d'autres services externes qui utilisent HTTPS. Les locataires peuvent remplacer le paramètre de port HTTP par défaut de 443 lors de la création d'un point de terminaison.
443	TCP	HTTPS	Nœuds de stockage	AWS	Les requêtes Cloud Storage Pools sont envoyées aux cibles AWS qui utilisent HTTPS. Les administrateurs de grille peuvent remplacer le paramètre de port HTTPS par défaut de 443 lors de la configuration d'un pool de stockage cloud.
903	TCP	NFS	Client NFS	Nœuds d'administration	Utilisé par l'exportation d'audit basée sur NFS(<code>rpc.mountd</code>). Remarque : ce port est requis uniquement si l'exportation d'audit basée sur NFS est activée. Remarque : la prise en charge de NFS est obsolète et sera supprimée dans une prochaine version.

Port	TCP ou UDP	Protocole	Depuis	À	Détails
2022	TCP	SSH	Ordinateur portable de service	Tous les nœuds	L'accès SSH ou à la console est requis pour les procédures comportant des étapes de console. En option, vous pouvez utiliser le port 22 au lieu du 2022.
2049	TCP	NFS	Client NFS	Nœuds d'administration	Utilisé par l'exportation d'audit basée sur NFS (nfs). Remarque : ce port est requis uniquement si l'exportation d'audit basée sur NFS est activée. Remarque : la prise en charge de NFS est obsolète et sera supprimée dans une prochaine version.
5353	UDP	mDNS	Tous les nœuds	Tous les nœuds	Fournit le service DNS multidiffusion (mDNS) utilisé pour les modifications d'adresse IP de grille complète et pour la découverte du nœud d'administration principal lors de l'installation, de l'extension et de la récupération.
5696	TCP	KMIP	Appareil	KMS	Trafic externe du protocole d'interopérabilité de gestion des clés (KMIP) provenant d'appareils configurés pour le chiffrement des nœuds vers le serveur de gestion des clés (KMS), sauf si un port différent est spécifié sur la page de configuration KMS du programme d'installation de l'appareil StorageGRID .
8022	TCP	SSH	Ordinateur portable de service	Tous les nœuds	SSH sur le port 8022 accorde l'accès au système d'exploitation de base sur les plateformes d'appareils et de nœuds virtuels pour l'assistance et le dépannage. Ce port n'est pas utilisé pour les nœuds basés sur Linux (bare metal) et n'a pas besoin d'être accessible entre les nœuds de grille ou pendant les opérations normales.

Port	TCP ou UDP	Protocole	Depuis	À	Détails
8443	TCP	HTTPS	Navigateur	Nœuds d'administration	Facultatif. Utilisé par les navigateurs Web et les clients API de gestion pour accéder au Grid Manager. Peut être utilisé pour séparer les communications de Grid Manager et de Tenant Manager. Remarque : si vous fermez les ports 443 ou 8443 de Grid Manager, 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. Voir "Configurer les contrôles du pare-feu" pour configurer des adresses IP privilégiées.
9022	TCP	SSH	Ordinateur portable de service	appareils électroménagers	Accorde l'accès aux appliances StorageGRID en mode de préconfiguration pour l'assistance et le dépannage. Il n'est pas nécessaire que ce port soit accessible entre les nœuds du réseau ou pendant les opérations normales.
9091	TCP	HTTPS	Service externe Grafana	Nœuds d'administration	Utilisé par les services Grafana externes pour un accès sécurisé au service StorageGRID Prometheus. Remarque : ce port est requis uniquement si l'accès Prometheus basé sur un certificat est activé.
9092	TCP	Kafka	Nœuds de stockage avec ADC	cluster Kafka	Utilisé pour les messages de services de plateforme envoyés à un cluster Kafka. Les locataires peuvent remplacer le paramètre de port Kafka par défaut de 9092 lors de la création d'un point de terminaison.
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 de Grid Manager et de Tenant Manager.
18082	TCP	HTTPS	Clients S3	Nœuds de stockage	Trafic client S3 directement vers les nœuds de stockage (HTTPS).
18083	TCP	HTTPS	Clients Swift	Nœuds de stockage	Trafic client Swift directement vers les nœuds de stockage (HTTPS).

Port	TCP ou UDP	Protocole	Depuis	À	Détails
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 client Swift directement vers les nœuds de stockage (HTTP).
23000-23999	TCP	HTTPS	Tous les nœuds de la grille source pour la réplication inter-grille	Nœuds d'administration et nœuds de passerelle sur la grille de destination pour la réplication inter-grille	Cette gamme 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 de haut niveau pour configurer et utiliser n'importe quel système StorageGRID .

1

Apprendre, planifier et collecter des données

Travaillez avec votre représentant de compte NetApp pour comprendre les options et planifier votre nouveau système StorageGRID . Considérez ces types de questions :

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

Vous pouvez également collaborer avec votre consultant NetApp Professional Services pour accéder à l'outil NetApp ConfigBuilder afin de compléter un classeur de configuration à utiliser lors de l'installation et du déploiement de votre nouveau système. Vous pouvez également utiliser cet outil pour automatiser la configuration de n'importe quel appareil StorageGRID . Voir "[Automatiser l'installation et la configuration des appareils](#)" .

Revoir "[En savoir plus sur StorageGRID](#)" et le "[Directives de mise en réseau](#)" .

2

Installer des nœuds

Un système StorageGRID se compose de nœuds individuels basés sur du matériel et des logiciels. Vous installez d'abord le matériel pour chaque nœud d'appliance et configurez chaque hôte Linux ou VMware.

Pour terminer l'installation, installez le logiciel StorageGRID sur chaque appliance ou hôte logiciel et connectez les nœuds à une grille. Au cours de cette étape, vous fournissez les noms de site et de nœud, les détails du sous-réseau et les adresses IP de vos serveurs NTP et DNS.

Apprenez comment :

- ["Installer le matériel de l'appareil"](#)
- ["Installer StorageGRID sur Red Hat Enterprise Linux"](#)
- ["Installer StorageGRID sur Ubuntu ou Debian"](#)
- ["Installer StorageGRID sur VMware"](#)

3

Sign in et vérifiez l'état du système

Dès que vous installez le nœud d'administration principal, vous pouvez vous connecter au gestionnaire de grille. À partir de là, vous pouvez vérifier l'état général de votre nouveau système, activer AutoSupport et les e-mails d'alerte, et configurer les noms de domaine de point de terminaison S3.

Apprenez comment :

- ["Sign in au gestionnaire de grille"](#)
- ["Surveiller la santé du système"](#)
- ["Configurer AutoSupport"](#)
- ["Configurer des notifications par e-mail pour les alertes"](#)
- ["Configurer les noms de domaine des points de terminaison S3"](#)

4

Configurer et gérer

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

Apprenez comment :

- ["Contrôler l'accès à StorageGRID"](#)
- ["Utiliser l'assistant de configuration S3"](#)
- ["Utiliser l'assistant de configuration de FabricPool"](#)
- ["Gérer la sécurité"](#)
- ["Renforcement du système"](#)

5

Configurer ILM

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

Apprenez comment : ["Gérer les objets avec ILM"](#)

6

Utiliser StorageGRID

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

Apprenez comment :

- ["Utiliser un compte locataire"](#)
- ["Utiliser l'API REST S3"](#)

7

Surveiller et dépanner

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

Apprenez comment :

- ["Surveiller StorageGRID"](#)
- ["Dépannage de StorageGRID"](#)

8

Développer, entretenir et récupérer

Vous pouvez ajouter des nœuds ou des sites pour étendre la capacité ou les fonctionnalités de votre système. Vous pouvez également effectuer diverses procédures de maintenance pour récupérer des pannes ou pour maintenir votre système StorageGRID à jour et performant.

Apprenez comment :

- ["Développer une grille"](#)
- ["Entretenez votre réseau"](#)
- ["Récupérer les nœuds"](#)

Installer, mettre à niveau et corriger StorageGRID

Appareils StorageGRID

Aller à "[Documentation de l'appliance StorageGRID](#)" pour apprendre à installer, configurer et entretenir les appliances de stockage et de services StorageGRID .

Installer StorageGRID sur Red Hat Enterprise Linux

Démarrage rapide pour l'installation de StorageGRID sur Red Hat Enterprise Linux

Suivez ces étapes de haut niveau pour installer un nœud Linux StorageGRID Red Hat Enterprise Linux (RHEL).

1

Préparation

- En savoir plus sur "[Architecture et topologie du réseau StorageGRID](#)" .
- Renseignez-vous sur les spécificités de "[Réseau StorageGRID](#)" .
- Rassemblez et préparez les "[Informations et matériel requis](#)" .
- Préparez le nécessaire "[CPU et RAM](#)" .
- Prévoir "[exigences de stockage et de performances](#)" .
- "[Préparer les serveurs Linux](#)" qui hébergera vos nœuds StorageGRID .

2

Déploiement

Déployer des nœuds de grille. Lorsque vous déployez des nœuds de grille, ils sont créés dans le cadre du système StorageGRID et connectés à un ou plusieurs réseaux.

- Pour déployer des nœuds de grille basés sur des logiciels sur les hôtes que vous avez préparés à l'étape 1, utilisez la ligne de commande Linux et "[fichiers de configuration des nœuds](#)" .
- Pour déployer les nœuds d'appliance StorageGRID , suivez les instructions "[Démarrage rapide pour l'installation du matériel](#)" .

3

Configuration

Lorsque tous les nœuds ont été déployés, utilisez le gestionnaire de grille pour "[configurer la grille et terminer l'installation](#)" .

Automatiser l'installation

Pour gagner du temps et assurer la cohérence, vous pouvez automatiser l'installation du service hôte StorageGRID et la configuration des nœuds de grille.

- Utilisez un framework d'orchestration standard tel qu'Ansible, Puppet ou Chef pour automatiser :

- Installation de RHEL
- Configuration du réseau et du stockage
- Installation du moteur de conteneur et du service hôte StorageGRID
- Déploiement de nœuds de réseau virtuels

Voir ["Automatiser l'installation et la configuration du service hôte StorageGRID"](#) .

- Après avoir déployé les nœuds de grille, ["automatiser la configuration du système StorageGRID"](#) en utilisant le script de configuration Python fourni dans l'archive d'installation.
- ["Automatiser l'installation et la configuration des nœuds de réseau d'appareils"](#)
- Si vous êtes un développeur avancé de déploiements StorageGRID , automatisez l'installation des nœuds de grille en utilisant le ["installation de l'API REST"](#) .

Planifier et préparer l'installation sur Red Hat

Informations et matériel requis

Avant d'installer StorageGRID, rassemblez et préparez les informations et le matériel requis.

Informations requises

Plan de réseau

Quels réseaux comptez-vous connecter à chaque nœud StorageGRID . StorageGRID prend en charge plusieurs réseaux pour la séparation du trafic, la sécurité et la commodité administrative.

Voir le StorageGRID ["Directives de mise en réseau"](#) .

Informations sur le réseau

Adresses IP à attribuer à chaque nœud de grille et les adresses IP des serveurs DNS et NTP.

Serveurs pour les nœuds de grille

Identifiez un ensemble de serveurs (physiques, virtuels ou les deux) qui, dans leur ensemble, fournissent suffisamment de ressources pour prendre en charge le nombre et le type de nœuds StorageGRID que vous prévoyez de déployer.



Si votre installation StorageGRID n'utilise pas de nœuds de stockage d'appliance StorageGRID (matériel), vous devez utiliser un stockage RAID matériel avec cache d'écriture alimenté par batterie (BBWC). StorageGRID ne prend pas en charge l'utilisation de réseaux de stockage virtuels (vSAN), de RAID logiciel ou d'aucune protection RAID.

Migration de nœuds (si nécessaire)

Comprendre le ["exigences pour la migration des nœuds"](#) , si vous souhaitez effectuer une maintenance planifiée sur des hôtes physiques sans aucune interruption de service.

Informations connexes

["Outil de matrice d'interopérabilité NetApp"](#)

Matériel requis

Licence NetApp StorageGRID

Vous devez disposer d'une licence NetApp valide et signée numériquement.



Une licence non-production, qui peut être utilisée pour les grilles de test et de preuve de concept, est incluse dans l'archive d'installation de StorageGRID .

Archive d'installation de StorageGRID

["Téléchargez l'archive d'installation de StorageGRID et extrayez les fichiers"](#) .

Ordinateur portable de service

Le système StorageGRID est installé via un ordinateur portable de service.

L'ordinateur portable de service doit avoir :

- Port réseau
- Client SSH (par exemple, PuTTY)
- ["Navigateur Web pris en charge"](#)

Documentation de StorageGRID

- ["Notes de version"](#)
- ["Instructions pour l'administration de StorageGRID"](#)

Téléchargez et extrayez les fichiers d'installation de StorageGRID

Vous devez télécharger l'archive d'installation de StorageGRID et extraire les fichiers requis. En option, vous pouvez vérifier manuellement les fichiers dans le package d'installation.

Étapes

1. Aller à la ["Page de téléchargement NetApp pour StorageGRID"](#) .
2. Sélectionnez le bouton pour télécharger la dernière version ou sélectionnez une autre version dans le menu déroulant et sélectionnez **Aller**.
3. Sign in avec le nom d'utilisateur et le mot de passe de votre compte NetApp .
4. Si une mention d'avertissement/à lire absolument apparaît, lisez-la et cochez la case.



Vous devez appliquer tous les correctifs requis après avoir installé la version StorageGRID . Pour plus d'informations, consultez le ["procédure de correctif dans les instructions de récupération et de maintenance"](#) .

5. Lisez le contrat de licence utilisateur final, cochez la case, puis sélectionnez **Accepter et continuer**.
6. Dans la colonne **Installer StorageGRID**, sélectionnez l'archive d'installation .tgz ou .zip pour Red Hat Enterprise Linux.



Sélectionnez le .zip fichier si vous exécutez Windows sur l'ordinateur portable de service.

7. Enregistrez l'archive d'installation.

8. Si vous devez vérifier l'archive d'installation :
 - a. Téléchargez le package de vérification de signature de code StorageGRID . Le nom de fichier de ce package utilise le format `StorageGRID_<version-number>_Code_Signature_Verification_Package.tar.gz` , où `<version-number>` est la version du logiciel StorageGRID .
 - b. Suivez les étapes pour "[vérifier manuellement les fichiers d'installation](#)" .
9. Extraire les fichiers de l'archive d'installation.
10. Choisissez les fichiers dont vous avez besoin.

Les fichiers dont vous avez besoin dépendent de la topologie de grille prévue et de la manière dont vous allez déployer votre système StorageGRID .



Les chemins répertoriés dans le tableau sont relatifs au répertoire de niveau supérieur installé par l'archive d'installation extraite

Chemin et nom du fichier	Description
	Un fichier texte qui décrit tous les fichiers contenus dans le fichier de téléchargement StorageGRID .
	Une licence gratuite qui ne fournit aucun droit d'assistance pour le produit.
	Package RPM pour l'installation des images de nœuds StorageGRID sur vos hôtes RHEL.
	Package RPM pour l'installation du service hôte StorageGRID sur vos hôtes RHEL.
Outil de script de déploiement	Description
	Un script Python utilisé pour automatiser la configuration d'un système StorageGRID .
	Un script Python utilisé pour automatiser la configuration des appliances StorageGRID .
	Un exemple de fichier de configuration à utiliser avec le <code>configure-storagegrid.py</code> scénario.
	Un 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 l'intégration de Ping Federate.

Chemin et nom du fichier	Description
	Un fichier de configuration vierge à utiliser avec le <code>configure-storagegrid.py</code> scénario.
	Exemple de rôle Ansible et de playbook pour la configuration des hôtes RHEL pour le déploiement du conteneur StorageGRID . Vous pouvez personnaliser le rôle ou le manuel selon vos besoins.
	Un exemple de script Python que vous pouvez utiliser pour vous connecter à l'API Grid Management lorsque l'authentification unique (SSO) est activée à l'aide d'Active Directory ou de Ping Federate.
	Un script d'aide appelé par le compagnon <code>storagegrid-ssoauth-azure.py</code> Script Python pour effectuer des interactions SSO avec Azure.
	Schémas d'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 hors production pour les tests de compatibilité de mise à niveau.

Vérifier manuellement les fichiers d'installation (facultatif)

Si nécessaire, vous pouvez vérifier manuellement les fichiers dans l'archive d'installation de StorageGRID .

Avant de commencer

Tu as ["téléchargé le package de vérification"](#) de la ["Page de téléchargement NetApp pour StorageGRID"](#) .

Étapes

1. Extraire les artefacts du package de vérification :

```
tar -xf StorageGRID_11.9.0_Code_Signature_Verification_Package.tar.gz
```

2. Assurez-vous que ces artefacts ont été extraits :

- Certificat de feuille : `Leaf-Cert.pem`
- Chaîne de certificats : `CA-Int-Cert.pem`
- Chaîne de réponse d'horodatage : `TS-Cert.pem`
- Fichier de somme de contrôle : `sha256sum`

- Signature de somme de contrôle : sha256sum.sig
- Fichier de réponse d'horodatage : sha256sum.sig.tsr

3. Utilisez la chaîne pour vérifier que le certificat de feuille est valide.

Exemple: `openssl verify -CAfile CA-Int-Cert.pem Leaf-Cert.pem`

Résultat attendu: Leaf-Cert.pem: OK

4. Si l'étape 2 a échoué en raison d'un certificat feuille expiré, utilisez le tsr fichier à vérifier.

Exemple: `openssl ts -CAfile CA-Int-Cert.pem -untrusted TS-Cert.pem -verify -data sha256sum.sig -in sha256sum.sig.tsr`

Les résultats attendus incluent : Verification: OK

5. Créez un fichier de clé publique à partir du certificat feuille.

Exemple: `openssl x509 -pubkey -noout -in Leaf-Cert.pem > Leaf-Cert.pub`

Sortie attendue : *aucun*

6. Utilisez la clé publique pour vérifier le sha256sum déposer contre sha256sum.sig .

Exemple: `openssl dgst -sha256 -verify Leaf-Cert.pub -signature sha256sum.sig sha256sum`

Résultat attendu: Verified OK

7. Vérifiez le sha256sum contenu du fichier par rapport aux sommes de contrôle nouvellement créées.

Exemple: `sha256sum -c sha256sum`

Résultat attendu: <filename>: OK

<filename> est le nom du fichier d'archive que vous avez téléchargé.

8. "[Complétez les étapes restantes](#)" pour extraire et choisir les fichiers appropriés dans l'archive d'installation.

Configuration logicielle requise pour Red Hat Enterprise Linux

Vous pouvez utiliser une machine virtuelle pour héberger n'importe quel type de nœud StorageGRID . Vous avez besoin d'une machine virtuelle pour chaque nœud de grille.

Pour installer StorageGRID sur Red Hat Enterprise Linux (RHEL), vous devez installer certains packages logiciels tiers. Certaines distributions Linux prises en charge ne contiennent pas ces packages par défaut. Les versions de progiciels sur lesquelles les installations StorageGRID sont testées incluent celles répertoriées sur cette page.

Si vous sélectionnez une distribution Linux et une option d'installation d'exécution de conteneur qui nécessitent l'un de ces packages et qu'ils ne sont pas installés automatiquement par la distribution Linux, installez l'une des versions répertoriées ici si elles sont disponibles auprès de votre fournisseur ou du fournisseur de support de votre distribution Linux. Sinon, utilisez les versions de package par défaut disponibles auprès de votre fournisseur.

Toutes les options d'installation nécessitent Podman ou Docker. N'installez pas les deux packages. Installez uniquement le package requis par votre option d'installation.



La prise en charge de Docker comme moteur de conteneur pour les déploiements uniquement logiciels est obsolète. Docker sera remplacé par un autre moteur de conteneur dans une prochaine version.

Versions Python testées

- 3.5.2-2
- 3.6.8-2
- 3.6.8-38
- 3.6.9-1
- 3.7.3-1
- 3.8.10-0
- 3.9.2-1
- 3.9.10-2
- 3.9.16-1
- 3.10.6-1
- 3.11.2-6

Versions Podman testées

- 3.2.3-0
- 3.4.4+ds1
- 4.1.1-7
- 4.2.0-11
- 4.3.1+ds1-8+b1
- 4.4.1-8
- 4.4.1-12

Versions de Docker testées



La prise en charge de Docker est obsolète et sera supprimée dans une prochaine version.

- Docker-CE 20.10.7
- Docker-CE 20.10.20-3
- Docker-CE 23.0.6-1
- Docker-CE 24.0.2-1
- Docker-CE 24.0.4-1
- Docker-CE 24.0.5-1
- Docker-CE 24.0.7-1
- 1,5-2

Exigences CPU et RAM

Avant d'installer le logiciel StorageGRID , vérifiez et configurez le matériel afin qu'il soit prêt à prendre en charge le système StorageGRID .

Chaque nœud StorageGRID nécessite les ressources minimales suivantes :

- Cœurs de processeur : 8 par nœud
- RAM : dépend de la RAM totale disponible et de la quantité de logiciels non StorageGRID exécutés sur le système
 - Généralement, au moins 24 Go par nœud et 2 à 16 Go de moins que la RAM totale du système
 - Un minimum de 64 Go pour chaque locataire qui aura environ 5 000 buckets

Les ressources de nœuds basées uniquement sur des métadonnées logicielles doivent correspondre aux ressources de nœuds de stockage existantes. Par exemple:

- Si le site StorageGRID existant utilise des appliances SG6000 ou SG6100, les nœuds de métadonnées uniquement basés sur des logiciels doivent répondre aux exigences minimales suivantes :
 - 128 Go de RAM
 - processeur à 8 cœurs
 - SSD de 8 To ou stockage équivalent pour la base de données Cassandra (rangedb/0)
- Si le site StorageGRID existant utilise des nœuds de stockage virtuels avec 24 Go de RAM, un processeur à 8 cœurs et 3 To ou 4 To de stockage de métadonnées, les nœuds de métadonnées uniquement basés sur un logiciel doivent utiliser des ressources similaires (24 Go de RAM, un processeur à 8 cœurs et 4 To de stockage de métadonnées (rangedb/0).

Lors de l'ajout d'un nouveau site StorageGRID , la capacité totale des métadonnées du nouveau site doit, au minimum, correspondre aux sites StorageGRID existants et les nouvelles ressources du site doivent correspondre aux nœuds de stockage des sites StorageGRID existants.

Assurez-vous 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 RAM physique disponible. Si les hôtes ne sont pas dédiés à l'exécution de StorageGRID (non recommandé), assurez-vous de 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 répondre à votre charge de travail. Par exemple, doubler l'allocation de RAM et de CPU pour les nœuds de stockage virtuels fournirait des ressources similaires à celles fournies pour les nœuds d'appliance StorageGRID . De plus, si la quantité de métadonnées par nœud dépasse 500 Go, envisagez d'augmenter la RAM par nœud à 48 Go ou plus. 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, consultez les instructions de [administrer](#) , [surveillance](#) , et [mise à niveau](#) StorageGRID.

Si l'hyperthreading est activé sur les hôtes physiques sous-jacents, vous pouvez fournir 8 cœurs virtuels (4 cœurs physiques) par nœud. Si l'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 comme hôtes et que vous contrôlez la taille et le nombre de machines virtuelles, vous devez utiliser une seule machine virtuelle pour chaque nœud StorageGRID et dimensionner la

machine virtuelle en conséquence.

Pour les déploiements de production, vous ne devez pas exécuter plusieurs nœuds de stockage sur le même matériel de stockage physique ou hôte virtuel. Chaque nœud de stockage d'un déploiement StorageGRID unique doit se trouver dans son propre domaine de défaillance isolé. Vous pouvez maximiser la durabilité et la disponibilité des données d'objet si vous vous assurez qu'une seule panne matérielle ne peut affecter qu'un seul nœud de stockage.

Voir aussi ["Exigences de stockage et de performances"](#) .

Exigences de stockage et de performances

Vous devez comprendre les exigences de stockage pour les nœuds StorageGRID , afin de pouvoir fournir suffisamment d'espace 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 performance (10 K SAS ou SSD) pour les conteneurs de nœuds, qui sera attribué au pilote de stockage du moteur de conteneur lorsque vous installerez et configurerez le moteur de conteneur sur les hôtes qui prendront en charge vos nœuds StorageGRID .
- **Données système** — Stockage de niveau de performance (SAS 10 K ou SSD) pour le stockage persistant par nœud des données système et des journaux de transactions, que les services hôtes StorageGRID consommeront et mapperont dans des nœuds individuels.
- **Données d'objet** — Stockage de niveau performance (10 K SAS ou SSD) et stockage en masse 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 blocs sauvegardés par RAID pour toutes les catégories de stockage. Les disques non redondants, SSD ou JBOD ne sont pas pris en charge. Vous pouvez utiliser un stockage RAID partagé ou local pour n'importe quelle catégorie 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, consultez la section ["Exigences de migration des conteneurs de nœuds"](#) .

Exigences de performance

Les performances des volumes utilisés pour le pool de conteneurs, les données système et les métadonnées d'objet ont un impact significatif sur les performances globales du système. Vous devez utiliser un stockage de niveau de performance (SAS 10K ou SSD) pour ces volumes afin de garantir des performances de disque adéquates en termes de latence, d'opérations d'entrée/sortie par seconde (IOPS) et de débit. Vous pouvez utiliser le stockage de niveau de capacité (NL-SAS/SATA) pour le stockage persistant des données d'objet.

Les volumes utilisés pour le pool de conteneurs, les données système et les données d'objet doivent avoir la mise en cache en écriture différée activée. Le cache doit être sur un support protégé ou persistant.

Exigences pour les hôtes qui utilisent le stockage NetApp ONTAP

Si le nœud StorageGRID utilise le stockage attribué à partir d'un système NetApp ONTAP , vérifiez que le volume n'a pas de stratégie de hiérarchisation FabricPool activée. La désactivation de la hiérarchisation FabricPool pour les volumes utilisés avec les nœuds StorageGRID simplifie le dépannage et les opérations de stockage.



N'utilisez jamais FabricPool pour hiérarchiser les données liées à StorageGRID vers StorageGRID lui-même. La hiérarchisation des données StorageGRID vers StorageGRID augmente le dépannage et la complexité opérationnelle.

Nombre d'hôtes requis

Chaque site StorageGRID nécessite un minimum de 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.

D'autres types de nœuds, tels que les nœuds d'administration ou les nœuds de passerelle, peuvent être déployés sur les mêmes hôtes ou sur leurs propres hôtes dédiés selon les besoins.

Nombre de volumes de stockage pour chaque hôte

Le tableau suivant indique le nombre de volumes de stockage (LUN) requis pour chaque hôte et la taille minimale requise pour chaque LUN, en fonction des nœuds qui seront déployés sur cet hôte.

La taille maximale du LUN testé est de 39 To.



Ces chiffres concernent chaque hôte, et non la grille entière.

Objectif du LUN	Catégorie de stockage	Nombre de LUN	Taille minimale/LUN
Piscine de stockage de moteurs de conteneurs	Piscine à conteneurs	1	Nombre total de nœuds × 100 Go
`/var/local` volume	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 nœud de stockage basé sur un logiciel peut avoir de 1 à 48 volumes de stockage ; au moins 3 volumes de stockage sont recommandés.	12 To (4 To/LUN) Voir Exigences de stockage pour les nœuds de stockage pour plus d'informations.

Objectif du LUN	Catégorie de stockage	Nombre de LUN	Taille minimale/LUN
Nœud de stockage (métadonnées uniquement)	Métadonnées de l'objet	1	4 To Voir Exigences de stockage pour les nœuds de stockage pour plus d'informations. Remarque : un seul rangedb est requis pour les nœuds de stockage contenant uniquement des métadonnées.
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



En fonction du niveau d'audit configuré, de la taille des entrées utilisateur telles que le nom de clé d'objet S3 et de la quantité de données de journal d'audit que vous devez conserver, vous devrez peut-être augmenter la taille du LUN du journal d'audit sur chaque nœud d'administration. En général, une grille génère environ 1 Ko de données d'audit par opération S3, ce qui signifie qu'un LUN de 200 Go prendrait 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 minimum requis pour chaque type de nœud. Vous pouvez utiliser ce tableau pour déterminer la quantité minimale de stockage que vous devez fournir à l'hôte dans chaque catégorie de stockage, en fonction des nœuds qui seront déployés sur cet hôte.



Les instantanés de disque ne peuvent pas être utilisés pour restaurer les nœuds de grille. Au lieu de cela, reportez-vous à la ["récupération des nœuds de réseau"](#) procédures pour chaque type de nœud.

Type de nœud	Piscine à 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)	<i>non applicable</i>
Nœud de passerelle	100 Go	90 Go	<i>non applicable</i>

Exemple : Calcul des besoins de stockage d'un hôte

Supposons que vous envisagiez de déployer trois nœuds sur le 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 niveau performance pour les conteneurs de nœuds, de 670 Go de stockage de niveau performance pour les données système et les journaux de transactions, et de 12 To de stockage de niveau capacité pour les données d'objet.

Type de nœud	Objectif du LUN	Nombre de LUN	Taille du LUN
Nœud de stockage	Piscine de stockage de moteurs de conteneurs	1	300 Go (100 Go/nœud)
Nœud de stockage	`/var/local` volume	1	90 Go
Nœud de stockage	Données d'objet	3	12 To (4 To/LUN)
Nœud d'administration	`/var/local` volume	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` volume	1	90 Go
Total		9	Pool de conteneurs : 300 Go Données système : 670 Go Données de l'objet : 12 000 Go

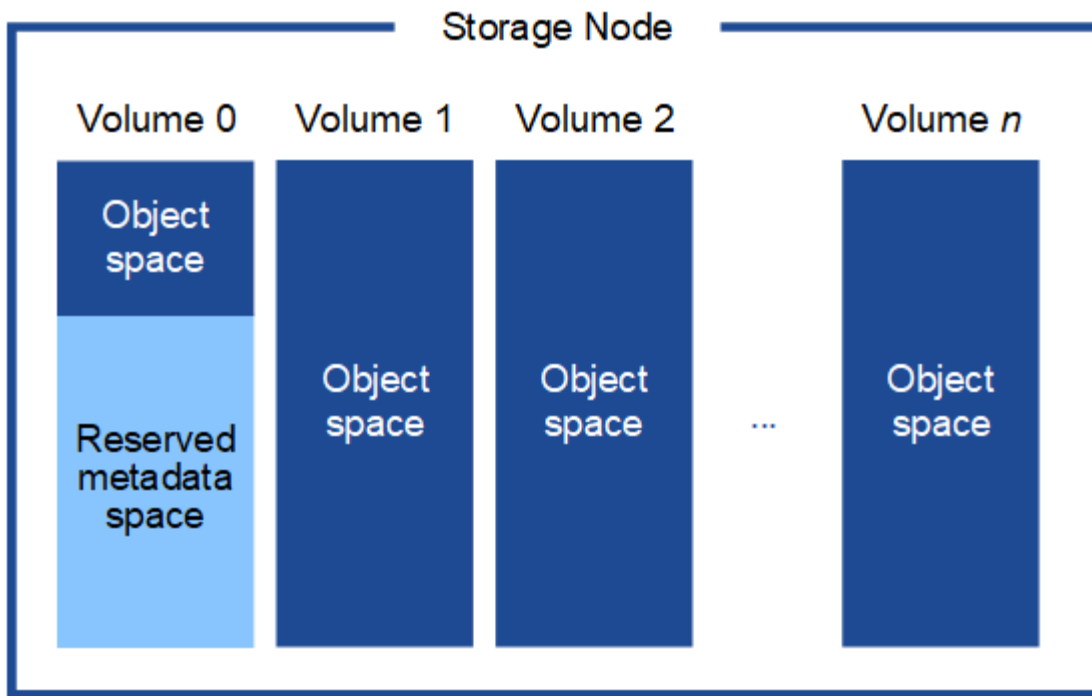
Exigences de stockage pour les nœuds de stockage

Un nœud de stockage basé sur un logiciel peut avoir de 1 à 48 volumes de stockage ; 3 volumes de stockage ou plus sont recommandés. Chaque volume de stockage doit être de 4 To ou plus.



Un nœud de stockage d'appareil peut également avoir jusqu'à 48 volumes de stockage.

Comme indiqué dans la figure, StorageGRID réserve de l'espace pour les métadonnées d'objet sur le volume de stockage 0 de chaque nœud de stockage. Tout espace restant sur le volume de stockage 0 et tous les autres volumes de stockage du nœud de stockage sont utilisés exclusivement pour les données d'objet.



Pour assurer la redondance et protéger les métadonnées des objets contre la perte, StorageGRID stocke trois copies des métadonnées de tous les objets du système sur chaque site. Les trois copies des métadonnées de l'objet sont réparties uniformément sur tous les nœuds de stockage de chaque site.

Lors de l'installation d'une grille avec des nœuds de stockage contenant uniquement des métadonnées, la grille doit également contenir un nombre minimum de nœuds pour le stockage d'objets. Voir "[Types de nœuds de stockage](#)" pour plus d'informations sur les nœuds de stockage contenant uniquement des métadonnées.

- Pour une grille à site unique, au moins deux nœuds de stockage sont configurés pour les objets et les métadonnées.
- Pour une grille multisite, au moins un nœud de stockage par site est configuré pour les objets et les métadonnées.

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 partie de ce nœud de toutes les métadonnées d'objet.

- Au minimum, vous devez attribuer au moins 4 To au volume 0.



Si vous utilisez 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 dans l'état de stockage en lecture seule au démarrage et stocker uniquement 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 sont réservés aux métadonnées.

- Les ressources de nœuds basées uniquement sur des métadonnées logicielles doivent correspondre aux ressources de nœuds de stockage existantes. Par exemple:
 - Si le site StorageGRID existant utilise des appliances SG6000 ou SG6100, les nœuds de métadonnées uniquement basés sur des logiciels doivent répondre aux exigences minimales suivantes :
 - 128 Go de RAM

- processeur à 8 cœurs
- SSD de 8 To ou stockage équivalent pour la base de données Cassandra (rangedb/0)
- Si le site StorageGRID existant utilise des nœuds de stockage virtuels avec 24 Go de RAM, un processeur à 8 cœurs et 3 To ou 4 To de stockage de métadonnées, les nœuds de métadonnées uniquement basés sur un logiciel doivent utiliser des ressources similaires (24 Go de RAM, un processeur à 8 cœurs et 4 To de stockage de métadonnées (rangedb/0)).

Lors de l'ajout d'un nouveau site StorageGRID, la capacité totale des métadonnées du nouveau site doit, au minimum, correspondre aux sites StorageGRID existants et les nouvelles ressources du site doivent correspondre aux nœuds de stockage des sites StorageGRID existants.

- 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.
- Lors de la configuration de 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 de détails, rendez-vous sur ["Gérer le stockage des métadonnées des objets"](#).

Exigences de migration des conteneurs de nœuds

La fonctionnalité de migration de nœud vous permet de déplacer manuellement un nœud d'un hôte à un autre. En règle générale, les deux hôtes se trouvent dans le même centre de données physique.

La migration de nœuds vous permet d'effectuer la maintenance de l'hôte physique sans perturber les opérations du réseau. Vous déplacez tous les nœuds StorageGRID, un par un, vers un autre hôte avant de mettre l'hôte physique hors ligne. La migration des nœuds ne nécessite qu'un court temps d'arrêt pour chaque nœud et ne devrait pas affecter le fonctionnement ou la disponibilité des services de grille.

Si vous souhaitez utiliser la fonctionnalité de migration de nœuds StorageGRID, votre déploiement doit répondre à des exigences supplémentaires :

- Noms d'interface réseau cohérents entre les hôtes d'un même centre de données physique
- Stockage partagé pour les volumes de métadonnées et de référentiel d'objets StorageGRID accessible par tous les hôtes dans un seul centre de données physique. Par exemple, vous pouvez utiliser des baies de stockage NetApp E-Series.

Si vous utilisez des hôtes virtuels et que la couche d'hyperviseur sous-jacente prend en charge la migration de machines virtuelles, vous souhaitez peut-être utiliser cette fonctionnalité à la place de la fonctionnalité de migration de nœuds dans StorageGRID. Dans ce cas, vous pouvez ignorer ces exigences supplémentaires.

Avant d'effectuer la migration ou la maintenance de l'hyperviseur, arrêtez les nœuds correctement. Voir les instructions pour ["fermeture d'un nœud de grille"](#).

VMware Live Migration n'est pas pris en charge

Lors de l'exécution d'une installation bare-metal sur des machines virtuelles VMware, OpenStack Live Migration et VMware Live vMotion provoquent un saut de l'heure de l'horloge de la machine virtuelle et ne sont pas pris en charge pour les nœuds de grille de tout type. Bien que rares, des heures d'horloge incorrectes

peuvent entraîner une perte de données ou des mises à jour de configuration.

La migration à froid est prise en charge. Lors d'une migration à froid, vous arrêtez les nœuds StorageGRID avant de les migrer entre les hôtes. Voir les instructions pour ["fermeture d'un nœud de grille"](#).

Noms d'interface réseau cohérents

Pour déplacer un nœud d'un hôte à un autre, le service hôte StorageGRID doit avoir la certitude 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 NodeA exécuté sur Host1 a été configuré avec les mappages d'interface suivants :

eth0 → bond0.1001

eth1 → bond0.1002

eth2 → bond0.1003

Le côté gauche des flèches correspond aux interfaces traditionnelles vues depuis un conteneur StorageGRID (c'est-à-dire respectivement les interfaces Grid, Admin et Client Network). 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.

Maintenant, supposons que vous souhaitiez migrer NodeA vers Host2. Si Host2 possède également des interfaces nommées bond0.1001, bond0.1002 et bond0.1003, le système autorisera le déplacement, en supposant que les interfaces portant le même nom fourniront la même connectivité sur Host2 que sur Host1. Si Host2 ne possède pas d'interfaces portant les mêmes noms, le déplacement ne sera pas autorisé.

Il existe de nombreuses façons d'obtenir une dénomination d'interface réseau cohérente sur plusieurs hôtes ; voir ["Configuration du réseau hôte"](#) pour quelques exemples.

Stockage partagé

Pour réaliser des migrations de nœuds rapides et à faible surcharge, la fonctionnalité de migration de nœuds StorageGRID ne déplace pas physiquement les données des nœuds. Au lieu de cela, la migration des nœuds est effectuée sous la forme d'une paire d'opérations d'exportation et d'importation, comme suit :

1. Pendant l'opération « exportation de nœud », une petite quantité de données d'état persistantes 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 nœuds sur HostA est désinstancié.
2. Pendant l'opération « importation de nœud », le conteneur de nœud sur HostB qui utilise la même interface réseau et les mêmes mappages de stockage de blocs qui étaient en vigueur sur HostA est instancié. Ensuite, les données d'état persistantes mises en cache sont insérées dans la nouvelle instance.

Compte tenu de ce mode de fonctionnement, toutes les données système et tous les volumes de stockage d'objets du nœud doivent être accessibles à la fois depuis HostA et HostB pour que la migration soit autorisée et fonctionne. De plus, ils doivent avoir été mappés dans le nœud à l'aide de noms qui font 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 le multipathing DM est utilisé sur les hôtes et le champ d'alias a été utilisé dans `/etc/multipath.conf` pour fournir des noms de périphériques de bloc cohérents et conviviaux disponibles sur tous les hôtes.

`/var/local` → `/dev/mapper/sgws-sn1-var-local`

`rangedb0` → `/dev/mapper/sgws-sn1-rangedb0`

`rangedb1` → `/dev/mapper/sgws-sn1-rangedb1`

`rangedb2` → `/dev/mapper/sgws-sn1-rangedb2`

`rangedb3` → `/dev/mapper/sgws-sn1-rangedb3`

Préparer les hôtes (Red Hat)

Comment les paramètres à l'échelle de l'hôte changent pendant l'installation

Sur les systèmes bare metal, StorageGRID apporte quelques modifications à l'échelle 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 RAM
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
```

Installer Linux

Vous devez installer StorageGRID sur tous les hôtes de grille Red Hat Enterprise Linux. Pour obtenir la liste des versions prises en charge, utilisez l'outil de matrice d'interopérabilité NetApp .

Avant de commencer

Assurez-vous que votre système d'exploitation répond aux exigences minimales de version du noyau de StorageGRID, comme indiqué ci-dessous. Utilisez la commande `uname -r` pour obtenir la version du noyau de votre système d'exploitation ou consultez le fournisseur de votre système d'exploitation.

Version de Red Hat Enterprise Linux	Version minimale du noyau	Nom du paquet du noyau
8.8 (obsolète)	4.18.0-477.10.1.el8_8.x86_64	noyau-4.18.0-477.10.1.el8_8.x86_64
8,10	4.18.0-553.el8_10.x86_64	noyau-4.18.0-553.el8_10.x86_64
9.0 (obsolète)	5.14.0-70.22.1.el9_0.x86_64	noyau-5.14.0-70.22.1.el9_0.x86_64
9.2 (obsolète)	5.14.0-284.11.1.el9_2.x86_64	noyau-5.14.0-284.11.1.el9_2.x86_64
9,4	5.14.0-427.18.1.el9_4.x86_64	noyau-5.14.0-427.18.1.el9_4.x86_64
9,6	5.14.0-570.18.1.el9_6.x86_64	noyau-5.14.0-570.18.1.el9_6.x86_64

Étapes

1. Installez Linux sur tous les hôtes de grille physiques ou virtuels conformément aux instructions du distributeur ou à votre procédure standard.



Si vous utilisez le programme d'installation Linux standard, sélectionnez la configuration logicielle « nœud de calcul », si disponible, 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 packages, y compris le canal Extras.

Vous pourriez avoir besoin de ces packages supplémentaires plus tard dans cette procédure d'installation.

3. Si l'échange est activé :

- a. Exécutez la commande suivante : `$ sudo swapoff --all`
- b. Supprimer toutes les entrées d'échange de `/etc/fstab` pour conserver les paramètres.



Ne pas désactiver complètement l'échange peut réduire considérablement les performances.

Configurer le réseau hôte (Red Hat Enterprise Linux)

Une fois l'installation de Linux terminée sur vos hôtes, vous devrez peut-être effectuer une configuration supplémentaire pour préparer un ensemble d'interfaces réseau sur chaque hôte adaptées au mappage dans les nœuds StorageGRID que vous déploierez ultérieurement.

Avant de commencer

- Vous avez examiné le ["Directives de mise en réseau StorageGRID"](#) .
- Vous avez examiné les informations sur ["exigences de migration des conteneurs de nœuds"](#) .
- Si vous utilisez des hôtes virtuels, vous avez lu le [considérations et recommandations pour le clonage d'adresses MAC](#) avant de configurer le réseau hôte.



Si vous utilisez des machines virtuelles comme hôtes, vous devez sélectionner VMXNET 3 comme adaptateur réseau virtuel. L'adaptateur réseau VMware E1000 a provoqué des problèmes de connectivité avec les conteneurs StorageGRID déployés sur certaines distributions de Linux.

À propos de cette tâche

Les nœuds de grille doivent pouvoir accéder au réseau de grille et, éventuellement, aux réseaux d'administration et de client. Vous fournissez cet accès en créant des mappages qui associent l'interface physique de l'hôte aux interfaces virtuelles de chaque nœud de grille. Lors de la création d'interfaces d'hôte, utilisez des noms conviviaux pour faciliter le déploiement sur tous les hôtes et pour permettre la migration.

La même interface peut être partagée entre l'hôte et un ou plusieurs nœuds. Par exemple, vous pouvez utiliser la même interface pour l'accès à l'hôte et l'accès au réseau d'administration du nœud, afin de faciliter la maintenance de l'hôte et du nœud. Bien que la même interface puisse être partagée entre l'hôte et les nœuds individuels, tous 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 pour tous les nœuds StorageGRID sur l'hôte ; vous pouvez utiliser une interface réseau hôte différente pour chaque nœud ; ou vous pouvez faire quelque chose entre les deux. Cependant, vous ne fournirez généralement pas la même interface réseau hôte que les interfaces réseau Grid et Admin pour un seul nœud, ou comme interface réseau Grid pour un nœud et comme interface réseau client pour un autre.

Vous pouvez réaliser 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 à 1. Si vous déployez plusieurs nœuds sur des hôtes bare metal pour une utilisation en production, vous pouvez tirer parti de la prise en charge de la pile réseau Linux pour VLAN et LACP pour la tolérance aux pannes et le partage de bande passante. Les sections suivantes fournissent 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 périphériques de liaison ou de pont directement comme interface réseau du conteneur. Cela pourrait empêcher le démarrage du 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 du conteneur. Utilisez plutôt un périphérique non lié, tel qu'un VLAN ou une paire Ethernet virtuelle (veth). Spécifiez ce périphérique comme interface réseau dans le fichier de configuration du nœud.

Informations connexes

["Création de fichiers de configuration de nœuds"](#)

Considérations et recommandations pour le clonage d'adresses MAC

Le clonage d'adresse MAC amène le conteneur à utiliser l'adresse MAC de l'hôte, et l'hôte à utiliser l'adresse MAC d'une adresse que vous spécifiez ou d'une adresse générée aléatoirement. Vous devez utiliser le clonage d'adresse MAC pour éviter l'utilisation de configurations réseau en mode promiscuité.

Activation du clonage MAC

Dans certains environnements, la sécurité peut être améliorée grâce au clonage d'adresse MAC, car cela vous permet d'utiliser une carte réseau virtuelle dédiée pour le réseau d'administration, le réseau de grille et le réseau client. Le fait que le conteneur utilise l'adresse MAC de la carte réseau dédiée sur l'hôte vous permet d'éviter d'utiliser des configurations réseau en mode promiscuité.



Le clonage d'adresse MAC est destiné à être utilisé avec des installations de serveur virtuel et peut ne pas fonctionner correctement avec toutes les configurations d'appareils physiques.



Si un nœud ne parvient pas à démarrer en raison d'une interface ciblée de clonage MAC occupée, vous devrez peut-être définir le lien sur « down » avant de démarrer le nœud. De plus, il est possible que l'environnement virtuel empêche 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 à démarrer en raison d'une interface occupée, définir le lien sur « down » avant de démarrer le nœud peut résoudre le problème.

Le clonage d'adresse MAC est désactivé par défaut et doit être défini par les clés de configuration du nœud. Vous devez l'activer lorsque vous installez 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

La définition de la clé sur « true » oblige le conteneur à utiliser l'adresse MAC de la carte réseau de l'hôte. De plus, l'hôte utilisera ensuite l'adresse MAC du réseau de conteneurs spécifié. Par défaut, l'adresse du conteneur est une adresse générée aléatoirement, mais si vous en avez défini une à l'aide de l' `_NETWORK_MAC` clé de configuration du 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 promiscuité sur l'hyperviseur peut entraîner l'arrêt du fonctionnement du réseau hôte Linux utilisant l'interface de l'hôte.

Cas d'utilisation du clonage MAC

Il y a deux cas d'utilisation à prendre en compte avec le clonage MAC :

- Clonage MAC non activé : lorsque le `_CLONE_MAC` Si la clé dans le fichier de configuration du nœud n'est pas définie ou définie sur « false », l'hôte utilisera le MAC de la carte réseau de l'hôte et le conteneur aura un MAC généré par StorageGRID, sauf si un MAC est spécifié dans le `_NETWORK_MAC` clé. Si une adresse est définie dans le `_NETWORK_MAC` clé, le conteneur aura l'adresse spécifiée dans le `_NETWORK_MAC` clé. Cette configuration de clés nécessite l'utilisation du mode promiscuité.
- Clonage MAC activé : lorsque le `_CLONE_MAC` dans le 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, sauf si un MAC est 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 touches, vous ne devez pas utiliser le mode promiscuité.



Si vous ne souhaitez pas utiliser le clonage d'adresse MAC et préférez autoriser toutes les interfaces à recevoir et à transmettre des données pour des 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 **Accepter** pour le mode promiscuité, les modifications d'adresse MAC et les transmissions falsifiées. Les valeurs définies sur le commutateur virtuel peuvent être remplacées par les valeurs au niveau du groupe de ports. Assurez-vous donc que les paramètres sont les mêmes aux deux endroits.

Pour activer le clonage MAC, consultez le ["instructions pour créer des fichiers de configuration de nœud"](#) .

Exemple de clonage MAC

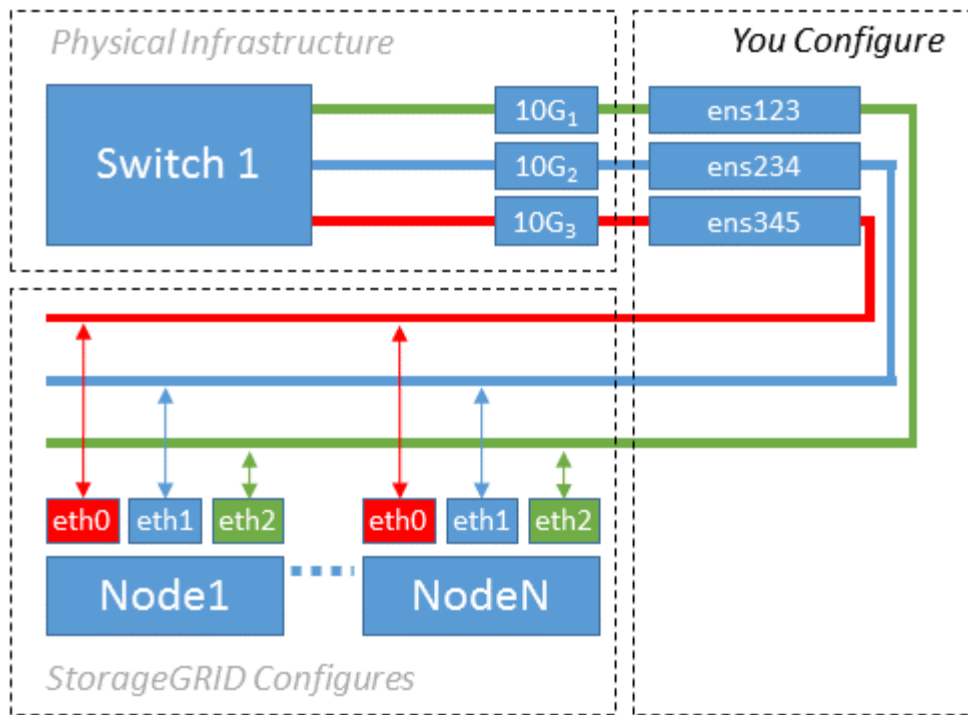
Exemple de clonage MAC activé avec un hôte ayant l'adresse MAC 11:22:33:44:55:66 pour l'interface ens256 et les clés suivantes dans le fichier de configuration du nœud :

- `ADMIN_NETWORK_TARGET = ens256`
- `ADMIN_NETWORK_MAC = b2:9c:02:c2:27:10`
- `ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC = true`

Résultat : l'adresse MAC de l'hôte pour ens256 est b2:9c:02:c2:27:10 et l'adresse MAC du réseau administrateur est 11:22:33:44:55:66

Exemple 1 : mappage 1 à 1 vers 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 requise, si ce n'est de s'assurer que les interfaces sont configurées pour s'afficher 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 montre plusieurs nœuds StorageGRID ; cependant, vous utiliseriez normalement cette configuration pour les machines virtuelles à nœud unique.

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 transportant des VLAN

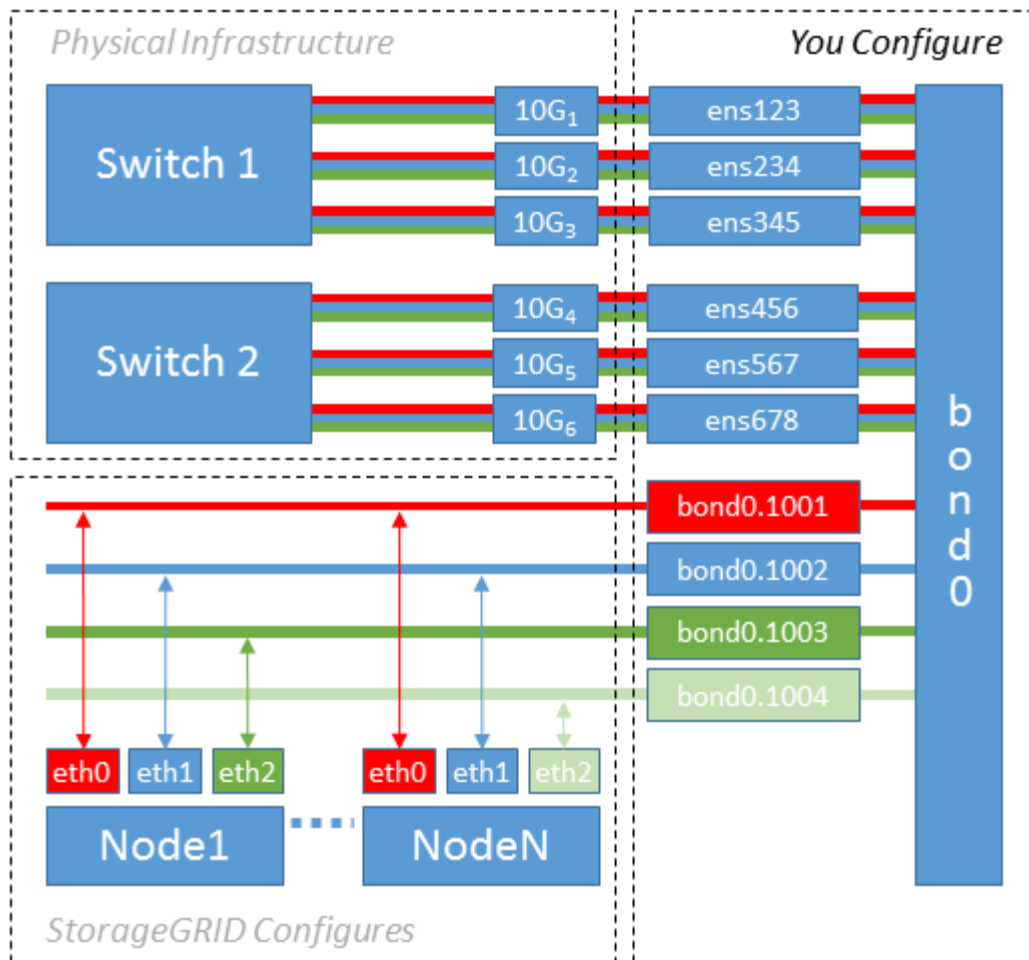
À propos de cette tâche

L'exemple 2 suppose que vous êtes familiarisé avec la liaison d'interfaces réseau 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 le VLAN qui facilite le partage de toute la bande passante réseau disponible sur tous les nœuds d'un seul hôte. Cet exemple est particulièrement applicable aux hôtes bare metal.

Pour comprendre cet exemple, supposons que vous disposez de 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 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 dans l'hôte (affiché comme `bond0.1004` dans l'illustration).



Étapes

1. Regroupez toutes les interfaces réseau physiques qui seront utilisées pour la connectivité réseau StorageGRID dans 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, en utilisant la convention de dénomination d'interface VLAN standard `physdev-name.VLAN ID` .

Notez que les étapes 1 et 2 nécessitent une configuration appropriée sur les commutateurs de périphérie terminant les autres extrémités des liaisons réseau. Les ports du commutateur périphérique doivent également être regroupés dans un canal de port LACP, configurés en tant que jonction et autorisés à transmettre tous les VLAN requis.

Des exemples de fichiers de configuration d'interface pour ce schéma de configuration réseau par hôte sont fournis.

Informations connexes

["Exemple /etc/sysconfig/network-scripts"](#)

Configurer le stockage hôte

Vous devez allouer des volumes de stockage en blocs à chaque hôte.

Avant de commencer

Vous avez examiné les rubriques suivantes, qui fournissent les informations dont vous avez besoin pour accomplir cette tâche :

- ["Exigences de stockage et de performances"](#)
- ["Exigences de migration des conteneurs de nœuds"](#)

À propos de cette tâche

Lors de l'allocation de volumes de stockage en blocs (LUN) aux hôtes, utilisez les tableaux 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 qui seront déployés sur cet hôte)
- Catégorie de stockage pour chaque volume (c'est-à-dire, données système ou données d'objet)
- Taille de chaque volume

Vous utiliserez ces informations ainsi que le nom persistant attribué par Linux à chaque volume physique lorsque vous déploierez des nœuds StorageGRID sur l'hôte.



Vous n'avez pas besoin de partitionner, de formater ou de monter l'un de ces volumes ; vous devez simplement vous assurer qu'ils sont visibles pour les hôtes.



Un seul LUN de données d'objet est requis pour les nœuds de stockage contenant uniquement des métadonnées.

Évitez d'utiliser des fichiers d'appareil spéciaux « bruts » (`/dev/sdb`, par exemple) lorsque vous composez votre liste de noms de volumes. Ces fichiers peuvent changer lors des redémarrages de l'hôte, ce qui aura un impact sur le bon fonctionnement du système. Si vous utilisez des LUN iSCSI et un mappeur de périphériques multi-chemins, pensez à utiliser des alias multi-chemins dans le `/dev/mapper` répertoire, en particulier si votre topologie SAN inclut des chemins réseau redondants vers le stockage partagé. Alternativement, vous pouvez utiliser les liens logiciels créés par le système sous `/dev/disk/by-path/` pour vos noms d'appareils 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 seront différents pour chaque installation.

Attribuez des noms conviviaux à chacun de ces volumes de stockage en blocs pour simplifier l'installation initiale de StorageGRID et les procédures de maintenance futures. Si vous utilisez le pilote multi-chemins du mappeur de périphériques pour un accès redondant aux volumes de stockage partagés, vous pouvez utiliser le `alias` champ dans votre `/etc/multipath.conf` déposer.

Par exemple:


```

multipaths {
    multipath {
        wwid 3600a09800059d6df00005df2573c2c30
        alias docker-storage-volume-hostA
    }
    multipath {
        wwid 3600a09800059d6df00005df3573c2c30
        alias sgws-adml-var-local
    }
    multipath {
        wwid 3600a09800059d6df00005df4573c2c30
        alias sgws-adml-audit-logs
    }
    multipath {
        wwid 3600a09800059d6df00005df5573c2c30
        alias sgws-adml-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
    }
    ...
}

```

L'utilisation du champ alias de cette manière fait apparaître les alias comme des périphériques de bloc dans le `/dev/mapper` répertoire sur l'hôte, vous permettant de spécifier un nom convivial et facilement validé chaque fois qu'une opération de configuration ou de maintenance nécessite 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 utilisez Device Mapper Multipathing, vous pouvez créer et installer un stockage partagé commun. `/etc/multipath.conf` sur tous les hôtes colocalisés. Assurez-vous simplement d'utiliser un volume de stockage de moteur de conteneur 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 du moteur de conteneur rendront cela facile à mémoriser et sont recommandées.



La prise en charge de Docker comme moteur de conteneur pour les déploiements uniquement logiciels est obsolète. Docker sera remplacé par un autre moteur de conteneur dans une prochaine version.

Informations connexes

["Configurer le volume de stockage du moteur de conteneur"](#)

Configurer le volume de stockage du moteur de conteneur

Avant d'installer le moteur de conteneur (Docker ou Podman), vous devrez peut-être formater le volume de stockage et le monter.



La prise en charge de Docker comme moteur de conteneur pour les déploiements uniquement logiciels est obsolète. Docker sera remplacé par un autre moteur de conteneur dans une prochaine version.

À propos de cette tâche

Vous pouvez ignorer ces étapes si vous prévoyez d'utiliser le stockage local pour le volume de stockage Docker ou Podman et que vous disposez de suffisamment d'espace 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. Créez 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 container-storage-volume-device dans `/etc/fstab`.

Cette étape garantit que le volume de stockage sera remonté automatiquement après le redémarrage de l'hôte.

Installer Docker

Le système StorageGRID fonctionne sur Red Hat Enterprise Linux en tant que collection de conteneurs. Si vous avez choisi d'utiliser le moteur de conteneur Docker, suivez ces étapes pour installer Docker.

Sinon, [installer 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 à partir du 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. Confirmez que vous avez installé la version attendue de Docker en saisissant ce qui suit :

```
sudo docker version
```

Les versions Client et Serveur doivent être 1.11.0 ou ultérieures.

Installer Podman

Le système StorageGRID fonctionne sur Red Hat Enterprise Linux en tant que collection de conteneurs. Si vous avez choisi d'utiliser le moteur de conteneur Podman, suivez ces étapes pour installer Podman. Sinon, [installer Docker](#) .



Podman est pris en charge uniquement sur Red Hat Enterprise Linux (RHEL).

Étapes

1. Installez Podman et Podman-Docker en suivant les instructions de votre distribution Linux.



Vous devez également installer le package Podman-Docker lorsque vous installez Podman.

2. Confirmez que vous avez installé la version attendue de Podman et Podman-Docker en saisissant ce qui suit :

```
sudo docker version
```



Le package Podman-Docker vous permet d'utiliser les commandes Docker.

Les versions Client et Serveur doivent être 3.2.3 ou ultérieures.

```
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
```

Installer les services hôtes StorageGRID

Vous utilisez le package RPM StorageGRID pour installer les services hôtes StorageGRID .

À propos de cette tâche

Ces instructions décrivent comment installer les services hôtes à partir des packages RPM. En guise d'alternative, vous pouvez utiliser les métadonnées du référentiel DNF incluses dans l'archive d'installation pour installer les packages RPM à distance. Consultez les instructions du référentiel DNF pour votre système d'exploitation Linux.

Étapes

1. Copiez les packages RPM StorageGRID sur chacun de vos hôtes ou rendez-les disponibles sur un stockage partagé.

Par exemple, placez-les dans le `/tmp` répertoire, vous pouvez donc utiliser l'exemple de commande 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 dnf --nogpgcheck localinstall /tmp/StorageGRID-Webscale-Images-  
version-SHA.rpm
```

```
sudo dnf --nogpgcheck localinstall /tmp/StorageGRID-Webscale-Service-  
version-SHA.rpm
```



Vous devez d'abord installer le package Images, puis le package Service.



Si vous avez placé les packages dans un répertoire autre que `/tmp` , modifiez la commande pour refléter le chemin que vous avez utilisé.

Automatiser l'installation de StorageGRID sur Red Hat Enterprise Linux

Vous pouvez automatiser l'installation du service hôte StorageGRID et la configuration des nœuds de grille.

L'automatisation du déploiement peut être utile dans l'un des cas suivants :

- Vous utilisez déjà un framework d'orchestration standard, tel qu'Ansible, Puppet ou Chef, pour déployer et configurer des hôtes physiques ou virtuels.
- Vous avez l'intention de déployer plusieurs instances StorageGRID .
- Vous déployez une instance StorageGRID volumineuse 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 en utilisant l'une de ces méthodes :

- ["Créer les fichiers de configuration"](#) de manière interactive lors d'une installation manuelle.
- Préparez les fichiers de configuration à l'avance (ou par programmation) pour permettre l'installation automatisée à l'aide de cadres d'orchestration standard, comme décrit dans cet article.

StorageGRID fournit des scripts Python facultatifs pour automatiser la configuration des appliances StorageGRID et de l'ensemble du système StorageGRID (la « grille »). Vous pouvez utiliser ces scripts directement ou les inspecter pour apprendre à les utiliser. ["API REST d'installation de StorageGRID"](#) dans les outils de déploiement et de configuration de réseau que vous développez vous-même.

Automatiser l'installation et la configuration du service hôte StorageGRID

Vous pouvez automatiser l'installation du service hôte StorageGRID à l'aide de frameworks d'orchestration standard tels qu'Ansible, Puppet, Chef, Fabric ou SaltStack.

Le service hôte StorageGRID est conditionné dans un RPM et est piloté par des fichiers de configuration que vous pouvez préparer à l'avance (ou par programmation) pour permettre une installation automatisée. Si vous utilisez déjà un framework d'orchestration standard pour installer et configurer RHEL, l'ajout de StorageGRID à vos playbooks ou recettes devrait être simple.

Voir l'exemple de rôle et de playbook Ansible dans le `/extras` dossier fourni avec l'archive d'installation. Le playbook Ansible montre comment le `storagegrid` le rôle prépare l'hôte et installe StorageGRID sur les serveurs cibles. Vous pouvez personnaliser le rôle ou le manuel selon vos besoins.



L'exemple de playbook 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 de préparation des hôtes et de déploiement des nœuds de grille virtuels.

Exemple de rôle et de manuel Ansible

Un exemple de rôle et de playbook Ansible est fourni avec l'archive d'installation dans le `/extras` dossier. Le playbook Ansible montre comment le `storagegrid` le rôle prépare les hôtes et installe StorageGRID sur les serveurs cibles. Vous pouvez personnaliser le rôle ou le manuel selon vos besoins.

Les tâches d'installation fournies `storagegrid` exemple de rôle utiliser le `ansible.builtin.dnf` module pour effectuer l'installation à partir des fichiers RPM locaux ou d'un référentiel Yum distant. Si le module n'est pas disponible ou n'est pas pris en charge, vous devrez peut-être modifier les tâches Ansible appropriées dans les fichiers suivants pour utiliser le `yum` ou `ansible.builtin.yum` module:

- `roles/storagegrid/tasks/rhel_install_from_repo.yml`
- `roles/storagegrid/tasks/rhel_install_from_local.yml`

Automatiser la configuration de StorageGRID

Après avoir déployé les nœuds de grille, 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 de fichier	Description
configure-storagegrid.py	Script Python utilisé pour automatiser la configuration
configure-storagegrid.sample.json	Exemple de fichier de configuration à utiliser avec le script
configure-storagegrid.blank.json	Fichier de configuration vide à utiliser avec le script

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

À propos de cette 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 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 plan de relance `.zip` Le fichier est généré pendant le processus de configuration et il est téléchargé dans le répertoire dans lequel vous exécutez le processus d'installation et de configuration. Vous devez

sauvegarder le fichier du package de récupération afin de pouvoir récupérer le système StorageGRID si un ou plusieurs nœuds de grille échouent. Par exemple, copiez-le vers un emplacement réseau sécurisé et sauvegardé et vers un emplacement de stockage cloud sécurisé.



Le fichier du package de récupération doit être sécurisé car il contient des clés de chiffrement et des mots de passe qui peuvent être utilisés pour obtenir des données à partir du système StorageGRID .

Si vous avez spécifié que des mots de passe aléatoires soient générés, ouvrez le `Passwords.txt` fichier et recherchez les mots de passe requis pour accéder à votre 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 connexes

["Installation de l'API REST"](#)

Déployer des nœuds de grille virtuels (Red Hat)

Créer des fichiers de configuration de nœud pour les déploiements Red Hat Enterprise Linux

Les fichiers de configuration de nœud sont de petits fichiers texte qui fournissent les informations dont le service hôte StorageGRID a besoin pour démarrer un nœud et le connecter au réseau approprié et aux ressources de stockage en bloc. Les fichiers de configuration de nœud sont utilisés pour les nœuds virtuels et ne sont pas utilisés pour les nœuds d'appliance.

Emplacement des fichiers de configuration des nœuds

Placez le fichier de configuration pour chaque nœud StorageGRID dans le `/etc/storagegrid/nodes` répertoire sur l'hôte où le nœud s'exécutera. 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 vous pouvez les créer ailleurs et les déplacer vers chaque hôte.

Nommage des fichiers de configuration des nœuds

Les noms des fichiers de configuration sont significatifs. 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 de StorageGRID et est utilisé pour les opérations de maintenance des nœuds, telles que la migration des nœuds.

Les noms de nœuds doivent suivre ces règles :

- Doit être unique
- Doit commencer par une lettre
- Peut contenir les caractères A à Z et a à z
- Peut contenir les chiffres de 0 à 9
- Peut contenir un ou plusieurs tirets (-)
- Ne doit pas dépasser 32 caractères, sans compter le `.conf` extension

Tous les fichiers dans `/etc/storagegrid/nodes` qui ne suivent pas ces conventions de nommage ne seront pas analysés par le service hôte.

Si vous avez prévu une topologie multi-sites pour votre réseau, un schéma de dénomination de nœud typique pourrait être :

`site-nodetype-nodenumbers.conf`

Par exemple, vous pouvez utiliser `dc1-adm1.conf` pour le premier nœud d'administration du centre de données 1, et `dc2-sn3.conf` pour le troisième nœud de stockage du centre de données 2. Cependant, vous pouvez utiliser le schéma de votre choix, à condition que tous les noms de nœuds respectent les règles de dénomination.

Contenu d'un fichier de configuration de nœud

Un fichier de configuration contient des paires clé/valeur, avec une clé et une valeur par ligne. Pour chaque paire clé/valeur, suivez ces règles :

- La clé et la valeur doivent être séparées par un signe égal(=) et des espaces facultatifs.
- Les clés ne peuvent contenir aucun espace.
- Les valeurs peuvent contenir des espaces intégrés.
- Tout espace blanc de début ou de fin est ignoré.

Le tableau suivant définit les valeurs de toutes les clés prises en charge. Chaque clé possède l'une des désignations suivantes :

- **Obligatoire** : Obligatoire pour chaque nœud ou pour les types de nœuds spécifiés
- **Meilleure pratique** : Facultatif, mais recommandé
- **Facultatif** : Facultatif pour tous les nœuds

Clés du réseau d'administration

ADMIN_IP

Valeur	Désignation
Adresse IPv4 du réseau de grille du nœud d'administration principal de la grille à laquelle appartient ce nœud. Utilisez la même valeur que celle que vous avez 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 découvrir un nœud d'administration principal à l'aide de mDNS. "Comment les nœuds de grille découvrent le nœud d'administration principal" Remarque : cette valeur est ignorée et peut être interdite sur le nœud d'administration principal.	Meilleures pratiques

CONFIG_RÉSEAU_ADMIN

Valeur	Désignation
DHCP, STATIQUE ou DÉSACTIVÉ	Facultatif

ADMIN_RESEAU_ESL

Valeur	Désignation
Liste séparée par des virgules des sous-réseaux en notation CIDR avec lesquels ce nœud doit communiquer à l'aide de la passerelle réseau d'administration. Exemple: 172.16.0.0/21, 172.17.0.0/21	Facultatif

PASSERELLE_RÉSEAU_ADMIN

Valeur	Désignation
Adresse IPv4 de la passerelle du réseau d'administration local 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. Exemples: 1.1.1.1 10.224.4.81	Obligatoire si ADMIN_NETWORK_ESL est spécifié. Facultatif sinon.

ADMIN_RESEAU_IP

Valeur	Désignation
Adresse IPv4 de ce nœud sur le réseau d'administration. Cette clé n'est requise que lorsque ADMIN_NETWORK_CONFIG = STATIC ; ne la spécifiez pas pour d'autres valeurs. Exemples: 1.1.1.1 10.224.4.81	Obligatoire lorsque ADMIN_NETWORK_CONFIG = STATIC. Facultatif sinon.

ADMIN_RESEAU_MAC

Valeur	Désignation
L'adresse MAC de l'interface réseau d'administration dans le conteneur. Ce champ est facultatif. Si elle est omise, une adresse MAC sera générée automatiquement. Doit être composé de 6 paires de chiffres hexadécimaux séparés par des deux points. Exemple: b2:9c:02:c2:27:10	Facultatif

MASQUE_RÉSEAU_ADMIN

Valeur	Désignation
Masque de réseau IPv4 pour ce nœud, sur le réseau d'administration. Spécifiez cette clé lorsque ADMIN_NETWORK_CONFIG = STATIC ; ne la spécifiez pas pour d'autres valeurs. Exemples: 255.255.255.0 255.255.248.0	Obligatoire si ADMIN_NETWORK_IP est spécifié et ADMIN_NETWORK_CONFIG = STATIC. Facultatif sinon.

ADMIN_RESEAU_MTU

Valeur	Désignation
L'unité de transmission maximale (MTU) pour ce nœud sur le réseau d'administration. Ne spécifiez pas si ADMIN_NETWORK_CONFIG = DHCP. Si spécifié, la valeur doit être comprise entre 1280 et 9216. Si omis, 1500 est utilisé. Si vous souhaitez utiliser des trames jumbo, définissez le MTU sur une valeur adaptée aux trames jumbo, telle que 9 000. 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 du réseau ou une perte de paquets pourraient survenir. Exemples: 1500 8192	Facultatif

ADMIN_RÉSEAU_CIBLE

Valeur	Désignation
Nom du périphérique hôte que vous utiliserez pour l'accès au réseau d'administration par le nœud StorageGRID . Seuls les noms d'interface réseau sont pris en charge. En règle générale, vous utilisez un nom d'interface différent de celui spécifié pour GRID_NETWORK_TARGET ou CLIENT_NETWORK_TARGET. Remarque : n'utilisez pas de périphériques 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 n'aura pas initialement d'adresse IP de réseau d'administration. Vous pouvez ensuite ajouter une adresse IP de réseau d'administration ultérieurement, sans avoir à reconfigurer le nœud sur l'hôte. Exemples: bond0.1002 ens256	Meilleures pratiques

TYPE_CIBLE_RÉSEAU_ADMIN

Valeur	Désignation
Interface (c'est la seule valeur prise en charge.)	Facultatif

ADMIN_RÉSEAU_TYPE_CIBLE_INTERFACE_CLONE_MAC

Valeur	Désignation
Vrai ou faux Définissez la clé sur « true » pour que le conteneur StorageGRID utilise l'adresse MAC de l'interface cible de l'hôte sur le réseau d'administration. Meilleure pratique : dans les réseaux où le mode promiscuité est requis, utilisez plutôt la clé ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC. Pour plus de détails sur le clonage MAC : • "Considérations et recommandations pour le clonage d'adresses MAC (Red Hat Enterprise Linux)" • "Considérations et recommandations pour le clonage d'adresses MAC (Ubuntu ou Debian)"	Meilleures pratiques

RÔLE_ADMIN

Valeur	Désignation
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.	Obligatoire lorsque NODE_TYPE = VM_Admin_Node Facultatif sinon.

Bloquer les clés de l'appareil

BLOQUER_LES_JOURNAUX_D'AUDIT_DE_L'APPAREIL

Valeur	Désignation
Chemin et nom du fichier spécial du périphérique de bloc que ce nœud utilisera pour le stockage persistant des journaux d'audit. Exemples: <pre>/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0</pre> <pre>/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd</pre> <pre>/dev/mapper/sgws-adml-audit-logs</pre>	Obligatoire pour les nœuds avec NODE_TYPE = VM_Admin_Node. Ne le spécifiez pas pour d'autres types de nœuds.

BLOCK_DEVICE_RANGEDB_nnn

Valeur	Désignation
Chemin et nom du fichier spécial du périphérique de bloc que ce nœud utilisera pour le stockage d'objets persistants. Cette clé n'est requise que pour les nœuds avec NODE_TYPE = VM_Storage_Node ; ne la spécifiez pas pour les autres types de nœuds. Seul BLOCK_DEVICE_RANGEDB_000 est requis ; les autres sont facultatifs. Le périphérique de bloc spécifié pour BLOCK_DEVICE_RANGEDB_000 doit être d'au moins 4 To ; les autres peuvent être plus petits. Ne laissez pas de trous. Si vous spécifiez BLOCK_DEVICE_RANGEDB_005, vous devez également spécifier BLOCK_DEVICE_RANGEDB_004. Remarque : pour des raisons de compatibilité avec les déploiements existants, les clés à deux chiffres sont prises en charge pour les nœuds mis à niveau. Exemples: <pre>/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0</pre> <pre>/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd</pre> <pre>/dev/mapper/sgws-snl-rangedb-000</pre>	Requis: BLOCK_DEVICE_RANGEDB_000 Facultatif: 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

BLOCK_DEVICE_TABLES

Valeur	Désignation
Chemin et nom du fichier spécial du périphérique de bloc que ce nœud utilisera pour le stockage persistant des tables de base de données. Cette clé n'est requise que pour les nœuds avec NODE_TYPE = VM_Admin_Node ; ne la spécifiez pas pour les autres types de nœuds. Exemples: <pre>/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0</pre> <pre>/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd</pre> <pre>/dev/mapper/sgws-adml-tables</pre>	Obligatoire

BLOC_DEVICE_VAR_LOCAL

Valeur	Désignation
Chemin et nom du fichier spécial du périphérique de bloc que ce nœud utilisera pour son /var/local stockage persistant. Exemples: <pre>/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0</pre> <pre>/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd</pre> <pre>/dev/mapper/sgws-sn1-var-local</pre>	Obligatoire

Clés du réseau client

CONFIG RÉSEAU_CLIENT

Valeur	Désignation
DHCP, STATIQUE ou DÉSACTIVÉ	Facultatif

PASSERELLE RÉSEAU_CLIENT

Valeur	Désignation

Adresse IPv4 de la passerelle réseau client locale pour ce nœud, qui doit se trouver sur le sous-réseau défini par <code>CLIENT_NETWORK_IP</code> et <code>CLIENT_NETWORK_MASK</code>. Cette valeur est ignorée pour les réseaux configurés par DHCP. Exemples: 1.1.1.1 10.224.4.81	Facultatif

IP_RÉSEAU_CLIENT

Valeur	Désignation
Adresse IPv4 de ce nœud sur le réseau client. Cette clé n'est requise que lorsque <code>CLIENT_NETWORK_CONFIG = STATIC</code> ; ne la spécifiez pas pour d'autres valeurs. Exemples: 1.1.1.1 10.224.4.81	Obligatoire lorsque <code>CLIENT_NETWORK_CONFIG = STATIC</code> Facultatif sinon.

CLIENT_RÉSEAU_MAC

Valeur	Désignation
L'adresse MAC de l'interface réseau client dans le conteneur. Ce champ est facultatif. Si elle est omise, une adresse MAC sera générée automatiquement. Doit être composé de 6 paires de chiffres hexadécimaux séparés par des deux points. Exemple: b2:9c:02:c2:27:20	Facultatif

MASQUE_RÉSEAU_CLIENT

Valeur	Désignation
Masque de réseau IPv4 pour ce nœud sur le réseau client. Spécifiez cette clé lorsque CLIENT_NETWORK_CONFIG = STATIC ; ne la spécifiez pas pour d'autres valeurs. Exemples: 255.255.255.0 255.255.248.0	Obligatoire si CLIENT_NETWORK_IP est spécifié et CLIENT_NETWORK_CONFIG = STATIC Facultatif sinon.

CLIENT_RESEAU_MTU

Valeur	Désignation
L'unité de transmission maximale (MTU) pour ce nœud sur le réseau client. Ne spécifiez pas si CLIENT_NETWORK_CONFIG = DHCP. Si spécifié, la valeur doit être comprise entre 1280 et 9216. Si omis, 1500 est utilisé. Si vous souhaitez utiliser des trames jumbo, définissez le MTU sur une valeur adaptée aux trames jumbo, telle que 9 000. 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 du réseau ou une perte de paquets pourraient survenir. Exemples: 1500 8192	Facultatif

CLIENT_RESEAU_CIBLE

Valeur	Désignation
Nom du périphérique hôte que vous utiliserez pour l'accès au réseau client par le nœud StorageGRID . Seuls les noms d'interface réseau sont pris en charge. En règle générale, vous utilisez un nom d'interface différent de celui spécifié pour GRID_NETWORK_TARGET ou ADMIN_NETWORK_TARGET. Remarque : n'utilisez pas de périphériques 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 n'aura pas initialement d'adresse IP de réseau client. Vous pouvez ensuite ajouter une adresse IP de réseau client ultérieurement, sans avoir à reconfigurer le nœud sur l'hôte. Exemples: bond0.1003 ens423	Meilleures pratiques

TYPE_CIBLE RÉSEAU_CLIENT

Valeur	Désignation
Interface (il s'agit de la seule valeur prise en charge.)	Facultatif

CLIENT RÉSEAU_TYPE_CIBLE_INTERFACE_CLONE_MAC

Valeur	Désignation
Vrai ou faux Définissez la clé sur « true » pour que le conteneur StorageGRID utilise l'adresse MAC de l'interface cible de l'hôte sur le réseau client. Meilleure pratique : dans les réseaux où le mode promiscuité est requis, utilisez plutôt la clé CLIENT_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC. Pour plus de détails sur le clonage MAC : • "Considérations et recommandations pour le clonage d'adresses MAC (Red Hat Enterprise Linux)" • "Considérations et recommandations pour le clonage d'adresses MAC (Ubuntu ou Debian)"	Meilleures pratiques

Clés du réseau Grid

CONFIG_RÉSEAU_GRILLE

Valeur	Désignation
STATIQUE ou DHCP La valeur par défaut est STATIC si elle n'est pas spécifiée.	Meilleures pratiques

PASSERELLE_RÉSEAU_GRILLE

Valeur	Désignation
Adresse IPv4 de la passerelle du réseau Grid local 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 (XYZ1), soit la valeur GRID_NETWORK_IP de ce nœud ; l'une ou l'autre valeur simplifiera les futures extensions potentielles du réseau Grid.	Obligatoire

IP_RÉSEAU_GRILLE

Valeur	Désignation
Adresse IPv4 de ce nœud sur le réseau Grid. Cette clé n'est requise que lorsque GRID_NETWORK_CONFIG = STATIC ; ne la spécifiez pas pour d'autres valeurs. Exemples: 1.1.1.1 10.224.4.81	Obligatoire lorsque GRID_NETWORK_CONFIG = STATIC Facultatif sinon.

GRILLE_RÉSEAU_MAC

Valeur	Désignation
L'adresse MAC de l'interface Grid Network dans le conteneur. Doit être composé de 6 paires de chiffres hexadécimaux séparés par des deux points. Exemple: b2:9c:02:c2:27:30	Facultatif Si elle est omise, une adresse MAC sera générée automatiquement.

MASQUE_RÉSEAU_GRILLE

Valeur	Désignation
Masque de réseau IPv4 pour ce nœud sur le réseau Grid. Spécifiez cette clé lorsque GRID_NETWORK_CONFIG = STATIC ; ne la spécifiez pas pour d'autres valeurs. Exemples: 255.255.255.0 255.255.248.0	Obligatoire lorsque GRID_NETWORK_IP est spécifié et GRID_NETWORK_CONFIG = STATIC. Facultatif sinon.

RÉSEAU_GRILLE_MTU

Valeur	Désignation
L'unité de transmission maximale (MTU) pour ce nœud sur le réseau Grid. Ne spécifiez pas si GRID_NETWORK_CONFIG = DHCP. Si spécifié, la valeur doit être comprise entre 1280 et 9216. Si omis, 1500 est utilisé. Si vous souhaitez utiliser des trames jumbo, définissez le MTU sur une valeur adaptée aux trames jumbo, telle que 9 000. 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 du réseau ou une perte de paquets pourraient survenir. IMPORTANT : pour des performances réseau optimales, tous les nœuds doivent être configurés avec des valeurs MTU similaires sur leurs interfaces Grid Network. L'alerte Incompatibilité MTU du réseau de grille est déclenchée s'il existe une différence significative dans les paramètres MTU du réseau de grille sur des nœuds individuels. Les valeurs MTU ne doivent pas nécessairement être les mêmes pour tous les types de réseaux. Exemples: 1500 8192	Facultatif

GRILLE_RÉSEAU_CIBLE

Valeur	Désignation
Nom du périphérique hôte que vous utiliserez pour l'accès au réseau Grid par le nœud StorageGRID . Seuls les noms d'interface réseau sont pris en charge. En règle générale, vous utilisez un nom d'interface différent de celui spécifié pour ADMIN_NETWORK_TARGET ou CLIENT_NETWORK_TARGET. Remarque : n'utilisez pas de périphériques 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	Obligatoire

TYPE_CIBLE RÉSEAU GRILLE

Valeur	Désignation
Interface (c'est la seule valeur prise en charge.)	Facultatif

GRID_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC

Valeur	Désignation
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 Grid. Meilleure pratique : dans les réseaux où le mode promiscuité est requis, utilisez plutôt la clé GRID_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC. Pour plus de détails sur le clonage MAC : • "Considérations et recommandations pour le clonage d'adresses MAC (Red Hat Enterprise Linux)" • "Considérations et recommandations pour le clonage d'adresses MAC (Ubuntu ou Debian)"	Meilleures pratiques

Clé de mot de passe d'installation (temporaire)

HACHAGE_DE_MOT_DE_PASSE_TEMPORAIRE_PERSONNALISÉ

Valeur	Désignation
Pour le nœud d'administration principal, définissez un mot de passe temporaire par défaut pour l'API d'installation StorageGRID pendant l'installation. Remarque : définissez un mot de passe d'installation sur le nœud d'administration principal uniquement. Si vous tentez de définir un mot de passe sur un autre type de nœud, la validation du fichier de configuration du nœud échouera. La définition de cette valeur n'a aucun effet une fois l'installation terminée. Si cette clé est omise, aucun mot de passe temporaire n'est défini par défaut. Vous pouvez également définir un mot de passe temporaire à l'aide de l'API d'installation StorageGRID . Doit être un <code>crypt()</code> Hachage de mot de passe SHA-512 avec format <code>\$6\$<salt>\$<password hash></code> pour un mot de passe d'au moins 8 et d'au plus 32 caractères. Ce hachage peut être généré à l'aide d'outils CLI, tels que <code>openssl passwd</code> commande en mode SHA-512.	Meilleures pratiques

Clé des interfaces

INTERFACE_CIBLE_nnnn

Valeur	Désignation
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 <i>nnnn</i>, spécifiez un numéro unique pour chaque entrée <code>INTERFACE_TARGET</code> 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 Interfaces VLAN et sur la page Groupes HA. Exemple: <code>INTERFACE_TARGET_0001=ens256, Trunk</code> Si vous ajoutez une interface de jonction, vous devez configurer une interface VLAN dans StorageGRID. Si vous ajoutez une interface d'accès, vous pouvez ajouter l'interface directement à un groupe HA ; vous n'avez pas besoin de configurer une interface VLAN.	Facultatif

Clé RAM maximale

RAM MAXIMALE

Valeur	Désignation
La 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, spécifiez une valeur d'au moins 24 Go et de 16 à 32 Go inférieure à la RAM totale du système. Remarque : la valeur RAM affecte l'espace réservé réel aux métadonnées d'un nœud. Voir le "description de ce qu'est l'espace réservé aux métadonnées". Le format de ce champ est <i>numberunit</i>, où <i>unit</i> 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.	Facultatif

Clés de type de nœud

TYPE_NOEUD

Valeur	Désignation
Type de nœud : • Nœud_Admin_VM • Nœud de stockage VM • Nœud d'archive VM • Passerelle VM_API	Obligatoire

TYPE_DE_STOCKAGE

Valeur	Désignation
Définit le type d'objets qu'un nœud de stockage contient. Pour plus d'informations, consultez la section "Types de nœuds de stockage". Cette clé n'est requise que pour les nœuds avec <code>NODE_TYPE = VM_Storage_Node</code> ; ne la spécifiez pas pour les autres types de nœuds. Types de stockage : • combiné • données • métadonnées Remarque : si le <code>STORAGE_TYPE</code> n'est pas spécifié, le type de nœud de stockage est défini sur combiné (données et métadonnées) par défaut.	Facultatif

Clés de remappage des ports

PORT_REMAP

Valeur	Désignation
Remappe tout port utilisé par un nœud pour les communications internes du nœud de grille ou les communications externes. Le remappage des ports est nécessaire si les politiques de réseau d'entreprise restreignent un ou plusieurs ports utilisés par StorageGRID, comme décrit dans "Communications internes des nœuds de réseau" ou "Communications externes". IMPORTANT : Ne remappez pas les ports que vous prévoyez d'utiliser pour configurer les points de terminaison de l'équilibreur de charge. Remarque : si seul <code>PORT_REMAP</code> est défini, le mappage que vous spécifiez est utilisé pour les communications entrantes et sortantes. Si <code>PORT_REMAP_INBOUND</code> est également spécifié, <code>PORT_REMAP</code> s'applique uniquement aux communications sortantes. Le format utilisé est : <i>network type/protocol/default port used by grid node/new port</i>, où <i>network type</i> est une grille, un administrateur ou un client, et <i>protocol</i> est tcp ou udp. Exemple: <code>PORT_REMAP = client/tcp/18082/443</code> Vous pouvez également remapper plusieurs ports à l'aide d'une liste séparée par des virgules. Exemple: <code>PORT_REMAP = client/tcp/18082/443, client/tcp/18083/80</code>	Facultatif

PORT_REMAP_ENTRANT

Valeur	Désignation
Remappe les communications entrantes vers le port spécifié. Si vous spécifiez <code>PORT_REMAP_INBOUND</code> mais ne spécifiez pas de valeur pour <code>PORT_REMAP</code>, les communications sortantes pour le port restent inchangées. IMPORTANT : Ne remappez pas les ports que vous prévoyez d'utiliser pour configurer les points de terminaison de l'équilibreur de charge. Le format utilisé est : <i>network type/protocol/remapped port /default port used by grid node</i>, où <i>network type</i> est une grille, un administrateur ou un client, et <i>protocol</i> est tcp ou udp. Exemple: <code>PORT_REMAP_INBOUND = grid/tcp/3022/22</code> Vous pouvez également remapper plusieurs ports entrants à l'aide d'une liste séparée par des virgules. Exemple: <code>PORT_REMAP_INBOUND = grid/tcp/3022/22, admin/tcp/3022/22</code>	Facultatif

Comment les nœuds de grille découvrent le nœud d'administration principal

Les nœuds de grille communiquent avec le nœud d'administration principal pour la configuration et la gestion. Chaque nœud de grille doit connaître l'adresse IP du nœud d'administration principal sur le réseau de grille.

Pour garantir 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 grille découvre automatiquement la valeur. La découverte 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 est réalisée à l'aide d'un système de noms de domaine multidiffusion (mDNS). Lorsque le nœud d'administration principal démarre pour la première fois, il publie son adresse IP à l'aide de mDNS. D'autres nœuds sur le même sous-réseau peuvent alors interroger l'adresse IP et l'acquérir automatiquement. Cependant, étant donné que le trafic IP multidiffusion n'est normalement pas routable sur les sous-réseaux, les nœuds des autres sous-réseaux ne peuvent pas acquérir directement l'adresse IP du nœud d'administration principal.

Si vous utilisez la découverte automatique :



- Vous devez inclure le paramètre ADMIN_IP pour au moins un nœud de grille sur tous les sous-réseaux auxquels le nœud d'administration principal n'est pas directement connecté. Ce nœud de grille publiera ensuite l'adresse IP du nœud d'administration principal pour que les autres nœuds du sous-réseau puissent la découvrir avec mDNS.
- Assurez-vous que votre infrastructure réseau prend en charge le passage du trafic IP multidiffusion au sein d'un sous-réseau.

Exemples de fichiers de configuration de nœuds

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 des fichiers de configuration de nœuds pour tous les types de nœuds de grille.

Pour la plupart des nœuds, vous pouvez ajouter des informations d'adressage réseau administrateur et client (IP, masque, passerelle, etc.) lorsque vous configurez la grille à l'aide du gestionnaire de grille ou de l'API d'installation. L'exception est le nœud d'administration principal. Si vous souhaitez accéder à l'adresse IP du réseau d'administration du nœud d'administration principal pour terminer la configuration de la grille (parce que le réseau de grille n'est pas routé, par exemple), vous devez configurer la connexion au réseau d'administration pour le nœud d'administration principal dans son fichier de configuration de nœud. Ceci est montré dans l'exemple.



Dans les exemples, la cible Réseau client a été configurée comme une meilleure pratique, 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
TEMPORARY_PASSWORD_TYPE = Use custom password
CUSTOM_TEMPORARY_PASSWORD = Passw0rd
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-adml-var-local
BLOCK_DEVICE_AUDIT_LOGS = /dev/mapper/dc1-adml-audit-logs
BLOCK_DEVICE_TABLES = /dev/mapper/dc1-adml-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 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 principal

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
```

Valider la configuration de StorageGRID

Après avoir créé les 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, la sortie affiche **PASSED** pour chaque fichier de configuration, comme indiqué dans l'exemple.



Lorsque vous utilisez un seul LUN sur des nœuds contenant uniquement des métadonnées, vous pouvez recevoir un message d'avertissement qui peut être ignoré.

```
Checking for misnamed node configuration files... PASSED
Checking configuration file for node dcl-adm1... PASSED
Checking configuration file for node dcl-gw1... PASSED
Checking configuration file for node dcl-sn1... PASSED
Checking configuration file for node dcl-sn2... PASSED
Checking configuration file for node dcl-sn3... PASSED
Checking for duplication of unique values between nodes... PASSED
```



Pour une installation automatisée, vous pouvez supprimer cette sortie en utilisant le `-q` ou `--quiet` options dans le `storagegrid` commande (par exemple, `storagegrid --quiet...`). Si vous supprimez la sortie, la commande aura une valeur de sortie différente de zéro si des avertissements ou des erreurs de configuration ont été détectés.

Si les fichiers de configuration sont incorrects, les problèmes sont affichés sous la forme **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/dcl-adml
WARNING: ignoring /etc/storagegrid/nodes/dcl-sn2.conf.keep
WARNING: ignoring /etc/storagegrid/nodes/my-file.txt
Checking configuration file for node dcl-adml...
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 dcl-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 dcl-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 dcl-sn2... PASSED
Checking configuration file for node dcl-sn3... PASSED
Checking for duplication of unique values between nodes...
ERROR: GRID_NETWORK_IP = 10.1.0.4
      dcl-sn2 and dcl-sn3 have the same GRID_NETWORK_IP
ERROR: BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-sn2-var-local
      dcl-sn2 and dcl-sn3 have the same BLOCK_DEVICE_VAR_LOCAL
ERROR: BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/sgws-sn2-rangedb-0
      dcl-sn2 and dcl-sn3 have the same BLOCK_DEVICE_RANGEDB_00

```

Démarrer le service hôte StorageGRID

Pour démarrer vos nœuds StorageGRID et garantir 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 vous assurer que le déploiement se poursuit :

```
sudo storagegrid node status node-name
```

3. Si un nœud renvoie l'état « Non en cours d'exécution » ou « Arrêté », 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 terminer l'installation (Red Hat)

Accéder au gestionnaire de grille

Vous utilisez le Grid Manager pour définir toutes les informations requises pour configurer votre 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 :

```
https://primary_admin_node_ip
```

Alternativement, vous pouvez accéder au Grid Manager sur le port 8443 :

```
https://primary_admin_node_ip:8443
```

Vous pouvez utiliser l'adresse IP du nœud d'administration principal sur le réseau de grille ou sur le réseau d'administration, selon la configuration de votre réseau.

2. Gérez un mot de passe d'installation temporaire selon vos besoins :
 - Si un mot de passe a déjà été défini à l'aide de l'une de ces méthodes, saisissez le mot de passe pour continuer.
 - Un utilisateur a défini le mot de passe lors de l'accès au programme d'installation précédemment
 - Le mot de passe a été automatiquement importé à partir du fichier de configuration du nœud à `/etc/storagegrid/nodes/<node_name>.conf`
 - Si aucun mot de passe n'a été défini, vous pouvez éventuellement définir un mot de passe pour sécuriser le programme d'installation de StorageGRID .
3. Sélectionnez ***Installer un système StorageGRID ***.

La page utilisée pour configurer un système StorageGRID apparaît.

NetApp® StorageGRID®

Help ▾

Install

1

2

3

4

5

6

7

8

License

Sites

Grid Network

Grid Nodes

NTP

DNS

Passwords

Summary

License

Enter a grid name and upload the license file provided by NetApp for your StorageGRID system.

Grid Name

License File

Browse

Spécifiez les informations de licence StorageGRID

Vous devez spécifier le nom de votre système StorageGRID et télécharger le fichier de licence fourni par NetApp.

Étapes

1. Sur la page Licence, saisissez 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 **Parcourir**, recherchez le fichier de licence NetApp(*NLF-unique-id.txt*), et sélectionnez **Ouvrir**.

Le fichier de licence est validé et le numéro de série est affiché.



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 niveau vers une licence qui offre un support après l'installation.

1

2

3

4

5

6

7

8

License

Sites

Grid Network

Grid Nodes

NTP

DNS

Passwords

Summary

License

Enter a grid name and upload the license file provided by NetApp for your StorageGRID system.

Grid Name

StorageGRID

License File

Browse

NLF-959007-Internal.txt

License Serial Number

959007

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 le **Nom du site**.
2. Pour ajouter des sites supplémentaires, cliquez sur le signe plus à côté de la dernière entrée de site et saisissez le nom dans la nouvelle zone de texte **Nom du site**.

Ajoutez autant de sites supplémentaires que nécessaire pour votre topologie de grille. Vous pouvez ajouter jusqu'à 16 sites.

NetApp® StorageGRID® Help ▾

Install

1 License 2 Sites 3 Grid Network 4 Grid Nodes 5 NTP 6 DNS 7 Passwords 8 Summary

Sites

In a single-site deployment, infrastructure and operations are centralized in one site.

In a multi-site deployment, infrastructure can be distributed asymmetrically across sites, and proportional to the needs of each site. Typically, sites are located in geographically different locations. Having multiple sites also allows the use of distributed replication and erasure coding for increased availability and resiliency.

Site Name 1 ✕

Site Name 2 + ✕

3. Cliquez sur **Suivant**.

Spécifier les sous-réseaux du réseau Grid

Vous devez spécifier les sous-réseaux utilisés sur le réseau Grid.

À propos de cette tâche

Les entrées de sous-réseau incluent les sous-réseaux du réseau Grid pour chaque site de votre système StorageGRID , ainsi que tous les sous-réseaux qui doivent être accessibles via le réseau Grid.

Si vous disposez de plusieurs sous-réseaux de grille, la passerelle Grid Network est requise. Tous les sous-réseaux de grille spécifiés doivent être accessibles via cette passerelle.

Étapes

1. Spécifiez l'adresse réseau CIDR pour au moins un réseau de grille 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. Vous devez spécifier tous les sous-réseaux pour tous les sites du réseau Grid.

- Si vous avez déjà déployé au moins un nœud, cliquez sur **Découvrir les sous-réseaux des réseaux de grille** pour remplir automatiquement la liste des sous-réseaux des réseaux de grille avec les sous-réseaux signalés par les nœuds de grille enregistrés auprès du gestionnaire de grille.
- Vous devez ajouter manuellement tous les sous-réseaux pour NTP, DNS, LDAP ou autres serveurs externes accessibles via la passerelle Grid Network.

NetApp® StorageGRID® Help ▾

Install

1 License 2 Sites 3 **Grid Network** 4 Grid Nodes 5 NTP 6 DNS 7 Passwords 8 Summary

Grid Network

You must specify the subnets that are used on the Grid Network. These entries typically include the subnets for the Grid Network for each site in your StorageGRID system. Select Discover Grid Networks to automatically add subnets based on the network configuration of all registered nodes.

Note: You must manually add any subnets for NTP, DNS, LDAP, or other external servers accessed through the Grid Network gateway.

Subnet 1 +

3. Cliquez sur **Suivant**.

Approuver les nœuds de grille en attente

Vous devez approuver chaque nœud de grille avant qu'il puisse rejoindre le système StorageGRID .

Avant de commencer

Vous avez déployé tous les nœuds de grille d'appliance virtuelle et StorageGRID .



Il est plus efficace d'effectuer une seule installation de tous les nœuds, plutôt que d'installer certains nœuds maintenant et certains nœuds plus tard.

Étapes

1. Consultez la liste des nœuds en attente et confirmez qu'elle affiche tous les nœuds de grille que vous avez déployés.



Si un nœud de grille est manquant, confirmez qu'il a été déployé avec succès et qu'il dispose de l'adresse IP du réseau de grille correcte du nœud d'administration principal défini pour ADMIN_IP.

2. Sélectionnez le bouton radio à côté d'un nœud en attente que vous souhaitez approuver.



Grid Nodes

Approve and configure grid nodes, so that they are added correctly to your StorageGRID system.

Pending Nodes

Grid nodes are listed as pending until they are assigned to a site, configured, and approved.

+ Approve		✖ Remove		Search		
	Grid Network MAC Address	Name	Type	Platform	Grid Network IPv4 Address	
☒	50:6b:4b:42:d7:00	NetApp-SGA	Storage Node	StorageGRID Appliance	172.16.5.20/21	

Approved Nodes

Grid nodes that have been approved and have been configured for installation. An approved grid node's configuration can be edited if errors are identified.

Edit		Reset		✖ Remove		Search	
	Grid Network MAC Address	Name	Site	Type	Platform	Grid Network IPv4 Address	
☐	00:50:56:87:42:ff	dc1-adm1	Raleigh	Admin Node	VMware VM	172.16.4.210/21	
☐	00:50:56:87:c0:16	dc1-s1	Raleigh	Storage Node	VMware VM	172.16.4.211/21	
☐	00:50:56:87:79:ee	dc1-s2	Raleigh	Storage Node	VMware VM	172.16.4.212/21	
☐	00:50:56:87:db:9c	dc1-s3	Raleigh	Storage Node	VMware VM	172.16.4.213/21	
☐	00:50:56:87:62:38	dc1-g1	Raleigh	API Gateway Node	VMware VM	172.16.4.214/21	

3. Cliquez sur **Approuver**.

4. Dans les paramètres généraux, modifiez les paramètres des propriétés suivantes, si nécessaire :

- **Site** : Le nom système du site pour ce nœud de grille.
- **Nom** : Le nom du système pour le nœud. Le nom par défaut est celui 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 du système selon vos besoins.

- **Rôle NTP** : Le rôle du protocole NTP (Network Time Protocol) du nœud de grille. Les options sont **Automatique**, **Principal** et **Client**. La sélection de **Automatique** attribue le rôle principal aux nœuds d'administration, aux nœuds de stockage avec services ADC, aux nœuds de passerelle et à tous les nœuds de grille dotés d'adresses IP non statiques. Tous les autres nœuds de grille se voient attribuer le rôle Client.



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 se produiront si ce nœud tombe en panne. De plus, la désignation de deux nœuds par site comme sources NTP principales garantit une synchronisation précise si un site est isolé du reste du réseau.

- **Type de stockage** (nœuds de stockage uniquement) : spécifiez qu'un nouveau nœud de stockage doit être utilisé exclusivement pour les données uniquement, les métadonnées uniquement ou les deux. Les options sont **Données et métadonnées** (« combinées »), **Données uniquement** et **Métadonnées uniquement**.



Voir "[Types de nœuds de stockage](#)" pour obtenir des informations sur les exigences relatives à ces types de nœuds.

- **Service ADC** (nœuds de stockage uniquement) : sélectionnez **Automatique** pour permettre au système de déterminer si le nœud nécessite le service de contrôleur de domaine administratif (ADC). Le service ADC suit l'emplacement et la disponibilité des services du réseau. Au moins trois nœuds de stockage sur chaque site doivent inclure le service ADC. Vous ne pouvez pas ajouter le service ADC à un nœud après son déploiement.

5. Dans Grid Network, modifiez les paramètres des propriétés suivantes si nécessaire :

- **Adresse IPv4 (CIDR)** : l'adresse réseau CIDR pour l'interface Grid Network (eth0 à l'intérieur du conteneur). Par exemple : 192.168.1.234/21
- **Passerelle** : La passerelle du réseau Grid. Par exemple : 192.168.0.1

La passerelle est requise s'il existe plusieurs sous-réseaux de grille.



Si vous avez sélectionné DHCP pour la configuration du réseau Grid et que vous modifiez la valeur ici, la nouvelle valeur sera configurée comme une adresse statique sur le nœud. Vous devez vous assurer que l'adresse IP configurée ne se trouve pas dans un pool d'adresses DHCP.

6. Si vous souhaitez configurer le réseau d'administration pour le nœud de grille, ajoutez ou mettez à jour les paramètres dans la section Réseau d'administration si nécessaire.

Saisissez les sous-réseaux de destination des itinéraires sortant de cette interface dans la zone de texte **Sous-réseaux (CIDR)**. S'il existe plusieurs sous-réseaux d'administration, 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 comme une adresse statique sur le nœud. Vous devez vous assurer que l'adresse IP configurée ne se trouve pas dans un pool d'adresses DHCP.

Appareils : pour un appareil 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'appareil StorageGRID , il ne peut pas être configuré dans cette boîte de dialogue Grid Manager. Au lieu de cela, vous devez suivre ces étapes :

- a. Redémarrez l'appareil : dans le programme d'installation de l'appareil, sélectionnez **Avancé > Redémarrer**.

Le redémarrage peut prendre plusieurs minutes.

- b. Sélectionnez **Configurer la mise en réseau > Configuration de liaison** et activez les réseaux appropriés.
- c. Sélectionnez **Configurer le 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 nœud.
- f. Supprimez le nœud de la table des nœuds en attente.
- g. Attendez que le nœud réapparaisse dans la liste des nœuds en attente.
- h. Confirmez que vous pouvez configurer les réseaux appropriés. Ils doivent déjà être renseignés avec les informations que vous avez fournies sur la page de configuration IP du programme d'installation de l'appliance.

Pour plus d'informations, consultez les 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 nœud 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 comme une adresse statique sur le nœud. Vous devez vous assurer que l'adresse IP configurée ne se trouve pas dans un pool d'adresses DHCP.

Appliances : 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 Grid Manager. Au lieu de cela, vous devez suivre ces étapes :

- a. Redémarrez l'appareil : dans le programme d'installation de l'appareil, sélectionnez **Avancé > Redémarrer**.

Le redémarrage peut prendre plusieurs minutes.

- b. Sélectionnez **Configurer la mise en réseau > Configuration de liaison** et activez les réseaux appropriés.
- c. Sélectionnez **Configurer le 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 nœud.
- f. Supprimez le nœud de la table des nœuds en attente.
- g. Attendez que le nœud réapparaisse dans la liste des nœuds en attente.
- h. Confirmez que vous pouvez configurer les réseaux appropriés. Ils doivent déjà être renseignés avec les informations que vous avez fournies sur la page de configuration IP du programme d'installation de l'appliance.

Pour plus d'informations, consultez les instructions d'installation de votre appareil.

8. Cliquez sur **Enregistrer**.

L'entrée du nœud de grille est déplacée vers la liste des nœuds approuvés.



Grid Nodes

Approve and configure grid nodes, so that they are added correctly to your StorageGRID system.

Pending Nodes

Grid nodes are listed as pending until they are assigned to a site, configured, and approved.

Grid Network MAC Address	Name	Type	Platform	Grid Network IPv4 Address
No results found.				

Approved Nodes

Grid nodes that have been approved and have been configured for installation. An approved grid node's configuration can be edited if errors are identified.

	Grid Network MAC Address	Name	Site	Type	Platform	Grid Network IPv4 Address
☐	00:50:56:87:42:ff	dc1-adm1	Raleigh	Admin Node	VMware VM	172.16.4.210/21
☐	00:50:56:87:c0:16	dc1-s1	Raleigh	Storage Node	VMware VM	172.16.4.211/21
☐	00:50:56:87:79:ee	dc1-s2	Raleigh	Storage Node	VMware VM	172.16.4.212/21
☐	00:50:56:87:db:9c	dc1-s3	Raleigh	Storage Node	VMware VM	172.16.4.213/21
☐	00:50:56:87:62:38	dc1-g1	Raleigh	API Gateway Node	VMware VM	172.16.4.214/21
☐	50:6b:4b:42:d7:00	NetApp-SGA	Raleigh	Storage Node	StorageGRID Appliance	172.16.5.20/21

9. Répétez ces étapes pour chaque nœud de grille en attente que vous souhaitez approuver.

Vous devez approuver tous les nœuds que vous souhaitez dans la grille. Cependant, vous pouvez revenir sur 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**.

Spécifier les informations du serveur Network Time Protocol

Vous devez spécifier les informations de configuration du protocole NTP (Network Time Protocol) pour le système StorageGRID, afin que les opérations effectuées sur des serveurs distincts puissent rester synchronisées.

À propos de cette tâche

Vous devez spécifier des adresses IPv4 pour les serveurs NTP.

Vous devez spécifier des serveurs NTP externes. Les serveurs NTP spécifiés doivent utiliser le protocole NTP.

Vous devez spécifier quatre références de serveur NTP de niveau 3 ou supérieur pour éviter les problèmes de dérive temporelle.



Lorsque vous spécifiez 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 de haute précision, tels que StorageGRID.

["Limite de prise en charge pour configurer le service de temps Windows pour les environnements de haute précision"](#)

Les serveurs NTP externes sont utilisés par les nœuds auxquels vous avez précédemment attribué des rôles NTP principaux.



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 se produiront si ce nœud tombe en panne. De plus, la désignation de deux nœuds par site comme sources NTP principales garantit une synchronisation précise si un site est isolé du reste du réseau.

Étapes

1. Spécifiez les adresses IPv4 pour au moins quatre serveurs NTP dans les zones de texte **Serveur 1** à **Serveur 4**.
2. Si nécessaire, sélectionnez le signe plus à côté de la dernière entrée pour ajouter des entrées de serveur supplémentaires.

NetApp® StorageGRID®

Help ▾

Install

1

License

2

Sites

3

Grid Network

4

Grid Nodes

5

NTP

6

DNS

7

Passwords

8

Summary

Network Time Protocol

Enter the IP addresses for at least four Network Time Protocol (NTP) servers, so that operations performed on separate servers are kept in sync.

Server 1

10.60.248.183

Server 2

10.227.204.142

Server 3

10.235.48.111

Server 4

0.0.0.0

+

3. Sélectionnez **Suivant**.

Spécifier les informations du serveur DNS

Vous devez spécifier les informations DNS pour votre système StorageGRID , afin de pouvoir accéder aux serveurs externes à l'aide de noms d'hôtes au lieu d'adresses IP.

À propos de cette tâche

Spécification "[Informations sur le serveur DNS](#)" vous permet d'utiliser des noms d'hôtes de nom de domaine complet (FQDN) plutôt que des adresses IP pour les notifications par e-mail et AutoSupport.

Pour garantir un bon fonctionnement, spécifiez deux ou trois serveurs DNS. Si vous spécifiez plus de trois, il est possible que seulement trois soient utilisés en raison de limitations connues du système d'exploitation sur certaines plates-formes. Si vous avez des restrictions de routage dans votre environnement, vous pouvez "[personnaliser la liste des serveurs DNS](#)" pour que les nœuds individuels (généralement tous les nœuds d'un site) utilisent un ensemble différent de trois serveurs DNS maximum.

Si possible, utilisez des serveurs DNS auxquels chaque site peut accéder localement pour garantir qu'un site isolé peut résoudre les noms de domaine complets pour les destinations externes.

Étapes

1. Spécifiez l'adresse IPv4 pour au moins un serveur DNS dans la zone de texte **Serveur 1**.
2. Si nécessaire, sélectionnez le signe plus à côté de la dernière entrée pour ajouter des entrées de serveur supplémentaires.

The screenshot shows the NetApp StorageGRID installation wizard interface. At the top, there's a blue header with "NetApp® StorageGRID®" and a "Help" dropdown. Below the header is a navigation bar with "Install" and a progress indicator. The progress indicator consists of eight numbered circles: 1 (License), 2 (Sites), 3 (Grid Network), 4 (Grid Nodes), 5 (NTP), 6 (DNS - currently selected and highlighted in blue), 7 (Passwords), and 8 (Summary). Below the progress bar, the section is titled "Domain Name Service". It contains a descriptive text: "Enter the IP address for at least one Domain Name System (DNS) server, so that server hostnames can be used instead of IP addresses. Specifying at least two DNS servers is recommended. Configuring DNS enables server connectivity, email notifications, and NetApp AutoSupport." Below this text, there are two input fields for DNS servers. "Server 1" has the IP address "10.224.223.130" and a minus sign icon to its right. "Server 2" has the IP address "10.224.223.136" and a plus-minus icon to its right, indicating that more servers can be added.

La meilleure pratique consiste à spécifier au moins deux serveurs DNS. Vous pouvez spécifier jusqu'à six serveurs DNS.

3. Sélectionnez **Suivant**.

Spécifiez les mots de passe du 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.

À propos de cette tâche

Utilisez la page Installer les mots de passe pour spécifier la phrase secrète de provisionnement et le mot de

mot de passe de l'utilisateur root de gestion de la grille.

- La phrase secrète de provisionnement est utilisée comme clé de chiffrement et n'est pas stockée par le système StorageGRID .
- Vous devez disposer de la phrase secrète de provisionnement pour les procédures d'installation, d'extension et de maintenance, y compris le téléchargement du package de récupération. Il est donc important de stocker la phrase secrète de provisionnement dans un endroit sûr.
- Vous pouvez modifier la phrase secrète de provisionnement à partir du gestionnaire de grille si vous disposez de la phrase secrète actuelle.
- Le mot de passe de l'utilisateur root de gestion de grille peut être modifié à l'aide du gestionnaire de grille.
- La console de ligne de commande générée aléatoirement et les mots de passe SSH sont stockés dans le `Passwords.txt` fichier dans le package de récupération.

Étapes

1. Dans **Provisioning Passphrase**, saisissez la phrase de passe de provisionnement qui sera requise pour apporter des modifications à la topologie de grille de votre système StorageGRID .

Stockez la phrase secrète de provisionnement dans un endroit sûr.



Si, une fois l'installation terminée, vous souhaitez modifier ultérieurement la phrase secrète de provisionnement, vous pouvez utiliser le gestionnaire de grille. Sélectionnez **CONFIGURATION > Contrôle d'accès > Mots de passe de la grille**.

2. Dans **Confirmer la phrase secrète de provisionnement**, saisissez à nouveau la phrase secrète de provisionnement pour la confirmer.
3. Dans **Mot de passe de l'utilisateur racine de gestion de grille**, saisissez le mot de passe à utiliser pour accéder au gestionnaire de grille en tant qu'utilisateur « root ».

Conservez le mot de passe dans un endroit sûr.

4. Dans **Confirmer le mot de passe de l'utilisateur root**, saisissez à nouveau le mot de passe du gestionnaire de grille pour le confirmer.

NetApp® StorageGRID®
Help

Install

1 License
2 Sites
3 Grid Network
4 Grid Nodes
5 NTP
6 DNS
7 Passwords
8 Summary

Passwords

Enter secure passwords that meet your organization's security policies. A text file containing the command line passwords must be downloaded during the final installation step.

Provisioning
Passphrase

Confirm
Provisioning
Passphrase

Grid Management
Root User
Password

Confirm Root User
Password

☒ Create random command line passwords.

- Si vous installez une grille à des fins de preuve de concept ou de démonstration, décochez éventuellement la case **Créer des mots de passe de ligne de commande aléatoires**.

Pour les déploiements de production, des mots de passe aléatoires doivent toujours être utilisés pour des raisons de sécurité. Cochez **Créer 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 la grille à partir de la ligne de commande à l'aide du compte « root » ou « admin ».



Vous êtes invité à télécharger le fichier du package de récupération(`sgws-recovery-package-id-revision.zip`) après avoir cliqué sur **Installer** sur la page Résumé. Vous devez "[télécharger 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 Recovery Package.

- Cliquez sur **Suivant**.

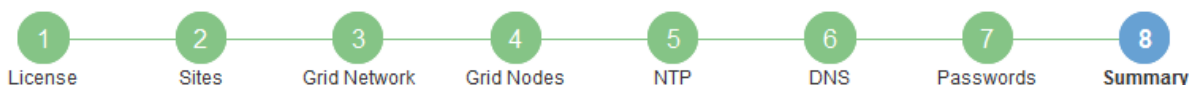
Vérifiez votre configuration et terminez l'installation

Vous devez examiner attentivement les informations de configuration que vous avez saisies pour vous assurer que l'installation se déroule correctement.

Étapes

- Voir la page **Résumé**.

Install



Summary

Verify that all of the grid configuration information is correct, and then click Install. You can view the status of each grid node as it installs. Click the Modify links to go back and change the associated information.

General Settings

Grid Name	Grid1	Modify License
Passwords	Auto-generated random command line passwords	Modify Passwords

Networking

NTP	10.60.248.183 10.227.204.142 10.235.48.111	Modify NTP
DNS	10.224.223.130 10.224.223.136	Modify DNS
Grid Network	172.16.0.0/21	Modify Grid Network

Topology

Topology	Atlanta	Modify Sites	Modify Grid Nodes
	Raleigh		
	dc1-adm1	dc1-g1	dc1-s1
	dc1-s2	dc1-s3	NetApp-SGA

- Vérifiez que toutes les informations de configuration de la grille sont correctes. Utilisez les liens Modifier sur la page Résumé pour revenir en arrière et corriger les erreurs.
- Cliquez sur **Installer**.



Si un nœud est configuré pour utiliser le réseau client, la passerelle par défaut de ce nœud passe du réseau de grille 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 "[Directives de mise en réseau](#)" pour plus de détails.

- Cliquez sur **Télécharger le package 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 package de récupération (.zip), et confirmez que vous pouvez accéder avec succès au contenu de ce fichier. Vous devez télécharger le fichier du package de récupération afin de pouvoir récupérer le système StorageGRID si un ou plusieurs nœuds de grille échouent. 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.

- Vérifiez que vous pouvez extraire le contenu du .zip fichier, puis enregistrez-le dans deux emplacements sûrs, sécurisés et distincts.



Le fichier du package de récupération doit être sécurisé car il contient des clés de chiffrement et des mots de passe qui peuvent être utilisés pour obtenir des données à partir du système StorageGRID.

6. Cochez la case **J'ai téléchargé et vérifié avec succès le fichier du package de récupération**, puis cliquez sur **Suivant**.

Si l'installation est toujours en cours, la page d'état apparaît. Cette page indique la progression de l'installation pour chaque nœud de grille.

Installation Status

If necessary, you may [Download the Recovery Package file](#) again.

						Search	
Name	IT	Site	IT	Grid Network IPv4 Address	Progress	IT	Stage
dc1-adm1		Site1		172.16.4.215/21			Starting services
dc1-g1		Site1		172.16.4.216/21			Complete
dc1-s1		Site1		172.16.4.217/21			Waiting for Dynamic IP Service peers
dc1-s2		Site1		172.16.4.218/21			Downloading hotfix from primary Admin if needed
dc1-s3		Site1		172.16.4.219/21			Downloading hotfix from primary Admin if needed

Lorsque l'étape Terminé est atteinte pour tous les nœuds de grille, la page de connexion au Gestionnaire de grille s'affiche.

7. Sign in au Grid Manager en utilisant l'utilisateur « root » et le mot de passe que vous avez spécifié lors de l'installation.

Consignes post-installation

Une fois le déploiement et la configuration du nœud de grille terminés, suivez ces instructions pour l'adressage DHCP et les modifications de configuration réseau.

- Si DHCP a été 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 lorsque la configuration du réseau de grille est modifiée par DHCP, ce qui peut provoquer des pannes si une modification DHCP affecte plusieurs nœuds en même temps.

- Vous devez utiliser les procédures de modification d'IP si vous souhaitez modifier les adresses IP, les masques de sous-réseau et les passerelles par défaut d'un nœud de grille. Voir "[Configurer les adresses IP](#)".
- Si vous apportez des modifications à la configuration du réseau, notamment au routage et à la passerelle, la connectivité client au nœud d'administration principal et aux autres nœuds de grille peut être perdue. En fonction des modifications réseau appliquées, vous devrez peut-être rétablir ces connexions.

Installation de l'API REST

StorageGRID fournit l'API d'installation StorageGRID pour effectuer des tâches d'installation.

L'API utilise la plate-forme API open source Swagger 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 comment 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 API que vous effectuez à l'aide de la page Web de documentation API 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 API REST inclut l'URL de l'API, une action HTTP, tous les paramètres d'URL obligatoires ou facultatifs et une réponse API attendue.

API d'installation de StorageGRID

L'API d'installation StorageGRID n'est disponible que lorsque vous configurez initialement votre système StorageGRID et si vous devez effectuer une récupération du nœud d'administration principal. L'API d'installation est accessible via HTTPS à partir du gestionnaire de grille.

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 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 répertorier la version du produit et les principales versions 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 du réseau de grille, les mots de passe de la grille et les adresses IP des serveurs NTP et DNS.
- **nodes** — Opérations de configuration au niveau du nœud. Vous pouvez récupérer une liste de nœuds de grille, supprimer un nœud de grille, configurer un nœud de grille, afficher un nœud de grille et réinitialiser la configuration d'un nœud de grille.
- **provision** — Opérations de provisionnement. Vous pouvez démarrer l'opération de provisionnement et afficher l'état de l'opération de provisionnement.
- **récupération** — Opérations de récupération du nœud d'administration principal. Vous pouvez réinitialiser les informations, télécharger le package de récupération, démarrer la récupération et afficher l'état de l'opération de récupération.
- **recovery-package** — Opérations de téléchargement du package de récupération.
- **sites** — Opérations de configuration au niveau du site. Vous pouvez créer, afficher, supprimer et modifier un site.
- **temporary-password** — Opérations sur le mot de passe temporaire pour sécuriser l'API de gestion pendant l'installation.

Où aller ensuite

Une fois l'installation terminée, effectuez les tâches d'intégration et de configuration requises. Vous pouvez effectuer les tâches facultatives selon vos besoins.

Tâches requises

- "[Créer un compte locataire](#)" pour le protocole client S3 qui sera utilisé pour stocker des objets sur votre système StorageGRID .
- "[Accès au système de contrôle](#)" en configurant des groupes et des comptes utilisateurs. En option, vous pouvez "[configurer une source d'identité fédérée](#)" (comme Active Directory ou OpenLDAP), afin de pouvoir

importer des groupes d'administration et des utilisateurs. Ou, vous pouvez "[créer des groupes et des utilisateurs locaux](#)".

- Intégrer et tester le "[API S3](#)" applications clientes que vous utiliserez pour télécharger des objets sur votre système StorageGRID .
- "[Configurer les règles de gestion du cycle de vie des informations \(ILM\) et la politique ILM](#)" vous souhaitez utiliser pour protéger les données de l'objet.
- Si votre installation inclut des nœuds de stockage d'appliance, utilisez SANtricity OS pour effectuer les tâches suivantes :
 - Connectez-vous à chaque appliance StorageGRID .
 - Vérifier la réception des données AutoSupport .

Voir "[Configurer le matériel](#)".

- Consultez et suivez les "[Directives de renforcement du système StorageGRID](#)" pour éliminer les risques de sécurité.
- "[Configurer les notifications par e-mail pour les alertes système](#)".

Tâches facultatives

- "[Mettre à jour les adresses IP des nœuds de 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.
- "[Configurer les interfaces VLAN](#)" pour isoler et partitionner le trafic réseau, si nécessaire.
- "[Configurer des groupes de haute disponibilité](#)" pour améliorer la disponibilité de la connexion pour les clients Grid Manager, Tenant Manager et S3, si nécessaire.
- "[Configurer les points de terminaison de l'équilibreur de charge](#)" pour la connectivité client S3, si nécessaire.

Résoudre les problèmes d'installation

Si des problèmes surviennent 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` (trouvé 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, consultez "[Collecter les fichiers journaux et les données système](#)".

Informations connexes

["Dépanner un système StorageGRID"](#)

Exemple /etc/sysconfig/network-scripts

Vous pouvez utiliser les fichiers d'exemple pour regrouper quatre interfaces physiques Linux dans une seule liaison LACP, puis établir trois interfaces VLAN sous-tendant la liaison à utiliser comme interfaces StorageGRID Grid, Admin et Client Network.

Interfaces physiques

Notez que les commutateurs aux autres extrémités des liaisons doivent également traiter les quatre ports comme un seul canal de port ou trunk LACP et doivent transmettre 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
```

Installer StorageGRID sur Ubuntu ou Debian

Démarrage rapide pour l'installation de StorageGRID sur Ubuntu ou Debian

Suivez ces étapes de haut niveau pour installer un nœud Ubuntu ou Debian StorageGRID .

1

Préparation

- En savoir plus sur "[Architecture et topologie du réseau StorageGRID](#)" .
- Renseignez-vous sur les spécificités de "[Réseau StorageGRID](#)" .
- Rassemblez et préparez les "[Informations et matériel requis](#)" .
- Préparez le nécessaire "[CPU et RAM](#)" .
- Prévoir "[exigences de stockage et de performances](#)" .
- "[Préparer les serveurs Linux](#)" qui hébergera vos nœuds StorageGRID .

2

Déploiement

Déployer des nœuds de grille. Lorsque vous déployez des nœuds de grille, ils sont créés dans le cadre du système StorageGRID et connectés à un ou plusieurs réseaux.

- Pour déployer des nœuds de grille basés sur des logiciels sur les hôtes que vous avez préparés à l'étape 1, utilisez la ligne de commande Linux et ["fichiers de configuration des nœuds"](#) .
- Pour déployer les nœuds d'appliance StorageGRID , suivez les instructions ["Démarrage rapide pour l'installation du matériel"](#) .

3

Configuration

Lorsque tous les nœuds ont été déployés, utilisez le gestionnaire de grille pour ["configurer la grille et terminer l'installation"](#) .

Automatiser l'installation

Pour gagner du temps et assurer la cohérence, vous pouvez automatiser l'installation du service hôte StorageGRID et la configuration des nœuds de grille.

- Utilisez un framework d'orchestration standard tel qu'Ansible, Puppet ou Chef pour automatiser :
 - Installation d'Ubuntu ou de Debian
 - Configuration du réseau et du stockage
 - Installation du moteur de conteneur et du service hôte StorageGRID
 - Déploiement de nœuds de réseau virtuels

Voir ["Automatiser l'installation et la configuration du service hôte StorageGRID"](#) .

- Après avoir déployé les nœuds de grille, ["automatiser la configuration du système StorageGRID"](#) en utilisant le script de configuration Python fourni dans l'archive d'installation.
- ["Automatiser l'installation et la configuration des nœuds de réseau d'appareils"](#)
- Si vous êtes un développeur avancé de déploiements StorageGRID , automatisez l'installation des nœuds de grille en utilisant le ["installation de l'API REST"](#) .

Planifier et préparer l'installation sur Ubuntu ou Debian

Informations et matériel requis

Avant d'installer StorageGRID, rassemblez et préparez les informations et le matériel requis.

Informations requises

Plan de réseau

Quels réseaux comptez-vous connecter à chaque nœud StorageGRID . StorageGRID prend en charge plusieurs réseaux pour la séparation du trafic, la sécurité et la commodité administrative.

Voir le StorageGRID ["Directives de mise en réseau"](#) .

Informations sur le réseau

Adresses IP à attribuer à chaque nœud de grille et les adresses IP des serveurs DNS et NTP.

Serveurs pour les nœuds de grille

Identifiez un ensemble de serveurs (physiques, virtuels ou les deux) qui, dans leur ensemble, fournissent suffisamment de ressources pour prendre en charge le nombre et le type de nœuds StorageGRID que vous prévoyez de déployer.



Si votre installation StorageGRID n'utilise pas de nœuds de stockage d'appliance StorageGRID (matériel), vous devez utiliser un stockage RAID matériel avec cache d'écriture alimenté par batterie (BBWC). StorageGRID ne prend pas en charge l'utilisation de réseaux de stockage virtuels (vSAN), de RAID logiciel ou d'aucune protection RAID.

Migration de nœuds (si nécessaire)

Comprendre le ["exigences pour la migration des nœuds"](#) , si vous souhaitez effectuer une maintenance planifiée sur des hôtes physiques sans aucune interruption de service.

Informations connexes

["Outil de matrice d'interopérabilité NetApp"](#)

Matériel requis

Licence NetApp StorageGRID

Vous devez disposer d'une licence NetApp valide et signée numériquement.



Une licence non-production, qui peut être utilisée pour les grilles de test et de preuve de concept, est incluse dans l'archive d'installation de StorageGRID .

Archive d'installation de StorageGRID

["Téléchargez l'archive d'installation de StorageGRID et extrayez les fichiers"](#) .

Ordinateur portable de service

Le système StorageGRID est installé via un ordinateur portable de service.

L'ordinateur portable de service doit avoir :

- Port réseau
- Client SSH (par exemple, PuTTY)
- ["Navigateur Web pris en charge"](#)

Documentation de StorageGRID

- ["Notes de version"](#)
- ["Instructions pour l'administration de StorageGRID"](#)

Téléchargez et extrayez les fichiers d'installation de StorageGRID

Vous devez télécharger l'archive d'installation de StorageGRID et extraire les fichiers requis. En option, vous pouvez vérifier manuellement les fichiers dans le package d'installation.

Étapes

1. Aller à la ["Page de téléchargement NetApp pour StorageGRID"](#) .

2. Sélectionnez le bouton pour télécharger la dernière version ou sélectionnez une autre version dans le menu déroulant et sélectionnez **Aller**.
3. Sign in avec le nom d'utilisateur et le mot de passe de votre compte NetApp .
4. Si une mention d'avertissement/à lire absolument apparaît, lisez-la et cochez la case.



Vous devez appliquer tous les correctifs requis après avoir installé la version StorageGRID . Pour plus d'informations, consultez le "[procédure de correctif dans les instructions de récupération et de maintenance](#)"

5. Lisez le contrat de licence utilisateur final, cochez la case, puis sélectionnez **Accepter et continuer**.
6. Dans la colonne **Installer StorageGRID**, sélectionnez l'archive d'installation .tgz ou .zip pour Ubuntu ou Debian.



Sélectionnez le .zip fichier si vous exécutez Windows sur l'ordinateur portable de service.

7. Enregistrez l'archive d'installation.
8. Si vous devez vérifier l'archive d'installation :
 - a. Téléchargez le package de vérification de signature de code StorageGRID . Le nom de fichier de ce package utilise le format `StorageGRID_<version-number>_Code_Signature_Verification_Package.tar.gz` , où <version-number> est la version du logiciel StorageGRID .
 - b. Suivez les étapes pour "[vérifier manuellement les fichiers d'installation](#)" .
9. Extraire les fichiers de l'archive d'installation.
10. Choisissez les fichiers dont vous avez besoin.

Les fichiers dont vous avez besoin dépendent de la topologie de grille prévue et de la manière dont vous allez déployer votre système StorageGRID .



Les chemins répertoriés dans le tableau sont relatifs au répertoire de niveau supérieur installé par l'archive d'installation extraite.

Chemin et nom du fichier	Description
	Un fichier texte qui décrit tous les fichiers contenus dans le fichier de téléchargement StorageGRID .
	Un fichier de licence NetApp non destiné à la production que vous pouvez utiliser pour les tests et les déploiements de preuve de concept.
	Paquet DEB pour l'installation des images de nœuds StorageGRID sur les hôtes Ubuntu ou Debian.
	Somme de contrôle MD5 pour le fichier <code>/debs/storagegrid-webscale-images-version-SHA.deb</code> .

Chemin et nom du fichier	Description
	Paquet DEB pour l'installation du service hôte StorageGRID sur les hôtes Ubuntu ou Debian.
Outil de script de déploiement	Description
	Un script Python utilisé pour automatiser la configuration d'un système StorageGRID .
	Un script Python utilisé pour automatiser la configuration des appliances StorageGRID .
	Un 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 l'intégration de Ping Federate.
	Un exemple de fichier de configuration à utiliser avec le <code>configure-storagegrid.py</code> scénario.
	Un fichier de configuration vierge à utiliser avec le <code>configure-storagegrid.py</code> scénario.
	Exemple de rôle Ansible et de playbook pour la configuration des hôtes Ubuntu ou Debian pour le déploiement du conteneur StorageGRID . Vous pouvez personnaliser le rôle ou le manuel selon vos besoins.
	Un exemple de script Python que vous pouvez utiliser pour vous connecter à l'API Grid Management lorsque l'authentification unique (SSO) est activée à l'aide d'Active Directory ou de Ping Federate.
	Un script d'aide appelé par le compagnon <code>storagegrid-ssoauth-azure.py</code> Script Python pour effectuer des interactions SSO avec Azure.

Chemin et nom du fichier	Description
	Schémas d'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 hors production pour les tests de compatibilité de mise à niveau.

Vérifier manuellement les fichiers d'installation (facultatif)

Si nécessaire, vous pouvez vérifier manuellement les fichiers dans l'archive d'installation de StorageGRID .

Avant de commencer

Tu as ["téléchargé le package de vérification"](#) de la ["Page de téléchargement NetApp pour StorageGRID"](#) .

Étapes

1. Extraire les artefacts du package de vérification :

```
tar -xf StorageGRID_11.9.0_Code_Signature_Verification_Package.tar.gz
```

2. Assurez-vous que ces artefacts ont été extraits :

- Certificat de feuille : Leaf-Cert.pem
- Chaîne de certificats : CA-Int-Cert.pem
- Chaîne de réponse d'horodatage : TS-Cert.pem
- Fichier de somme de contrôle : sha256sum
- Signature de somme de contrôle : sha256sum.sig
- Fichier de réponse d'horodatage : sha256sum.sig.tsr

3. Utilisez la chaîne pour vérifier que le certificat de feuille est valide.

Exemple: `openssl verify -CAfile CA-Int-Cert.pem Leaf-Cert.pem`

Résultat attendu: Leaf-Cert.pem: OK

4. Si l'étape 2 a échoué en raison d'un certificat feuille expiré, utilisez le tsr fichier à vérifier.

Exemple: `openssl ts -CAfile CA-Int-Cert.pem -untrusted TS-Cert.pem -verify -data sha256sum.sig -in sha256sum.sig.tsr`

Les résultats attendus incluent : Verification: OK

5. Créez un fichier de clé publique à partir du certificat feuille.

Exemple: `openssl x509 -pubkey -noout -in Leaf-Cert.pem > Leaf-Cert.pub`

Sortie attendue : *aucun*

6. Utilisez la clé publique pour vérifier le sha256sum déposer contre sha256sum.sig .

Exemple: `openssl dgst -sha256 -verify Leaf-Cert.pub -signature sha256sum.sig sha256sum`

Résultat attendu: Verified OK

7. Vérifiez le sha256sum contenu du fichier par rapport aux sommes de contrôle nouvellement créées.

Exemple: `sha256sum -c sha256sum`

Résultat attendu: `<filename>: OK`

`<filename>` est le nom du fichier d'archive que vous avez téléchargé.

8. "[Complétez les étapes restantes](#)" pour extraire et choisir les fichiers d'installation appropriés.

Configuration logicielle requise pour Ubuntu et Debian

Vous pouvez utiliser une machine virtuelle pour héberger n'importe quel type de nœud StorageGRID . Vous avez besoin d'une machine virtuelle pour chaque nœud de grille.

Pour installer StorageGRID sur Ubuntu ou Debian, vous devez installer certains packages logiciels tiers. Certaines distributions Linux prises en charge ne contiennent pas ces packages par défaut. Les versions de progiciels sur lesquelles les installations StorageGRID sont testées incluent celles répertoriées sur cette page.

Si vous sélectionnez une distribution Linux et une option d'installation d'exécution de conteneur qui nécessitent l'un de ces packages et qu'ils ne sont pas installés automatiquement par la distribution Linux, installez l'une des versions répertoriées ici si elles sont disponibles auprès de votre fournisseur ou du fournisseur de support de votre distribution Linux. Sinon, utilisez les versions de package par défaut disponibles auprès de votre fournisseur.

Toutes les options d'installation nécessitent Podman ou Docker. N'installez pas les deux packages. Installez uniquement le package requis par votre option d'installation.



La prise en charge de Docker comme moteur de conteneur pour les déploiements uniquement logiciels est obsolète. Docker sera remplacé par un autre moteur de conteneur dans une prochaine version.

Versions Python testées

- 3.5.2-2
- 3.6.8-2
- 3.6.8-38
- 3.6.9-1
- 3.7.3-1
- 3.8.10-0

- 3.9.2-1
- 3.9.10-2
- 3.9.16-1
- 3.10.6-1
- 3.11.2-6

Versions Podman testées

- 3.2.3-0
- 3.4.4+ds1
- 4.1.1-7
- 4.2.0-11
- 4.3.1+ds1-8+b1
- 4.4.1-8
- 4.4.1-12

Versions de Docker testées



La prise en charge de Docker est obsolète et sera supprimée dans une prochaine version.

- Docker-CE 20.10.7
- Docker-CE 20.10.20-3
- Docker-CE 23.0.6-1
- Docker-CE 24.0.2-1
- Docker-CE 24.0.4-1
- Docker-CE 24.0.5-1
- Docker-CE 24.0.7-1
- 1,5-2

Exigences CPU et RAM

Avant d'installer le logiciel StorageGRID , vérifiez et configurez le matériel afin qu'il soit prêt à prendre en charge le système StorageGRID .

Chaque nœud StorageGRID nécessite les ressources minimales suivantes :

- Cœurs de processeur : 8 par nœud
- RAM : dépend de la RAM totale disponible et de la quantité de logiciels non StorageGRID exécutés sur le système
 - Généralement, au moins 24 Go par nœud et 2 à 16 Go de moins que la RAM totale du système
 - Un minimum de 64 Go pour chaque locataire qui aura environ 5 000 buckets

Les ressources de nœuds basées uniquement sur des métadonnées logicielles doivent correspondre aux ressources de nœuds de stockage existantes. Par exemple:

- Si le site StorageGRID existant utilise des appliances SG6000 ou SG6100, les nœuds de métadonnées uniquement basés sur des logiciels doivent répondre aux exigences minimales suivantes :
 - 128 Go de RAM
 - processeur à 8 cœurs
 - SSD de 8 To ou stockage équivalent pour la base de données Cassandra (rangedb/0)
- Si le site StorageGRID existant utilise des nœuds de stockage virtuels avec 24 Go de RAM, un processeur à 8 cœurs et 3 To ou 4 To de stockage de métadonnées, les nœuds de métadonnées uniquement basés sur un logiciel doivent utiliser des ressources similaires (24 Go de RAM, un processeur à 8 cœurs et 4 To de stockage de métadonnées (rangedb/0)).

Lors de l'ajout d'un nouveau site StorageGRID, la capacité totale des métadonnées du nouveau site doit, au minimum, correspondre aux sites StorageGRID existants et les nouvelles ressources du site doivent correspondre aux nœuds de stockage des sites StorageGRID existants.

Assurez-vous 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 RAM physique disponible. Si les hôtes ne sont pas dédiés à l'exécution de StorageGRID (non recommandé), assurez-vous de 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 répondre à votre charge de travail. Par exemple, doubler l'allocation de RAM et de CPU pour les nœuds de stockage virtuels fournirait des ressources similaires à celles fournies pour les nœuds d'appliance StorageGRID. De plus, si la quantité de métadonnées par nœud dépasse 500 Go, envisagez d'augmenter la RAM par nœud à 48 Go ou plus. 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, consultez les instructions de [administrer](#), [surveillance](#), et [mise à niveau](#) StorageGRID.

Si l'hyperthreading est activé sur les hôtes physiques sous-jacents, vous pouvez fournir 8 cœurs virtuels (4 cœurs physiques) par nœud. Si l'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 comme hôtes et que vous contrôlez la taille et le nombre de machines virtuelles, vous devez utiliser une seule machine virtuelle pour chaque nœud StorageGRID et dimensionner la machine virtuelle en conséquence.

Pour les déploiements de production, vous ne devez pas exécuter plusieurs nœuds de stockage sur le même matériel de stockage physique ou hôte virtuel. Chaque nœud de stockage d'un déploiement StorageGRID unique doit se trouver dans son propre domaine de défaillance isolé. Vous pouvez maximiser la durabilité et la disponibilité des données d'objet si vous vous assurez qu'une seule panne matérielle ne peut affecter qu'un seul nœud de stockage.

Voir aussi ["Exigences de stockage et de performances"](#).

Exigences de stockage et de performances

Vous devez comprendre les exigences de stockage pour les nœuds StorageGRID, afin de pouvoir fournir suffisamment d'espace 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 performance (10 K SAS ou SSD) pour les conteneurs de nœuds, qui sera attribué au pilote de stockage Docker lorsque vous installerez et configurerez Docker sur les hôtes qui prendront en charge vos nœuds StorageGRID .
- **Données système** — Stockage de niveau de performance (SAS 10 K ou SSD) pour le stockage persistant par nœud des données système et des journaux de transactions, que les services hôtes StorageGRID consommeront et mapperont dans des nœuds individuels.
- **Données d'objet** — Stockage de niveau performance (10 K SAS ou SSD) et stockage en masse 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 blocs sauvegardés par RAID pour toutes les catégories de stockage. Les disques non redondants, SSD ou JBOD ne sont pas pris en charge. Vous pouvez utiliser un stockage RAID partagé ou local pour n'importe quelle catégorie 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, consultez la section "[Exigences de migration des conteneurs de nœuds](#)".

Exigences de performance

Les performances des volumes utilisés pour le pool de conteneurs, les données système et les métadonnées d'objet ont un impact significatif sur les performances globales du système. Vous devez utiliser un stockage de niveau de performance (SAS 10K ou SSD) pour ces volumes afin de garantir des performances de disque adéquates en termes de latence, d'opérations d'entrée/sortie par seconde (IOPS) et de débit. Vous pouvez utiliser le stockage de niveau de capacité (NL-SAS/SATA) pour le stockage persistant des données d'objet.

Les volumes utilisés pour le pool de conteneurs, les données système et les données d'objet doivent avoir la mise en cache en écriture différée activée. Le cache doit être sur un support protégé ou persistant.

Exigences pour les hôtes qui utilisent le stockage NetApp ONTAP

Si le nœud StorageGRID utilise le stockage attribué à partir d'un système NetApp ONTAP , vérifiez que le volume n'a pas de stratégie de hiérarchisation FabricPool activée. La désactivation de la hiérarchisation FabricPool pour les volumes utilisés avec les nœuds StorageGRID simplifie le dépannage et les opérations de stockage.



N'utilisez jamais FabricPool pour hiérarchiser les données liées à StorageGRID vers StorageGRID lui-même. La hiérarchisation des données StorageGRID vers StorageGRID augmente le dépannage et la complexité opérationnelle.

Nombre d'hôtes requis

Chaque site StorageGRID nécessite un minimum de 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.

D'autres types de nœuds, tels que les nœuds d'administration ou les nœuds de passerelle, peuvent être déployés sur les mêmes hôtes ou sur leurs propres hôtes dédiés selon les besoins.

Nombre de volumes de stockage pour chaque hôte

Le tableau suivant indique le nombre de volumes de stockage (LUN) requis pour chaque hôte et la taille

minimale requise pour chaque LUN, en fonction des nœuds qui seront déployés sur cet hôte.

La taille maximale du LUN testé est de 39 To.



Ces chiffres concernent chaque hôte, et non la grille entière.

Objectif du LUN	Catégorie de stockage	Nombre de LUN	Taille minimale/LUN
Piscine de stockage de moteurs de conteneurs	Piscine à conteneurs	1	Nombre total de nœuds × 100 Go
`/var/local` volume	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 nœud de stockage basé sur un logiciel peut avoir de 1 à 48 volumes de stockage ; au moins 3 volumes de stockage sont recommandés.	12 To (4 To/LUN) Voir Exigences de stockage pour les nœuds de stockage pour plus d'informations.
Nœud de stockage (métadonnées uniquement)	Métadonnées de l'objet	1	4 To Voir Exigences de stockage pour les nœuds de stockage pour plus d'informations. Remarque : un seul rangedb est requis pour les nœuds de stockage contenant uniquement des métadonnées.
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



En fonction du niveau d'audit configuré, de la taille des entrées utilisateur telles que le nom de clé d'objet S3 et de la quantité de données de journal d'audit que vous devez conserver, vous devrez peut-être augmenter la taille du LUN du journal d'audit sur chaque nœud d'administration. En général, une grille génère environ 1 Ko de données d'audit par opération S3, ce qui signifie qu'un LUN de 200 Go prendrait 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 minimum requis pour chaque type de nœud. Vous pouvez utiliser ce tableau pour déterminer la quantité minimale de stockage que vous devez fournir à l'hôte dans chaque catégorie de stockage, en fonction des nœuds qui seront déployés sur cet hôte.



Les instantanés de disque ne peuvent pas être utilisés pour restaurer les nœuds de grille. Au lieu de cela, reportez-vous à la "[récupération des nœuds de réseau](#)" procédures pour chaque type de nœud.

Type de nœud	Piscine à 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)	<i>non applicable</i>
Nœud de passerelle	100 Go	90 Go	<i>non applicable</i>

Exemple : Calcul des besoins de stockage d'un hôte

Supposons que vous envisagiez de déployer trois nœuds sur le 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 niveau performance pour les conteneurs de nœuds, de 670 Go de stockage de niveau performance pour les données système et les journaux de transactions, et de 12 To de stockage de niveau capacité pour les données d'objet.

Type de nœud	Objectif du LUN	Nombre de LUN	Taille du LUN
Nœud de stockage	Pool de stockage Docker	1	300 Go (100 Go/nœud)
Nœud de stockage	`/var/local` volume	1	90 Go
Nœud de stockage	Données d'objet	3	12 To (4 To/LUN)
Nœud d'administration	`/var/local` volume	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` volume	1	90 Go

Type de nœud	Objectif du LUN	Nombre de LUN	Taille du LUN
Total		9	Pool de conteneurs : 300 Go Données système : 670 Go Données de l'objet : 12 000 Go

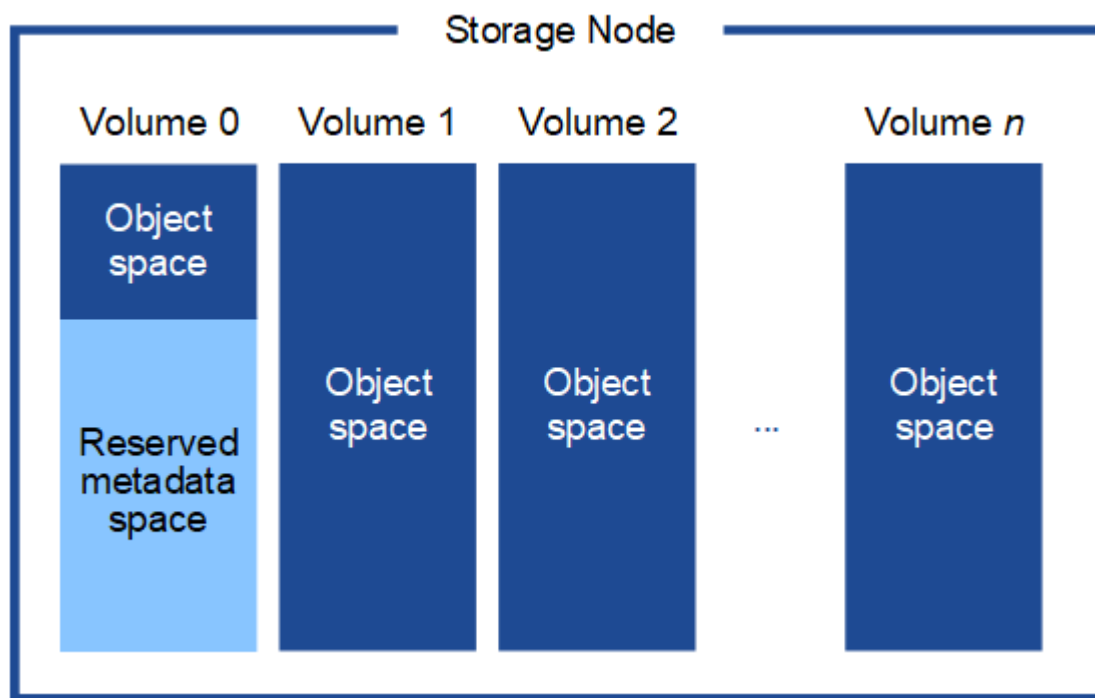
Exigences de stockage pour les nœuds de stockage

Un nœud de stockage basé sur un logiciel peut avoir de 1 à 48 volumes de stockage ; 3 volumes de stockage ou plus sont recommandés. Chaque volume de stockage doit être de 4 To ou plus.



Un nœud de stockage d'appareil peut également avoir jusqu'à 48 volumes de stockage.

Comme indiqué dans la figure, StorageGRID réserve de l'espace pour les métadonnées d'objet sur le volume de stockage 0 de chaque nœud de stockage. Tout espace restant sur le volume de stockage 0 et tous les autres volumes de stockage du nœud de stockage sont utilisés exclusivement pour les données d'objet.



Pour assurer la redondance et protéger les métadonnées des objets contre la perte, StorageGRID stocke trois copies des métadonnées de tous les objets du système sur chaque site. Les trois copies des métadonnées de l'objet sont réparties uniformément sur tous les nœuds de stockage de chaque site.

Lors de l'installation d'une grille avec des nœuds de stockage contenant uniquement des métadonnées, la grille doit également contenir un nombre minimum de nœuds pour le stockage d'objets. Voir ["Types de nœuds de stockage"](#) pour plus d'informations sur les nœuds de stockage contenant uniquement des métadonnées.

- Pour une grille à site unique, au moins deux nœuds de stockage sont configurés pour les objets et les métadonnées.

- Pour une grille multisite, au moins un nœud de stockage par site est configuré pour les objets et les métadonnées.

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 partie de ce nœud de toutes les métadonnées d'objet.

- Au minimum, vous devez attribuer au moins 4 To au volume 0.



Si vous utilisez 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 dans l'état de stockage en lecture seule au démarrage et stocker uniquement 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 sont réservés aux métadonnées.

- Les ressources de nœuds basées uniquement sur des métadonnées logicielles doivent correspondre aux ressources de nœuds de stockage existantes. Par exemple:
 - Si le site StorageGRID existant utilise des appliances SG6000 ou SG6100, les nœuds de métadonnées uniquement basés sur des logiciels doivent répondre aux exigences minimales suivantes :
 - 128 Go de RAM
 - processeur à 8 cœurs
 - SSD de 8 To ou stockage équivalent pour la base de données Cassandra (rangedb/0)
 - Si le site StorageGRID existant utilise des nœuds de stockage virtuels avec 24 Go de RAM, un processeur à 8 cœurs et 3 To ou 4 To de stockage de métadonnées, les nœuds de métadonnées uniquement basés sur un logiciel doivent utiliser des ressources similaires (24 Go de RAM, un processeur à 8 cœurs et 4 To de stockage de métadonnées (rangedb/0)).

Lors de l'ajout d'un nouveau site StorageGRID , la capacité totale des métadonnées du nouveau site doit, au minimum, correspondre aux sites StorageGRID existants et les nouvelles ressources du site doivent correspondre aux nœuds de stockage des sites StorageGRID existants.

- 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.
- Lors de la configuration de 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 de détails, rendez-vous sur ["Gérer le stockage des métadonnées des objets"](#) .

Exigences de migration des conteneurs de nœuds

La fonctionnalité de migration de nœud vous permet de déplacer manuellement un nœud d'un hôte à un autre. En règle générale, les deux hôtes se trouvent dans le même centre de données physique.

La migration de nœuds vous permet d'effectuer la maintenance de l'hôte physique sans perturber les opérations du réseau. Vous déplacez tous les nœuds StorageGRID , un par un, vers un autre hôte avant de

mettre l'hôte physique hors ligne. La migration des nœuds ne nécessite qu'un court temps d'arrêt pour chaque nœud et ne devrait pas affecter le fonctionnement ou la disponibilité des services de grille.

Si vous souhaitez utiliser la fonctionnalité de migration de nœuds StorageGRID , votre déploiement doit répondre à des exigences supplémentaires :

- Noms d'interface réseau cohérents entre les hôtes d'un même centre de données physique
- Stockage partagé pour les volumes de métadonnées et de référentiel d'objets StorageGRID accessible par tous les hôtes dans un seul centre de données physique. Par exemple, vous pouvez utiliser des baies de stockage NetApp E-Series.

Si vous utilisez des hôtes virtuels et que la couche d'hyperviseur sous-jacente prend en charge la migration de machines virtuelles, vous souhaitez peut-être utiliser cette fonctionnalité à la place de la fonctionnalité de migration de nœuds dans StorageGRID. Dans ce cas, vous pouvez ignorer ces exigences supplémentaires.

Avant d'effectuer la migration ou la maintenance de l'hyperviseur, arrêtez les nœuds correctement. Voir les instructions pour ["fermeture d'un nœud de grille"](#) .

VMware Live Migration n'est pas pris en charge

Lors de l'exécution d'une installation bare-metal sur des machines virtuelles VMware, OpenStack Live Migration et VMware Live vMotion provoquent un saut de l'heure de l'horloge de la machine virtuelle et ne sont pas pris en charge pour les nœuds de grille de tout type. Bien que rares, des heures d'horloge incorrectes peuvent entraîner une perte de données ou des mises à jour de configuration.

La migration à froid est prise en charge. Lors d'une migration à froid, vous arrêtez les nœuds StorageGRID avant de les migrer entre les hôtes. Voir les instructions pour ["fermeture d'un nœud de grille"](#) .

Noms d'interface réseau cohérents

Pour déplacer un nœud d'un hôte à un autre, le service hôte StorageGRID doit avoir la certitude 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 NodeA exécuté sur Host1 a été configuré avec les mappages d'interface suivants :

eth0 → **bond0.1001**

eth1 → **bond0.1002**

eth2 → **bond0.1003**

Le côté gauche des flèches correspond aux interfaces traditionnelles vues depuis un conteneur StorageGRID (c'est-à-dire respectivement les interfaces Grid, Admin et Client Network). 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.

Maintenant, supposons que vous souhaitiez migrer NodeA vers Host2. Si Host2 possède également des interfaces nommées bond0.1001, bond0.1002 et bond0.1003, le système autorisera le déplacement, en supposant que les interfaces portant le même nom fourniront la même connectivité sur Host2 que sur Host1. Si Host2 ne possède pas d'interfaces portant les mêmes noms, le déplacement ne sera pas autorisé.

Il existe de nombreuses façons d'obtenir une dénomination d'interface réseau cohérente sur plusieurs hôtes ; voir "[Configurer le réseau hôte](#)" pour quelques exemples.

Stockage partagé

Pour réaliser des migrations de nœuds rapides et à faible surcharge, la fonctionnalité de migration de nœuds StorageGRID ne déplace pas physiquement les données des nœuds. Au lieu de cela, la migration des nœuds est effectuée sous la forme d'une paire d'opérations d'exportation et d'importation, comme suit :

Étapes

1. Pendant l'opération « exportation de nœud », une petite quantité de données d'état persistantes 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 nœuds sur HostA est désinstancié.
2. Pendant l'opération « importation de nœud », le conteneur de nœud sur HostB qui utilise la même interface réseau et les mêmes mappages de stockage de blocs qui étaient en vigueur sur HostA est instancié. Ensuite, les données d'état persistantes mises en cache sont insérées dans la nouvelle instance.

Compte tenu de ce mode de fonctionnement, toutes les données système et tous les volumes de stockage d'objets du nœud doivent être accessibles à la fois depuis HostA et HostB pour que la migration soit autorisée et fonctionne. De plus, ils doivent avoir été mappés dans le nœud à l'aide de noms qui font 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 le multipathing DM est utilisé sur les hôtes et le champ d'alias a été utilisé dans `/etc/multipath.conf` pour fournir des noms de périphériques de bloc cohérents et conviviaux disponibles sur tous les hôtes.

`/var/local` ➔ `/dev/mapper/sgws-sn1-var-local`

`rangedb0` ➔ `/dev/mapper/sgws-sn1-rangedb0`

`rangedb1` ➔ `/dev/mapper/sgws-sn1-rangedb1`

`rangedb2` ➔ `/dev/mapper/sgws-sn1-rangedb2`

`rangedb3` ➔ `/dev/mapper/sgws-sn1-rangedb3`

Préparez les hôtes (Ubuntu ou Debian)

Comment les paramètres à l'échelle de l'hôte changent pendant l'installation

Sur les systèmes bare metal, StorageGRID apporte quelques modifications à l'échelle 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
```

Installer Linux

Vous devez installer StorageGRID sur tous les hôtes de grille Ubuntu ou Debian. Pour obtenir la liste des versions prises en charge, utilisez l'outil de matrice d'interopérabilité NetApp .

Avant de commencer

Assurez-vous que votre système d'exploitation répond aux exigences minimales de version du noyau de StorageGRID, comme indiqué ci-dessous. Utilisez la commande `uname -r` pour obtenir la version du noyau de votre système d'exploitation ou consultez le fournisseur de votre système d'exploitation.

Remarque : la prise en charge des versions Ubuntu 18.04 et 20.04 est obsolète et sera supprimée dans une prochaine version.

Version d'Ubuntu	Version minimale du noyau	Nom du paquet du noyau
18.04.6 (obsolète)	5.4.0-150-générique	linux-image-5.4.0-150-generic/bionic-updates,bionic-security,maintenant 5.4.0-150.167~18.04.1

Version d'Ubuntu	Version minimale du noyau	Nom du paquet du noyau
20.04.5 (obsolète)	5.4.0-131-générique	linux-image-5.4.0-131-generic/focal-updates, maintenant 5.4.0-131.147
22.04.1	5.15.0-47-générique	linux-image-5.15.0-47-generic/jammy-updates,jammy-security,maintenant 5.15.0-47.51
24,04	6.8.0-31-générique	linux-image-6.8.0-31-generic/noble, maintenant 6.8.0-31.31

Remarque : la prise en charge de la version 11 de Debian est obsolète et sera supprimée dans une prochaine version.

Version Debian	Version minimale du noyau	Nom du paquet du noyau
11 (obsolète)	5.10.0-18-amd64	linux-image-5.10.0-18-amd64/stable, maintenant 5.10.150-1
12	6.1.0-9-amd64	linux-image-6.1.0-9-amd64/stable, maintenant 6.1.27-1

Étapes

1. Installez Linux sur tous les hôtes de grille physiques ou virtuels conformément aux instructions du distributeur ou à votre procédure standard.



N'installez aucun environnement de bureau graphique. Lors de l'installation d'Ubuntu, vous devez sélectionner les **utilitaires système standard**. Il est recommandé de sélectionner **Serveur OpenSSH** 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 packages Ubuntu ou Debian.
3. Si l'échange est activé :
 - a. Exécutez la commande suivante : `$ sudo swapoff --all`
 - b. Supprimer toutes les entrées d'échange de `/etc/fstab` pour conserver les paramètres.



Ne pas désactiver complètement l'échange peut réduire considérablement les performances.

Comprendre l'installation du profil AppArmor

Si vous travaillez dans un environnement Ubuntu auto-déployé et utilisez le système de contrôle d'accès obligatoire AppArmor, les profils AppArmor associés aux packages que vous installez sur le système de base peuvent être bloqués par les packages 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 packages de base DHCP, MySQL, NTP et tcdump sont en conflit avec AppArmor, et d'autres packages de base peuvent également être en conflit.

Vous avez deux choix pour gérer les profils AppArmor :

- Désactivez les profils individuels pour les packages installés sur le système de base qui chevauchent 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.

Utilisez 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 complètement AppArmor. Pour Ubuntu 9.10 ou version ultérieure, suivez les instructions de la communauté en ligne Ubuntu : ["Désactiver AppArmor"](#). La désactivation complète d'AppArmor peut ne pas être possible sur les versions plus récentes d'Ubuntu.

Une fois AppArmor désactivé, aucune entrée indiquant qu'AppArmor est activé n'apparaîtra dans les fichiers journaux StorageGRID.

Configurer le réseau hôte (Ubuntu ou Debian)

Une fois l'installation de Linux terminée sur vos hôtes, vous devrez peut-être effectuer une configuration supplémentaire pour préparer un ensemble d'interfaces réseau sur chaque hôte adaptées au mappage dans les nœuds StorageGRID que vous déploierez ultérieurement.

Avant de commencer

- Vous avez examiné le ["Directives de mise en réseau StorageGRID"](#).
- Vous avez examiné les informations sur ["exigences de migration des conteneurs de nœuds"](#).
- Si vous utilisez des hôtes virtuels, vous avez lu le [considérations et recommandations pour le clonage d'adresses MAC](#) avant de configurer le réseau hôte.



Si vous utilisez des machines virtuelles comme hôtes, vous devez sélectionner VMXNET 3 comme adaptateur réseau virtuel. L'adaptateur réseau VMware E1000 a provoqué des problèmes de connectivité avec les conteneurs StorageGRID déployés sur certaines distributions de Linux.

À propos de cette tâche

Les nœuds de grille doivent pouvoir accéder au réseau de grille et, éventuellement, aux réseaux

d'administration et de client. Vous fournissez cet accès en créant des mappages qui associent l'interface physique de l'hôte aux interfaces virtuelles de chaque nœud de grille. Lors de la création d'interfaces d'hôte, utilisez des noms conviviaux pour faciliter le déploiement sur tous les hôtes et pour permettre la migration.

La même interface peut être partagée entre l'hôte et un ou plusieurs nœuds. Par exemple, vous pouvez utiliser la même interface pour l'accès à l'hôte et l'accès au réseau d'administration du nœud, afin de faciliter la maintenance de l'hôte et du nœud. Bien que la même interface puisse être partagée entre l'hôte et les nœuds individuels, tous 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 pour tous les nœuds StorageGRID sur l'hôte ; vous pouvez utiliser une interface réseau hôte différente pour chaque nœud ; ou vous pouvez faire quelque chose entre les deux. Cependant, vous ne fournirez généralement pas la même interface réseau hôte que les interfaces réseau Grid et Admin pour un seul nœud, ou comme interface réseau Grid pour un nœud et comme interface réseau client pour un autre.

Vous pouvez réaliser 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 à 1. Si vous déployez plusieurs nœuds sur des hôtes bare metal pour une utilisation en production, vous pouvez tirer parti de la prise en charge de la pile réseau Linux pour VLAN et LACP pour la tolérance aux pannes et le partage de bande passante. Les sections suivantes fournissent 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 périphériques de liaison ou de pont directement comme interface réseau du conteneur. Cela pourrait empêcher le démarrage du 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 du conteneur. Utilisez plutôt un périphérique non lié, tel qu'un VLAN ou une paire Ethernet virtuelle (veth). Spécifiez ce périphérique comme interface réseau dans le fichier de configuration du nœud.

Considérations et recommandations pour le clonage d'adresses MAC

Le clonage d'adresse MAC amène le conteneur à utiliser l'adresse MAC de l'hôte, et l'hôte à utiliser l'adresse MAC d'une adresse que vous spécifiez ou d'une adresse générée aléatoirement. Vous devez utiliser le clonage d'adresse MAC pour éviter l'utilisation de configurations réseau en mode promiscuité.

Activation du clonage MAC

Dans certains environnements, la sécurité peut être améliorée grâce au clonage d'adresse MAC, car cela vous permet d'utiliser une carte réseau virtuelle dédiée pour le réseau d'administration, le réseau de grille et le réseau client. Le fait que le conteneur utilise l'adresse MAC de la carte réseau dédiée sur l'hôte vous permet d'éviter d'utiliser des configurations réseau en mode promiscuité.



Le clonage d'adresse MAC est destiné à être utilisé avec des installations de serveur virtuel et peut ne pas fonctionner correctement avec toutes les configurations d'appareils physiques.



Si un nœud ne parvient pas à démarrer en raison d'une interface ciblée de clonage MAC occupée, vous devrez peut-être définir le lien sur « down » avant de démarrer le nœud. De plus, il est possible que l'environnement virtuel empêche 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 à démarrer en raison d'une interface occupée, définir le lien sur « down » avant de démarrer le nœud peut résoudre le problème.

Le clonage d'adresse MAC est désactivé par défaut et doit être défini par les clés de configuration du nœud. Vous devez l'activer lorsque vous installez 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

La définition de la clé sur « true » oblige le conteneur à utiliser l'adresse MAC de la carte réseau de l'hôte. De plus, l'hôte utilisera ensuite l'adresse MAC du réseau de conteneurs spécifié. Par défaut, l'adresse du conteneur est une adresse générée aléatoirement, mais si vous en avez défini une à l'aide de l' `_NETWORK_MAC` clé de configuration du 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 promiscuité sur l'hyperviseur peut entraîner l'arrêt du fonctionnement du réseau hôte Linux utilisant l'interface de l'hôte.

Cas d'utilisation du clonage MAC

Il y a deux cas d'utilisation à prendre en compte avec le clonage MAC :

- Clonage MAC non activé : lorsque le `_CLONE_MAC` Si la clé dans le fichier de configuration du nœud n'est pas définie ou définie sur « false », l'hôte utilisera le MAC de la carte réseau de l'hôte et le conteneur aura un MAC généré par StorageGRID, sauf si un MAC est spécifié dans le `_NETWORK_MAC` clé. Si une adresse est définie dans le `_NETWORK_MAC` clé, le conteneur aura l'adresse spécifiée dans le `_NETWORK_MAC` clé. Cette configuration de clés nécessite l'utilisation du mode promiscuité.
- Clonage MAC activé : lorsque le `_CLONE_MAC` dans le 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, sauf si un MAC est 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 touches, vous ne devez pas utiliser le mode promiscuité.



Si vous ne souhaitez pas utiliser le clonage d'adresse MAC et préférez autoriser toutes les interfaces à recevoir et à transmettre des données pour des 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 **Accepter** pour le mode promiscuité, les modifications d'adresse MAC et les transmissions falsifiées. Les valeurs définies sur le commutateur virtuel peuvent être remplacées par les valeurs au niveau du groupe de ports. Assurez-vous donc que les paramètres sont les mêmes aux deux endroits.

Pour activer le clonage MAC, consultez le ["instructions pour créer des fichiers de configuration de nœud"](#) .

Exemple de clonage MAC

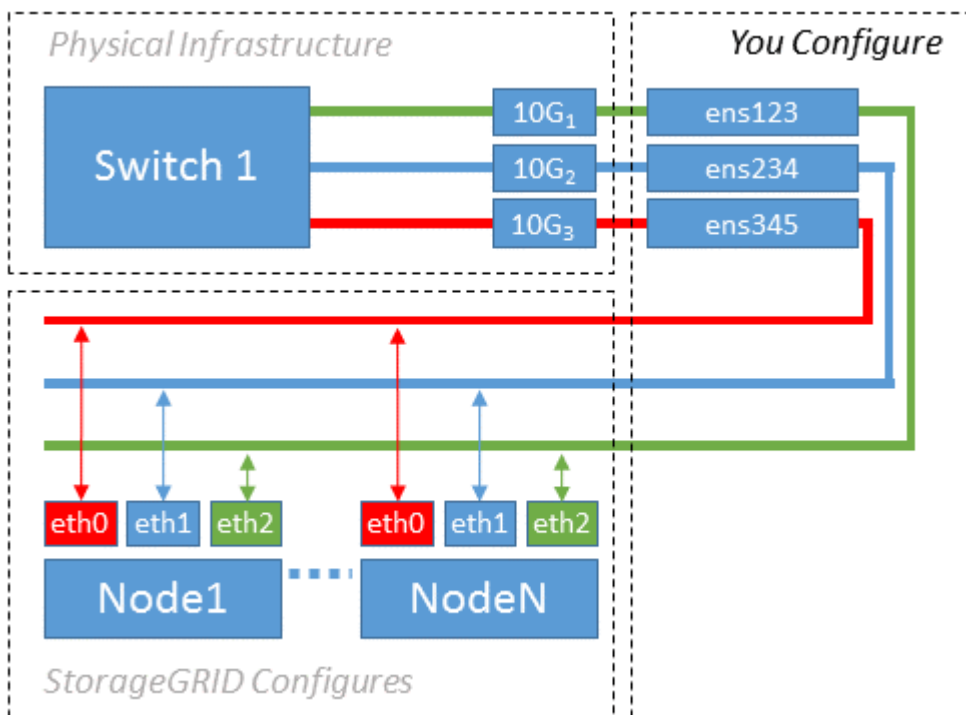
Exemple de clonage MAC activé avec un hôte ayant l'adresse MAC 11:22:33:44:55:66 pour l'interface ens256 et les clés suivantes dans le fichier de configuration du nœud :

- ADMIN_NETWORK_TARGET = ens256
- ADMIN_NETWORK_MAC = b2:9c:02:c2:27:10
- ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC = true

Résultat : l'adresse MAC de l'hôte pour ens256 est b2:9c:02:c2:27:10 et l'adresse MAC du réseau administrateur est 11:22:33:44:55:66

Exemple 1 : mappage 1 à 1 vers 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 ensXYZ lors de l'installation ou du démarrage, ou lorsque les interfaces sont ajoutées à chaud. Aucune configuration n'est requise, si ce n'est de s'assurer que les interfaces sont configurées pour s'afficher automatiquement après le démarrage. Vous devez déterminer quel ensXYZ correspond à quel réseau StorageGRID (Grid, Admin ou Client) afin de pouvoir fournir les mappages corrects plus tard dans le processus de configuration.

Notez que la figure montre plusieurs nœuds StorageGRID ; cependant, vous utiliseriez normalement cette configuration pour les machines virtuelles à nœud unique.

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 transportant des VLAN

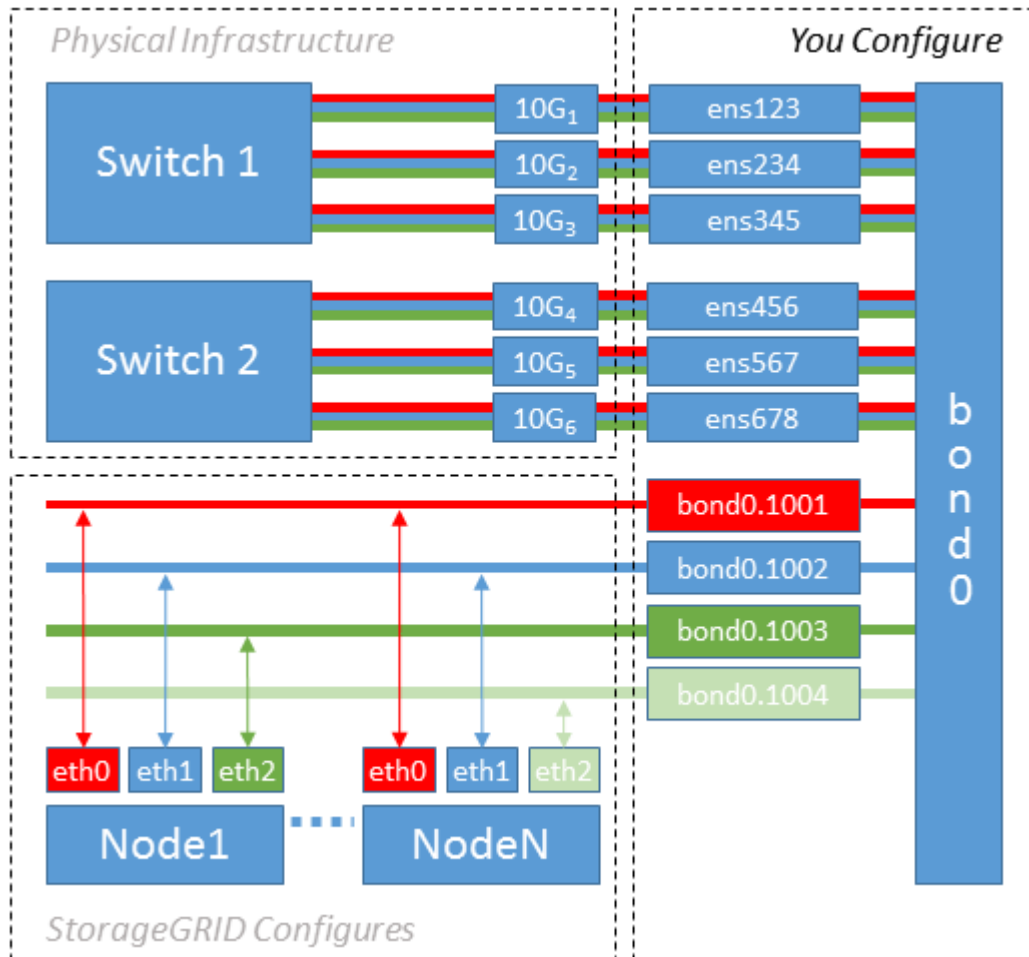
L'exemple 2 suppose que vous êtes familiarisé avec la liaison d'interfaces réseau et avec la création d'interfaces VLAN sur la distribution Linux que vous utilisez.

À propos de cette tâche

L'exemple 2 décrit un schéma générique, flexible et basé sur le VLAN qui facilite le partage de toute la bande passante réseau disponible sur tous les nœuds d'un seul hôte. Cet exemple est particulièrement applicable aux hôtes bare metal.

Pour comprendre cet exemple, supposons que vous disposez de 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 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 dans l'hôte (affiché comme bond0.1004 dans l'illustration).



Étapes

1. Regroupez toutes les interfaces réseau physiques qui seront utilisées pour la connectivité réseau StorageGRID dans 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, en utilisant la convention de dénomination d'interface VLAN standard `physdev-name.VLAN ID`.

Notez que les étapes 1 et 2 nécessitent une configuration appropriée sur les commutateurs de périphérie terminant les autres extrémités des liaisons réseau. Les ports du commutateur périphérique doivent également être regroupés dans un canal de port LACP, configurés en tant que jonction et autorisés à transmettre tous les VLAN requis.

Des exemples de fichiers de configuration d'interface pour ce schéma de configuration réseau par hôte sont fournis.

Informations connexes

["Exemple /etc/network/interfaces"](#)

Configurer le stockage hôte

Vous devez allouer des volumes de stockage en blocs à chaque hôte.

Avant de commencer

Vous avez examiné les rubriques suivantes, qui fournissent les informations dont vous avez besoin pour accomplir cette tâche :

- ["Exigences de stockage et de performances"](#)
- ["Exigences de migration des conteneurs de nœuds"](#)

À propos de cette tâche

Lors de l'allocation de volumes de stockage en blocs (LUN) aux hôtes, utilisez les tableaux 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 qui seront déployés sur cet hôte)
- Catégorie de stockage pour chaque volume (c'est-à-dire, données système ou données d'objet)
- Taille de chaque volume

Vous utiliserez ces informations ainsi que le nom persistant attribué par Linux à chaque volume physique lorsque vous déploierez des nœuds StorageGRID sur l'hôte.



Vous n'avez pas besoin de partitionner, de formater ou de monter l'un de ces volumes ; vous devez simplement vous assurer qu'ils sont visibles pour les hôtes.



Un seul LUN de données d'objet est requis pour les nœuds de stockage contenant uniquement des métadonnées.

Évitez d'utiliser des fichiers d'appareil spéciaux « bruts » (`/dev/sdb`, par exemple) lorsque vous composez votre liste de noms de volumes. Ces fichiers peuvent changer lors des redémarrages de l'hôte, ce qui aura un impact sur le bon fonctionnement du système. Si vous utilisez des LUN iSCSI et un mappeur de périphériques multi-chemins, pensez à utiliser des alias multi-chemins dans le `/dev/mapper` répertoire, en particulier si votre topologie SAN inclut des chemins réseau redondants vers le stockage partagé. Alternativement, vous pouvez utiliser les liens logiciels créés par le système sous `/dev/disk/by-path/` pour vos noms d'appareils 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 seront différents pour chaque installation.

Attribuez des noms conviviaux à chacun de ces volumes de stockage en blocs pour simplifier l'installation initiale de StorageGRID et les procédures de maintenance futures. Si vous utilisez le pilote multi-chemins du mappeur de périphériques pour un accès redondant aux volumes de stockage partagés, vous pouvez utiliser le `alias` champ dans votre `/etc/multipath.conf` déposer.

Par exemple:

```

multipaths {
    multipath {
        wwid 3600a09800059d6df00005df2573c2c30
        alias docker-storage-volume-hostA
    }
    multipath {
        wwid 3600a09800059d6df00005df3573c2c30
        alias sgws-adml-var-local
    }
    multipath {
        wwid 3600a09800059d6df00005df4573c2c30
        alias sgws-adml-audit-logs
    }
    multipath {
        wwid 3600a09800059d6df00005df5573c2c30
        alias sgws-adml-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
    }
    ...
}

```

L'utilisation du champ `alias` de cette manière fait apparaître les alias comme des périphériques de bloc dans le `/dev/mapper` répertoire sur l'hôte, vous permettant de spécifier un nom convivial et facilement validé chaque fois qu'une opération de configuration ou de maintenance nécessite 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 utilisez Device Mapper Multipathing, vous pouvez créer et installer un stockage partagé commun. `/etc/multipath.conf` sur tous les hôtes colocalisés. Assurez-vous simplement d'utiliser un volume de stockage Docker 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 Docker rendront cela facile à mémoriser et sont recommandées.



La prise en charge de Docker comme moteur de conteneur pour les déploiements uniquement logiciels est obsolète. Docker sera remplacé par un autre moteur de conteneur dans une prochaine version.

Informations connexes

- ["Exigences de stockage et de performances"](#)
- ["Exigences de migration des conteneurs de nœuds"](#)

Configurer le volume de stockage du moteur de conteneur

Avant d'installer le moteur de conteneur (Docker ou Podman), vous devrez peut-être formater le volume de stockage et le monter.



La prise en charge de Docker comme moteur de conteneur pour les déploiements uniquement logiciels est obsolète. Docker sera remplacé par un autre moteur de conteneur dans une prochaine version.

À propos de cette tâche

Vous pouvez ignorer ces étapes si vous prévoyez d'utiliser le stockage local pour le volume de stockage Docker et que vous disposez de suffisamment d'espace disponible 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` à `/etc/fstab`.

Cette étape garantit que le volume de stockage sera remonté automatiquement après le redémarrage de l'hôte.

Installer Docker

Le système StorageGRID fonctionne sous Linux en tant que collection de conteneurs Docker. Avant de pouvoir installer StorageGRID, vous devez installer Docker.



La prise en charge de Docker comme moteur de conteneur pour les déploiements uniquement logiciels est obsolète. Docker sera remplacé par un autre moteur de conteneur dans une prochaine version.

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 à partir du 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. Confirmez que vous avez installé la version attendue de Docker en saisissant ce qui suit :

```
sudo docker version
```

Les versions Client et Serveur doivent être 1.11.0 ou ultérieures.

Informations connexes

["Configurer le stockage hôte"](#)

Installer les services hôtes StorageGRID

Vous utilisez le package DEB StorageGRID pour installer les services hôtes StorageGRID .

À propos de cette tâche

Ces instructions décrivent comment installer les services hôtes à partir des packages DEB. Comme alternative, vous pouvez 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 DEB StorageGRID sur chacun de vos hôtes ou rendez-les disponibles sur un stockage partagé.

Par exemple, placez-les dans le `/tmp` répertoire, vous pouvez donc utiliser l'exemple de commande 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` paquet d'abord, et le `service` paquet deuxième. 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 packages StorageGRID puissent être installés. Le `sudo dpkg --install /tmp/storagegrid-webscale-images-version-SHA.deb` la commande échouera jusqu'à ce que vous l'ayez fait.

Automatiser l'installation (Ubuntu ou Debian)

Vous pouvez automatiser l'installation du service hôte StorageGRID et la configuration des nœuds de grille.

À propos de cette tâche

L'automatisation du déploiement peut être utile dans l'un des cas suivants :

- Vous utilisez déjà un framework d'orchestration standard, tel qu'Ansible, Puppet ou Chef, pour déployer et configurer des hôtes physiques ou virtuels.
- Vous avez l'intention de déployer plusieurs instances StorageGRID .
- Vous déployez une instance StorageGRID volumineuse 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 une installation automatisée à l'aide de cadres d'orchestration standard. StorageGRID fournit des scripts Python facultatifs pour automatiser la configuration des appliances StorageGRID et de l'ensemble du système StorageGRID (la « grille »). Vous pouvez utiliser ces scripts directement ou les inspecter pour apprendre à utiliser l'API REST d'installation de StorageGRID dans les outils de déploiement et de configuration de grille que vous développez vous-même.

Automatiser l'installation et la configuration du service hôte StorageGRID

Vous pouvez automatiser l'installation du service hôte StorageGRID à l'aide de frameworks d'orchestration standard tels qu'Ansible, Puppet, Chef, Fabric ou SaltStack.

Le service hôte StorageGRID est empaqueté dans un DEB et est piloté par des fichiers de configuration qui peuvent être préparés à l'avance (ou par programmation) pour permettre une installation automatisée. Si vous utilisez déjà un framework d'orchestration standard pour installer et configurer Ubuntu ou Debian, l'ajout de StorageGRID à vos playbooks ou recettes devrait 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 de StorageGRID
4. Configuration du stockage hôte pour répondre aux exigences de 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 des nœuds StorageGRID
9. Démarrage du service hôte StorageGRID

Exemple de rôle et de manuel Ansible

Un exemple de rôle et de playbook Ansible est fourni avec l'archive d'installation dans le `/extras` dossier. Le playbook Ansible montre comment le `storagegrid` le rôle prépare les hôtes et installe StorageGRID sur les serveurs cibles. Vous pouvez personnaliser le rôle ou le manuel selon vos besoins.

Automatiser la configuration de StorageGRID

Après avoir déployé les nœuds de grille, 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 de fichier	Description
<code>configure-storagegrid.py</code>	Script Python utilisé pour automatiser la configuration
<code>configure-storagegrid.sample.json</code>	Exemple de fichier de configuration à utiliser avec le script
<code>configure-storagegrid.blank.json</code>	Fichier de configuration vide à utiliser avec le script

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

À propos de cette 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 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 plan de relance `.zip` Le fichier est généré pendant le processus de configuration et il est téléchargé dans le répertoire dans lequel vous exécutez le processus d'installation et de configuration. Vous devez sauvegarder le fichier du package de récupération afin de pouvoir récupérer le système StorageGRID si un ou plusieurs nœuds de grille échouent. Par exemple, copiez-le vers un emplacement réseau sécurisé et sauvegardé et vers un emplacement de stockage cloud sécurisé.



Le fichier du package de récupération doit être sécurisé car il contient des clés de chiffrement et des mots de passe qui peuvent être utilisés pour obtenir des données à partir du système StorageGRID .

Si vous avez spécifié que des mots de passe aléatoires doivent être générés, ouvrez le `Passwords.txt` fichier et recherchez les mots de passe requis pour accéder à votre 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 connexes

["Installation de l'API REST"](#)

Déployer des nœuds de grille virtuels (Ubuntu ou Debian)

Créer des fichiers de configuration de nœud pour les déploiements Ubuntu ou Debian

Les fichiers de configuration de nœud sont de petits fichiers texte qui fournissent les informations dont le service hôte StorageGRID a besoin pour démarrer un nœud et le connecter au réseau approprié et aux ressources de stockage en bloc. Les fichiers de configuration de nœud sont utilisés pour les nœuds virtuels et ne sont pas utilisés pour les nœuds d'appliance.

Emplacement des fichiers de configuration des nœuds

Placez le fichier de configuration pour chaque nœud StorageGRID dans le `/etc/storagegrid/nodes` répertoire sur l'hôte où le nœud s'exécutera. 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 vous pouvez les créer ailleurs et les déplacer vers chaque hôte.

Nommage des fichiers de configuration des nœuds

Les noms des fichiers de configuration sont significatifs. 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 de StorageGRID et est utilisé pour les opérations de maintenance des nœuds, telles que la migration des nœuds.

Les noms de nœuds doivent suivre ces règles :

- Doit être unique
- Doit commencer par une lettre
- Peut contenir les caractères A à Z et a à z
- Peut contenir les chiffres de 0 à 9
- Peut contenir un ou plusieurs tirets (-)
- Ne doit pas dépasser 32 caractères, sans compter le `.conf` extension

Tous les fichiers dans `/etc/storagegrid/nodes` qui ne suivent pas ces conventions de nommage ne seront pas analysés par le service hôte.

Si vous avez prévu une topologie multi-sites pour votre réseau, un schéma de dénomination de nœud typique pourrait être :

`site-nodetype-nodenumbers.conf`

Par exemple, vous pouvez utiliser `dc1-adm1.conf` pour le premier nœud d'administration du centre de données 1, et `dc2-sn3.conf` pour le troisième nœud de stockage du centre de données 2. Cependant, vous pouvez utiliser le schéma de votre choix, à condition que tous les noms de nœuds respectent les règles de dénomination.

Contenu d'un fichier de configuration de nœud

Un fichier de configuration contient des paires clé/valeur, avec une clé et une valeur par ligne. Pour chaque paire clé/valeur, suivez ces règles :

- La clé et la valeur doivent être séparées par un signe égal(=) et des espaces facultatifs.
- Les clés ne peuvent contenir aucun espace.
- Les valeurs peuvent contenir des espaces intégrés.
- Tout espace blanc de début ou de fin est ignoré.

Le tableau suivant définit les valeurs de toutes les clés prises en charge. Chaque clé possède l'une des désignations suivantes :

- **Obligatoire** : Obligatoire pour chaque nœud ou pour les types de nœuds spécifiés
- **Meilleure pratique** : Facultatif, mais recommandé
- **Facultatif** : Facultatif pour tous les nœuds

Clés du réseau d'administration

ADMIN_IP

Valeur	Désignation
Adresse IPv4 du réseau de grille du nœud d'administration principal de la grille à laquelle appartient ce nœud. Utilisez la même valeur que celle que vous avez 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 découvrir un nœud d'administration principal à l'aide de mDNS. "Comment les nœuds de grille découvrent le nœud d'administration principal" Remarque : cette valeur est ignorée et peut être interdite sur le nœud d'administration principal.	Meilleures pratiques

CONFIG RÉSEAU ADMIN

Valeur	Désignation
DHCP, STATIQUE ou DÉSACTIVÉ	Facultatif

ADMIN_RESEAU_ESL

Valeur	Désignation
Liste séparée par des virgules des sous-réseaux en notation CIDR avec lesquels ce nœud doit communiquer à l'aide de la passerelle réseau d'administration. Exemple: 172.16.0.0/21, 172.17.0.0/21	Facultatif

PASSERELLE RÉSEAU ADMIN

Valeur	Désignation
Adresse IPv4 de la passerelle du réseau d'administration local 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. Exemples: 1.1.1.1 10.224.4.81	Obligatoire si ADMIN_NETWORK_ESL est spécifié. Facultatif sinon.

ADMIN_RESEAU_IP

Valeur	Désignation
Adresse IPv4 de ce nœud sur le réseau d'administration. Cette clé n'est requise que lorsque ADMIN_NETWORK_CONFIG = STATIC ; ne la spécifiez pas pour d'autres valeurs. Exemples: 1.1.1.1 10.224.4.81	Obligatoire lorsque ADMIN_NETWORK_CONFIG = STATIC. Facultatif sinon.

ADMIN_RESEAU_MAC

Valeur	Désignation
L'adresse MAC de l'interface réseau d'administration dans le conteneur. Ce champ est facultatif. Si elle est omise, une adresse MAC sera générée automatiquement. Doit être composé de 6 paires de chiffres hexadécimaux séparés par des deux points. Exemple: b2:9c:02:c2:27:10	Facultatif

MASQUE_RESEAU_ADMIN

Valeur	Désignation
Masque de réseau IPv4 pour ce nœud, sur le réseau d'administration. Spécifiez cette clé lorsque ADMIN_NETWORK_CONFIG = STATIC ; ne la spécifiez pas pour d'autres valeurs. Exemples: 255.255.255.0 255.255.248.0	Obligatoire si ADMIN_NETWORK_IP est spécifié et ADMIN_NETWORK_CONFIG = STATIC. Facultatif sinon.

ADMIN_RESEAU_MTU

Valeur	Désignation
L'unité de transmission maximale (MTU) pour ce nœud sur le réseau d'administration. Ne spécifiez pas si ADMIN_NETWORK_CONFIG = DHCP. Si spécifié, la valeur doit être comprise entre 1280 et 9216. Si omis, 1500 est utilisé. Si vous souhaitez utiliser des trames jumbo, définissez le MTU sur une valeur adaptée aux trames jumbo, telle que 9 000. 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 du réseau ou une perte de paquets pourraient survenir. Exemples: 1500 8192	Facultatif

ADMIN_RÉSEAU_CIBLE

Valeur	Désignation
Nom du périphérique hôte que vous utiliserez pour l'accès au réseau d'administration par le nœud StorageGRID . Seuls les noms d'interface réseau sont pris en charge. En règle générale, vous utilisez un nom d'interface différent de celui spécifié pour GRID_NETWORK_TARGET ou CLIENT_NETWORK_TARGET. Remarque : n'utilisez pas de périphériques 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 n'aura pas initialement d'adresse IP de réseau d'administration. Vous pouvez ensuite ajouter une adresse IP de réseau d'administration ultérieurement, sans avoir à reconfigurer le nœud sur l'hôte. Exemples: bond0.1002 ens256	Meilleures pratiques

TYPE_CIBLE_RÉSEAU_ADMIN

Valeur	Désignation
Interface (c'est la seule valeur prise en charge.)	Facultatif

ADMIN_RÉSEAU_TYPE_CIBLE_INTERFACE_CLONE_MAC

Valeur	Désignation
Vrai ou faux Définissez la clé sur « true » pour que le conteneur StorageGRID utilise l'adresse MAC de l'interface cible de l'hôte sur le réseau d'administration. Meilleure pratique : dans les réseaux où le mode promiscuité est requis, utilisez plutôt la clé ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC. Pour plus de détails sur le clonage MAC : • "Considérations et recommandations pour le clonage d'adresses MAC (Red Hat Enterprise Linux)" • "Considérations et recommandations pour le clonage d'adresses MAC (Ubuntu ou Debian)"	Meilleures pratiques

RÔLE_ADMIN

Valeur	Désignation
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.	Obligatoire lorsque NODE_TYPE = VM_Admin_Node Facultatif sinon.

Bloquer les clés de l'appareil

BLOQUER_LES_JOURNAUX_D'AUDIT_DE_L'APPAREIL

Valeur	Désignation
Chemin et nom du fichier spécial du périphérique de bloc que ce nœud utilisera pour le stockage persistant des journaux d'audit. Exemples: <pre>/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0</pre> <pre>/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd</pre> <pre>/dev/mapper/sgws-adml-audit-logs</pre>	Obligatoire pour les nœuds avec NODE_TYPE = VM_Admin_Node. Ne le spécifiez pas pour d'autres types de nœuds.

BLOCK_DEVICE_RANGEDB_nnn

Valeur	Désignation
Chemin et nom du fichier spécial du périphérique de bloc que ce nœud utilisera pour le stockage d'objets persistants. Cette clé n'est requise que pour les nœuds avec NODE_TYPE = VM_Storage_Node ; ne la spécifiez pas pour les autres types de nœuds. Seul BLOCK_DEVICE_RANGEDB_000 est requis ; les autres sont facultatifs. Le périphérique de bloc spécifié pour BLOCK_DEVICE_RANGEDB_000 doit être d'au moins 4 To ; les autres peuvent être plus petits. Ne laissez pas de trous. Si vous spécifiez BLOCK_DEVICE_RANGEDB_005, vous devez également spécifier BLOCK_DEVICE_RANGEDB_004. Remarque : pour des raisons de compatibilité avec les déploiements existants, les clés à deux chiffres sont prises en charge pour les nœuds mis à niveau. Exemples: <pre>/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0</pre> <pre>/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd</pre> <pre>/dev/mapper/sgws-snl-rangedb-000</pre>	Requis: BLOCK_DEVICE_RANGEDB_000 Facultatif: 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

BLOCK_DEVICE_TABLES

Valeur	Désignation
Chemin et nom du fichier spécial du périphérique de bloc que ce nœud utilisera pour le stockage persistant des tables de base de données. Cette clé n'est requise que pour les nœuds avec NODE_TYPE = VM_Admin_Node ; ne la spécifiez pas pour les autres types de nœuds. Exemples: <pre>/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0</pre> <pre>/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd</pre> <pre>/dev/mapper/sgws-adml-tables</pre>	Obligatoire

BLOC_DEVICE_VAR_LOCAL

Valeur	Désignation
Chemin et nom du fichier spécial du périphérique de bloc que ce nœud utilisera pour son /var/local stockage persistant. Exemples: <pre>/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0</pre> <pre>/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd</pre> <pre>/dev/mapper/sgws-sn1-var-local</pre>	Obligatoire

Clés du réseau client

CONFIG RÉSEAU_CLIENT

Valeur	Désignation
DHCP, STATIQUE ou DÉSACTIVÉ	Facultatif

PASSERELLE RÉSEAU_CLIENT

Valeur	Désignation

Adresse IPv4 de la passerelle réseau client locale pour ce nœud, qui doit se trouver sur le sous-réseau défini par <code>CLIENT_NETWORK_IP</code> et <code>CLIENT_NETWORK_MASK</code>. Cette valeur est ignorée pour les réseaux configurés par DHCP. Exemples: 1.1.1.1 10.224.4.81	Facultatif

IP_RÉSEAU_CLIENT

Valeur	Désignation
Adresse IPv4 de ce nœud sur le réseau client. Cette clé n'est requise que lorsque <code>CLIENT_NETWORK_CONFIG = STATIC</code> ; ne la spécifiez pas pour d'autres valeurs. Exemples: 1.1.1.1 10.224.4.81	Obligatoire lorsque <code>CLIENT_NETWORK_CONFIG = STATIC</code> Facultatif sinon.

CLIENT_RÉSEAU_MAC

Valeur	Désignation
L'adresse MAC de l'interface réseau client dans le conteneur. Ce champ est facultatif. Si elle est omise, une adresse MAC sera générée automatiquement. Doit être composé de 6 paires de chiffres hexadécimaux séparés par des deux points. Exemple: b2:9c:02:c2:27:20	Facultatif

MASQUE_RÉSEAU_CLIENT

Valeur	Désignation
Masque de réseau IPv4 pour ce nœud sur le réseau client. Spécifiez cette clé lorsque CLIENT_NETWORK_CONFIG = STATIC ; ne la spécifiez pas pour d'autres valeurs. Exemples: 255.255.255.0 255.255.248.0	Obligatoire si CLIENT_NETWORK_IP est spécifié et CLIENT_NETWORK_CONFIG = STATIC Facultatif sinon.

CLIENT_RESEAU_MTU

Valeur	Désignation
L'unité de transmission maximale (MTU) pour ce nœud sur le réseau client. Ne spécifiez pas si CLIENT_NETWORK_CONFIG = DHCP. Si spécifié, la valeur doit être comprise entre 1280 et 9216. Si omis, 1500 est utilisé. Si vous souhaitez utiliser des trames jumbo, définissez le MTU sur une valeur adaptée aux trames jumbo, telle que 9 000. 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 du réseau ou une perte de paquets pourraient survenir. Exemples: 1500 8192	Facultatif

CLIENT_RESEAU_CIBLE

Valeur	Désignation
Nom du périphérique hôte que vous utiliserez pour l'accès au réseau client par le nœud StorageGRID . Seuls les noms d'interface réseau sont pris en charge. En règle générale, vous utilisez un nom d'interface différent de celui spécifié pour GRID_NETWORK_TARGET ou ADMIN_NETWORK_TARGET. Remarque : n'utilisez pas de périphériques 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 n'aura pas initialement d'adresse IP de réseau client. Vous pouvez ensuite ajouter une adresse IP de réseau client ultérieurement, sans avoir à reconfigurer le nœud sur l'hôte. Exemples: <pre>bond0.1003</pre> <pre>ens423</pre>	Meilleures pratiques

TYPE_CIBLE RÉSEAU_CLIENT

Valeur	Désignation
Interface (il s'agit de la seule valeur prise en charge.)	Facultatif

CLIENT RÉSEAU_TYPE_CIBLE_INTERFACE_CLONE_MAC

Valeur	Désignation
Vrai ou faux Définissez la clé sur « true » pour que le conteneur StorageGRID utilise l'adresse MAC de l'interface cible de l'hôte sur le réseau client. Meilleure pratique : dans les réseaux où le mode promiscuité est requis, utilisez plutôt la clé CLIENT_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC. Pour plus de détails sur le clonage MAC : • "Considérations et recommandations pour le clonage d'adresses MAC (Red Hat Enterprise Linux)" • "Considérations et recommandations pour le clonage d'adresses MAC (Ubuntu ou Debian)"	Meilleures pratiques

Clés du réseau Grid

CONFIG_RÉSEAU_GRILLE

Valeur	Désignation
STATIQUE ou DHCP La valeur par défaut est STATIC si elle n'est pas spécifiée.	Meilleures pratiques

PASSERELLE_RÉSEAU_GRILLE

Valeur	Désignation
Adresse IPv4 de la passerelle du réseau Grid local 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 (XYZ1), soit la valeur GRID_NETWORK_IP de ce nœud ; l'une ou l'autre valeur simplifiera les futures extensions potentielles du réseau Grid.	Obligatoire

IP_RÉSEAU_GRILLE

Valeur	Désignation
Adresse IPv4 de ce nœud sur le réseau Grid. Cette clé n'est requise que lorsque GRID_NETWORK_CONFIG = STATIC ; ne la spécifiez pas pour d'autres valeurs. Exemples: 1.1.1.1 10.224.4.81	Obligatoire lorsque GRID_NETWORK_CONFIG = STATIC Facultatif sinon.

GRILLE_RÉSEAU_MAC

Valeur	Désignation
L'adresse MAC de l'interface Grid Network dans le conteneur. Doit être composé de 6 paires de chiffres hexadécimaux séparés par des deux points. Exemple: b2:9c:02:c2:27:30	Facultatif Si elle est omise, une adresse MAC sera générée automatiquement.

MASQUE_RÉSEAU_GRILLE

Valeur	Désignation
Masque de réseau IPv4 pour ce nœud sur le réseau Grid. Spécifiez cette clé lorsque GRID_NETWORK_CONFIG = STATIC ; ne la spécifiez pas pour d'autres valeurs. Exemples: 255.255.255.0 255.255.248.0	Obligatoire lorsque GRID_NETWORK_IP est spécifié et GRID_NETWORK_CONFIG = STATIC. Facultatif sinon.

RÉSEAU_GRILLE_MTU

Valeur	Désignation
L'unité de transmission maximale (MTU) pour ce nœud sur le réseau Grid. Ne spécifiez pas si GRID_NETWORK_CONFIG = DHCP. Si spécifié, la valeur doit être comprise entre 1280 et 9216. Si omis, 1500 est utilisé. Si vous souhaitez utiliser des trames jumbo, définissez le MTU sur une valeur adaptée aux trames jumbo, telle que 9 000. 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 du réseau ou une perte de paquets pourraient survenir. IMPORTANT : pour des performances réseau optimales, tous les nœuds doivent être configurés avec des valeurs MTU similaires sur leurs interfaces Grid Network. L'alerte Incompatibilité MTU du réseau de grille est déclenchée s'il existe une différence significative dans les paramètres MTU du réseau de grille sur des nœuds individuels. Les valeurs MTU ne doivent pas nécessairement être les mêmes pour tous les types de réseaux. Exemples: 1500 8192	Facultatif

GRILLE_RÉSEAU_CIBLE

Valeur	Désignation
Nom du périphérique hôte que vous utiliserez pour l'accès au réseau Grid par le nœud StorageGRID . Seuls les noms d'interface réseau sont pris en charge. En règle générale, vous utilisez un nom d'interface différent de celui spécifié pour ADMIN_NETWORK_TARGET ou CLIENT_NETWORK_TARGET. Remarque : n'utilisez pas de périphériques 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	Obligatoire

TYPE_CIBLE RÉSEAU GRILLE

Valeur	Désignation
Interface (c'est la seule valeur prise en charge.)	Facultatif

GRID_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC

Valeur	Désignation
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 Grid. Meilleure pratique : dans les réseaux où le mode promiscuité est requis, utilisez plutôt la clé GRID_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC. Pour plus de détails sur le clonage MAC : • "Considérations et recommandations pour le clonage d'adresses MAC (Red Hat Enterprise Linux)" • "Considérations et recommandations pour le clonage d'adresses MAC (Ubuntu ou Debian)"	Meilleures pratiques

Clé de mot de passe d'installation (temporaire)

HACHAGE_DE_MOT_DE_PASSE_TEMPORAIRE_PERSONNALISÉ

Valeur	Désignation
Pour le nœud d'administration principal, définissez un mot de passe temporaire par défaut pour l'API d'installation StorageGRID pendant l'installation. Remarque : définissez un mot de passe d'installation sur le nœud d'administration principal uniquement. Si vous tentez de définir un mot de passe sur un autre type de nœud, la validation du fichier de configuration du nœud échouera. La définition de cette valeur n'a aucun effet une fois l'installation terminée. Si cette clé est omise, aucun mot de passe temporaire n'est défini par défaut. Vous pouvez également définir un mot de passe temporaire à l'aide de l'API d'installation StorageGRID . Doit être un <code>crypt()</code> Hachage de mot de passe SHA-512 avec format <code>\$6\$<salt>\$<password hash></code> pour un mot de passe d'au moins 8 et d'au plus 32 caractères. Ce hachage peut être généré à l'aide d'outils CLI, tels que <code>openssl passwd</code> commande en mode SHA-512.	Meilleures pratiques

Clé des interfaces

INTERFACE_CIBLE_nnnn

Valeur	Désignation
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 <i>nnnn</i>, spécifiez un numéro unique pour chaque entrée <code>INTERFACE_TARGET</code> 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 Interfaces VLAN et sur la page Groupes HA. Exemple: <code>INTERFACE_TARGET_0001=ens256, Trunk</code> Si vous ajoutez une interface de jonction, vous devez configurer une interface VLAN dans StorageGRID. Si vous ajoutez une interface d'accès, vous pouvez ajouter l'interface directement à un groupe HA ; vous n'avez pas besoin de configurer une interface VLAN.	Facultatif

Clé RAM maximale

RAM MAXIMALE

Valeur	Désignation
La 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, spécifiez une valeur d'au moins 24 Go et de 16 à 32 Go inférieure à la RAM totale du système. Remarque : la valeur RAM affecte l'espace réservé réel aux métadonnées d'un nœud. Voir le "description de ce qu'est l'espace réservé aux métadonnées". Le format de ce champ est <i>numberunit</i>, où <i>unit</i> 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.	Facultatif

Clés de type de nœud

TYPE_NOEUD

Valeur	Désignation
Type de nœud : • Nœud_Admin_VM • Nœud de stockage VM • Nœud d'archive VM • Passerelle VM_API	Obligatoire

TYPE_DE_STOCKAGE

Valeur	Désignation
Définit le type d'objets qu'un nœud de stockage contient. Pour plus d'informations, consultez la section "Types de nœuds de stockage". Cette clé n'est requise que pour les nœuds avec <code>NODE_TYPE = VM_Storage_Node</code> ; ne la spécifiez pas pour les autres types de nœuds. Types de stockage : • combiné • données • métadonnées Remarque : si le <code>STORAGE_TYPE</code> n'est pas spécifié, le type de nœud de stockage est défini sur combiné (données et métadonnées) par défaut.	Facultatif

Clés de remappage des ports

PORT_REMAP

Valeur	Désignation
Remappe tout port utilisé par un nœud pour les communications internes du nœud de grille ou les communications externes. Le remappage des ports est nécessaire si les politiques de réseau d'entreprise restreignent un ou plusieurs ports utilisés par StorageGRID, comme décrit dans "Communications internes des nœuds de réseau" ou "Communications externes". IMPORTANT : Ne remappez pas les ports que vous prévoyez d'utiliser pour configurer les points de terminaison de l'équilibreur de charge. Remarque : si seul <code>PORT_REMAP</code> est défini, le mappage que vous spécifiez est utilisé pour les communications entrantes et sortantes. Si <code>PORT_REMAP_INBOUND</code> est également spécifié, <code>PORT_REMAP</code> s'applique uniquement aux communications sortantes. Le format utilisé est : <i>network type/protocol/default port used by grid node/new port</i>, où <i>network type</i> est une grille, un administrateur ou un client, et <i>protocol</i> est tcp ou udp. Exemple: <code>PORT_REMAP = client/tcp/18082/443</code> Vous pouvez également remapper plusieurs ports à l'aide d'une liste séparée par des virgules. Exemple: <code>PORT_REMAP = client/tcp/18082/443, client/tcp/18083/80</code>	Facultatif

PORT_REMAP_ENTRANT

Valeur	Désignation
Remappe les communications entrantes vers le port spécifié. Si vous spécifiez PORT_REMAP_INBOUND mais ne spécifiez pas de valeur pour PORT_REMAP, les communications sortantes pour le port restent inchangées. IMPORTANT : Ne remappez pas les ports que vous prévoyez d'utiliser pour configurer les points de terminaison de l'équilibreur de charge. Le format utilisé est : <i>network type/protocol/remapped port /default port used by grid node</i>, où <i>network type</i> est une grille, un administrateur ou un client, et <i>protocol</i> est tcp ou udp. Exemple: <code>PORT_REMAP_INBOUND = grid/tcp/3022/22</code> Vous pouvez également remapper plusieurs ports entrants à l'aide d'une liste séparée par des virgules. Exemple: <code>PORT_REMAP_INBOUND = grid/tcp/3022/22, admin/tcp/3022/22</code>	Facultatif

Comment les nœuds de grille découvrent le nœud d'administration principal

Les nœuds de grille communiquent avec le nœud d'administration principal pour la configuration et la gestion. Chaque nœud de grille doit connaître l'adresse IP du nœud d'administration principal sur le réseau de grille.

Pour garantir 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 grille découvre automatiquement la valeur. La découverte 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 est réalisée à l'aide d'un système de noms de domaine multidiffusion (mDNS). Lorsque le nœud d'administration principal démarre pour la première fois, il publie son adresse IP à l'aide de mDNS. D'autres nœuds sur le même sous-réseau peuvent alors interroger l'adresse IP et l'acquérir automatiquement. Cependant, étant donné que le trafic IP multidiffusion n'est normalement pas routable sur les sous-réseaux, les nœuds des autres sous-réseaux ne peuvent pas acquérir directement l'adresse IP du nœud d'administration principal.

Si vous utilisez la découverte automatique :



- Vous devez inclure le paramètre ADMIN_IP pour au moins un nœud de grille sur tous les sous-réseaux auxquels le nœud d'administration principal n'est pas directement connecté. Ce nœud de grille publiera ensuite l'adresse IP du nœud d'administration principal pour que les autres nœuds du sous-réseau puissent la découvrir avec mDNS.
- Assurez-vous que votre infrastructure réseau prend en charge le passage du trafic IP multidiffusion au sein d'un sous-réseau.

Exemples de fichiers de configuration de nœuds

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 des fichiers de configuration de nœuds pour tous les types de nœuds de grille.

Pour la plupart des nœuds, vous pouvez ajouter des informations d'adressage réseau administrateur et client (IP, masque, passerelle, etc.) lorsque vous configurez la grille à l'aide du gestionnaire de grille ou de l'API d'installation. L'exception est le nœud d'administration principal. Si vous souhaitez accéder à l'adresse IP du réseau d'administration du nœud d'administration principal pour terminer la configuration de la grille (parce que le réseau de grille n'est pas routé, par exemple), vous devez configurer la connexion au réseau d'administration pour le nœud d'administration principal dans son fichier de configuration de nœud. Ceci est montré dans l'exemple.



Dans les exemples, la cible Réseau client a été configurée comme une meilleure pratique, 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
TEMPORARY_PASSWORD_TYPE = Use custom password
CUSTOM_TEMPORARY_PASSWORD = Passw0rd
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-adml-var-local
BLOCK_DEVICE_AUDIT_LOGS = /dev/mapper/dc1-adml-audit-logs
BLOCK_DEVICE_TABLES = /dev/mapper/dc1-adml-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 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 principal

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
```

Valider la configuration de StorageGRID

Après avoir créé les 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, la sortie affiche **PASSED** pour chaque fichier de configuration, comme indiqué dans l'exemple.



Lorsque vous utilisez un seul LUN sur des nœuds contenant uniquement des métadonnées, vous pouvez recevoir un message d'avertissement qui peut être ignoré.

```
Checking for misnamed node configuration files... PASSED
Checking configuration file for node dcl-adm1... PASSED
Checking configuration file for node dcl-gw1... PASSED
Checking configuration file for node dcl-sn1... PASSED
Checking configuration file for node dcl-sn2... PASSED
Checking configuration file for node dcl-sn3... PASSED
Checking for duplication of unique values between nodes... PASSED
```



Pour une installation automatisée, vous pouvez supprimer cette sortie en utilisant le `-q` ou `--quiet` options dans le `storagegrid` commande (par exemple, `storagegrid --quiet...`). Si vous supprimez la sortie, la commande aura une valeur de sortie différente de zéro si des avertissements ou des erreurs de configuration ont été détectés.

Si les fichiers de configuration sont incorrects, les problèmes sont affichés sous la forme **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/dcl-adml
WARNING: ignoring /etc/storagegrid/nodes/dcl-sn2.conf.keep
WARNING: ignoring /etc/storagegrid/nodes/my-file.txt
Checking configuration file for node dcl-adml...
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 dcl-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 dcl-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 dcl-sn2... PASSED
Checking configuration file for node dcl-sn3... PASSED
Checking for duplication of unique values between nodes...
ERROR: GRID_NETWORK_IP = 10.1.0.4
      dcl-sn2 and dcl-sn3 have the same GRID_NETWORK_IP
ERROR: BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-sn2-var-local
      dcl-sn2 and dcl-sn3 have the same BLOCK_DEVICE_VAR_LOCAL
ERROR: BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/sgws-sn2-rangedb-0
      dcl-sn2 and dcl-sn3 have the same BLOCK_DEVICE_RANGEDB_00

```

Démarrer le service hôte StorageGRID

Pour démarrer vos nœuds StorageGRID et garantir 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 vous assurer que le déploiement se poursuit :

```
sudo storagegrid node status node-name
```

3. Si un nœud renvoie l'état « Non en cours d'exécution » ou « Arrêté », 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 terminer l'installation (Ubuntu ou Debian)

Accéder au gestionnaire de grille

Vous utilisez le Grid Manager pour définir toutes les informations requises pour configurer votre 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 :

```
https://primary_admin_node_ip
```

Alternativement, vous pouvez accéder au Grid Manager sur le port 8443 :

```
https://primary_admin_node_ip:8443
```

Vous pouvez utiliser l'adresse IP du nœud d'administration principal sur le réseau de grille ou sur le réseau d'administration, selon la configuration de votre réseau.

2. Gérez un mot de passe d'installation temporaire selon vos besoins :
 - Si un mot de passe a déjà été défini à l'aide de l'une de ces méthodes, saisissez le mot de passe pour continuer.
 - Un utilisateur a défini le mot de passe lors de l'accès au programme d'installation précédemment
 - Le mot de passe a été automatiquement importé à partir du fichier de configuration du nœud à `/etc/storagegrid/nodes/<node_name>.conf`
 - Si aucun mot de passe n'a été défini, vous pouvez éventuellement définir un mot de passe pour sécuriser le programme d'installation de StorageGRID .
3. Sélectionnez ***Installer un système StorageGRID ***.

La page utilisée pour configurer un système StorageGRID apparaît.

NetApp® StorageGRID®

Help ▾

Install

1

2

3

4

5

6

7

8

License

Sites

Grid Network

Grid Nodes

NTP

DNS

Passwords

Summary

License

Enter a grid name and upload the license file provided by NetApp for your StorageGRID system.

Grid Name

License File

Browse

Spécifiez les informations de licence StorageGRID

Vous devez spécifier le nom de votre système StorageGRID et télécharger le fichier de licence fourni par NetApp.

Étapes

1. Sur la page Licence, saisissez 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 **Parcourir**, recherchez le fichier de licence NetApp(*NLF-unique-id.txt*), et sélectionnez **Ouvrir**.

Le fichier de licence est validé et le numéro de série est affiché.



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 niveau vers une licence qui offre un support après l'installation.

1

2

3

4

5

6

7

8

License

Sites

Grid Network

Grid Nodes

NTP

DNS

Passwords

Summary

License

Enter a grid name and upload the license file provided by NetApp for your StorageGRID system.

Grid Name

StorageGRID

License File

Browse

NLF-959007-Internal.txt

License Serial Number

959007

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 le **Nom du site**.
2. Pour ajouter des sites supplémentaires, cliquez sur le signe plus à côté de la dernière entrée de site et saisissez le nom dans la nouvelle zone de texte **Nom du site**.

Ajoutez autant de sites supplémentaires que nécessaire pour votre topologie de grille. Vous pouvez ajouter jusqu'à 16 sites.

NetApp® StorageGRID® Help ▾

Install

1 License 2 Sites 3 Grid Network 4 Grid Nodes 5 NTP 6 DNS 7 Passwords 8 Summary

Sites

In a single-site deployment, infrastructure and operations are centralized in one site.

In a multi-site deployment, infrastructure can be distributed asymmetrically across sites, and proportional to the needs of each site. Typically, sites are located in geographically different locations. Having multiple sites also allows the use of distributed replication and erasure coding for increased availability and resiliency.

Site Name 1 Raleigh ✕

Site Name 2 Atlanta + ✕

3. Cliquez sur **Suivant**.

Spécifier les sous-réseaux du réseau Grid

Vous devez spécifier les sous-réseaux utilisés sur le réseau Grid.

À propos de cette tâche

Les entrées de sous-réseau incluent les sous-réseaux du réseau Grid pour chaque site de votre système StorageGRID , ainsi que tous les sous-réseaux qui doivent être accessibles via le réseau Grid.

Si vous disposez de plusieurs sous-réseaux de grille, la passerelle Grid Network est requise. Tous les sous-réseaux de grille spécifiés doivent être accessibles via cette passerelle.

Étapes

1. Spécifiez l'adresse réseau CIDR pour au moins un réseau de grille 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. Vous devez spécifier tous les sous-réseaux pour tous les sites du réseau Grid.

- Si vous avez déjà déployé au moins un nœud, cliquez sur **Découvrir les sous-réseaux des réseaux de grille** pour remplir automatiquement la liste des sous-réseaux des réseaux de grille avec les sous-réseaux signalés par les nœuds de grille enregistrés auprès du gestionnaire de grille.
- Vous devez ajouter manuellement tous les sous-réseaux pour NTP, DNS, LDAP ou autres serveurs externes accessibles via la passerelle Grid Network.

NetApp® StorageGRID® Help ▾

Install

1 License 2 Sites 3 **Grid Network** 4 Grid Nodes 5 NTP 6 DNS 7 Passwords 8 Summary

Grid Network

You must specify the subnets that are used on the Grid Network. These entries typically include the subnets for the Grid Network for each site in your StorageGRID system. Select Discover Grid Networks to automatically add subnets based on the network configuration of all registered nodes.

Note: You must manually add any subnets for NTP, DNS, LDAP, or other external servers accessed through the Grid Network gateway.

Subnet 1 +

3. Cliquez sur **Suivant**.

Approuver les nœuds de grille en attente

Vous devez approuver chaque nœud de grille avant qu'il puisse rejoindre le système StorageGRID .

Avant de commencer

Vous avez déployé tous les nœuds de grille d'appliance virtuelle et StorageGRID .



Il est plus efficace d'effectuer une seule installation de tous les nœuds, plutôt que d'installer certains nœuds maintenant et certains nœuds plus tard.

Étapes

1. Consultez la liste des nœuds en attente et confirmez qu'elle affiche tous les nœuds de grille que vous avez déployés.



Si un nœud de grille est manquant, confirmez qu'il a été déployé avec succès et qu'il dispose de l'adresse IP du réseau de grille correcte du nœud d'administration principal défini pour ADMIN_IP.

2. Sélectionnez le bouton radio à côté d'un nœud en attente que vous souhaitez approuver.



Grid Nodes

Approve and configure grid nodes, so that they are added correctly to your StorageGRID system.

Pending Nodes

Grid nodes are listed as pending until they are assigned to a site, configured, and approved.

+ Approve ✕ Remove		Search				
	Grid Network MAC Address	Name	Type	Platform	Grid Network IPv4 Address	
☒	50:6b:4b:42:d7:00	NetApp-SGA	Storage Node	StorageGRID Appliance	172.16.5.20/21	
						◀ ▶

Approved Nodes

Grid nodes that have been approved and have been configured for installation. An approved grid node's configuration can be edited if errors are identified.

Edit Reset ✕ Remove		Search				
	Grid Network MAC Address	Name	Site	Type	Platform	Grid Network IPv4 Address
☐	00:50:56:87:42:ff	dc1-adm1	Raleigh	Admin Node	VMware VM	172.16.4.210/21
☐	00:50:56:87:c0:16	dc1-s1	Raleigh	Storage Node	VMware VM	172.16.4.211/21
☐	00:50:56:87:79:ee	dc1-s2	Raleigh	Storage Node	VMware VM	172.16.4.212/21
☐	00:50:56:87:db:9c	dc1-s3	Raleigh	Storage Node	VMware VM	172.16.4.213/21
☐	00:50:56:87:62:38	dc1-g1	Raleigh	API Gateway Node	VMware VM	172.16.4.214/21
						◀ ▶

3. Cliquez sur **Approuver**.

4. Dans les paramètres généraux, modifiez les paramètres des propriétés suivantes, si nécessaire :

- **Site** : Le nom système du site pour ce nœud de grille.
- **Nom** : Le nom du système pour le nœud. Le nom par défaut est celui 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 du système selon vos besoins.

- **Rôle NTP** : Le rôle du protocole NTP (Network Time Protocol) du nœud de grille. Les options sont **Automatique**, **Principal** et **Client**. La sélection de **Automatique** attribue le rôle principal aux nœuds d'administration, aux nœuds de stockage avec services ADC, aux nœuds de passerelle et à tous les nœuds de grille dotés d'adresses IP non statiques. Tous les autres nœuds de grille se voient attribuer le rôle Client.



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 se produiront si ce nœud tombe en panne. De plus, la désignation de deux nœuds par site comme sources NTP principales garantit une synchronisation précise si un site est isolé du reste du réseau.

- **Type de stockage** (nœuds de stockage uniquement) : spécifiez qu'un nouveau nœud de stockage doit être utilisé exclusivement pour les données uniquement, les métadonnées uniquement ou les deux. Les options sont **Données et métadonnées** (« combinées »), **Données uniquement** et **Métadonnées uniquement**.



Voir "[Types de nœuds de stockage](#)" pour obtenir des informations sur les exigences relatives à ces types de nœuds.

- **Service ADC** (nœuds de stockage uniquement) : sélectionnez **Automatique** pour permettre au système de déterminer si le nœud nécessite le service de contrôleur de domaine administratif (ADC). Le service ADC suit l'emplacement et la disponibilité des services du réseau. Au moins trois nœuds de stockage sur chaque site doivent inclure le service ADC. Vous ne pouvez pas ajouter le service ADC à un nœud après son déploiement.

5. Dans Grid Network, modifiez les paramètres des propriétés suivantes si nécessaire :

- **Adresse IPv4 (CIDR)** : l'adresse réseau CIDR pour l'interface Grid Network (eth0 à l'intérieur du conteneur). Par exemple : 192.168.1.234/21
- **Passerelle** : La passerelle du réseau Grid. Par exemple : 192.168.0.1

La passerelle est requise s'il existe plusieurs sous-réseaux de grille.



Si vous avez sélectionné DHCP pour la configuration du réseau Grid et que vous modifiez la valeur ici, la nouvelle valeur sera configurée comme une adresse statique sur le nœud. Vous devez vous assurer que l'adresse IP configurée ne se trouve pas dans un pool d'adresses DHCP.

6. Si vous souhaitez configurer le réseau d'administration pour le nœud de grille, ajoutez ou mettez à jour les paramètres dans la section Réseau d'administration si nécessaire.

Saisissez les sous-réseaux de destination des itinéraires sortant de cette interface dans la zone de texte **Sous-réseaux (CIDR)**. S'il existe plusieurs sous-réseaux d'administration, 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 comme une adresse statique sur le nœud. Vous devez vous assurer que l'adresse IP configurée ne se trouve pas dans un pool d'adresses DHCP.

Appareils : pour un appareil 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'appareil StorageGRID , il ne peut pas être configuré dans cette boîte de dialogue Grid Manager. Au lieu de cela, vous devez suivre ces étapes :

- Redémarrez l'appareil : dans le programme d'installation de l'appareil, sélectionnez **Avancé > Redémarrer**.

Le redémarrage peut prendre plusieurs minutes.

- b. Sélectionnez **Configurer la mise en réseau > Configuration de liaison** et activez les réseaux appropriés.
- c. Sélectionnez **Configurer le 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 nœud.
- f. Supprimez le nœud de la table des nœuds en attente.
- g. Attendez que le nœud réapparaisse dans la liste des nœuds en attente.
- h. Confirmez que vous pouvez configurer les réseaux appropriés. Ils doivent déjà être renseignés avec les informations que vous avez fournies sur la page de configuration IP du programme d'installation de l'appliance.

Pour plus d'informations, consultez le ["Démarrage rapide pour l'installation du matériel"](#) pour localiser 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 nœud 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 comme une adresse statique sur le nœud. Vous devez vous assurer que l'adresse IP configurée ne se trouve pas dans un pool d'adresses DHCP.

Appliances : 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 Grid Manager. Au lieu de cela, vous devez suivre ces étapes :

- a. Redémarrez l'appareil : dans le programme d'installation de l'appareil, sélectionnez **Avancé > Redémarrer**.

Le redémarrage peut prendre plusieurs minutes.

- b. Sélectionnez **Configurer la mise en réseau > Configuration de liaison** et activez les réseaux appropriés.
- c. Sélectionnez **Configurer le 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 nœud.
- f. Supprimez le nœud de la table des nœuds en attente.
- g. Attendez que le nœud réapparaisse dans la liste des nœuds en attente.
- h. Confirmez que vous pouvez configurer les réseaux appropriés. Ils doivent déjà être renseignés avec les informations que vous avez fournies sur la page de 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 localiser les instructions relatives à votre appareil.

8. Cliquez sur **Enregistrer**.

L'entrée du nœud de grille est déplacée vers la liste des nœuds approuvés.



Grid Nodes

Approve and configure grid nodes, so that they are added correctly to your StorageGRID system.

Pending Nodes

Grid nodes are listed as pending until they are assigned to a site, configured, and approved.

+ Approve

✖ Remove

Search

Grid Network MAC Address	Name	Type	Platform	Grid Network IPv4 Address
No results found.				

◀

▶

Approved Nodes

Grid nodes that have been approved and have been configured for installation. An approved grid node's configuration can be edited if errors are identified.

Edit

Reset

✖ Remove

Search

	Grid Network MAC Address	Name	Site	Type	Platform	Grid Network IPv4 Address
☐	00:50:56:87:42:ff	dc1-adm1	Raleigh	Admin Node	VMware VM	172.16.4.210/21
☐	00:50:56:87:c0:16	dc1-s1	Raleigh	Storage Node	VMware VM	172.16.4.211/21
☐	00:50:56:87:79:ee	dc1-s2	Raleigh	Storage Node	VMware VM	172.16.4.212/21
☐	00:50:56:87:db:9c	dc1-s3	Raleigh	Storage Node	VMware VM	172.16.4.213/21
☐	00:50:56:87:62:38	dc1-g1	Raleigh	API Gateway Node	VMware VM	172.16.4.214/21
☐	50:6b:4b:42:d7:00	NetApp-SGA	Raleigh	Storage Node	StorageGRID Appliance	172.16.5.20/21

◀

▶

9. Répétez ces étapes pour chaque nœud de grille en attente que vous souhaitez approuver.

Vous devez approuver tous les nœuds que vous souhaitez dans la grille. Cependant, vous pouvez revenir sur 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**.

Spécifier les informations du serveur Network Time Protocol

Vous devez spécifier les informations de configuration du protocole NTP (Network Time Protocol) pour le système StorageGRID , afin que les opérations effectuées sur des serveurs distincts puissent rester synchronisées.

À propos de cette tâche

Vous devez spécifier des adresses IPv4 pour les serveurs NTP.

Vous devez spécifier des serveurs NTP externes. Les serveurs NTP spécifiés doivent utiliser le protocole NTP.

Vous devez spécifier quatre références de serveur NTP de niveau 3 ou supérieur pour éviter les problèmes de dérive temporelle.



Lorsque vous spécifiez 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 de haute précision, tels que StorageGRID.

["Limite de prise en charge pour configurer le service de temps Windows pour les environnements de haute précision"](#)

Les serveurs NTP externes sont utilisés par les nœuds auxquels vous avez précédemment attribué des rôles NTP principaux.



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 se produiront si ce nœud tombe en panne. De plus, la désignation de deux nœuds par site comme sources NTP principales garantit une synchronisation précise si un site est isolé du reste du réseau.

Étapes

1. Spécifiez les adresses IPv4 pour au moins quatre serveurs NTP dans les zones de texte **Serveur 1** à **Serveur 4**.
2. Si nécessaire, sélectionnez le signe plus à côté de la dernière entrée pour ajouter des entrées de serveur supplémentaires.

NetApp® StorageGRID®

Help ▾

Install

1

License

2

Sites

3

Grid Network

4

Grid Nodes

5

NTP

6

DNS

7

Passwords

8

Summary

Network Time Protocol

Enter the IP addresses for at least four Network Time Protocol (NTP) servers, so that operations performed on separate servers are kept in sync.

Server 1

10.60.248.183

Server 2

10.227.204.142

Server 3

10.235.48.111

Server 4

0.0.0.0

+

3. Sélectionnez **Suivant**.

Informations connexes

Spécifier les informations du serveur DNS

Vous devez spécifier les informations DNS pour votre système StorageGRID , afin de pouvoir accéder aux serveurs externes à l'aide de noms d'hôtes au lieu d'adresses IP.

À propos de cette tâche

Spécification "[Informations sur le serveur DNS](#)" vous permet d'utiliser des noms d'hôtes de nom de domaine complet (FQDN) plutôt que des adresses IP pour les notifications par e-mail et AutoSupport.

Pour garantir un bon fonctionnement, spécifiez deux ou trois serveurs DNS. Si vous spécifiez plus de trois, il est possible que seulement trois soient utilisés en raison de limitations connues du système d'exploitation sur certaines plates-formes. Si vous avez des restrictions de routage dans votre environnement, vous pouvez "[personnaliser la liste des serveurs DNS](#)" pour que les nœuds individuels (généralement tous les nœuds d'un site) utilisent un ensemble différent de trois serveurs DNS maximum.

Si possible, utilisez des serveurs DNS auxquels chaque site peut accéder localement pour garantir qu'un site isolé peut résoudre les noms de domaine complets pour les destinations externes.

Étapes

1. Spécifiez l'adresse IPv4 pour au moins un serveur DNS dans la zone de texte **Serveur 1**.
2. Si nécessaire, sélectionnez le signe plus à côté de la dernière entrée pour ajouter des entrées de serveur supplémentaires.

The screenshot shows the NetApp StorageGRID installation wizard interface. At the top, there's a blue header with "NetApp® StorageGRID®" and a "Help" link. Below the header is a progress bar with eight steps: 1. License, 2. Sites, 3. Grid Network, 4. Grid Nodes, 5. NTP, 6. DNS (highlighted in blue), 7. Passwords, and 8. Summary. Below the progress bar, the "Domain Name Service" section is visible. It contains instructions: "Enter the IP address for at least one Domain Name System (DNS) server, so that server hostnames can be used instead of IP addresses. Specifying at least two DNS servers is recommended. Configuring DNS enables server connectivity, email notifications, and NetApp AutoSupport." Below this, there are two input fields for DNS servers. "Server 1" has the IP address "10.224.223.130" and a minus sign icon. "Server 2" has the IP address "10.224.223.136" and a plus-minus icon.

La meilleure pratique consiste à spécifier au moins deux serveurs DNS. Vous pouvez spécifier jusqu'à six serveurs DNS.

3. Sélectionnez **Suivant**.

Spécifiez les mots de passe du 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.

À propos de cette tâche

Utilisez la page Installer les mots de passe pour spécifier la phrase secrète de provisionnement et le mot de passe de l'utilisateur root de gestion de la grille.

- La phrase secrète de provisionnement est utilisée comme clé de chiffrement et n'est pas stockée par le système StorageGRID .
- Vous devez disposer de la phrase secrète de provisionnement pour les procédures d'installation, d'extension et de maintenance, y compris le téléchargement du package de récupération. Il est donc important de stocker la phrase secrète de provisionnement dans un endroit sûr.
- Vous pouvez modifier la phrase secrète de provisionnement à partir du gestionnaire de grille si vous disposez de la phrase secrète actuelle.
- Le mot de passe de l'utilisateur root de gestion de grille peut être modifié à l'aide du gestionnaire de grille.
- La console de ligne de commande générée aléatoirement et les mots de passe SSH sont stockés dans le `Passwords.txt` fichier dans le package de récupération.

Étapes

1. Dans **Provisioning Passphrase**, saisissez la phrase de passe de provisionnement qui sera requise pour apporter des modifications à la topologie de grille de votre système StorageGRID .

Stockez la phrase secrète de provisionnement dans un endroit sûr.



Si, une fois l'installation terminée, vous souhaitez modifier ultérieurement la phrase secrète de provisionnement, vous pouvez utiliser le gestionnaire de grille. Sélectionnez **CONFIGURATION > Contrôle d'accès > Mots de passe de la grille**.

2. Dans **Confirmer la phrase secrète de provisionnement**, saisissez à nouveau la phrase secrète de provisionnement pour la confirmer.
3. Dans **Mot de passe de l'utilisateur racine de gestion de grille**, saisissez le mot de passe à utiliser pour accéder au gestionnaire de grille en tant qu'utilisateur « root ».

Conservez le mot de passe dans un endroit sûr.

4. Dans **Confirmer le mot de passe de l'utilisateur root**, saisissez à nouveau le mot de passe du gestionnaire de grille pour le confirmer.

NetApp® StorageGRID®
Help

Install

1 License
2 Sites
3 Grid Network
4 Grid Nodes
5 NTP
6 DNS
7 Passwords
8 Summary

Passwords

Enter secure passwords that meet your organization's security policies. A text file containing the command line passwords must be downloaded during the final installation step.

Provisioning
Passphrase

Confirm
Provisioning
Passphrase

Grid Management
Root User
Password

Confirm Root User
Password

☒ Create random command line passwords.

- Si vous installez une grille à des fins de preuve de concept ou de démonstration, décochez éventuellement la case **Créer des mots de passe de ligne de commande aléatoires**.

Pour les déploiements de production, des mots de passe aléatoires doivent toujours être utilisés pour des raisons de sécurité. Cochez **Créer 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 la grille à partir de la ligne de commande à l'aide du compte « root » ou « admin ».



Vous êtes invité à télécharger le fichier du package de récupération(`sgws-recovery-package-id-revision.zip`) après avoir cliqué sur **Installer** sur la page Résumé. Vous devez "[télécharger 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 Recovery Package.

- Cliquez sur **Suivant**.

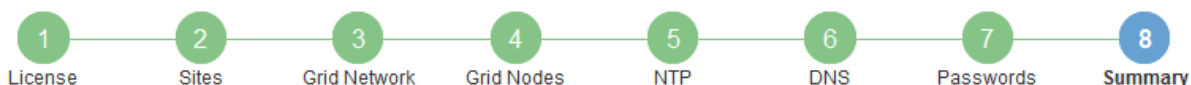
Vérifiez votre configuration et terminez l'installation

Vous devez examiner attentivement les informations de configuration que vous avez saisies pour vous assurer que l'installation se déroule correctement.

Étapes

- Voir la page **Résumé**.

Install



Summary

Verify that all of the grid configuration information is correct, and then click Install. You can view the status of each grid node as it installs. Click the Modify links to go back and change the associated information.

General Settings

Grid Name	Grid1	Modify License
Passwords	Auto-generated random command line passwords	Modify Passwords

Networking

NTP	10.60.248.183 10.227.204.142 10.235.48.111	Modify NTP
DNS	10.224.223.130 10.224.223.136	Modify DNS
Grid Network	172.16.0.0/21	Modify Grid Network

Topology

Topology	Atlanta	Modify Sites	Modify Grid Nodes
	Raleigh		
	dc1-adm1	dc1-g1	dc1-s1
	dc1-s2	dc1-s3	NetApp-SGA

- Vérifiez que toutes les informations de configuration de la grille sont correctes. Utilisez les liens Modifier sur la page Résumé pour revenir en arrière et corriger les erreurs.
- Cliquez sur **Installer**.



Si un nœud est configuré pour utiliser le réseau client, la passerelle par défaut de ce nœud passe du réseau de grille 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 "[Directives de mise en réseau](#)" pour plus de détails.

- Cliquez sur **Télécharger le package 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 package de récupération (.zip), et confirmez que vous pouvez accéder avec succès au contenu de ce fichier. Vous devez télécharger le fichier du package de récupération afin de pouvoir récupérer le système StorageGRID si un ou plusieurs nœuds de grille échouent. 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.

- Vérifiez que vous pouvez extraire le contenu du .zip fichier, puis enregistrez-le dans deux emplacements sûrs, sécurisés et distincts.



Le fichier du package de récupération doit être sécurisé car il contient des clés de chiffrement et des mots de passe qui peuvent être utilisés pour obtenir des données à partir du système StorageGRID.

6. Cochez la case **J'ai téléchargé et vérifié avec succès le fichier du package de récupération**, puis cliquez sur **Suivant**.

Si l'installation est toujours en cours, la page d'état apparaît. Cette page indique la progression de l'installation pour chaque nœud de grille.

Installation Status

If necessary, you may [Download the Recovery Package file](#) again.

Name	IT	Site	IT	Grid Network IPv4 Address	Progress	IT	Stage	IT
dc1-adm1		Site1		172.16.4.215/21			Starting services	
dc1-g1		Site1		172.16.4.216/21			Complete	
dc1-s1		Site1		172.16.4.217/21			Waiting for Dynamic IP Service peers	
dc1-s2		Site1		172.16.4.218/21			Downloading hotfix from primary Admin if needed	
dc1-s3		Site1		172.16.4.219/21			Downloading hotfix from primary Admin if needed	

Lorsque l'étape Terminé est atteinte pour tous les nœuds de grille, la page de connexion au Gestionnaire de grille s'affiche.

7. Sign in au Grid Manager en utilisant l'utilisateur « root » et le mot de passe que vous avez spécifié lors de l'installation.

Consignes post-installation

Une fois le déploiement et la configuration du nœud de grille terminés, suivez ces instructions pour l'adressage DHCP et les modifications de configuration réseau.

- Si DHCP a été 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 lorsque la configuration du réseau de grille est modifiée par DHCP, ce qui peut provoquer des pannes si une modification DHCP affecte plusieurs nœuds en même temps.

- Vous devez utiliser les procédures de modification d'IP si vous souhaitez modifier les adresses IP, les masques de sous-réseau et les passerelles par défaut d'un nœud de grille. Voir "[Configurer les adresses IP](#)".
- Si vous apportez des modifications à la configuration du réseau, notamment au routage et à la passerelle, la connectivité client au nœud d'administration principal et aux autres nœuds de grille peut être perdue. En fonction des modifications réseau appliquées, vous devrez peut-être rétablir ces connexions.

Installation de l'API REST

StorageGRID fournit l'API d'installation StorageGRID pour effectuer des tâches d'installation.

L'API utilise la plate-forme API open source Swagger 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 comment 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 API que vous effectuez à l'aide de la page Web de documentation API 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 API REST inclut l'URL de l'API, une action HTTP, tous les paramètres d'URL obligatoires ou facultatifs et une réponse API attendue.

API d'installation de StorageGRID

L'API d'installation StorageGRID n'est disponible que lorsque vous configurez initialement votre système StorageGRID et si vous devez effectuer une récupération du nœud d'administration principal. L'API d'installation est accessible via HTTPS à partir du gestionnaire de grille.

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 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 répertorier la version du produit et les principales versions 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 du réseau de grille, les mots de passe de la grille et les adresses IP des serveurs NTP et DNS.
- **nodes** — Opérations de configuration au niveau du nœud. Vous pouvez récupérer une liste de nœuds de grille, supprimer un nœud de grille, configurer un nœud de grille, afficher un nœud de grille et réinitialiser la configuration d'un nœud de grille.
- **provision** — Opérations de provisionnement. Vous pouvez démarrer l'opération de provisionnement et afficher l'état de l'opération de provisionnement.
- **récupération** — Opérations de récupération du nœud d'administration principal. Vous pouvez réinitialiser les informations, télécharger le package de récupération, démarrer la récupération et afficher l'état de l'opération de récupération.
- **recovery-package** — Opérations de téléchargement du package de récupération.
- **sites** — Opérations de configuration au niveau du site. Vous pouvez créer, afficher, supprimer et modifier un site.
- **temporary-password** — Opérations sur le mot de passe temporaire pour sécuriser l'API de gestion pendant l'installation.

Informations connexes

["Automatiser l'installation"](#)

Où aller ensuite

Une fois l'installation terminée, effectuez les tâches d'intégration et de configuration requises. Vous pouvez effectuer les tâches facultatives selon vos besoins.

Tâches requises

- ["Créer un compte locataire"](#) pour le protocole client S3 qui sera utilisé pour stocker des objets sur votre

système StorageGRID .

- "[Accès au système de contrôle](#)" en configurant des groupes et des comptes utilisateurs. En option, vous pouvez "[configurer une source d'identité fédérée](#)" (comme Active Directory ou OpenLDAP), afin de pouvoir importer des groupes d'administration et des utilisateurs. Ou, vous pouvez "[créer des groupes et des utilisateurs locaux](#)" .
- Intégrer et tester le "[API S3](#)" applications clientes que vous utiliserez pour télécharger des objets sur votre système StorageGRID .
- "[Configurer les règles de gestion du cycle de vie des informations \(ILM\) et la politique ILM](#)" vous souhaitez utiliser pour protéger les données de l'objet.
- Si votre installation inclut des nœuds de stockage d'appliance, utilisez SANtricity OS pour effectuer les tâches suivantes :
 - Connectez-vous à chaque appliance StorageGRID .
 - Vérifier la réception des données AutoSupport .

Voir "[Configurer le matériel](#)" .

- Consultez et suivez les "[Directives de renforcement du système StorageGRID](#)" pour éliminer les risques de sécurité.
- "[Configurer les notifications par e-mail pour les alertes système](#)" .

Tâches facultatives

- "[Mettre à jour les adresses IP des nœuds de 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.
- "[Configurer les interfaces VLAN](#)" pour isoler et partitionner le trafic réseau, si nécessaire.
- "[Configurer des groupes de haute disponibilité](#)" pour améliorer la disponibilité de la connexion pour les clients Grid Manager, Tenant Manager et S3, si nécessaire.
- "[Configurer les points de terminaison de l'équilibreur de charge](#)" pour la connectivité client S3, si nécessaire.

Résoudre les problèmes d'installation

Si des problèmes surviennent 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` (trouvé 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, consultez ["Collecter les fichiers journaux et les données système"](#).

Informations connexes

["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 les trois sections d'exemple dans un seul fichier, qui regroupera quatre interfaces physiques Linux dans une seule liaison LACP, puis établira trois interfaces VLAN sous-tendant la liaison pour une utilisation comme interfaces StorageGRID Grid, Admin et Client Network.

Interfaces physiques

Notez que les commutateurs aux autres extrémités des liaisons doivent également traiter les quatre ports comme un seul canal de port ou trunk LACP et doivent transmettre 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
```

Installer StorageGRID sur VMware

Démarrage rapide pour l'installation de StorageGRID sur VMware

Suivez ces étapes de haut niveau pour installer un nœud VMware StorageGRID .

1

Préparation

- En savoir plus sur ["Architecture et topologie du réseau StorageGRID"](#) .
- Renseignez-vous sur les spécificités de ["Réseau StorageGRID"](#) .
- Rassemblez et préparez les ["Informations et matériel requis"](#) .
- Installer et configurer ["Hyperviseur VMware vSphere, vCenter et les hôtes ESX"](#) .
- Préparez le nécessaire ["CPU et RAM"](#) .
- Prévoir ["exigences de stockage et de performances"](#) .

2

Déploiement

Déployer des nœuds de grille. Lorsque vous déployez des nœuds de grille, ils sont créés dans le cadre du système StorageGRID et connectés à un ou plusieurs réseaux.

- Utilisez le client Web VMware vSphere, un fichier .vmdk et un ensemble de modèles de fichiers .ovf pour "[déployer les nœuds logiciels en tant que machines virtuelles \(VM\)](#)" sur les serveurs que vous avez préparés à l'étape 1.
- Pour déployer les nœuds d'appliance StorageGRID, suivez les instructions "[Démarrage rapide pour l'installation du matériel](#)".

3

Configuration

Lorsque tous les nœuds ont été déployés, utilisez le gestionnaire de grille pour "[configurer la grille et terminer l'installation](#)".

Automatiser l'installation

Pour gagner du temps et assurer la cohérence, vous pouvez automatiser le déploiement et la configuration des nœuds de grille ainsi que la configuration du système StorageGRID.

- "[Automatiser le déploiement des nœuds de grille à l'aide de VMware vSphere](#)".
- Après avoir déployé les nœuds de grille, "[automatiser la configuration du système StorageGRID](#)" en utilisant le script de configuration Python fourni dans l'archive d'installation.
- "[Automatiser l'installation et la configuration des nœuds de réseau d'appareils](#)".
- Si vous êtes un développeur avancé de déploiements StorageGRID, automatisez l'installation des nœuds de grille en utilisant le "[installation de l'API REST](#)".

Planifier et préparer l'installation sur VMware

Informations et matériel requis

Avant d'installer StorageGRID, rassemblez et préparez les informations et le matériel requis.

Informations requises

Plan de réseau

Quels réseaux comptez-vous connecter à chaque nœud StorageGRID. StorageGRID prend en charge plusieurs réseaux pour la séparation du trafic, la sécurité et la commodité administrative.

Voir le StorageGRID "[Directives de mise en réseau](#)".

Informations sur le réseau

Adresses IP à attribuer à chaque nœud de grille et les adresses IP des serveurs DNS et NTP.

Serveurs pour les nœuds de grille

Identifiez un ensemble de serveurs (physiques, virtuels ou les deux) qui, dans leur ensemble, fournissent suffisamment de ressources pour prendre en charge le nombre et le type de nœuds StorageGRID que vous prévoyez de déployer.



Si votre installation StorageGRID n'utilise pas de nœuds de stockage d'appliance StorageGRID (matériel), vous devez utiliser un stockage RAID matériel avec cache d'écriture alimenté par batterie (BBWC). StorageGRID ne prend pas en charge l'utilisation de réseaux de stockage virtuels (vSAN), de RAID logiciel ou d'aucune protection RAID.

Informations connexes

["Outil de matrice d'interopérabilité NetApp"](#)

Matériel requis

Licence NetApp StorageGRID

Vous devez disposer d'une licence NetApp valide et signée numériquement.



Une licence non-production, qui peut être utilisée pour les grilles de test et de preuve de concept, est incluse dans l'archive d'installation de StorageGRID .

Archive d'installation de StorageGRID

["Téléchargez l'archive d'installation de StorageGRID et extrayez les fichiers"](#) .

Ordinateur portable de service

Le système StorageGRID est installé via un ordinateur portable de service.

L'ordinateur portable de service doit avoir :

- Port réseau
- Client SSH (par exemple, PuTTY)
- ["Navigateur Web pris en charge"](#)

Documentation de StorageGRID

- ["Notes de version"](#)
- ["Instructions pour l'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. En option, vous pouvez vérifier manuellement les fichiers dans le package d'installation.

Étapes

1. Aller à la ["Page de téléchargement NetApp pour StorageGRID"](#) .
2. Sélectionnez le bouton pour télécharger la dernière version ou sélectionnez une autre version dans le menu déroulant et sélectionnez **Aller**.
3. Sign in avec le nom d'utilisateur et le mot de passe de votre compte NetApp .
4. Si une mention d'avertissement/à lire absolument apparaît, lisez-la et cochez la case.



Vous devez appliquer tous les correctifs requis après avoir installé la version StorageGRID . Pour plus d'informations, consultez le ["procédure de correctif dans les instructions de récupération et de maintenance"](#)

5. Lisez le contrat de licence utilisateur final, cochez la case, puis sélectionnez **Accepter et continuer**.
6. Dans la colonne **Installer StorageGRID**, sélectionnez l'archive d'installation .tgz ou .zip pour VMware.



Utilisez le .zip fichier si vous exécutez Windows sur l'ordinateur portable de service.

7. Enregistrez l'archive d'installation.
8. Si vous devez vérifier l'archive d'installation :
 - a. Téléchargez le package de vérification de signature de code StorageGRID . Le nom de fichier de ce package utilise le format `StorageGRID_<version-number>_Code_Signature_Verification_Package.tar.gz` , où `<version-number>` est la version du logiciel StorageGRID .
 - b. Suivez les étapes pour "[vérifier manuellement les fichiers d'installation](#)" .
9. Extraire les fichiers de l'archive d'installation.
10. Choisissez les fichiers dont vous avez besoin.

Les fichiers dont vous avez besoin dépendent de la topologie de grille prévue et de la manière dont vous allez déployer votre système StorageGRID .



Les chemins répertoriés dans le tableau sont relatifs au répertoire de niveau supérieur installé par l'archive d'installation extraite.

Chemin et nom du fichier	Description
	Un fichier texte qui décrit tous les fichiers contenus dans le fichier de téléchargement StorageGRID .
	Une licence gratuite qui ne fournit aucun droit d'assistance pour le produit.
	Le fichier de disque de machine virtuelle utilisé comme modèle pour la création de machines virtuelles de nœuds de grille.
	Le fichier modèle Open Virtualization Format(.ovf) et fichier manifeste(.mf) pour déployer le nœud d'administration principal.
	Le fichier modèle(.ovf) et fichier manifeste(.mf) pour déployer des nœuds d'administration non principaux.
	Le fichier modèle(.ovf) et fichier manifeste(.mf) pour le déploiement de nœuds de passerelle.

Chemin et nom du fichier	Description
	Le fichier modèle(<code>.ovf</code>) et fichier manifeste(<code>.mf</code>) pour déployer des nœuds de stockage basés sur des machines virtuelles.
Outil de script de déploiement	Description
	Un script shell Bash utilisé pour automatiser le déploiement de nœuds de grille virtuels.
	Un exemple de fichier de configuration à utiliser avec le <code>deploy-vsphere-ovftool.sh</code> scénario.
	Un script Python utilisé pour automatiser la configuration d'un système StorageGRID .
	Un script Python utilisé pour automatiser la configuration des appliances StorageGRID .
	Un exemple de script Python que vous pouvez utiliser pour vous connecter à l'API Grid Management lorsque l'authentification unique (SSO) est activée. Vous pouvez également utiliser ce script pour l'intégration de Ping Federate.
	Un exemple de fichier de configuration à utiliser avec le <code>configure-storagegrid.py</code> scénario.
	Un fichier de configuration vierge à utiliser avec le <code>configure-storagegrid.py</code> scénario.
	Un exemple de script Python que vous pouvez utiliser pour vous connecter à l'API Grid Management lorsque l'authentification unique (SSO) est activée à l'aide d'Active Directory ou de Ping Federate.
	Un script d'aide appelé par le compagnon <code>storagegrid-ssoauth-azure.py</code> Script Python pour effectuer des interactions SSO avec Azure.

Chemin et nom du fichier	Description
	Schémas d'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 hors production pour les tests de compatibilité de mise à niveau.

Vérifier manuellement les fichiers d'installation (facultatif)

Si nécessaire, vous pouvez vérifier manuellement les fichiers dans l'archive d'installation de StorageGRID .

Avant de commencer

Tu as ["téléchargé le package de vérification"](#) de la ["Page de téléchargement NetApp pour StorageGRID"](#) .

Étapes

1. Extraire les artefacts du package de vérification :

```
tar -xf StorageGRID_11.9.0_Code_Signature_Verification_Package.tar.gz
```

2. Assurez-vous que ces artefacts ont été extraits :

- Certificat de feuille : Leaf-Cert.pem
- Chaîne de certificats : CA-Int-Cert.pem
- Chaîne de réponse d'horodatage : TS-Cert.pem
- Fichier de somme de contrôle : sha256sum
- Signature de somme de contrôle : sha256sum.sig
- Fichier de réponse d'horodatage : sha256sum.sig.tsr

3. Utilisez la chaîne pour vérifier que le certificat de feuille est valide.

Exemple: `openssl verify -CAfile CA-Int-Cert.pem Leaf-Cert.pem`

Résultat attendu: Leaf-Cert.pem: OK

4. Si l'étape 2 a échoué en raison d'un certificat feuille expiré, utilisez le tsr fichier à vérifier.

Exemple: `openssl ts -CAfile CA-Int-Cert.pem -untrusted TS-Cert.pem -verify -data sha256sum.sig -in sha256sum.sig.tsr`

Les résultats attendus incluent : Verification: OK

5. Créez un fichier de clé publique à partir du certificat feuille.

Exemple: `openssl x509 -pubkey -noout -in Leaf-Cert.pem > Leaf-Cert.pub`

Sortie attendue : *aucun*

6. Utilisez la clé publique pour vérifier le sha256sum déposer contre sha256sum.sig .

Exemple: `openssl dgst -sha256 -verify Leaf-Cert.pub -signature sha256sum.sig
sha256sum`

Résultat attendu: Verified OK

7. Vérifiez le sha256sum contenu du fichier par rapport aux sommes de contrôle nouvellement créées.

Exemple: `sha256sum -c sha256sum`

Résultat attendu: `<filename>: OK`

`<filename>` est le nom du fichier d'archive que vous avez téléchargé.

8. "[Complétez les étapes restantes](#)" pour extraire et choisir les fichiers d'installation appropriés.

Configuration logicielle requise pour VMware

Vous pouvez utiliser une machine virtuelle pour héberger n'importe quel type de nœud StorageGRID . Vous avez besoin d'une machine virtuelle pour chaque nœud de grille.

Hyperviseur VMware vSphere

Vous devez installer VMware vSphere Hypervisor sur un serveur physique préparé. Le matériel doit être configuré correctement (y compris les versions du micrologiciel et les paramètres du BIOS) avant d'installer le logiciel VMware.

- Configurez la mise en réseau dans l'hyperviseur selon les besoins pour prendre en charge la mise en réseau du système StorageGRID que vous installez.

"Directives de mise en réseau"

- Assurez-vous que le magasin de données est suffisamment grand pour les machines virtuelles et les disques virtuels nécessaires pour héberger les nœuds de grille.
- Si vous créez plusieurs banques de données, nommez chaque banque de données afin de pouvoir facilement identifier la banque de données à utiliser pour chaque nœud de grille lorsque vous créez des machines virtuelles.

Exigences de configuration de l'hôte ESX



Vous devez configurer correctement le protocole de temps réseau (NTP) sur chaque hôte ESX. Si l'heure de l'hôte est incorrecte, des effets négatifs, notamment une perte de données, peuvent se produire.

Configuration requise pour VMware

Vous devez installer et configurer VMware vSphere et vCenter avant de déployer les nœuds StorageGRID .

Pour connaître les versions prises en charge des logiciels VMware vSphere Hypervisor et VMware vCenter

Server, consultez le ["Outil de matrice d'interopérabilité NetApp"](#) .

Pour connaître les étapes requises pour installer ces produits VMware, consultez la documentation VMware.

Exigences CPU et RAM

Avant d'installer le logiciel StorageGRID , vérifiez et configurez le matériel afin qu'il soit prêt à prendre en charge le système StorageGRID .

Chaque nœud StorageGRID nécessite les ressources minimales suivantes :

- Cœurs de processeur : 8 par nœud
- RAM : dépend de la RAM totale disponible et de la quantité de logiciels non StorageGRID exécutés sur le système
 - Généralement, au moins 24 Go par nœud et 2 à 16 Go de moins que la RAM totale du système
 - Un minimum de 64 Go pour chaque locataire qui aura environ 5 000 buckets

Les ressources de nœuds basées uniquement sur des métadonnées logicielles doivent correspondre aux ressources de nœuds de stockage existantes. Par exemple:

- Si le site StorageGRID existant utilise des appliances SG6000 ou SG6100, les nœuds de métadonnées uniquement basés sur des logiciels doivent répondre aux exigences minimales suivantes :
 - 128 Go de RAM
 - processeur à 8 cœurs
 - SSD de 8 To ou stockage équivalent pour la base de données Cassandra (rangedb/0)
- Si le site StorageGRID existant utilise des nœuds de stockage virtuels avec 24 Go de RAM, un processeur à 8 cœurs et 3 To ou 4 To de stockage de métadonnées, les nœuds de métadonnées uniquement basés sur un logiciel doivent utiliser des ressources similaires (24 Go de RAM, un processeur à 8 cœurs et 4 To de stockage de métadonnées (rangedb/0)).

Lors de l'ajout d'un nouveau site StorageGRID , la capacité totale des métadonnées du nouveau site doit, au minimum, correspondre aux sites StorageGRID existants et les nouvelles ressources du site doivent correspondre aux nœuds de stockage des sites StorageGRID existants.

VMware prend en charge un nœud par machine virtuelle. Assurez-vous que le nœud StorageGRID ne dépasse pas la RAM physique disponible. Chaque machine virtuelle doit être dédiée à l'exécution de StorageGRID.



Surveillez régulièrement l'utilisation de votre processeur et de votre mémoire pour vous assurer que ces ressources continuent de répondre à votre charge de travail. Par exemple, doubler l'allocation de RAM et de CPU pour les nœuds de stockage virtuels fournirait des ressources similaires à celles fournies pour les nœuds d'appliance StorageGRID . De plus, si la quantité de métadonnées par nœud dépasse 500 Go, envisagez d'augmenter la RAM par nœud à 48 Go ou plus. 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, consultez les instructions de ["administrer"](#) , ["surveillance"](#) , et ["mise à niveau"](#) StorageGRID.

Si l'hyperthreading est activé sur les hôtes physiques sous-jacents, vous pouvez fournir 8 cœurs virtuels (4 cœurs physiques) par nœud. Si l'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 comme hôtes et que vous contrôlez la taille et le nombre de machines virtuelles, vous devez utiliser une seule machine virtuelle pour chaque nœud StorageGRID et dimensionner la machine virtuelle en conséquence.

Voir aussi ["Exigences de stockage et de performances"](#) .

Exigences de stockage et de performances

Vous devez comprendre les exigences de stockage et de performances des nœuds StorageGRID hébergés par des machines virtuelles, afin de pouvoir fournir suffisamment d'espace pour prendre en charge la configuration initiale et l'extension future du stockage.

Exigences de performance

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 qu'ils offrent des performances de disque adéquates 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 la mise en cache en écriture différée activée. Le cache doit être sur un support protégé ou persistant.

Exigences pour les machines virtuelles qui utilisent le stockage NetApp ONTAP

Si vous déployez un nœud StorageGRID en tant que machine virtuelle avec un stockage attribué à partir d'un système NetApp ONTAP , vous avez confirmé qu'aucune stratégie de hiérarchisation FabricPool n'est activée sur le volume. Par exemple, si un nœud StorageGRID s'exécute en tant que machine virtuelle sur un hôte VMware, assurez-vous que le volume qui sauvegarde la banque de données du nœud n'a pas de stratégie de hiérarchisation FabricPool activée. La désactivation de la hiérarchisation FabricPool pour les volumes utilisés avec les nœuds StorageGRID simplifie le dépannage et les opérations de stockage.



N'utilisez jamais FabricPool pour hiérarchiser les données liées à StorageGRID vers StorageGRID lui-même. La hiérarchisation des données StorageGRID vers StorageGRID augmente le dépannage et la complexité opérationnelle.

Nombre de machines virtuelles requises

Chaque site StorageGRID nécessite un minimum de trois nœuds de stockage.

Besoins de stockage par type de nœud

Dans un environnement de production, les machines virtuelles pour les nœuds StorageGRID doivent répondre à différentes exigences, selon les types de nœuds.



Les instantanés de disque ne peuvent pas être utilisés pour restaurer les nœuds de grille. Au lieu de cela, reportez-vous à la ["récupération des nœuds de réseau"](#) procédures pour chaque type de nœud.

Type de nœud	Stockage
Nœud d'administration	100 Go LUN pour le système d'exploitation LUN de 200 Go pour les tables de nœuds d'administration Journal d'audit du nœud d'administration avec un LUN de 200 Go
Nœud de stockage	100 Go LUN pour le système d'exploitation 3 LUN pour chaque nœud de stockage sur cet hôte Remarque : un nœud de stockage peut avoir de 1 à 16 LUN de stockage ; au moins 3 LUN de stockage sont recommandés. Taille minimale par LUN : 4 To Taille maximale du LUN testé : 39 To.
Nœud de stockage (métadonnées uniquement)	100 Go LUN pour le système d'exploitation 1 LUN Taille minimale par LUN : 4 To Taille maximale du LUN testé : 39 To. Remarque : un seul rangedb est requis pour les nœuds de stockage contenant uniquement des métadonnées.
Nœud de passerelle	100 Go LUN pour le système d'exploitation



En fonction du niveau d'audit configuré, de la taille des entrées utilisateur telles que le nom de clé d'objet S3 et de la quantité de données de journal d'audit que vous devez conserver, vous devrez peut-être augmenter la taille du LUN du journal d'audit sur chaque nœud d'administration. En général, une grille génère environ 1 Ko de données d'audit par opération S3, ce qui signifie qu'un LUN de 200 Go prendrait en charge 70 millions d'opérations par jour ou 800 opérations par seconde pendant deux à trois jours.

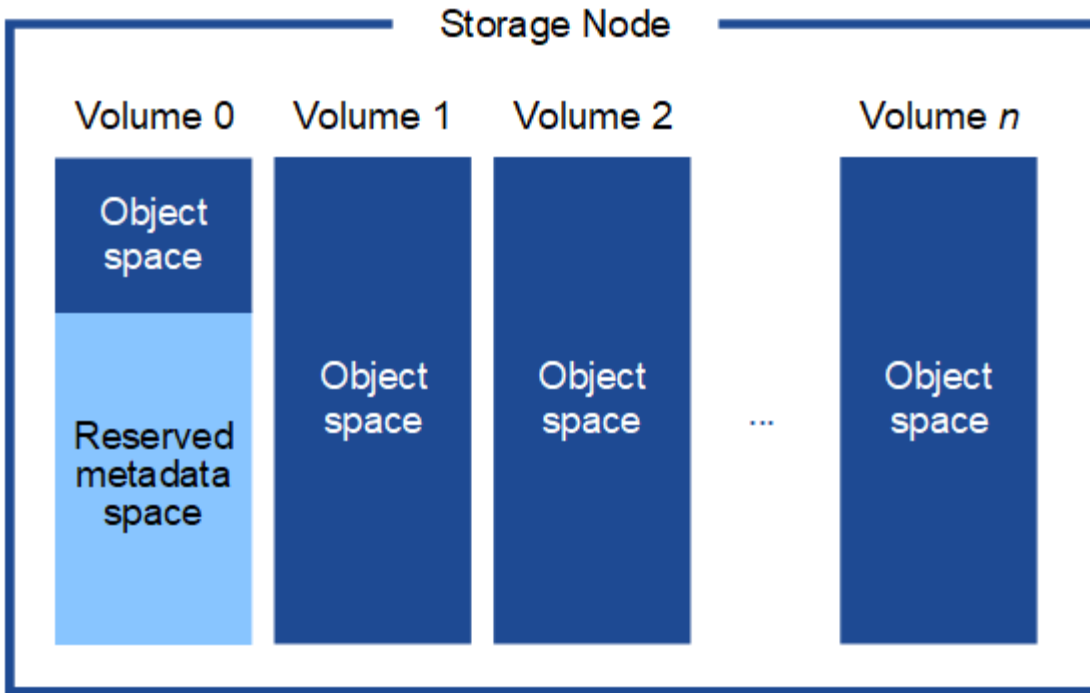
Exigences de stockage pour les nœuds de stockage

Un nœud de stockage basé sur un logiciel peut avoir de 1 à 16 volumes de stockage ; 3 volumes de stockage ou plus sont recommandés. Chaque volume de stockage doit être de 4 To ou plus.



Un nœud de stockage d'appareil peut également avoir jusqu'à 48 volumes de stockage.

Comme indiqué dans la figure, StorageGRID réserve de l'espace pour les métadonnées d'objet sur le volume de stockage 0 de chaque nœud de stockage. Tout espace restant sur le volume de stockage 0 et tous les autres volumes de stockage du nœud de stockage sont utilisés exclusivement pour les données d'objet.



Pour assurer la redondance et protéger les métadonnées des objets contre la perte, StorageGRID stocke trois copies des métadonnées de tous les objets du système sur chaque site. Les trois copies des métadonnées de l'objet sont réparties uniformément sur tous les nœuds de stockage de chaque site.

Lors de l'installation d'une grille avec des nœuds de stockage contenant uniquement des métadonnées, la grille doit également contenir un nombre minimum de nœuds pour le stockage d'objets. Voir "[Types de nœuds de stockage](#)" pour plus d'informations sur les nœuds de stockage contenant uniquement des métadonnées.

- Pour une grille à site unique, au moins deux nœuds de stockage sont configurés pour les objets et les métadonnées.
- Pour une grille multisite, au moins un nœud de stockage par site est configuré pour les objets et les métadonnées.

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 partie de ce nœud de toutes les métadonnées d'objet.

- Au minimum, vous devez attribuer au moins 4 To au volume 0.



Si vous utilisez 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 dans l'état de stockage en lecture seule au démarrage et stocker uniquement 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 sont réservés aux métadonnées.

- Les ressources de nœuds basées uniquement sur des métadonnées logicielles doivent correspondre aux ressources de nœuds de stockage existantes. Par exemple:
 - Si le site StorageGRID existant utilise des appliances SG6000 ou SG6100, les nœuds de métadonnées uniquement basés sur des logiciels doivent répondre aux exigences minimales suivantes :
 - 128 Go de RAM

- processeur à 8 cœurs
- SSD de 8 To ou stockage équivalent pour la base de données Cassandra (rangedb/0)
- Si le site StorageGRID existant utilise des nœuds de stockage virtuels avec 24 Go de RAM, un processeur à 8 cœurs et 3 To ou 4 To de stockage de métadonnées, les nœuds de métadonnées uniquement basés sur un logiciel doivent utiliser des ressources similaires (24 Go de RAM, un processeur à 8 cœurs et 4 To de stockage de métadonnées (rangedb/0)).

Lors de l'ajout d'un nouveau site StorageGRID, la capacité totale des métadonnées du nouveau site doit, au minimum, correspondre aux sites StorageGRID existants et les nouvelles ressources du site doivent correspondre aux nœuds de stockage des sites StorageGRID existants.

- 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.
- Lors de la configuration de 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 de détails, rendez-vous sur ["Gérer le stockage des métadonnées des objets"](#).

Automatiser l'installation (VMware)

Vous pouvez utiliser l'outil VMware OVF pour automatiser le déploiement des nœuds de grille. Vous pouvez également automatiser la configuration de StorageGRID.

Automatiser le déploiement des nœuds de grille

Utilisez l'outil VMware OVF pour automatiser le déploiement des nœuds de grille.

Avant de commencer

- Vous avez accès à un système Linux/Unix avec Bash 3.2 ou version ultérieure.
- Vous disposez de VMware vSphere avec vCenter
- Vous avez installé et correctement configuré VMware OVF Tool 4.1.
- Vous connaissez le nom d'utilisateur et le mot de passe pour accéder à VMware vSphere à l'aide de l'outil OVF
- Vous disposez des autorisations suffisantes pour déployer des machines virtuelles à partir de fichiers OVF et les mettre sous tension, ainsi que des autorisations pour créer des volumes supplémentaires à attacher aux machines virtuelles. Voir le `ovftool` documentation pour plus de détails.
- Vous connaissez l'URL de l'infrastructure virtuelle (VI) de l'emplacement dans vSphere où vous souhaitez déployer les machines virtuelles StorageGRID. Cette URL sera 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 le `ovftool` documentation pour plus de détails).



Si vous effectuez un déploiement sur une vApp, les machines virtuelles ne démarreront pas automatiquement la première fois et vous devrez les mettre sous tension manuellement.

- Vous avez collecté toutes les informations requises pour le fichier de configuration de déploiement. Voir "[Collectez des informations sur votre environnement de déploiement](#)" pour information.
- Vous avez accès aux fichiers suivants à partir de l'archive d'installation de VMware pour StorageGRID:

Nom de fichier	Description
NetApp-SG-version-SHA.vmdk	Le fichier de disque de machine virtuelle utilisé comme modèle pour la création de machines virtuelles de nœuds de grille. Remarque : ce fichier doit se trouver dans le même dossier que le <code>.ovf</code> et <code>.mf</code> fichiers.
vsphere-primary-admin.ovf vsphere-primary-admin.mf	Le fichier modèle Open Virtualization Format (<code>.ovf</code>) et fichier manifeste (<code>.mf</code>) pour déployer le nœud d'administration principal.
vsphere-non-primary-admin.ovf vsphere-non-primary-admin.mf	Le fichier modèle (<code>.ovf</code>) et fichier manifeste (<code>.mf</code>) pour déployer des nœuds d'administration non principaux.
passerelle vsphere.ovf passerelle vsphere.mf	Le fichier modèle (<code>.ovf</code>) et fichier manifeste (<code>.mf</code>) pour le déploiement de nœuds de passerelle.
vsphere-storage.ovf vsphere-storage.mf	Le fichier modèle (<code>.ovf</code>) et fichier manifeste (<code>.mf</code>) pour déployer des nœuds de stockage basés sur des machines virtuelles.
déployer-vsphere-ovftool.sh	Le script shell Bash utilisé pour automatiser le déploiement de nœuds de grille virtuels.
déployer-vsphere-ovftool-sample.ini	L'exemple de fichier de configuration à utiliser avec le <code>deploy-vsphere-ovftool.sh</code> scénario.

Définissez le fichier de configuration pour votre déploiement

Vous spécifiez les informations nécessaires pour déployer des nœuds de grille virtuelle pour StorageGRID dans un fichier de configuration, qui est utilisé par le `deploy-vsphere-ovftool.sh` Script Bash. Vous pouvez modifier un exemple de fichier de configuration, de sorte que vous n'avez pas à créer le fichier à partir de zéro.

Étapes

1. Faire une copie du fichier de configuration d'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. Ouvrir `deploy-vsphere-ovftool.ini`.
3. Saisissez toutes les informations requises pour déployer les nœuds de grille virtuelle VMware.

Voir [Paramètres du fichier de configuration](#) pour information.

4. Lorsque vous avez saisi et vérifié toutes les informations nécessaires, enregistrez et fermez le fichier.

Paramètres du fichier de configuration

Le `deploy-vmware-ovftool.ini` Le fichier de configuration contient les paramètres requis pour déployer des nœuds de grille virtuels.

Le fichier de configuration répertorie d'abord les paramètres globaux, puis répertorie les paramètres spécifiques au nœud dans des sections définies par le nom du nœud. Lorsque le fichier est utilisé :

- Les *paramètres globaux* sont appliqués à tous les nœuds de la grille.
- Les *paramètres spécifiques au nœud* remplacent 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 des nœuds individuels.

- **OVFTOOL_ARGUMENTS**: Vous pouvez spécifier OVFTOOL_ARGUMENTS comme paramètres globaux ou 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 pour arrêter et remplacer les machines virtuelles existantes.



Vous devez déployer des nœuds sur différents magasins de données et spécifier OVFTOOL_ARGUMENTS pour chaque nœud, plutôt que globalement.

- **SOURCE** : Le chemin d'accès au modèle de machine virtuelle StorageGRID(.vmdk) fichier et le .ovf et .mf fichiers pour les nœuds de grille individuels. La valeur par défaut est le répertoire actuel.

```
SOURCE = /downloads/StorageGRID-Webscale-version/vsphere
```

- **CIBLE** : L'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** : La méthode utilisée pour acquérir des adresses IP, soit STATIQUE, soit DHCP. La valeur par défaut est STATIC. Si tous ou la plupart des nœuds utilisent la même méthode pour acquérir des adresses IP, vous pouvez spécifier cette méthode ici. Vous pouvez ensuite remplacer le paramètre global en spécifiant des paramètres différents pour un ou plusieurs nœuds individuels. Par exemple:

```
GRID_NETWORK_CONFIG = STATIC
```

- **GRID_NETWORK_TARGET** : le nom d'un réseau VMware existant à utiliser pour le réseau Grid. Si tous ou la plupart des nœuds utilisent le même nom de réseau, vous pouvez le spécifier ici. Vous pouvez ensuite remplacer le paramètre global en spécifiant des paramètres différents pour un ou plusieurs nœuds individuels. Par exemple:

```
GRID_NETWORK_TARGET = SG Admin Network
```

- **GRID_NETWORK_MASK** : Le masque de réseau pour le réseau Grid. Si tous ou la plupart des nœuds utilisent le même masque de réseau, vous pouvez le spécifier ici. Vous pouvez ensuite remplacer le paramètre global en spécifiant des paramètres différents pour un ou plusieurs nœuds individuels. Par exemple:

```
GRID_NETWORK_MASK = 255.255.255.0
```

- **GRID_NETWORK_GATEWAY** : La passerelle réseau pour le réseau Grid. Si tous ou la plupart des nœuds utilisent la même passerelle réseau, vous pouvez le spécifier ici. Vous pouvez ensuite remplacer le paramètre global en spécifiant des paramètres différents 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 électrique. Si spécifié, la valeur doit être comprise entre 1280 et 9216. Par exemple:

```
GRID_NETWORK_MTU = 9000
```

Si omis, 1400 est utilisé.

Si vous souhaitez utiliser des trames jumbo, définissez le MTU sur une valeur adaptée aux trames jumbo, telle que 9 000. Sinon, conservez la valeur par défaut.



La valeur MTU du réseau doit correspondre à la valeur configurée sur le port du commutateur virtuel dans vSphere auquel le nœud est connecté. Dans le cas contraire, des problèmes de performances du réseau ou une perte de paquets pourraient survenir.



Pour des performances réseau optimales, tous les nœuds doivent être configurés avec des valeurs MTU similaires sur leurs interfaces Grid Network. L'alerte **Incompatibilité MTU du réseau de grille** est déclenchée s'il existe une différence significative dans les paramètres MTU du réseau de grille sur des nœuds individuels. Les valeurs MTU ne doivent pas nécessairement être les mêmes pour tous les types de réseaux.

- **ADMIN_NETWORK_CONFIG** : La méthode utilisée pour acquérir les adresses IP, soit DÉSACTIVÉE, STATIQUE ou DHCP. La valeur par défaut est DÉSACTIVÉE. Si tous ou la plupart des nœuds utilisent la

même méthode pour acquérir des adresses IP, vous pouvez spécifier cette méthode ici. Vous pouvez ensuite remplacer le paramètre global en spécifiant des paramètres différents pour un ou plusieurs nœuds individuels. Par exemple:

```
ADMIN_NETWORK_CONFIG = STATIC
```

- **ADMIN_NETWORK_TARGET** : le nom d'un réseau VMware existant à utiliser pour le réseau d'administration. Ce paramètre est requis sauf si le réseau d'administration est désactivé. Si tous ou la plupart des nœuds utilisent le même nom de réseau, vous pouvez le spécifier ici. Contrairement au réseau Grid, tous les nœuds n'ont pas besoin d'être connectés au même réseau d'administration. Vous pouvez ensuite remplacer le paramètre global en spécifiant des paramètres différents pour un ou plusieurs nœuds individuels. Par exemple:

```
ADMIN_NETWORK_TARGET = SG Admin Network
```

- **ADMIN_NETWORK_MASK** : Le masque réseau pour le réseau d'administration. Ce paramètre est requis si vous utilisez une adresse IP statique. Si tous ou la plupart des nœuds utilisent le même masque de réseau, vous pouvez le spécifier ici. Vous pouvez ensuite remplacer le paramètre global en spécifiant des paramètres différents pour un ou plusieurs nœuds individuels. Par exemple:

```
ADMIN_NETWORK_MASK = 255.255.255.0
```

- **ADMIN_NETWORK_GATEWAY** : la passerelle réseau pour le réseau d'administration. Ce paramètre est requis si vous utilisez une adresse 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 ou la plupart des nœuds utilisent la même passerelle réseau, vous pouvez le spécifier ici. Vous pouvez ensuite remplacer le paramètre global en spécifiant des paramètres différents pour un ou plusieurs nœuds individuels. Par exemple:

```
ADMIN_NETWORK_GATEWAY = 10.3.0.1
```

- **ADMIN_NETWORK_ESL** : la liste des sous-réseaux externes (routes) pour le réseau d'administration, spécifiée sous la forme d'une liste séparée par des virgules de destinations de route CIDR. Si tous ou la plupart des nœuds utilisent la même liste de sous-réseaux externes, vous pouvez le spécifier ici. Vous pouvez ensuite remplacer le paramètre global en spécifiant des paramètres différents 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. L'unité de transmission maximale (MTU) sur le réseau d'administration. Ne spécifiez pas si ADMIN_NETWORK_CONFIG = DHCP. Si spécifié, la valeur doit être comprise entre 1280 et 9216. Si omis, 1400 est utilisé. Si vous souhaitez utiliser des trames jumbo, définissez le MTU sur une valeur adaptée aux trames jumbo, telle que 9 000. Sinon, conservez la valeur par défaut. Si tous ou la plupart des nœuds utilisent le même MTU pour le réseau d'administration, vous pouvez le spécifier ici. Vous pouvez ensuite remplacer le paramètre global en spécifiant des paramètres différents pour un ou plusieurs nœuds individuels. Par exemple:

```
ADMIN_NETWORK_MTU = 8192
```

- **CLIENT_NETWORK_CONFIG** : La méthode utilisée pour acquérir les adresses IP, soit DÉSACTIVÉE, STATIQUE ou DHCP. La valeur par défaut est DÉSACTIVÉE. Si tous ou la plupart des nœuds utilisent la même méthode pour acquérir des adresses IP, vous pouvez spécifier cette méthode ici. Vous pouvez ensuite remplacer le paramètre global en spécifiant des paramètres différents pour un ou plusieurs nœuds individuels. Par exemple:

```
CLIENT_NETWORK_CONFIG = STATIC
```

- **CLIENT_NETWORK_TARGET** : le 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 ou la plupart des nœuds utilisent le même nom de réseau, vous pouvez le spécifier ici. Contrairement au réseau Grid, tous les nœuds n'ont pas besoin d'être connectés au même réseau client. Vous pouvez ensuite remplacer le paramètre global en spécifiant des paramètres différents pour un ou plusieurs nœuds individuels. Par exemple:

```
CLIENT_NETWORK_TARGET = SG Client Network
```

- **CLIENT_NETWORK_MASK** : Le masque réseau pour le réseau client. Ce paramètre est requis si vous utilisez une adresse IP statique. Si tous ou la plupart des nœuds utilisent le même masque de réseau, vous pouvez le spécifier ici. Vous pouvez ensuite remplacer le paramètre global en spécifiant des paramètres différents pour un ou plusieurs nœuds individuels. Par exemple:

```
CLIENT_NETWORK_MASK = 255.255.255.0
```

- **CLIENT_NETWORK_GATEWAY** : la passerelle réseau pour le réseau client. Ce paramètre est requis si vous utilisez une adresse IP statique. Si tous ou la plupart des nœuds utilisent la même passerelle réseau, vous pouvez le spécifier ici. Vous pouvez ensuite remplacer le paramètre global en spécifiant des paramètres différents pour un ou plusieurs nœuds individuels. Par exemple:

```
CLIENT_NETWORK_GATEWAY = 10.4.0.1
```

- **CLIENT_NETWORK_MTU** : Facultatif. L'unité de transmission maximale (MTU) sur le réseau client. Ne spécifiez pas si CLIENT_NETWORK_CONFIG = DHCP. Si spécifié, la valeur doit être comprise entre 1280 et 9216. Si omis, 1400 est utilisé. Si vous souhaitez utiliser des trames jumbo, définissez le MTU sur une valeur adaptée aux trames jumbo, telle que 9 000. Sinon, conservez la valeur par défaut. Si tous ou la plupart des nœuds utilisent le même MTU pour le réseau client, vous pouvez le spécifier ici. Vous pouvez ensuite remplacer le paramètre global en spécifiant des paramètres différents pour un ou plusieurs nœuds individuels. Par exemple:

```
CLIENT_NETWORK_MTU = 8192
```

- **PORT_REMAP** : remappe tout port utilisé par un nœud pour les communications internes du nœud de grille ou les communications externes. Le remappage des ports est nécessaire si les politiques de réseau

d'entreprise restreignent un ou plusieurs ports utilisés par StorageGRID. Pour la liste des ports utilisés par StorageGRID, voir les communications internes des nœuds de grille et les communications externes dans "[Directives de mise en réseau](#)".



Ne remappez pas les ports que vous prévoyez d'utiliser pour configurer les points de terminaison de l'équilibreur de charge.



Si seul PORT_REMAP est défini, le mappage que vous spécifiez est utilisé pour les communications entrantes et sortantes. Si PORT_REMAP_INBOUND est également spécifié, PORT_REMAP 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 grille, administrateur ou client, et le protocole est TCP ou UDP.

Par exemple:

```
PORT_REMAP = client/tcp/18082/443
```

Si utilisé seul, cet exemple de paramètre mappe symétriquement les communications entrantes et sortantes pour le nœud de grille du port 18082 au port 443. Si utilisé conjointement avec PORT_REMAP_INBOUND, cet exemple de paramètre mappe les communications sortantes du port 18082 au port 443.

Vous pouvez également remapper plusieurs ports à l'aide d'une liste séparée par des virgules.

Par exemple:

```
PORT_REMAP = client/tcp/18082/443, client/tcp/18083/80
```

- **PORT_REMAP_INBOUND** : remappe les communications entrantes pour le port spécifié. Si vous spécifiez PORT_REMAP_INBOUND mais ne spécifiez pas de valeur pour PORT_REMAP, les communications sortantes pour le port restent inchangées.



Ne remappez pas les ports que vous prévoyez d'utiliser pour configurer les points de terminaison 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 grille, administrateur ou client, et le protocole est TCP ou UDP.

Par exemple:

```
PORT_REMAP_INBOUND = client/tcp/443/18082
```

Cet exemple prend le trafic envoyé au port 443 pour passer un pare-feu interne et le dirige vers le port 18082, où le nœud de grille écoute les requêtes S3.

Vous pouvez également remapper plusieurs ports entrants à l'aide d'une liste séparée par des virgules.

Par exemple:

```
PORT_REMAP_INBOUND = grid/tcp/3022/22, admin/tcp/3022/22
```

- **TEMPORARY_PASSWORD_TYPE** : le type de mot de passe d'installation temporaire à utiliser lors de l'accès à la console de la machine virtuelle ou à l'API d'installation StorageGRID , ou à l'aide de SSH, avant que le nœud ne rejoigne la grille.



Si tous ou la plupart des nœuds utilisent le même type de mot de passe d'installation temporaire, spécifiez le type dans la section des paramètres globaux. Ensuite, utilisez éventuellement un paramètre différent pour un nœud individuel. Par exemple, si vous sélectionnez **Utiliser un mot de passe personnalisé** globalement, vous pouvez utiliser **CUSTOM_TEMPORARY_PASSWORD=<mot de passe>** pour définir le mot de passe pour chaque nœud.

TEMPORARY_PASSWORD_TYPE peut être l'un des suivants :

- **Utiliser le nom du nœud** : le nom du nœud est utilisé comme mot de passe d'installation temporaire et fournit l'accès à la console de la machine virtuelle, à l'API d'installation StorageGRID et à SSH.
- **Désactiver le mot de passe** : Aucun mot de passe d'installation temporaire ne sera utilisé. Si vous devez accéder à la machine virtuelle pour déboguer les problèmes d'installation, consultez ["Résoudre les problèmes d'installation"](#) .
- **Utiliser un mot de passe personnalisé**: La valeur fournie avec **CUSTOM_TEMPORARY_PASSWORD=<password>** est utilisée comme mot de passe d'installation temporaire et donne accès à la console VM, à l'API d'installation StorageGRID et à SSH.



En option, vous pouvez omettre le paramètre **TEMPORARY_PASSWORD_TYPE** et spécifier uniquement **CUSTOM_TEMPORARY_PASSWORD=<mot de passe>**.

- **CUSTOM_TEMPORARY_PASSWORD=<mot de passe>** Facultatif. Le mot de passe temporaire à utiliser lors de l'installation lors de l'accès à la console VM, à l'API d'installation StorageGRID et à SSH. Ignorez si **TEMPORARY_PASSWORD_TYPE** est défini sur **Utiliser le nom du nœud** ou **Désactiver le mot de passe**.

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 gestionnaire de grille. Vous pouvez remplacer cette valeur en spécifiant le paramètre facultatif **NODE_NAME** pour le nœud.
- **NODE_TYPE** : VM_Admin_Node, VM_Storage_Node ou VM_API_Gateway_Node
- **STORAGE_TYPE** : combiné, données ou métadonnées. Ce paramètre facultatif pour les nœuds de stockage est défini par défaut sur combiné (données et métadonnées) s'il n'est pas spécifié. Pour plus d'informations, consultez la section ["Types de nœuds de stockage"](#) .
- **GRID_NETWORK_IP** : l'adresse IP du nœud sur le réseau Grid.
- **ADMIN_NETWORK_IP** : l'adresse IP du nœud sur le réseau d'administration. Requis uniquement si le nœud est connecté au réseau d'administration et que **ADMIN_NETWORK_CONFIG** est défini sur **STATIC**.

- **CLIENT_NETWORK_IP** : l'adresse IP du nœud sur le réseau client. Obligatoire uniquement si le nœud est connecté au réseau client et que CLIENT_NETWORK_CONFIG pour ce nœud est défini sur STATIC.
- **ADMIN_IP** : l'adresse IP du nœud d'administration principal sur le réseau Grid. Utilisez la valeur que vous spécifiez comme GRID_NETWORK_IP pour le nœud d'administration principal. Si vous omettez ce paramètre, le nœud tente de découvrir l'adresse IP du nœud d'administration principal à l'aide de mDNS. Pour plus d'informations, consultez la section "[Comment les nœuds de grille découvrent 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 attaché au réseau d'administration 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** : nœud VM_Admin_Node
- **ADMIN_ROLE** : Principal

Cet exemple d'entrée concerne un nœud d'administration principal présent sur les trois réseaux :

```
[DC1-ADM1]
  ADMIN_ROLE = Primary
  NODE_TYPE = VM_Admin_Node
  TEMPORARY_PASSWORD_TYPE = Use custom password
  CUSTOM_TEMPORARY_PASSWORD = Passw0rd

  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 se voient attribuer 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 DISK. Par exemple:

```
DISK = INSTANCES=2, CAPACITY=300
```



Pour les nœuds d'administration, les INSTANCES doivent toujours être égales à 2.

Nœud de stockage

Le paramètre supplémentaire suivant est requis pour les nœuds de stockage :

- **NODE_TYPE** : nœud de stockage VM

Cet exemple d'entrée concerne un nœud de stockage qui se trouve sur les réseaux de grille et 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 de grille.

```
[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 où la politique de réseau d'entreprise du client stipule qu'une application client S3 est uniquement autorisée à accéder au nœud de stockage à l'aide du port 80 ou 443. L'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
```

Les paramètres supplémentaires suivants sont facultatifs pour les nœuds de stockage :

- **DISQUE** : Par défaut, les nœuds de stockage se voient attribuer trois disques de 4 To pour l'utilisation de RangeDB. Vous pouvez augmenter ces paramètres avec le paramètre DISK. Par exemple:

```
DISK = INSTANCES=16, CAPACITY=4096
```

- **STORAGE_TYPE** : Par défaut, tous les nouveaux nœuds de stockage sont configurés pour stocker à la fois les données d'objet et les métadonnées, appelés nœuds de stockage *combinés*. Vous pouvez modifier le type de nœud de stockage pour stocker uniquement des données ou des métadonnées avec le paramètre **STORAGE_TYPE**. Par exemple:

```
STORAGE_TYPE = data
```

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 de réseau client n'a été spécifié dans la section globale du fichier de configuration, ils doivent donc être spécifiés 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 principal

Les paramètres supplémentaires suivants sont requis pour les nœuds d'administration non principaux :

- **NODE_TYPE** : nœud VM_Admin_Node
- **ADMIN_ROLE** : Non principal

Cet exemple d'entrée concerne un nœud d'administration non principal qui ne se trouve 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 principaux :

- **DISQUE** : Par défaut, les nœuds d'administration se voient attribuer 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 DISK. Par exemple:

```
DISK = INSTANCES=2, CAPACITY=300
```



Pour les nœuds d'administration, les INSTANCES doivent toujours être égales à 2.

Exécutez le script Bash

Vous pouvez utiliser le `deploy-vsphere-ovftool.sh` Script Bash et fichier de configuration `deploy-vsphere-ovftool.ini` que vous avez modifiés pour automatiser le déploiement des nœuds 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 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 réexécutez le script Bash uniquement pour ce nœud.

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 « Réussi ».

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

Après avoir déployé les nœuds de grille, 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 de fichier	Description
configure-storagegrid.py	Script Python utilisé pour automatiser la configuration

Nom de fichier	Description
configure-storagegrid.sample.json	Exemple de fichier de configuration à utiliser avec le script
configure-storagegrid.blank.json	Fichier de configuration vide à utiliser avec le script

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

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



Vous pouvez également configurer le système à l'aide du gestionnaire de grille 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 plan de relance `.zip` Le fichier est généré pendant le processus de configuration et il est téléchargé dans le répertoire dans lequel vous exécutez le processus d'installation et de configuration. Vous devez sauvegarder le fichier du package de récupération afin de pouvoir récupérer le système StorageGRID si un ou plusieurs nœuds de grille échouent. Par exemple, copiez-le vers un emplacement réseau sécurisé et sauvegardé et vers un emplacement de stockage cloud sécurisé.



Le fichier du package de récupération doit être sécurisé car il contient des clés de chiffrement et des mots de passe qui peuvent être utilisés pour obtenir des données à partir du système StorageGRID .

Si vous avez spécifié que des mots de passe aléatoires doivent être générés, ouvrez le `Passwords.txt`

fichier et recherchez les mots de passe requis pour accéder à votre 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 connexes

- ["Accéder au gestionnaire de grille"](#)
- ["Installation de l'API REST"](#)

Déployer des nœuds de grille de machines virtuelles (VMware)

Collectez des informations sur votre environnement de déploiement

Avant de déployer des nœuds de grille, vous devez collecter des informations sur votre configuration réseau et votre environnement VMware.



Il est plus efficace d'effectuer une seule installation de tous les nœuds, plutôt que d'installer certains nœuds maintenant et certains nœuds plus tard.

Informations 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 ; et les types de volumes de stockage que vous prévoyez d'utiliser pour les nœuds de stockage.

Vous devez collecter des informations sur votre environnement VMware, notamment les suivantes :

- Le nom d'utilisateur et le mot de passe d'un compte VMware vSphere disposant des autorisations appropriées pour terminer le déploiement.
- Informations de configuration de l'hôte, de la banque de données et du réseau pour chaque machine virtuelle de nœud StorageGRID .



VMware Live vMotion provoque un saut de l'heure de l'horloge de la machine virtuelle et n'est pas pris en charge pour les nœuds de grille de tout type. Bien que rares, des heures d'horloge incorrectes peuvent entraîner une perte de données ou des mises à jour de configuration.

Informations sur le réseau de grille

Vous devez collecter des informations sur le réseau VMware créé pour le réseau StorageGRID Grid

(obligatoire), notamment :

- Le nom du réseau.
- La méthode utilisée pour attribuer des adresses IP, statiques ou DHCP.
 - Si vous utilisez des adresses IP statiques, les détails de mise en réseau requis pour chaque nœud de grille (adresse IP, passerelle, masque de réseau).
 - Si vous utilisez DHCP, l'adresse IP du nœud d'administration principal sur le réseau de grille. Voir ["Comment les nœuds de grille découvrent le nœud d'administration principal"](#) pour plus d'informations.

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 :

- Le nom du réseau.
- La méthode utilisée pour attribuer des adresses IP, statiques ou DHCP.
 - Si vous utilisez des adresses IP statiques, les détails de mise en réseau requis pour chaque nœud de grille (adresse IP, passerelle, masque de réseau).
 - Si vous utilisez DHCP, l'adresse IP du nœud d'administration principal sur le réseau de grille. Voir ["Comment les nœuds de grille découvrent le nœud d'administration principal"](#) pour plus d'informations.
- La liste des sous-réseaux externes (ESL) pour le réseau d'administration.

Informations sur le réseau client

Pour les nœuds qui seront connectés au réseau client StorageGRID facultatif, vous devez collecter des informations sur le réseau VMware créé pour ce réseau, notamment :

- Le nom du réseau.
- La méthode utilisée pour attribuer des adresses IP, statiques ou DHCP.
- Si vous utilisez des adresses IP statiques, les détails de mise en réseau requis pour chaque nœud de grille (adresse IP, passerelle, masque de réseau).

Informations sur les interfaces supplémentaires

Vous pouvez éventuellement ajouter des interfaces de jonction ou d'accès à la machine virtuelle dans vCenter après avoir installé le nœud. Par exemple, vous souhaitez peut-être ajouter une interface de jonction à un nœud d'administration ou de passerelle, afin de pouvoir utiliser des interfaces VLAN pour séparer le trafic appartenant à différentes applications ou locataires. Ou, vous souhaitez peut-être ajouter une interface d'accès à utiliser dans un groupe de haute disponibilité (HA).

Les interfaces que vous ajoutez sont affichées sur la page Interfaces VLAN et sur la page Groupes HA dans le Gestionnaire de grille.

- Si vous ajoutez une interface trunk, configurez une ou plusieurs interfaces VLAN pour chaque nouvelle interface parent. Voir ["configurer les interfaces VLAN"](#).
- Si vous ajoutez une interface d'accès, vous devez l'ajouter directement aux groupes HA. Voir ["configurer des groupes de haute disponibilité"](#).

Volumes de stockage pour les nœuds de stockage virtuels

Vous devez collecter les informations suivantes pour les nœuds de stockage basés sur une machine virtuelle :

- Le nombre et la taille des volumes de stockage (LUN) que vous prévoyez d'ajouter. Voir ["Exigences de stockage et de performances"](#) .

Informations sur la configuration du réseau

Vous devez collecter des informations pour configurer votre grille :

- Licence de réseau
- Adresses IP du serveur NTP (Network Time Protocol)
- Adresses IP du serveur DNS

Comment les nœuds de grille découvrent le nœud d'administration principal

Les nœuds de grille communiquent avec le nœud d'administration principal pour la configuration et la gestion. Chaque nœud de grille doit connaître l'adresse IP du nœud d'administration principal sur le réseau de grille.

Pour garantir 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 grille découvre automatiquement la valeur. La découverte 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 est réalisée à l'aide d'un système de noms de domaine multidiffusion (mDNS). Lorsque le nœud d'administration principal démarre pour la première fois, il publie son adresse IP à l'aide de mDNS. D'autres nœuds sur le même sous-réseau peuvent alors interroger l'adresse IP et l'acquérir automatiquement. Cependant, étant donné que le trafic IP multidiffusion n'est normalement pas routable sur les sous-réseaux, les nœuds des autres sous-réseaux ne peuvent pas acquérir directement l'adresse IP du nœud d'administration principal.

Si vous utilisez la découverte automatique :



- Vous devez inclure le paramètre ADMIN_IP pour au moins un nœud de grille sur tous les sous-réseaux auxquels le nœud d'administration principal n'est pas directement connecté. Ce nœud de grille publiera ensuite l'adresse IP du nœud d'administration principal pour que les autres nœuds du sous-réseau puissent la découvrir avec mDNS.
- Assurez-vous que votre infrastructure réseau prend en charge le passage du trafic IP multidiffusion au sein d'un sous-réseau.

Déployer un nœud StorageGRID en tant que machine virtuelle

Vous utilisez VMware vSphere Web Client pour déployer chaque nœud de grille en tant que machine virtuelle. Lors du déploiement, chaque nœud de grille est créé et connecté à un ou plusieurs réseaux StorageGRID .

Si vous devez déployer des nœuds de stockage d'appliance StorageGRID , consultez ["Déployer le nœud de stockage de l'appliance"](#) .

En option, vous pouvez remapper les ports du nœud ou augmenter les paramètres du processeur ou de la mémoire du nœud avant de le mettre sous tension.

Avant de commencer

- Vous avez examiné comment faire["planifier et préparer l'installation"](#) , et vous comprenez les exigences en matière de logiciels, de processeur et de RAM, ainsi que de stockage et de performances.
- Vous connaissez VMware vSphere Hypervisor et avez de l'expérience dans le déploiement de machines virtuelles 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 de StorageGRID pour VMware.



Si vous déployez le nouveau nœud dans le cadre d'une opération d'extension ou de récupération, vous devez utiliser la version de StorageGRID actuellement en cours d'exécution sur la grille.

- Vous disposez du disque de machine virtuelle StorageGRID(`.vmdk`) déposer:

```
NetApp-SG-version-SHA.vmdk
```

- Vous avez le `.ovf` et `.mf` fichiers pour chaque type de nœud de grille que vous déployez :

Nom de fichier	Description
vsphere-primary-admin.ovf vsphere-primary-admin.mf	Le fichier modèle et le fichier manifeste pour le nœud d'administration principal.
vsphere-non-primary-admin.ovf vsphere-non-primary-admin.mf	Le fichier modèle et le fichier manifeste pour un nœud d'administration non principal.
vsphere-storage.ovf vsphere-storage.mf	Le fichier modèle et le fichier manifeste pour un nœud de stockage.
passerelle vsphere.ovf passerelle vsphere.mf	Le fichier modèle et le fichier manifeste pour un nœud de passerelle.

- Le `.vmdk` , `.ovf` , et `.mf` les fichiers sont tous dans le même répertoire.
- Vous avez un plan pour minimiser les domaines de défaillance. Par exemple, vous ne devez pas déployer tous les nœuds de passerelle sur un seul hôte vSphere ESXi.



Dans un déploiement de production, n'exécutez pas plus d'un nœud de stockage sur une seule machine virtuelle. N'exécutez pas plusieurs machines virtuelles sur le même hôte ESXi si cela risque de créer un problème de domaine de défaillance inacceptable.

- Si vous déployez un nœud dans le cadre d'une opération d'extension ou de récupération, vous disposez des ["instructions pour étendre un système StorageGRID"](#) ou le ["instructions de récupération et d'entretien"](#).
- Si vous déployez un nœud StorageGRID en tant que machine virtuelle avec un stockage attribué à partir d'un système NetApp ONTAP, vous avez confirmé qu'aucune stratégie de hiérarchisation FabricPool n'est activée sur le volume. Par exemple, si un nœud StorageGRID s'exécute en tant que machine virtuelle sur un hôte VMware, assurez-vous que le volume qui sauvegarde la banque de données du nœud n'a pas de stratégie de hiérarchisation FabricPool activée. La désactivation de la hiérarchisation FabricPool pour les volumes utilisés avec les nœuds StorageGRID simplifie le dépannage et les opérations de stockage.



N'utilisez jamais FabricPool pour hiérarchiser les données liées à StorageGRID vers StorageGRID lui-même. La hiérarchisation des données StorageGRID vers StorageGRID augmente le dépannage et la complexité opérationnelle.

À propos de cette tâche

Suivez ces instructions pour déployer initialement des nœuds VMware, ajouter un nouveau nœud VMware dans une extension ou remplacer un nœud VMware dans le cadre d'une opération de récupération. Sauf indication contraire dans les étapes, la procédure de déploiement de nœud est la même pour tous les types de nœuds, y compris les nœuds d'administration, les nœuds de stockage et les nœuds de passerelle.

Si vous installez un nouveau système StorageGRID :

- Vous pouvez déployer des nœuds dans n'importe quel ordre.
- Vous devez vous assurer que chaque machine virtuelle peut se connecter au nœud d'administration principal via le réseau de grille.
- Vous devez déployer tous les nœuds de grille avant de configurer la grille.

Si vous effectuez une opération d'extension ou de récupération :

- Vous devez vous assurer que la nouvelle machine virtuelle peut se connecter à tous les autres nœuds via le réseau Grid.

Si vous devez remapper l'un des ports du nœud, ne mettez pas le nouveau nœud sous tension tant que la configuration de remappage 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  
vsphere-primary-admin.ovf  
vsphere-primary-admin.mf
```

2. Donnez un nom à la machine virtuelle.

La pratique courante consiste à utiliser le même nom pour la machine virtuelle et le nœud de grille.

3. Placez la machine virtuelle dans le vApp ou le pool de ressources approprié.

4. Si vous déployez le nœud d'administration principal, lisez et acceptez le contrat de licence utilisateur final.

Selon votre version de vCenter, l'ordre des étapes varie pour accepter le contrat de licence utilisateur final, spécifier le nom de la machine virtuelle et sélectionner une banque de données.

5. Sélectionnez le stockage pour la machine virtuelle.

Si vous déployez un nœud dans le cadre d'une opération de récupération, suivez les instructions de [la étape de récupération du stockage](#) pour ajouter de nouveaux disques virtuels, rattacher les disques durs virtuels du nœud de grille défaillant, ou les deux.

Lors du déploiement d'un nœud de stockage, utilisez 3 volumes de stockage ou plus, chaque volume de stockage étant de 4 To ou plus. Vous devez attribuer au moins 4 To au volume 0.



Le fichier .ovf du 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 les VMDK ou RDM appropriés pour le stockage avant de mettre le nœud sous tension. Les VMDK sont plus couramment utilisés dans les environnements VMware et sont plus faciles à gérer, tandis que les RDM peuvent offrir de meilleures performances pour les charges de travail qui utilisent des tailles d'objet plus grandes (par exemple, supérieures à 100 Mo).



Certaines installations StorageGRID peuvent utiliser des volumes de stockage plus importants et plus actifs que les charges de travail virtualisées classiques. Vous devrez peut-être ajuster certains paramètres de l'hyperviseur, tels que `MaxAddressableSpaceTB`, pour atteindre des performances optimales. Si vous rencontrez des performances médiocres, contactez votre ressource de support de virtualisation pour déterminer si votre environnement pourrait bénéficier d'un réglage de configuration spécifique à la charge de travail.

6. Sélectionnez les 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. + Le réseau Grid est utilisé pour tout le trafic interne StorageGRID. Il fournit une connectivité entre tous les nœuds du réseau, sur tous les sites et sous-réseaux. Tous les nœuds du réseau Grid doivent pouvoir communiquer avec tous les autres nœuds.
- Si vous utilisez le réseau d'administration, 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 de 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 même destination que celle que vous avez sélectionnée pour le réseau de grille.
- Si vous utilisez un réseau administrateur ou client, les nœuds ne doivent pas nécessairement se trouver sur les mêmes réseaux administrateur ou client.

7. Pour **Personnaliser le modèle**, configurez les propriétés de nœud StorageGRID requises.

a. Entrez le **Nom du nœud**.



Si vous récupérez un nœud de grille, vous devez saisir le nom du nœud que vous récupérez.

b. Utilisez la liste déroulante **Mot de passe d'installation temporaire** pour spécifier un mot de passe d'installation temporaire, afin de pouvoir accéder à la console de la machine virtuelle ou à l'API d'installation StorageGRID, ou utiliser SSH, avant que le nouveau nœud ne rejoigne la grille.



Le mot de passe d'installation temporaire n'est utilisé que pendant l'installation du nœud. Une fois qu'un nœud a été ajouté à la grille, vous pouvez y accéder en utilisant le "[mot de passe de la console du nœud](#)", qui est répertorié dans le `Passwords.txt` fichier dans le package de récupération.

- **Utiliser le nom du nœud** : la valeur que vous avez fournie pour le champ **Nom du nœud** est utilisée comme mot de passe d'installation temporaire.
 - **Utiliser un mot de passe personnalisé** : un mot de passe personnalisé est utilisé comme mot de passe d'installation temporaire.
 - **Désactiver le mot de passe** : Aucun mot de passe d'installation temporaire ne sera utilisé. Si vous devez accéder à la machine virtuelle pour déboguer les problèmes d'installation, consultez "[Résoudre les problèmes d'installation](#)".
- c. Si vous avez sélectionné **Utiliser un mot de passe personnalisé**, spécifiez le mot de passe d'installation temporaire que vous souhaitez utiliser dans le champ **Mot de passe personnalisé**.
- d. Dans la section **Réseau de grille (eth0)**, sélectionnez STATIQUE ou DHCP pour la **Configuration IP du réseau de grille**.
- Si vous sélectionnez STATIQUE, entrez l'**IP du réseau grille**, le **Masque du réseau grille**, la **Passerelle du réseau grille** et le **MTU du réseau grille**.
 - Si vous sélectionnez DHCP, l'**IP du réseau grille**, le **masque du réseau grille** et la **passerelle du réseau grille** sont automatiquement attribués.
- e. Dans le champ **IP d'administration principale**, saisissez l'adresse IP du nœud d'administration principal du 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 sera automatiquement détectée si le nœud d'administration principal, ou au moins un autre nœud de 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 **Réseau administrateur (eth1)**, sélectionnez STATIQUE, DHCP ou DÉSACTIVÉ pour la **Configuration IP du réseau administrateur**.
 - 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, entrez l'**IP du réseau administrateur**, le **Masque de réseau administrateur**, la **Passerelle du réseau administrateur** et le **MTU du réseau administrateur**.
 - Si vous sélectionnez STATIQUE, entrez la **Liste des sous-réseaux externes du réseau administrateur**. Vous devez également configurer une passerelle.
 - Si vous sélectionnez DHCP, l'**IP du réseau administrateur**, le **masque de réseau administrateur** et la **passerelle du réseau administrateur** sont automatiquement attribués.
- b. Dans la section **Réseau client (eth2)**, sélectionnez STATIQUE, DHCP ou DÉSACTIVÉ pour la **Configuration IP du 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'**IP du réseau client**, le **Masque de réseau client**, la **Passerelle réseau client** et le **MTU du réseau client**.
 - Si vous sélectionnez DHCP, l'**IP du réseau client**, le **masque de réseau client** et la **passerelle du réseau client** sont automatiquement attribués.
8. Vérifiez la configuration de la machine virtuelle et apportez les modifications nécessaires.
9. Lorsque vous êtes prêt à terminer, sélectionnez **Terminer** pour démarrer le téléchargement de la machine virtuelle.
10. Si vous avez déployé ce nœud dans le cadre d'une opération de récupération et qu'il ne s'agit pas d'une récupération complète du nœud, effectuez ces étapes une fois le déploiement terminé :
 - a. Cliquez avec le bouton droit sur la machine virtuelle et sélectionnez **Modifier les paramètres**.
 - b. Sélectionnez chaque disque dur virtuel par défaut qui a été désigné pour le stockage et sélectionnez **Supprimer**.
 - c. En fonction des circonstances de récupération de vos données, ajoutez de nouveaux disques virtuels en fonction de vos besoins de stockage, rattachez tous les disques durs virtuels conservés à partir du nœud de grille défaillant précédemment supprimé, ou les deux.

Veuillez noter 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 récupération du nœud.
 - Le fichier .ovf du 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 les VMDK ou RDM appropriés pour le stockage avant de mettre le nœud sous tension. Les VMDK sont plus couramment utilisés dans les environnements VMware et sont plus faciles à gérer, tandis que les RDM peuvent offrir de meilleures performances pour les charges de travail qui utilisent des tailles d'objet plus grandes (par exemple, supérieures à 100 Mo).
11. Si vous devez remapper les ports utilisés par ce nœud, procédez comme suit.

Vous devrez peut-être remapper un port si les politiques de réseau de votre entreprise restreignent l'accès à un ou plusieurs ports utilisés par StorageGRID. Voir le "[directives de mise en réseau](#)" pour les ports utilisés par StorageGRID.



Ne remappez pas les ports utilisés dans les points de terminaison de l'équilibreur de charge.

- a. Sélectionnez la nouvelle VM.
- b. Dans l'onglet Configurer, sélectionnez **Paramètres > Options vApp**. L'emplacement des **Options vApp** dépend de la version de vCenter.
- c. Dans la table **Propriétés**, recherchez **PORT_REMAP_INBOUND** et **PORT_REMAP**.
- d. Pour mapper symétriquement les communications entrantes et sortantes d'un port, sélectionnez **PORT_REMAP**.



Si seul **PORT_REMAP** est défini, le mappage que vous spécifiez s'applique aux communications entrantes et sortantes. Si **PORT_REMAP_INBOUND** est également spécifié, **PORT_REMAP** s'applique uniquement aux communications sortantes.

- i. Sélectionnez **Définir la valeur**.
- ii. Entrez le mappage des ports :

```
<network type>/<protocol>/<default port used by grid node>/<new port>
```

<network type>`est une grille, un administrateur ou un client, et
`<protocol> est tcp ou udp.

Par exemple, pour remapper le trafic SSH du port 22 vers le port 3022, entrez :

```
client/tcp/22/3022
```

Vous pouvez remapper plusieurs ports à l'aide d'une liste séparée par des virgules.

Par exemple:

```
client/tcp/18082/443, client/tcp/18083/80
```

- i. Sélectionnez **OK**.
- e. Pour spécifier le port utilisé pour les communications entrantes vers le nœud, sélectionnez **PORT_REMAP_INBOUND**.



Si vous spécifiez **PORT_REMAP_INBOUND** et ne spécifiez pas de valeur pour **PORT_REMAP**, les communications sortantes pour le port restent inchangées.

- i. Sélectionnez **Définir la valeur**.
- ii. Entrez le mappage des ports :

```
<network type>/<protocol>/<remapped inbound port>/<default inbound port  
used by grid node>
```

<network type>`est une grille, un administrateur ou un client, et
`<protocol> est tcp ou udp.

Par exemple, pour remapper 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
```


Vous pouvez remapper plusieurs ports entrants à l'aide d'une liste séparée par des virgules.

Par exemple:

```
grid/tcp/3022/22, admin/tcp/3022/22
```

i. Sélectionnez **OK**

12. Si vous souhaitez augmenter le CPU ou la mémoire du nœud à partir des paramètres par défaut :

- a. Cliquez avec le bouton droit sur la machine virtuelle et sélectionnez **Modifier les paramètres**.
- b. Modifiez le nombre de processeurs ou la quantité de mémoire selon vos besoins.

Définissez la **Réservation de mémoire** sur la même taille que la **Mémoire** allouée à la machine virtuelle.

c. Sélectionnez **OK**.

13. Allumez la machine virtuelle.

Après avoir terminé

Si vous avez déployé ce nœud dans le cadre d'une procédure d'extension ou de récupération, revenez à ces instructions pour terminer la procédure.

Configurer la grille et terminer l'installation (VMware)

Accéder au gestionnaire de grille

Vous utilisez le Grid Manager pour définir toutes les informations requises pour configurer votre 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 :

```
https://primary_admin_node_ip
```

Alternativement, vous pouvez accéder au Grid Manager sur le port 8443 :

```
https://primary_admin_node_ip:8443
```

Vous pouvez utiliser l'adresse IP du nœud d'administration principal sur le réseau de grille ou sur le réseau d'administration, selon la configuration de votre réseau. Vous devrez peut-être utiliser l'option sécurité/avancée de votre navigateur pour accéder à un certificat non fiable.

2. Gérez un mot de passe d'installation temporaire selon vos besoins :

- Si un mot de passe a déjà été défini à l'aide de l'une de ces méthodes, saisissez le mot de passe pour continuer.
 - Un utilisateur a défini le mot de passe lors de l'accès au programme d'installation précédemment
 - Le mot de passe SSH/console a été automatiquement importé depuis les propriétés OVF

- Si aucun mot de passe n'a été défini, vous pouvez éventuellement définir un mot de passe pour sécuriser le programme d'installation de StorageGRID .

3. Sélectionnez *Installer un système StorageGRID* .

La page utilisée pour configurer une grille StorageGRID apparaît.

NetApp® StorageGRID® Help ▾

Install

1 License 2 Sites 3 Grid Network 4 Grid Nodes 5 NTP 6 DNS 7 Passwords 8 Summary

License

Enter a grid name and upload the license file provided by NetApp for your StorageGRID system.

Grid Name

License File

Spécifiez les informations de licence StorageGRID

Vous devez spécifier le nom de votre système StorageGRID et télécharger le fichier de licence fourni par NetApp.

Étapes

1. Sur la page Licence, saisissez 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 **Parcourir**, recherchez le fichier de licence NetApp(*NLF-unique-id.txt*), et sélectionnez **Ouvrir**.

Le fichier de licence est validé et le numéro de série est affiché.



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 niveau vers une licence qui offre un support après l'installation.

1 License 2 Sites 3 Grid Network 4 Grid Nodes 5 NTP 6 DNS 7 Passwords 8 Summary

License

Enter a grid name and upload the license file provided by NetApp for your StorageGRID system.

Grid Name:

License File: NLF-959007-Internal.txt

License Serial Number:

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 le **Nom du site**.
2. Pour ajouter des sites supplémentaires, cliquez sur le signe plus à côté de la dernière entrée de site et saisissez le nom dans la nouvelle zone de texte **Nom du site**.

Ajoutez autant de sites supplémentaires que nécessaire pour votre topologie de grille. Vous pouvez ajouter jusqu'à 16 sites.

NetApp® StorageGRID® Help ▾

Install

1 License **2** Sites 3 Grid Network 4 Grid Nodes 5 NTP 6 DNS 7 Passwords 8 Summary

Sites

In a single-site deployment, infrastructure and operations are centralized in one site.

In a multi-site deployment, infrastructure can be distributed asymmetrically across sites, and proportional to the needs of each site. Typically, sites are located in geographically different locations. Having multiple sites also allows the use of distributed replication and erasure coding for increased availability and resiliency.

Site Name 1: ✕

Site Name 2: + ✕

3. Cliquez sur **Suivant**.

Spécifier les sous-réseaux du réseau Grid

Vous devez spécifier les sous-réseaux utilisés sur le réseau Grid.

À propos de cette tâche

Les entrées de sous-réseau incluent les sous-réseaux du réseau Grid pour chaque site de votre système StorageGRID, ainsi que tous les sous-réseaux qui doivent être accessibles via le réseau Grid.

Si vous disposez de plusieurs sous-réseaux de grille, la passerelle Grid Network est requise. Tous les sous-réseaux de grille spécifiés doivent être accessibles via cette passerelle.

Étapes

1. Spécifiez l'adresse réseau CIDR pour au moins un réseau de grille 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. Vous devez spécifier tous les sous-réseaux pour tous les sites du réseau Grid.
 - Si vous avez déjà déployé au moins un nœud, cliquez sur **Découvrir les sous-réseaux des réseaux de grille** pour remplir automatiquement la liste des sous-réseaux des réseaux de grille avec les sous-réseaux signalés par les nœuds de grille enregistrés auprès du gestionnaire de grille.
 - Vous devez ajouter manuellement tous les sous-réseaux pour NTP, DNS, LDAP ou autres serveurs externes accessibles via la passerelle Grid Network.

NetApp® StorageGRID® Help ▾

Install

1 License 2 Sites 3 **Grid Network** 4 Grid Nodes 5 NTP 6 DNS 7 Passwords 8 Summary

Grid Network

You must specify the subnets that are used on the Grid Network. These entries typically include the subnets for the Grid Network for each site in your StorageGRID system. Select Discover Grid Networks to automatically add subnets based on the network configuration of all registered nodes.

Note: You must manually add any subnets for NTP, DNS, LDAP, or other external servers accessed through the Grid Network gateway.

Subnet 1 +

3. Cliquez sur **Suivant**.

Approuver les nœuds de grille en attente

Vous devez approuver chaque nœud de grille avant qu'il puisse rejoindre le système StorageGRID.

Avant de commencer

Vous avez déployé tous les nœuds de grille d'appliance virtuelle et StorageGRID.



Il est plus efficace d'effectuer une seule installation de tous les nœuds, plutôt que d'installer certains nœuds maintenant et certains nœuds plus tard.

Étapes

- 1. Consultez la liste des nœuds en attente et confirmez qu'elle affiche tous les nœuds de grille que vous avez déployés.



Si un nœud de grille est manquant, confirmez qu'il a été déployé avec succès et qu'il dispose de l'adresse IP du réseau de grille correcte du nœud d'administration principal défini pour ADMIN_IP.

- 2. Sélectionnez le bouton radio à côté d'un nœud en attente que vous souhaitez approuver.



Grid Nodes

Approve and configure grid nodes, so that they are added correctly to your StorageGRID system.

Pending Nodes

Grid nodes are listed as pending until they are assigned to a site, configured, and approved.

+ Approve

✕ Remove

Search

	Grid Network MAC Address	Name	Type	Platform	Grid Network IPv4 Address
☒	50:6b:4b:42:d7:00	NetApp-SGA	Storage Node	StorageGRID Appliance	172.16.5.20/21

◀

▶

Approved Nodes

Grid nodes that have been approved and have been configured for installation. An approved grid node's configuration can be edited if errors are identified.

Edit

Reset

✕ Remove

Search

	Grid Network MAC Address	Name	Site	Type	Platform	Grid Network IPv4 Address
☐	00:50:56:87:42:ff	dc1-adm1	Raleigh	Admin Node	VMware VM	172.16.4.210/21
☐	00:50:56:87:c0:16	dc1-s1	Raleigh	Storage Node	VMware VM	172.16.4.211/21
☐	00:50:56:87:79:ee	dc1-s2	Raleigh	Storage Node	VMware VM	172.16.4.212/21
☐	00:50:56:87:db:9c	dc1-s3	Raleigh	Storage Node	VMware VM	172.16.4.213/21
☐	00:50:56:87:62:38	dc1-g1	Raleigh	API Gateway Node	VMware VM	172.16.4.214/21

◀

▶

- 3. Cliquez sur **Approuver**.
- 4. Dans les paramètres généraux, modifiez les paramètres des propriétés suivantes, si nécessaire :
 - **Site** : Le nom système du site pour ce nœud de grille.
 - **Nom** : Le nom du système pour le nœud. Le nom par défaut est celui 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 du système selon vos besoins.



Pour un nœud VMware, vous pouvez modifier le nom ici, mais cette action ne modifiera pas le nom de la machine virtuelle dans vSphere.

- **Rôle NTP** : Le rôle du protocole NTP (Network Time Protocol) du nœud de grille. Les options sont **Automatique**, **Principal** et **Client**. La sélection de **Automatique** attribue le rôle principal aux nœuds d'administration, aux nœuds de stockage avec services ADC, aux nœuds de passerelle et à tous les nœuds de grille dotés d'adresses IP non statiques. Tous les autres nœuds de grille se voient attribuer le rôle Client.



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 se produiront si ce nœud tombe en panne. De plus, la désignation de deux nœuds par site comme sources NTP principales garantit une synchronisation précise si un site est isolé du reste du réseau.

- **Type de stockage** (nœuds de stockage uniquement) : spécifiez qu'un nouveau nœud de stockage doit être utilisé exclusivement pour les données uniquement, les métadonnées uniquement ou les deux. Les options sont **Données et métadonnées** (« combinées »), **Données uniquement** et **Métadonnées uniquement**.



Voir "[Types de nœuds de stockage](#)" pour obtenir des informations sur les exigences relatives à ces types de nœuds.

- **Service ADC** (nœuds de stockage uniquement) : sélectionnez **Automatique** pour permettre au système de déterminer si le nœud nécessite le service de contrôleur de domaine administratif (ADC). Le service ADC suit l'emplacement et la disponibilité des services du réseau. Au moins trois nœuds de stockage sur chaque site doivent inclure le service ADC. Vous ne pouvez pas ajouter le service ADC à un nœud après son déploiement.

5. Dans Grid Network, modifiez les paramètres des propriétés suivantes si nécessaire :

- **Adresse IPv4 (CIDR)** : l'adresse réseau CIDR pour l'interface Grid Network (eth0 à l'intérieur du conteneur). Par exemple : 192.168.1.234/21
- **Passerelle** : La passerelle du réseau Grid. Par exemple : 192.168.0.1



La passerelle est requise s'il existe plusieurs sous-réseaux de grille.



Si vous avez sélectionné DHCP pour la configuration du réseau Grid et que vous modifiez la valeur ici, la nouvelle valeur sera configurée comme une adresse statique sur le nœud. Vous devez vous assurer que l'adresse IP configurée ne se trouve pas dans un pool d'adresses DHCP.

6. Si vous souhaitez configurer le réseau d'administration pour le nœud de grille, ajoutez ou mettez à jour les paramètres dans la section Réseau d'administration si nécessaire.

Saisissez les sous-réseaux de destination des itinéraires sortant de cette interface dans la zone de texte **Sous-réseaux (CIDR)**. S'il existe plusieurs sous-réseaux d'administration, 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 comme une adresse statique sur le nœud. Vous devez vous assurer que l'adresse IP configurée ne se trouve pas dans un pool d'adresses DHCP.

Appareils : pour un appareil 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'appareil StorageGRID , il ne peut pas être configuré dans cette boîte de dialogue Grid Manager. Au lieu de cela, vous devez suivre ces étapes :

- a. Redémarrez l'appareil : dans le programme d'installation de l'appareil, sélectionnez **Avancé > Redémarrer**.

Le redémarrage peut prendre plusieurs minutes.

- b. Sélectionnez **Configurer la mise en réseau > Configuration de liaison** et activez les réseaux appropriés.
- c. Sélectionnez **Configurer le 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 nœud.
- f. Supprimez le nœud de la table des nœuds en attente.
- g. Attendez que le nœud réapparaisse dans la liste des nœuds en attente.
- h. Confirmez que vous pouvez configurer les réseaux appropriés. Ils doivent déjà être renseignés avec les informations que vous avez fournies sur la page de configuration IP du programme d'installation de l'appliance.

Pour plus d'informations, consultez le "[Démarrage rapide pour l'installation du matériel](#)" pour localiser 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 nœud 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 comme une adresse statique sur le nœud. Vous devez vous assurer que l'adresse IP configurée ne se trouve pas dans un pool d'adresses DHCP.

Appliances : 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 Grid Manager. Au lieu de cela, vous devez suivre ces étapes :

- a. Redémarrez l'appareil : dans le programme d'installation de l'appareil, sélectionnez **Avancé > Redémarrer**.

Le redémarrage peut prendre plusieurs minutes.

- b. Sélectionnez **Configurer la mise en réseau > Configuration de liaison** et activez les réseaux appropriés.
- c. Sélectionnez **Configurer le 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 nœud.
- f. Supprimez le nœud de la table des nœuds en attente.
- g. Attendez que le nœud réapparaisse dans la liste des nœuds en attente.
- h. Confirmez que vous pouvez configurer les réseaux appropriés. Ils doivent déjà être renseignés avec les informations que vous avez fournies sur la page de configuration IP du programme d'installation de l'appliance.

Pour plus d'informations, consultez le "[Démarrage rapide pour l'installation du matériel](#)" pour localiser les instructions relatives à votre appareil.

8. Cliquez sur **Enregistrer**.

L'entrée du nœud de grille est déplacée vers la liste des nœuds approuvés.



Grid Nodes

Approve and configure grid nodes, so that they are added correctly to your StorageGRID system.

Pending Nodes

Grid nodes are listed as pending until they are assigned to a site, configured, and approved.

Approve

Remove

Search

Grid Network MAC Address	Name	Type	Platform	Grid Network IPv4 Address
No results found.				

Approved Nodes

Grid nodes that have been approved and have been configured for installation. An approved grid node's configuration can be edited if errors are identified.

Edit
 Reset
 Remove

Search

	Grid Network MAC Address ⓘ	Name ⓘ	Site ⓘ	Type ⓘ	Platform ⓘ	Grid Network IPv4 Address ▼
☐	00:50:56:87:42:ff	dc1-adm1	Raleigh	Admin Node	VMware VM	172.16.4.210/21
☐	00:50:56:87:c0:16	dc1-s1	Raleigh	Storage Node	VMware VM	172.16.4.211/21
☐	00:50:56:87:79:ee	dc1-s2	Raleigh	Storage Node	VMware VM	172.16.4.212/21
☐	00:50:56:87:db:9c	dc1-s3	Raleigh	Storage Node	VMware VM	172.16.4.213/21
☐	00:50:56:87:62:38	dc1-g1	Raleigh	API Gateway Node	VMware VM	172.16.4.214/21
☐	50:6b:4b:42:d7:00	NetApp-SGA	Raleigh	Storage Node	StorageGRID Appliance	172.16.5.20/21

◀

▶

9. Répétez ces étapes pour chaque nœud de grille en attente que vous souhaitez approuver.

Vous devez approuver tous les nœuds que vous souhaitez dans la grille. Cependant, vous pouvez revenir sur 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**.

Spécifier les informations du serveur Network Time Protocol

Vous devez spécifier les informations de configuration du protocole NTP (Network Time Protocol) pour le système StorageGRID , afin que les opérations effectuées sur des serveurs distincts puissent rester synchronisées.

À propos de cette tâche

Vous devez spécifier des adresses IPv4 pour les serveurs NTP.

Vous devez spécifier des serveurs NTP externes. Les serveurs NTP spécifiés doivent utiliser le protocole NTP.

Vous devez spécifier quatre références de serveur NTP de niveau 3 ou supérieur pour éviter les problèmes de dérive temporelle.



Lorsque vous spécifiez 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 de haute précision, tels que StorageGRID.

["Limite de prise en charge pour configurer le service de temps Windows pour les environnements de haute précision"](#)

Les serveurs NTP externes sont utilisés par les nœuds auxquels vous avez précédemment attribué des rôles NTP principaux.



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 se produiront si ce nœud tombe en panne. De plus, la désignation de deux nœuds par site comme sources NTP principales garantit une synchronisation précise si un site est isolé du reste du réseau.

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 **Serveur 1** à **Serveur 4**.
2. Si nécessaire, sélectionnez le signe plus à côté de la dernière entrée pour ajouter des entrées de serveur supplémentaires.

NetApp® StorageGRID®
Help

Install

1 License
2 Sites
3 Grid Network
4 Grid Nodes
5 NTP
6 DNS
7 Passwords
8 Summary

Network Time Protocol

Enter the IP addresses for at least four Network Time Protocol (NTP) servers, so that operations performed on separate servers are kept in sync.

Server 1	10.60.248.183
Server 2	10.227.204.142
Server 3	10.235.48.111
Server 4	0.0.0.0

+

3. Sélectionnez **Suivant**.

Spécifier les informations du serveur DNS

Vous devez spécifier les informations DNS pour votre système StorageGRID , afin de pouvoir accéder aux serveurs externes à l'aide de noms d'hôtes au lieu d'adresses IP.

À propos de cette tâche

Spécification "[Informations sur le serveur DNS](#)" vous permet d'utiliser des noms d'hôtes de nom de domaine complet (FQDN) plutôt que des adresses IP pour les notifications par e-mail et AutoSupport.

Pour garantir un bon fonctionnement, spécifiez deux ou trois serveurs DNS. Si vous spécifiez plus de trois, il est possible que seulement trois soient utilisés en raison de limitations connues du système d'exploitation sur certaines plates-formes. Si vous avez des restrictions de routage dans votre environnement, vous pouvez "[personnaliser la liste des serveurs DNS](#)" pour que les nœuds individuels (généralement tous les nœuds d'un site) utilisent un ensemble différent de trois serveurs DNS maximum.

Si possible, utilisez des serveurs DNS auxquels chaque site peut accéder localement pour garantir qu'un site isolé peut résoudre les noms de domaine complets pour les destinations externes.

Étapes

1. Spécifiez l'adresse IPv4 pour au moins un serveur DNS dans la zone de texte **Serveur 1**.
2. Si nécessaire, sélectionnez le signe plus à côté de la dernière entrée pour ajouter des entrées de serveur supplémentaires.

NetApp® StorageGRID®
Help

Install

1 License
2 Sites
3 Grid Network
4 Grid Nodes
5 NTP
6 DNS
7 Passwords
8 Summary

Domain Name Service

Enter the IP address for at least one Domain Name System (DNS) server, so that server hostnames can be used instead of IP addresses. Specifying at least two DNS servers is recommended. Configuring DNS enables server connectivity, email notifications, and NetApp AutoSupport.

Server 1
10.224.223.130
✕

Server 2
10.224.223.136
+ ✕

La meilleure pratique consiste à spécifier au moins deux serveurs DNS. Vous pouvez spécifier jusqu'à six serveurs DNS.

3. Sélectionnez **Suivant**.

Spécifiez les mots de passe du 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.

À propos de cette tâche

Utilisez la page Installer les mots de passe pour spécifier la phrase secrète de provisionnement et le mot de passe de l'utilisateur root de gestion de la grille.

- La phrase secrète de provisionnement est utilisée comme clé de chiffrement et n'est pas stockée par le système StorageGRID .
- Vous devez disposer de la phrase secrète de provisionnement pour les procédures d'installation, d'extension et de maintenance, y compris le téléchargement du package de récupération. Il est donc important de stocker la phrase secrète de provisionnement dans un endroit sûr.
- Vous pouvez modifier la phrase secrète de provisionnement à partir du gestionnaire de grille si vous disposez de la phrase secrète actuelle.
- Le mot de passe de l'utilisateur root de gestion de grille peut être modifié à l'aide du gestionnaire de grille.
- La console de ligne de commande générée aléatoirement et les mots de passe SSH sont stockés dans le `Passwords.txt` fichier dans le package de récupération.

Étapes

1. Dans **Provisioning Passphrase**, saisissez la phrase secrète de provisionnement qui sera requise pour apporter des modifications à la topologie de grille de votre système StorageGRID .

Stockez la phrase secrète de provisionnement dans un endroit sûr.



Si, une fois l'installation terminée, vous souhaitez modifier ultérieurement la phrase secrète de provisionnement, vous pouvez utiliser le gestionnaire de grille. Sélectionnez **CONFIGURATION > Contrôle d'accès > Mots de passe de la grille**.

2. Dans **Confirmer la phrase secrète de provisionnement**, saisissez à nouveau la phrase secrète de provisionnement pour la confirmer.
3. Dans **Mot de passe de l'utilisateur racine de gestion de grille**, saisissez le mot de passe à utiliser pour accéder au gestionnaire de grille en tant qu'utilisateur « root ».

Conservez le mot de passe dans un endroit sûr.

4. Dans **Confirmer le mot de passe de l'utilisateur root**, saisissez à nouveau le mot de passe du gestionnaire de grille pour le confirmer.

The screenshot shows the NetApp StorageGRID installation wizard interface. At the top, there's a blue header with "NetApp® StorageGRID®" and a "Help" link. Below the header is a progress bar with eight steps: 1. License, 2. Sites, 3. Grid Network, 4. Grid Nodes, 5. NTP, 6. DNS, 7. Passwords (highlighted in blue), and 8. Summary. Below the progress bar, the title "Passwords" is displayed. A note states: "Enter secure passwords that meet your organization's security policies. A text file containing the command line passwords must be downloaded during the final installation step." There are four password input fields, each with a label and a masked input box (dots): "Provisioning Passphrase", "Confirm Provisioning Passphrase", "Grid Management Root User Password", and "Confirm Root User Password". At the bottom, there is a checkbox labeled "Create random command line passwords." which is checked.

5. Si vous installez une grille à des fins de preuve de concept ou de démonstration, décochez éventuellement la case **Créer des mots de passe de ligne de commande aléatoires**.

Pour les déploiements de production, des mots de passe aléatoires doivent toujours être utilisés pour des raisons de sécurité. Cochez **Créer 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 la grille à partir de la ligne de commande à l'aide du compte « root » ou « admin ».



Vous êtes invité à télécharger le fichier du package de récupération(`sgws-recovery-package-id-revision.zip`) après avoir cliqué sur **Installer** sur la page Résumé. Vous devez "[télécharger 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 Recovery Package.

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 se déroule correctement.

Étapes

1. Voir la page **Résumé**.

NetApp® StorageGRID®

Help ▾

Install

1

2

3

4

5

6

7

8

License

Sites

Grid Network

Grid Nodes

NTP

DNS

Passwords

Summary

Summary

Verify that all of the grid configuration information is correct, and then click Install. You can view the status of each grid node as it installs. Click the Modify links to go back and change the associated information.

General Settings

Grid Name

Grid1

Modify License

Passwords

Auto-generated random command line passwords

Modify Passwords

Networking

NTP

10.60.248.183 10.227.204.142 10.235.48.111

Modify NTP

DNS

10.224.223.130 10.224.223.136

Modify DNS

Grid Network

172.16.0.0/21

Modify Grid Network

Topology

Topology

Atlanta

Modify Sites

Raleigh

dc1-adm1

dc1-g1

dc1-s1

dc1-s2

dc1-s3

NetApp-SGA

Modify Grid Nodes

2. Vérifiez que toutes les informations de configuration de la grille sont correctes. Utilisez les liens Modifier sur 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 de grille 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 "[Directives de mise en réseau](#)" pour plus de détails.

4. Cliquez sur **Télécharger le package 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 package de récupération(. zip), et confirmez que vous pouvez accéder avec succès au contenu de ce fichier. Vous devez télécharger le fichier du package de récupération afin de

pouvoir récupérer le système StorageGRID si un ou plusieurs nœuds de grille échouent. 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.

- Vérifiez que vous pouvez extraire le contenu du .zip fichier, puis enregistrez-le dans deux emplacements sûrs, sécurisés et distincts.



Le fichier du package de récupération doit être sécurisé car il contient des clés de chiffrement et des mots de passe qui peuvent être utilisés pour obtenir des données à partir du système StorageGRID .

- Cochez la case **J'ai téléchargé et vérifié avec succès le fichier du package de récupération**, puis cliquez sur **Suivant**.

Si l'installation est toujours en cours, la page d'état apparaît. Cette page indique la progression de l'installation pour chaque nœud de grille.

Installation Status

If necessary, you may [Download the Recovery Package file](#) again.

							Search	
Name	IT	Site	IT	Grid Network IPv4 Address	Progress	IT	Stage	IT
dc1-adm1		Site1		172.16.4.215/21			Starting services	
dc1-g1		Site1		172.16.4.216/21			Complete	
dc1-s1		Site1		172.16.4.217/21			Waiting for Dynamic IP Service peers	
dc1-s2		Site1		172.16.4.218/21			Downloading hotfix from primary Admin if needed	
dc1-s3		Site1		172.16.4.219/21			Downloading hotfix from primary Admin if needed	

Lorsque l'étape Terminé est atteinte pour tous les nœuds de grille, la page de connexion au Gestionnaire de grille s'affiche.

- Sign in au Grid Manager en utilisant l'utilisateur « root » et le mot de passe que vous avez spécifié lors de l'installation.

Consignes post-installation

Une fois le déploiement et la configuration du nœud de grille terminés, suivez ces instructions pour l'adressage DHCP et les modifications de configuration réseau.

- Si DHCP a été 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 lorsque la configuration du réseau de grille est modifiée par DHCP, ce qui peut provoquer des pannes si une modification DHCP affecte plusieurs nœuds en même temps.

- Vous devez utiliser les procédures de modification d'IP si vous souhaitez modifier les adresses IP, les masques de sous-réseau et les passerelles par défaut d'un nœud de grille. Voir "[Configurer les adresses IP](#)".
- Si vous apportez des modifications à la configuration du réseau, notamment au routage et à la passerelle,

la connectivité client au nœud d'administration principal et aux autres nœuds de grille peut être perdue. En fonction des modifications réseau appliquées, vous devrez peut-être rétablir ces connexions.

Installation de l'API REST

StorageGRID fournit l'API d'installation StorageGRID pour effectuer des tâches d'installation.

L'API utilise la plate-forme API open source Swagger 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 comment 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 API que vous effectuez à l'aide de la page Web de documentation API 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 API REST inclut l'URL de l'API, une action HTTP, tous les paramètres d'URL obligatoires ou facultatifs et une réponse API attendue.

API d'installation de StorageGRID

L'API d'installation StorageGRID n'est disponible que lorsque vous configurez initialement votre système StorageGRID et si vous devez effectuer une récupération du nœud d'administration principal. L'API d'installation est accessible via HTTPS à partir du gestionnaire de grille.

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 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 répertorier la version du produit et les principales versions 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 du réseau de grille, les mots de passe de la grille et les adresses IP des serveurs NTP et DNS.
- **nodes** — Opérations de configuration au niveau du nœud. Vous pouvez récupérer une liste de nœuds de grille, supprimer un nœud de grille, configurer un nœud de grille, afficher un nœud de grille et réinitialiser la configuration d'un nœud de grille.
- **provision** — Opérations de provisionnement. Vous pouvez démarrer l'opération de provisionnement et afficher l'état de l'opération de provisionnement.
- **récupération** — Opérations de récupération du nœud d'administration principal. Vous pouvez réinitialiser les informations, télécharger le package de récupération, démarrer la récupération et afficher l'état de l'opération de récupération.
- **recovery-package** — Opérations de téléchargement du package de récupération.
- **sites** — Opérations de configuration au niveau du site. Vous pouvez créer, afficher, supprimer et modifier un site.
- **temporary-password** — Opérations sur le mot de passe temporaire pour sécuriser l'API de gestion pendant l'installation.

Où aller ensuite

Une fois l'installation terminée, effectuez les tâches d'intégration et de configuration requises. Vous pouvez effectuer les tâches facultatives selon vos besoins.

Tâches requises

- Configurez VMware vSphere Hypervisor pour un 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 grille restent arrêtés après le redémarrage du serveur. Pour plus de détails, consultez la documentation de VMware vSphere Hypervisor.

- "[Créer un compte locataire](#)" pour le protocole client S3 qui sera utilisé pour stocker des objets sur votre système StorageGRID .
- "[Accès au système de contrôle](#)" en configurant des groupes et des comptes utilisateurs. En option, vous pouvez "[configurer une source d'identité fédérée](#)" (comme Active Directory ou OpenLDAP), afin de pouvoir importer des groupes d'administration et des utilisateurs. Ou, vous pouvez "[créer des groupes et des utilisateurs locaux](#)" .
- Intégrer et tester le "[API S3](#)" applications clientes que vous utiliserez pour télécharger des objets sur votre système StorageGRID .
- "[Configurer les règles de gestion du cycle de vie des informations \(ILM\) et la politique ILM](#)" vous souhaitez utiliser pour protéger les données de l'objet.
- Si votre installation inclut des nœuds de stockage d'appliance, utilisez SANtricity OS pour effectuer les tâches suivantes :
 - Connectez-vous à chaque appliance StorageGRID .
 - Vérifier la réception des données AutoSupport .Voir "[Configurer le matériel](#)" .
- Consultez et suivez les "[Directives de renforcement du système StorageGRID](#)" pour éliminer les risques de sécurité.
- "[Configurer les notifications par e-mail pour les alertes système](#)" .

Tâches facultatives

- "[Mettre à jour les adresses IP des nœuds de 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.
- "[Configurer les interfaces VLAN](#)" pour isoler et partitionner le trafic réseau, si nécessaire.
- "[Configurer des groupes de haute disponibilité](#)" pour améliorer la disponibilité de la connexion pour les clients Grid Manager, Tenant Manager et S3, si nécessaire.
- "[Configurer les points de terminaison de l'équilibreur de charge](#)" pour la connectivité client S3, si nécessaire.

Résoudre les problèmes d'installation

Si des problèmes surviennent 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`(trouvé sur tous les nœuds de la grille)
- `/var/local/log/gdu-server.log`(trouvé sur le nœud d'administration principal)

Informations connexes

Pour savoir comment accéder aux fichiers journaux, consultez ["Référence des fichiers journaux"](#) .

Si vous avez besoin d'aide supplémentaire, contactez ["Assistance NetApp"](#) .

La réservation des ressources de la 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 démarreront pas.

À propos de cette tâche

Si vous êtes certain que l'hôte de la machine virtuelle dispose de ressources suffisantes pour chaque nœud de grille, ajustez manuellement les ressources allouées à chaque machine virtuelle, puis essayez de démarrer les machines virtuelles.

Étapes

1. Dans l'arborescence client VMware vSphere Hypervisor, sélectionnez la machine virtuelle qui n'est pas démarrée.
2. Cliquez avec le bouton droit sur la machine virtuelle et sélectionnez **Modifier les paramètres**.
3. Dans la fenêtre Propriétés des machines virtuelles, sélectionnez l'onglet **Ressources**.
4. Ajuster les ressources allouées à la machine virtuelle :
 - a. Sélectionnez **CPU**, puis utilisez le curseur Réservez pour ajuster le MHz réservé à cette machine virtuelle.
 - b. Sélectionnez **Mémoire**, puis utilisez le curseur Réservez pour ajuster les Mo réservés à cette machine virtuelle.
5. Cliquez sur **OK**.
6. Répétez si nécessaire pour les autres machines virtuelles hébergées sur le même hôte VM.

Le mot de passe d'installation temporaire a été désactivé

Lorsque vous déployez un nœud VMware, vous pouvez éventuellement spécifier un mot de passe d'installation temporaire. Vous devez disposer de ce mot de passe pour accéder à la console VM ou utiliser SSH avant que le nouveau nœud ne rejoigne la grille.

Si vous avez choisi de désactiver le mot de passe d'installation temporaire, vous devez effectuer des étapes supplémentaires pour déboguer les problèmes d'installation.

Vous pouvez effectuer l'une des opérations suivantes :

- Redéployez la machine virtuelle, mais spécifiez un mot de passe d'installation temporaire afin de pouvoir accéder à la console ou utiliser SSH pour déboguer les problèmes d'installation.
- Utilisez vCenter pour définir le mot de passe :
 - a. Éteignez la VM.
 - b. Accédez à **VM**, sélectionnez l'onglet **Configurer** et sélectionnez **Options vApp**.
 - c. Spécifiez le type de mot de passe d'installation temporaire à définir :
 - Sélectionnez **CUSTOM_TEMPORARY_PASSWORD** pour définir un mot de passe temporaire personnalisé.
 - Sélectionnez **TEMPORARY_PASSWORD_TYPE** pour utiliser le nom du nœud comme mot de passe temporaire.
 - d. Sélectionnez **Définir la valeur**.
 - e. Définir le mot de passe temporaire :
 - Remplacez **CUSTOM_TEMPORARY_PASSWORD** par une valeur de mot de passe personnalisée.
 - Mettez à jour **TEMPORARY_PASSWORD_TYPE** avec la valeur **Utiliser le nom du nœud**.
 - f. Redémarrez la VM pour appliquer le nouveau mot de passe.

Mettre à niveau le logiciel StorageGRID

Mettre à niveau le logiciel StorageGRID

Utilisez ces instructions pour mettre à niveau un système StorageGRID vers une nouvelle version.

Lorsque vous effectuez la mise à niveau, tous les nœuds de votre système StorageGRID sont mis à niveau.

Avant de commencer

Consultez ces rubriques pour en savoir plus sur les nouvelles fonctionnalités et améliorations de StorageGRID 11.9, déterminer si des fonctionnalités ont été obsolètes ou supprimées et découvrir les modifications apportées aux API StorageGRID .

- ["Quoi de neuf dans StorageGRID 11.9"](#)
- ["Fonctionnalités supprimées ou obsolètes"](#)
- ["Modifications apportées à l'API de gestion de la grille"](#)
- ["Modifications apportées à l'API de gestion des locataires"](#)

Quoi de neuf dans StorageGRID 11.9

Cette version de StorageGRID introduit les fonctionnalités et modifications fonctionnelles suivantes.

Évolutivité

Nœuds de stockage de données uniquement

Pour permettre une mise à l'échelle plus granulaire, vous pouvez désormais installer ["nœuds de stockage de données uniquement"](#) . Lorsque le traitement des métadonnées n'est pas critique, vous pouvez optimiser votre infrastructure de manière rentable. Cette flexibilité permet de s'adapter à des charges de travail et des modèles de croissance variés.

Améliorations du pool de stockage cloud

Rôles IAM partout

StorageGRID prend désormais en charge les informations d'identification à court terme à l'aide de ["Rôles IAM partout dans Amazon S3 pour les pools de stockage cloud"](#) .

L'utilisation d'informations d'identification à long terme pour accéder aux buckets S3 présente des risques de sécurité si ces informations d'identification sont compromises. Les informations d'identification à court terme ont une durée de vie limitée, ce qui réduit le risque d'accès non autorisé.

Compartiments de verrouillage d'objet S3

Vous pouvez désormais ["configurer un pool de stockage cloud à l'aide d'un point de terminaison Amazon S3"](#) . S3 Object Lock permet d'empêcher la suppression accidentelle ou malveillante d'objets. Si vous hiérarchisez les données de StorageGRID vers Amazon S3, l'activation du verrouillage des objets sur les deux systèmes améliore la protection des données tout au long du cycle de vie des données.

Multi-location

Limites de compartiment

Par ["définition de limites sur les buckets S3"](#) , vous pouvez empêcher les locataires de monopoliser la capacité. De plus, une croissance incontrôlée peut entraîner des coûts inattendus. En définissant des limites, vous pouvez mieux estimer les dépenses de stockage des locataires.

5 000 seaux par locataire

Pour améliorer l'évolutivité, StorageGRID prend désormais en charge jusqu'à ["5 000 compartiments S3 par locataire"](#) . Chaque grille peut contenir un maximum de 100 000 buckets.

Pour prendre en charge 5 000 buckets, chaque nœud de stockage de la grille doit disposer d'un minimum de 64 Go de RAM.

Améliorations du verrouillage des objets S3

Les capacités de configuration par locataire offrent l'équilibre approprié entre flexibilité et sécurité des données. Vous pouvez désormais configurer les paramètres de rétention par locataire pour :

- Autoriser ou interdire le mode de conformité
- Définir une durée de conservation maximale

Se référer à :

- ["Gérer les objets avec S3 Object Lock"](#)

- ["Comment les administrateurs de réseau contrôlent la conservation des objets"](#)
- ["Créer un compte locataire"](#)

Compatibilité S3

x-amz-checksum-somme de contrôle sha256

- L'API REST S3 prend désormais en charge le lien :.../s3/operations-on-objects.html[x-amz-checksum-sha256 [somme de contrôle].
- StorageGRID fournit désormais la prise en charge de la somme de contrôle SHA-256 pour les opérations PUT, GET et HEAD. Ces sommes de contrôle améliorent l'intégrité des données.

Modifications apportées à la prise en charge du protocole S3

- Ajout de la prise en charge de Mountpoint pour Amazon S3, qui permet aux applications de se connecter directement aux compartiments S3 comme s'il s'agissait de systèmes de fichiers locaux. Vous pouvez désormais utiliser StorageGRID avec davantage d'applications et de cas d'utilisation.
- Dans le cadre de l'ajout de la prise en charge de Mountpoint, StorageGRID 11.9 contient ["modifications supplémentaires apportées à la prise en charge du protocole S3"](#) .

Maintenance et supportabilité

AutoSupport

["AutoSupport"](#) crée désormais automatiquement des cas de défaillance matérielle pour les appareils hérités.

Opérations de clonage de nœuds étendues

La facilité d'utilisation du clonage de nœuds a été étendue pour prendre en charge des nœuds de stockage plus grands.

Gestion ILM améliorée des marqueurs de suppression expirés

Les règles de temps d'ingestion ILM avec une période de jours suppriment désormais également les marqueurs de suppression d'objets expirés. Les marqueurs de suppression ne sont supprimés que lorsqu'une période de jours s'est écoulée et que le marqueur de suppression actuel a expiré (il n'existe aucune version non actuelle).

Se référer à ["Comment les objets versionnés S3 sont supprimés"](#) et ["Exemple de cycle de vie d'un bucket prioritaire sur la politique ILM"](#) .

Amélioration de la mise hors service des nœuds

Pour assurer une transition fluide et efficace vers le matériel de nouvelle génération StorageGRID, ["déclassement des nœuds"](#) a été amélioré.

Syslog pour les points de terminaison de l'équilibreur de charge

Les journaux d'accès aux points de terminaison de l'équilibreur de charge contiennent des informations de dépannage, telles que les codes d'état HTTP. StorageGRID prend désormais en charge ["exporter ces journaux vers un serveur syslog externe"](#) . Cette amélioration permet une gestion des journaux plus efficace et une intégration avec les systèmes de surveillance et d'alerte existants.

Améliorations supplémentaires pour la maintenance et la prise en charge

- Mise à jour de l'interface utilisateur des métriques
- Qualifications du nouveau système d'exploitation
- Prise en charge de nouveaux composants tiers

Sécurité

Rotation des clés d'accès SSH

Les administrateurs de réseau peuvent désormais ["mettre à jour et faire pivoter les clés SSH"](#) . La possibilité de faire tourner les clés SSH est une bonne pratique de sécurité et un mécanisme de défense proactif.

Alertes pour les connexions root

Lorsqu'une entité inconnue se connecte au Grid Manager en tant que root, ["une alerte est déclenchée"](#) . La surveillance des connexions SSH root est une étape proactive vers la protection de votre infrastructure.

Améliorations du gestionnaire de grille

Page des profils de codage d'effacement déplacée

La page des profils de codage d'effacement se trouve désormais dans **CONFIGURATION > Système > Codage d'effacement**. Il était dans le menu ILM.

Améliorations de la recherche

Le ["champ de recherche dans le gestionnaire de grille"](#) inclut désormais une meilleure logique de correspondance, vous permettant de trouver des pages en recherchant des abréviations courantes et par les noms de certains paramètres dans une page. Vous pouvez également rechercher d'autres types d'éléments, tels que des nœuds, des utilisateurs et des comptes locataires.

Fonctionnalités et capacités supprimées ou obsolètes

Certaines fonctionnalités et capacités ont été supprimées ou obsolètes dans cette version. Passez en revue ces éléments pour comprendre si vous devez mettre à jour les applications clientes ou modifier votre configuration avant la mise à niveau.

Définitions

Obsolète

Cette fonctionnalité **ne devrait pas** être utilisée dans les nouveaux environnements de production. Les environnements de production existants peuvent continuer à utiliser la fonctionnalité.

Fin de vie

Dernière version livrée prenant en charge la fonctionnalité. Dans certains cas, la documentation de la fonctionnalité peut être supprimée à ce stade.

Supprimé

Première version qui **ne** prend pas en charge la fonctionnalité.

Fin de la prise en charge des fonctionnalités de StorageGRID

Les fonctionnalités obsolètes seront supprimées dans les versions majeures N+2. Par exemple, si une fonctionnalité est obsolète dans la version N (par exemple, 6.3), la dernière version où la fonctionnalité existera est N+1 (par exemple, 6.4). La version N+2 (par exemple, 6.5) est la première version lorsque la fonctionnalité n'existe pas dans le produit.

Voir le "[Page de support des versions logicielles](#)" pour plus d'informations.



Dans certaines situations, NetApp peut mettre fin à la prise en charge de fonctionnalités particulières plus tôt que prévu.

Fonctionnalité	Obsolète	Fin de vie	Supprimé	Liens vers la documentation antérieure
Alarmes héritées (<i>pas des alertes</i>)	11,7	11,8	11,9	"Référence des alarmes (StorageGRID 11.8)"
Prise en charge du nœud d'archivage	11,7	11,8	11,9	"Considérations relatives à la mise hors service des nœuds d'archive (StorageGRID 11.8)" Remarque : Avant de commencer votre mise à niveau, vous devez : 1. Désaffecter tous les nœuds d'archives. Voir "Mise hors service des nœuds de grille (site de documentation StorageGRID 11.8)" . 2. Supprimez toutes les références de nœud d'archive des pools de stockage et des stratégies ILM. Voir "Base de connaissances NetApp : Guide de résolution de la mise à niveau du logiciel StorageGRID 11.9" .
Exportation d'audit via CIFS/Samba	11,1	11,6	11,7	
Service CLB	11,4	11,6	11,7	
Moteur de conteneur Docker	11,8	11,9	À déterminer	La prise en charge de Docker comme moteur de conteneur pour les déploiements uniquement logiciels est obsolète. Docker sera remplacé par un autre moteur de conteneur dans une prochaine version. Reportez-vous à la "liste des versions de Docker actuellement prises en charge" .

Fonctionnalité	Obsolète	Fin de vie	Supprimé	Liens vers la documentation antérieure
Exportation d'audit NFS	11,8	11,9	12,0	"Configurer l'accès client d'audit pour NFS (StorageGRID 11.8)"
Prise en charge de l'API Swift	11,7	11,9	12,0	"Utiliser l'API REST Swift (StorageGRID 11.8)"
RHEL 8,8	11,9	11,9	12,0	
RHEL 9,0	11,9	11,9	12,0	
RHEL 9,2	11,9	11,9	12,0	
Ubuntu 18,04	11,9	11,9	12,0	
Ubuntu 20,04	11,9	11,9	12,0	
Debian 11	11,9	11,9	12,0	

Voir aussi :

- ["Modifications apportées à l'API de gestion de la grille"](#)
- ["Modifications apportées à l'API de gestion des locataires"](#)

Modifications apportées à l'API de gestion de la grille

StorageGRID 11.9 utilise la version 4 de l'API Grid Management. La version 4 rend obsolète la version 3 ; cependant, les versions 1, 2 et 3 sont toujours prises en charge.



Vous pouvez continuer à utiliser les versions obsolètes de l'API de gestion avec StorageGRID 11.9 ; toutefois, la prise en charge de ces versions de l'API sera supprimée dans une future version de StorageGRID. Après la mise à niveau vers StorageGRID 11.9, vous pouvez désactiver les API obsolètes à l'aide de l' `PUT /grid/config/management` API.

Pour en savoir plus, rendez-vous sur ["Utiliser l'API de gestion de grille"](#) .

Vérifier les paramètres de conformité après avoir activé le verrouillage global des objets S3

Vérifiez les paramètres de conformité des locataires existants après avoir activé le paramètre global de verrouillage d'objet S3. Lorsque vous activez ce paramètre, les paramètres de verrouillage d'objet S3 par locataire dépendent de la version de StorageGRID au moment de la création du locataire.

Suppression des requêtes héritées de l'API de gestion

Ces demandes héritées ont été supprimées :

`/grid/server-types`

Modifications apportées à GET /private/storage-usage API

- Une nouvelle propriété, `usageCacheDuration`, a été ajoutée au corps de la réponse. Cette propriété spécifie la durée (en secondes) pendant laquelle le cache de recherche d'utilisation reste valide. Cette valeur s'applique lors de la vérification de l'utilisation par rapport au quota de stockage du locataire et aux limites de capacité du bucket.
- Le GET /api/v4/private/storage-usage le comportement a été corrigé pour correspondre à l'imbrication du schéma.
- Ces modifications s'appliquent uniquement à l'API privée.

Modifications apportées à GET cross-grid-replication API

L'API GET **/org/containers/:name/cross-grid-replication** ne nécessite plus l'accès `root(rootAccess)` autorisation ; cependant, vous devez appartenir à un groupe d'utilisateurs disposant de l'autorisation `Gérer tous les compartiments(manageAllContainers)` ou `Voir tous les buckets(viewAllContainers)` autorisation.

L'API PUT **/org/containers/:name/cross-grid-replication** est inchangée et nécessite toujours l'accès `root(rootAccess)` autorisation.

Modifications apportées à l'API de gestion des locataires

StorageGRID 11.9 utilise la version 4 de l'API de gestion des locataires. La version 4 rend obsolète la version 3 ; cependant, les versions 1, 2 et 3 sont toujours prises en charge.



Vous pouvez continuer à utiliser les versions obsolètes de l'API de gestion des locataires avec StorageGRID 11.9 ; toutefois, la prise en charge de ces versions de l'API sera supprimée dans une future version de StorageGRID. Après la mise à niveau vers StorageGRID 11.9, vous pouvez désactiver les API obsolètes à l'aide de l' PUT /grid/config/management API.

Pour en savoir plus, rendez-vous sur ["Comprendre l'API de gestion des locataires"](#) .

Nouvelle API pour la limite de capacité du bucket

Vous pouvez utiliser le `/org/containers/{bucketName}/quota-object-bytes` API avec opérations GET/PUT pour obtenir et définir la limite de capacité de stockage d'un bucket.

Planifier et préparer la mise à niveau

Estimez le temps nécessaire pour effectuer une mise à niveau

Réfléchissez au moment de la mise à niveau, en fonction de la durée de la mise à niveau. Soyez conscient des opérations que vous pouvez et ne pouvez pas effectuer à chaque étape de la mise à niveau.

À propos de cette tâche

Le temps nécessaire pour effectuer une mise à niveau de 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 suivant 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 vérifications préalables et mettez à niveau le nœud d'administration principal	Les vérifications préalables de mise à niveau sont exécutées et le nœud d'administration principal est arrêté, mis à niveau et redémarré.	30 minutes à 1 heure, les nœuds d'appareils de services nécessitant le plus de temps. Les erreurs de pré-vérification non résolues augmenteront 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 pré-vérifications de mise à niveau avant de démarrer la mise à niveau vous permet de résoudre les erreurs avant la fenêtre de maintenance de mise à niveau planifiée.
Démarrer le service de mise à niveau	Le fichier logiciel est distribué et le service de mise à niveau est démarré.	3 minutes par nœud de grille	
Mettre à niveau d'autres nœuds de grille	Le logiciel de tous les autres nœuds de grille est mis à niveau, dans l'ordre dans lequel vous approuvez les nœuds. Chaque nœud de votre système sera mis hors service un par un.	15 minutes à 1 heure par nœud, les nœuds d'appareils nécessitant 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 ne pouvez pas effectuer d'autres procédures de maintenance, telles que la correction à chaud, la mise hors service ou l'extension. Remarque : Si vous devez effectuer une récupération, contactez le support technique.
Activer les fonctionnalités	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.

Tâche de mise à niveau	Description	Temps approximatif requis	Au cours de cette tâche
Mettre à jour 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 de la grille	La mise à niveau de StorageGRID 11.8 vers 11.9 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 des fonctionnalités de StorageGRID , l'étape de mise à jour de la base de données Cassandra peut prendre plusieurs jours.
Étapes finales de mise à niveau	Les fichiers temporaires sont supprimés et la mise à niveau vers la nouvelle version est terminée.	5 minutes	Une fois la tâche Étapes de mise à niveau finales terminée, vous pouvez effectuer toutes les procédures de maintenance.

Étapes

1. Estimez le temps nécessaire pour mettre à niveau tous les nœuds du réseau.
 - a. Multipliez le nombre de nœuds de votre système StorageGRID par 1 heure/nœud.

En règle générale, la mise à niveau des nœuds d'appareil prend plus de temps que celle des nœuds logiciels.
 - b. Ajoutez 1 heure à ce temps pour tenir compte du temps nécessaire au téléchargement du `.upgrade` fichier, exécutez les validations de pré-vérification et terminez les étapes de mise à niveau finales.
2. Si vous avez des nœuds Linux, ajoutez 15 minutes pour chaque nœud pour tenir compte du temps nécessaire au téléchargement et à l'installation du package RPM ou DEB.
3. Calculez le temps total estimé pour la mise à niveau en additionnant les résultats des étapes 1 et 2.

Exemple : Temps estimé pour la mise à niveau vers StorageGRID 11.9

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 tenir compte du téléchargement, de la pré-vérification et des étapes finales.

Le temps estimé pour mettre à niveau tous les nœuds est de 15 heures.

3. Multipliez 8 par 15 minutes/nœud pour tenir compte du temps d'installation du package RPM ou DEB sur les nœuds Linux.

Le temps estimé pour cette étape est de 2 heures.

4. Additionnez les valeurs ensemble.

Vous devez prévoir jusqu'à 17 heures pour terminer la mise à niveau de votre système vers StorageGRID 11.9.0.



Si nécessaire, vous pouvez diviser la fenêtre de maintenance en fenêtres plus petites en approuvant des sous-ensembles de nœuds de grille à mettre à niveau dans plusieurs sessions. Par exemple, vous préférerez peut-être mettre à niveau les nœuds du site A au cours d'une session, puis mettre à niveau les nœuds du site B au cours d'une session ultérieure. Si vous choisissez d'effectuer la mise à niveau en plusieurs sessions, sachez que vous ne pourrez pas commencer à utiliser les nouvelles fonctionnalités tant que tous les nœuds n'auront pas été mis à niveau.

Comment votre système est affecté pendant la mise à niveau

Découvrez comment votre système StorageGRID sera affecté lors de la mise à niveau.

Les mises à niveau de StorageGRID ne provoquent aucune interruption

Le système StorageGRID peut ingérer et récupérer des données à partir des applications clientes 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, les nœuds de stockage), les nœuds sont arrêtés un par un, de sorte qu'il n'y a aucun moment où tous les nœuds de grille ou tous les nœuds de grille d'un certain type sont indisponibles.

Pour permettre une disponibilité continue, assurez-vous que votre politique ILM contient des règles qui spécifient le stockage de plusieurs copies de chaque objet. Vous devez également vous assurer que tous les clients S3 externes sont configurés pour envoyer des requêtes à l'un des éléments suivants :

- Une adresse IP virtuelle de groupe haute disponibilité (HA)
- Un équilibreur de charge tiers à haute disponibilité
- Plusieurs nœuds de passerelle pour chaque client
- Plusieurs nœuds de stockage pour chaque client

Les applications clientes peuvent subir des perturbations à court terme

Le système StorageGRID peut ingérer et récupérer des données à partir d'applications clientes tout au long du processus de mise à niveau. Cependant, les connexions clientes aux nœuds de passerelle ou aux nœuds de stockage individuels peuvent être temporairement interrompues si la mise à niveau doit redémarrer les services sur ces nœuds. La connectivité sera restaurée une fois le processus de mise à niveau terminé et les services reprendront sur les nœuds individuels.

Vous devrez peut-être planifier un temps d'arrêt pour appliquer une mise à niveau si la perte de connectivité pendant une courte période n'est pas acceptable. Vous pouvez utiliser l'approbation sélective pour planifier le moment où certains nœuds sont mis à jour.



Vous pouvez utiliser plusieurs passerelles et groupes de haute disponibilité (HA) pour assurer un basculement automatique pendant le processus de mise à niveau. Voir les instructions pour "[configuration des groupes de haute disponibilité](#)".

Le micrologiciel de l'appareil est mis à niveau

Pendant la mise à niveau vers StorageGRID 11.9 :

- Tous les nœuds d'appliance StorageGRID sont automatiquement mis à niveau vers la version 3.9 du micrologiciel du programme d'installation de l'appliance StorageGRID .
- Les appareils SG6060 et SGF6024 sont automatiquement mis à niveau vers la version 3B08.EX du micrologiciel du BIOS et la version 4.00.07 du micrologiciel BMC .

- Les appareils SG100 et SG1000 sont automatiquement mis à niveau vers la version 3B13.EC du micrologiciel du BIOS et la version 4.74.07 du micrologiciel BMC .
- Les appareils SGF6112, SG6160, SG110 et SG1100 sont automatiquement mis à niveau vers la version 3.16.07 du micrologiciel BMC .

Les politiques ILM sont traitées différemment selon leur statut

- La politique active restera la même après la mise à niveau.
- Seules les 10 dernières politiques historiques sont conservées lors de la mise à niveau.
- S'il existe une politique proposée, elle sera supprimée lors de la mise à niveau.

Des alertes peuvent être déclenchées

Des alertes peuvent être déclenchées lorsque les services démarrent et s'arrêtent et lorsque le système StorageGRID fonctionne dans un environnement à versions mixtes (certains nœuds de grille exécutant une version antérieure, tandis que d'autres ont été mis à niveau vers une version ultérieure). 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 **Erreur de communication Cassandra** lorsque certains nœuds ont été mis à niveau vers StorageGRID 11.9 mais que d'autres nœuds exécutent toujours StorageGRID 11.8. En général, ces alertes disparaissent une fois la mise à niveau terminée.

L'alerte **Placement ILM impossible** peut être déclenchée lorsque les nœuds de stockage sont arrêtés pendant la mise à niveau vers StorageGRID 11.9. Cette alerte peut persister pendant 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 du gestionnaire de grille.

De nombreuses notifications SNMP sont générées

Sachez qu'un grand nombre de notifications SNMP peuvent être générées lorsque les nœuds de grille sont arrêtés et redémarrés pendant la mise à niveau. Pour éviter les notifications excessives, décochez la case **Activer les notifications de l'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 11.8 vers StorageGRID 11.9. 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 ce que la tâche **Activer la nouvelle fonctionnalité** soit terminée :

- N'apportez aucune modification à la configuration de la grille.
- N'activez ni ne désactivez aucune nouvelle fonctionnalité.
- Ne mettez pas à jour la configuration ILM. Dans le cas contraire, vous risquez de rencontrer un comportement ILM incohérent et inattendu.

- N'appliquez pas de correctif ni ne récupérez un nœud de grille.



Contactez le support technique si vous devez récupérer un nœud pendant la mise à niveau.

- Vous ne devez pas gérer les groupes HA, les interfaces VLAN ou les points de terminaison d'équilibrage de charge pendant la mise à niveau vers StorageGRID 11.9.
- Ne supprimez aucun groupe HA tant que la mise à niveau vers StorageGRID 11.9 n'est pas terminée. Les adresses IP virtuelles dans d'autres groupes HA peuvent devenir inaccessibles.

Jusqu'à ce que la tâche **Étapes de mise à niveau finales** soit terminée :

- N'effectuez pas de procédure d'expansion.
- N'effectuez pas de procédure de mise hors service.

Vous ne pouvez pas afficher les détails des buckets ni les gérer à partir du gestionnaire de locataires.

Lors de la mise à niveau vers StorageGRID 11.9 (c'est-à-dire lorsque le système fonctionne comme un environnement de version mixte), vous ne pouvez pas afficher les détails des buckets ni gérer les buckets à l'aide du gestionnaire de locataires. L'une des erreurs suivantes apparaît sur la page Buckets dans Tenant Manager :

- Vous ne pouvez pas utiliser cette API pendant la mise à niveau vers la version 11.9.
- Vous ne pouvez pas afficher les détails de version du bucket dans le gestionnaire de locataires pendant que vous effectuez une mise à niveau vers la version 11.9.

Cette erreur sera résolue une fois la mise à niveau vers la version 11.9 terminée.

Solution de contournement

Pendant que la mise à niveau vers la version 11.9 est en cours, utilisez les outils suivants pour afficher les détails des buckets ou gérer les buckets, au lieu d'utiliser le gestionnaire de locataires :

- Pour effectuer des opérations S3 standard sur un bucket, utilisez soit le ["API REST S3"](#) ou le ["API de gestion des locataires"](#) .
- Pour effectuer des opérations personnalisées StorageGRID sur un bucket (par exemple, afficher et modifier la cohérence du bucket, activer ou désactiver les mises à jour de l'heure du dernier accès ou configurer l'intégration de la recherche), utilisez l'API de gestion des locataires.

Vérifiez la version installée de StorageGRID

Avant de commencer la mise à niveau, vérifiez que la version précédente de StorageGRID est actuellement installée avec le dernier correctif disponible appliqué.

À propos de cette tâche

Avant de procéder à la mise à niveau vers StorageGRID 11.9, StorageGRID 11.8 doit être installé sur votre grille. Si vous utilisez actuellement une version antérieure de StorageGRID, vous devez installer tous les fichiers de mise à niveau précédents ainsi que leurs derniers correctifs (fortement recommandé) jusqu'à ce que la version actuelle de votre grille soit StorageGRID 11.8.x.y.

Un chemin de mise à niveau possible est indiqué dans le [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 pour chaque nouvelle version que vous installez. Dans certains cas, vous devez appliquer un correctif pour éviter le risque de perte de données. Voir ["Téléchargements NetApp : StorageGRID"](#) et les notes de publication de chaque correctif pour en savoir plus.

Étapes

1. Sign in au Grid Manager à l'aide d'un ["navigateur Web pris en charge"](#).
2. En haut du Gestionnaire de grille, sélectionnez **Aide > À propos**.
3. Vérifiez que la **Version** est 11.8.x.y.

Dans le numéro de version StorageGRID 11.8.x.y :

- La **version majeure** a une valeur x de 0 (11.8.0).
 - Un **hotfix**, s'il a été appliqué, a une valeur y (par exemple, 11.8.0.1).
4. Si **Version** n'est pas 11.8.x.y, accédez à ["Téléchargements 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. Ensuite, effectuez la procédure de mise à niveau du logiciel pour cette version et appliquez le dernier correctif pour cette version (fortement recommandé).

Voir le ["Procédure de correctif logiciel StorageGRID"](#).

Exemple : Mise à niveau vers StorageGRID 11.9 à partir de la version 11.6

L'exemple suivant montre les étapes de mise à niveau de StorageGRID version 11.6 vers la version 11.8 en préparation d'une mise à niveau vers StorageGRID 11.9.

Téléchargez et installez le logiciel dans l'ordre suivant pour préparer votre système à la mise à niveau :

1. Mise à niveau vers la version majeure de StorageGRID 11.6.0.
2. Appliquez le dernier correctif StorageGRID 11.6.0.y.
3. Mise à niveau vers la version majeure de StorageGRID 11.7.0.
4. Appliquez le dernier correctif StorageGRID 11.7.0.y.
5. Mise à niveau vers la version majeure de StorageGRID 11.8.0.
6. Appliquez le dernier correctif StorageGRID 11.8.0.y.

Obtenir le matériel nécessaire à une mise à niveau logicielle

Avant de commencer la mise à niveau du logiciel, procurez-vous tout le matériel nécessaire.

Article	Remarques
Ordinateur portable de service	L'ordinateur portable de service doit avoir : • Port réseau • Client SSH (par exemple, PuTTY)
"Navigateur Web pris en charge"	La prise en charge du navigateur change généralement pour chaque version de StorageGRID . Assurez-vous que votre navigateur est compatible avec la nouvelle version de StorageGRID .
Mot de passe d'approvisionnement	La phrase secrète est créée et documentée lors de la première installation du système StorageGRID . La phrase secrète de provisionnement n'est pas répertoriée dans le <code>Passwords.txt</code> déposer.
Archive Linux RPM ou DEB	Si des nœuds sont déployés sur des hôtes Linux, vous devez "téléchargez et installez le package RPM ou DEB sur tous les hôtes" avant de commencer la mise à niveau. Assurez-vous que votre système d'exploitation répond aux exigences minimales de version du noyau de StorageGRID : • "Installer StorageGRID sur les hôtes Red Hat Enterprise Linux" • "Installer StorageGRID sur des hôtes Ubuntu ou Debian"
Documentation de StorageGRID	• "Notes de version" pour StorageGRID 11.9 (connexion requise). Assurez-vous de les lire attentivement avant de commencer la mise à niveau. • "Guide de résolution de mise à niveau du logiciel StorageGRID" pour la version majeure vers laquelle vous effectuez la mise à niveau (connexion requise) • Autre "Documentation de StorageGRID" , selon les besoins.

Vérifiez l'état du système

Avant de mettre à niveau un système StorageGRID , vérifiez que le système est prêt à accueillir la mise à niveau. Assurez-vous que le système fonctionne normalement et que tous les nœuds du réseau sont opérationnels.

Étapes

1. Sign in au Grid Manager à l'aide d'un ["navigateur Web pris en charge"](#) .
2. Vérifiez et résolvez toutes les alertes actives.
3. Confirmez qu'aucune tâche de grille conflictuelle n'est active ou en attente.
 - a. Sélectionnez **SUPPORT > Outils > Topologie de grille**.
 - b. Sélectionnez **site > nœud d'administration principal > CMN > Tâches de la grille > Configuration**.

Les tâches d'évaluation de la gestion du cycle de vie de l'information (ILME) sont les seules tâches de grille qui peuvent s'exécuter simultanément avec la mise à niveau du logiciel.

- c. Si d'autres tâches de la grille sont actives ou en attente, attendez qu'elles se terminent ou libérez leur verrou.



Contactez le support technique si une tâche ne se termine pas ou ne libère pas son verrou.

4. Se référer à "[Communications internes des nœuds de réseau](#)" et "[Communications externes](#)" pour vous assurer que tous les ports requis pour StorageGRID 11.9 sont ouverts avant la mise à niveau.



Aucun port supplémentaire n'est requis lors de la mise à niveau vers StorageGRID 11.9.

Le port requis suivant a été ajouté dans StorageGRID 11.7. Assurez-vous qu'il est disponible avant de procéder à la mise à niveau vers StorageGRID 11.9.

Port	Description
18086	Port TCP utilisé pour les requêtes S3 de l'équilibreur de charge StorageGRID vers LDR et le nouveau service LDR. Avant la mise à niveau, vérifiez que ce port est ouvert depuis tous les nœuds de grille vers tous les nœuds de stockage. Le blocage de ce port entraînera des interruptions de service S3 après la mise à niveau vers StorageGRID 11.9.



Si vous avez ouvert des ports de pare-feu personnalisés, vous en êtes informé lors de la vérification préalable de la mise à niveau. Vous devez contacter le support technique avant de procéder à la mise à niveau.

Mettre à niveau le logiciel

Démarrage rapide de la mise à niveau

Avant de commencer la mise à niveau, examinez le flux de travail général. La page de mise à niveau de StorageGRID vous guide à travers chaque étape de mise à niveau.

1

Préparer les hôtes Linux

Si des nœuds StorageGRID sont déployés sur des hôtes Linux, "[installer le package RPM ou DEB sur chaque hôte](#)" avant de commencer la mise à niveau.

2

Télécharger les fichiers de mise à niveau et de correctifs

À partir du nœud d'administration principal, accédez à la page de mise à niveau de StorageGRID et téléchargez le fichier de mise à niveau et le fichier de correctif, si nécessaire.

3

Télécharger le package de récupération

Téléchargez le package de récupération actuel avant de commencer la mise à niveau.

4

Exécuter des vérifications préalables de mise à niveau

Les vérifications préalables à la mise à niveau vous aident à détecter les problèmes afin que vous puissiez les résoudre avant de commencer la mise à niveau proprement dite.

5

Démarrer la mise à niveau

Lorsque vous démarrez la mise à niveau, les vérifications préalables sont à nouveau exécutées et le nœud d'administration principal est mis à niveau automatiquement. Vous ne pouvez pas accéder au gestionnaire de grille pendant que le nœud d'administration principal est en cours de mise à niveau. Les journaux d'audit ne seront pas non plus disponibles. Cette mise à niveau peut prendre jusqu'à 30 minutes.

6

Télécharger le package de récupération

Une fois le nœud d'administration principal mis à niveau, téléchargez un nouveau package de récupération.

7

Approuver les nœuds

Vous pouvez approuver des nœuds de grille individuels, des groupes de nœuds de grille ou tous les nœuds de grille.



N'approuvez pas la mise à niveau d'un nœud de grille à moins d'être 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, les nouvelles fonctionnalités sont activées et vous pouvez reprendre vos opérations. Vous devez attendre que la tâche d'arrière-plan **Mettre à niveau la base de données** et la tâche **Étapes finales de mise à niveau** soient terminées avant d'effectuer une procédure de mise hors service ou d'extension.

Informations connexes

["Estimez le temps nécessaire pour effectuer une mise à niveau"](#)

Linux : téléchargez et installez le package RPM ou DEB sur tous les hôtes

Si des nœuds StorageGRID sont déployés sur des hôtes Linux, téléchargez et installez un package RPM ou DEB supplémentaire sur chacun de ces hôtes avant de démarrer la mise à niveau.

Télécharger les fichiers de mise à niveau, Linux et de correctifs

Lorsque vous effectuez une mise à niveau de StorageGRID à partir du Grid Manager, vous êtes invité à télécharger l'archive de mise à niveau et tout correctif requis comme première étape. Cependant, si vous devez télécharger des fichiers pour mettre à niveau les hôtes Linux, vous pouvez gagner du temps en téléchargeant tous les fichiers requis à l'avance.

Étapes

1. Aller à ["Téléchargements NetApp : StorageGRID"](#) .
2. Sélectionnez le bouton pour télécharger la dernière version ou sélectionnez une autre version dans le menu déroulant et sélectionnez **Aller**.

Les versions du logiciel StorageGRID ont ce format : 11.x.y. Les correctifs StorageGRID ont ce format : 11.x.y.z.

3. Sign in avec le nom d'utilisateur et le mot de passe de votre compte NetApp .
4. Si un avis d'avertissement/à lire absolument apparaît, notez le numéro du correctif et cochez la case.
5. Lisez le contrat de licence utilisateur final (CLUF), cochez la case, puis sélectionnez **Accepter et continuer**.

La page de téléchargement de la version que vous avez sélectionnée apparaît. La page contient trois colonnes.

6. À 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**). Bien que ce fichier ne soit pas nécessaire jusqu'à ce que vous effectuiez la mise à niveau, le télécharger maintenant vous fera gagner du temps.
 - Une archive RPM ou DEB dans l'un ou l'autre .tgz ou .zip format. Sélectionnez le .zip fichier si vous exécutez Windows sur l'ordinateur portable de service.
 - Red Hat Enterprise Linux
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 de mise en garde/de lecture obligatoire en raison d'un correctif requis, téléchargez le correctif :
 - a. Retourner à ["Téléchargements NetApp : StorageGRID"](#) .
 - b. Sélectionnez le numéro du correctif dans la liste déroulante.
 - c. Acceptez à nouveau l'avertissement 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 de mise à niveau de StorageGRID lorsque vous démarrerez la mise à niveau.

Installer l'archive sur tous les hôtes Linux

Effectuez ces étapes 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.

Consultez les étapes d'installation des services hôtes StorageGRID dans les instructions d'installation :

- ["Red Hat Enterprise Linux : installer les services hôtes StorageGRID"](#)
- ["Ubuntu ou Debian : installer les services hôtes StorageGRID"](#)

Les nouveaux packages sont installés en tant que packages supplémentaires.

Supprimer les archives d'installation des versions précédentes

Pour libérer de l'espace sur les hôtes Linux, vous pouvez supprimer les archives d'installation des versions précédentes de StorageGRID dont vous n'avez plus besoin.

Étapes

1. Supprimez les anciennes archives d'installation de StorageGRID .

Chapeau rouge

1. Capturez la liste des packages StorageGRID installés : `dnf list | grep -i storagegrid`.

Exemple:

```
[root@rhel-example ~]# dnf list | grep -i storagegrid
StorageGRID-Webscale-Images-11-6-0.x86_64 11.6.0-
20220210.0232.8d56cfe @System
StorageGRID-Webscale-Images-11-7-0.x86_64 11.7.0-
20230424.2238.1a2cf8c @System
StorageGRID-Webscale-Images-11-8-0.x86_64 11.8.0-
20240131.0139.e3e0c87 @System
StorageGRID-Webscale-Images-11-9-0.x86_64 11.9.0-
20240826.1753.4aeeb70 @System
StorageGRID-Webscale-Service-11-6-0.x86_64 11.6.0-
20220210.0232.8d56cfe @System
StorageGRID-Webscale-Service-11-7-0.x86_64 11.7.0-
20230424.2238.1a2cf8c @System
StorageGRID-Webscale-Service-11-8-0.x86_64 11.8.0-
20240131.0139.e3e0c87 @System
StorageGRID-Webscale-Service-11-9-0.x86_64 11.9.0-
20240826.1753.4aeeb70 @System
[root@rhel-example ~]#
```

2. Supprimer les packages StorageGRID précédents : `dnf remove images-package service-package`



Ne supprimez pas les archives d'installation de la version de StorageGRID que vous exécutez actuellement ou des versions de StorageGRID vers lesquelles vous prévoyez de mettre à niveau.

Vous pouvez ignorer en toute sécurité les avertissements qui s'affichent. Ils font référence aux fichiers qui ont été remplacés lors de l'installation de packages StorageGRID plus récents.

Exemple:

```
[root@rhel-example ~]# dnf remove StorageGRID-Webscale-Images-11-6-
0.x86_64 StorageGRID-Webscale-Service-11-6-0.x86_64
Updating Subscription Management repositories.
Unable to read consumer identity

This system is not registered with an entitlement server. You can
use subscription-manager to register.

Dependencies resolved.
```

```

=====
=====
Package                Architecture      Version           Repository
Size
=====
=====
Removing:
StorageGRID-Webscale-Images-11-6-0 x86_64 11.6.0-
20220210.0232.8d56cfe @System 2.7 G
StorageGRID-Webscale-Service-11-6-0 x86_64 11.6.0-
20220210.0232.8d56cfe @System 7.5 M

Transaction Summary
=====
=====
Remove 2 Packages

Freed space: 2.8 G
Is this ok [y/N]: y
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing: 1/1
  Running scriptlet: StorageGRID-Webscale-Service-11-6-0-11.6.0-
20220210.0232.8d56cfe.x86_64 1/2
  Erasing: StorageGRID-Webscale-Service-11-6-0-11.6.0-
20220210.0232.8d56cfe.x86_64 1/2
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/strategy/ipv6.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/strategy/ipv4.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/strategy/eui64.pyc
: remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/strategy/eui48.pyc
: remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/strategy/__init__
.pyc: remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/ip/sets.pyc:

```

```
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/ip/rfc1924.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/ip/nmap.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/ip/iana.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/ip/glob.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/ip/__init__.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/fbsocket.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/eui/ieee.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/eui/__init__.pyc:
remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/core.pyc: remove
failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/contrib/subnet_spl
itter.pyc: remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/contrib/__init__.p
yc: remove failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/compat.pyc: remove
failed: No such file or directory
warning: file /usr/lib64/python2.7/site-
packages/netapp/storagegrid/vendor/latest/netaddr/__init__.pyc:
remove failed: No such file or directory
```

```
Erasing: StorageGRID-Webscale-Images-11-6-0-11.6.0-
20220210.0232.8d56cfe.x86_64 2/2
```

```
Verifying: StorageGRID-Webscale-Images-11-6-0-11.6.0-
20220210.0232.8d56cfe.x86_64 1/2
```

```
Verifying: StorageGRID-Webscale-Service-11-6-0-11.6.0-
```

```
20220210.0232.8d56cfe.x86_64 2/2
```

Installed products updated.

Removed:

```
StorageGRID-Webscale-Images-11-6-0-11.6.0-  
20220210.0232.8d56cfe.x86_64  
StorageGRID-Webscale-Service-11-6-0-11.6.0-  
20220210.0232.8d56cfe.x86_64
```

Complete!

```
[root@rhel-example ~]#
```

Ubuntu et Debian

1. Capturez la liste des packages StorageGRID installés : `dpkg -l | grep storagegrid`

Exemple:

```
root@debian-example:~# dpkg -l | grep storagegrid  
ii storagegrid-webscale-images-11-6-0 11.6.0-20220210.0232.8d56cfe  
amd64 StorageGRID Webscale docker images for 11.6.0  
ii storagegrid-webscale-images-11-7-0 11.7.0-  
20230424.2238.1a2cf8c.dev-signed amd64 StorageGRID Webscale docker  
images for 11.7.0  
ii storagegrid-webscale-images-11-8-0 11.8.0-20240131.0139.e3e0c87  
amd64 StorageGRID Webscale docker images for 11.8.0  
ii storagegrid-webscale-images-11-9-0 11.9.0-20240826.1753.4aeeb70  
amd64 StorageGRID Webscale docker images for 11.9.0  
ii storagegrid-webscale-service-11-6-0 11.6.0-20220210.0232.8d56cfe  
amd64 StorageGRID Webscale host services for 11.6.0  
ii storagegrid-webscale-service-11-7-0 11.7.0-20230424.2238.1a2cf8c  
amd64 StorageGRID Webscale host services for 11.7.0  
ii storagegrid-webscale-service-11-8-0 11.8.0-20240131.0139.e3e0c87  
amd64 StorageGRID Webscale host services for 11.8.0  
ii storagegrid-webscale-service-11-9-0 11.9.0-20240826.1753.4aeeb70  
amd64 StorageGRID Webscale host services for 11.9.0  
root@debian-example:~#
```

2. Supprimer les packages StorageGRID précédents : `dpkg -r images-package service-package`



Ne supprimez pas les archives d'installation de la version de StorageGRID que vous exécutez actuellement ou des versions de StorageGRID vers lesquelles vous prévoyez de mettre à niveau.

Exemple:

```
root@debian-example:~# dpkg -r storagegrid-webscale-service-11-6-0
storagegrid-webscale-images-11-6-0
(Reading database ... 38190 files and directories currently
installed.)
Removing storagegrid-webscale-service-11-6-0 (11.6.0-
20220210.0232.8d56cfe) ...
locale: Cannot set LC_CTYPE to default locale: No such file or
directory
locale: Cannot set LC_MESSAGES to default locale: No such file or
directory
locale: Cannot set LC_ALL to default locale: No such file or
directory
dpkg: warning: while removing storagegrid-webscale-service-11-6-0,
directory '/usr/lib/python2.7/dist-
packages/netapp/storagegrid/vendor/latest' not empty so not removed
Removing storagegrid-webscale-images-11-6-0 (11.6.0-
20220210.0232.8d56cfe) ...
root@debian-example:~#
```

1. Supprimez les images de conteneur StorageGRID .

Docker

1. Capturez la liste des images de conteneur installées : `docker images`

Exemple:

```
[root@docker-example ~]# docker images
REPOSITORY          TAG                 IMAGE ID            CREATED
SIZE
storagegrid-11.9.0  Admin_Node         610f2595bcb4       2 days ago
2.77GB
storagegrid-11.9.0  Storage_Node       7f73d33eb880       2 days ago
2.65GB
storagegrid-11.9.0  API_Gateway        2f0bb79526e9       2 days ago
1.82GB
storagegrid-11.8.0  Storage_Node       7125480de71b       7 months ago
2.54GB
storagegrid-11.8.0  Admin_Node         404e9f1bd173       7 months ago
2.63GB
storagegrid-11.8.0  Archive_Node       c3294a29697c       7 months ago
2.39GB
storagegrid-11.8.0  API_Gateway        1f88f24b9098       7 months ago
1.74GB
storagegrid-11.7.0  Storage_Node       1655350eff6f       16 months ago
2.51GB
storagegrid-11.7.0  Admin_Node         872258dd0dc8       16 months ago
2.48GB
storagegrid-11.7.0  Archive_Node       121e7c8b6d3b       16 months ago
2.41GB
storagegrid-11.7.0  API_Gateway        5b7a26e382de       16 months ago
1.77GB
storagegrid-11.6.0  Admin_Node         ee39f71a73e1       2 years ago
2.38GB
storagegrid-11.6.0  Storage_Node       f5ef895dcad0       2 years ago
2.08GB
storagegrid-11.6.0  Archive_Node       5782de552db0       2 years ago
1.95GB
storagegrid-11.6.0  API_Gateway        cb480ed37eea       2 years ago
1.35GB
[root@docker-example ~]#
```

2. Supprimez les images de conteneur pour les versions précédentes de StorageGRID : `docker rmi image id`



Ne supprimez pas les images de conteneur pour la version de StorageGRID que vous exécutez actuellement ou les versions de StorageGRID vers lesquelles vous prévoyez de mettre à niveau.

Exemple:

```
[root@docker-example ~]# docker rmi cb480ed37eea
Untagged: storagegrid-11.6.0:API_Gateway
Deleted:
sha256:cb480ed37eea0ae9cf3522de1dadfbff0075010d89c1c0a2337a3178051ddf02
Deleted:
sha256:5f269aabbf15c32c1fe6f36329c304b6c6ecb563d973794b9b59e8e5ab8cccafa
Deleted:
sha256:47c2b2c295a77b312b8db69db58a02d8e09e929e121352bec713fa12dae66bde
[root@docker-example ~]#
```

Podman

1. Capturez la liste des images de conteneur installées : `podman images`

Exemple:

```
[root@podman-example ~]# podman images
```

REPOSITORY SIZE	TAG	IMAGE ID	CREATED
localhost/storagegrid-11.8.0 2.57 GB	Storage_Node	7125480de71b	7 months ago
localhost/storagegrid-11.8.0 2.67 GB	Admin_Node	404e9f1bd173	7 months ago
localhost/storagegrid-11.8.0 2.42 GB	Archive_Node	c3294a29697c	7 months ago
localhost/storagegrid-11.8.0 1.77 GB	API_Gateway	1f88f24b9098	7 months ago
localhost/storagegrid-11.7.0 2.54 GB	Storage_Node	1655350eff6f	16 months ago
localhost/storagegrid-11.7.0 2.51 GB	Admin_Node	872258dd0dc8	16 months ago
localhost/storagegrid-11.7.0 2.44 GB	Archive_Node	121e7c8b6d3b	16 months ago
localhost/storagegrid-11.7.0 1.8 GB	API_Gateway	5b7a26e382de	16 months ago
localhost/storagegrid-11.6.0 2.42 GB	Admin_Node	ee39f71a73e1	2 years ago
localhost/storagegrid-11.6.0 2.11 GB	Storage_Node	f5ef895dcad0	2 years ago
localhost/storagegrid-11.6.0 1.98 GB	Archive_Node	5782de552db0	2 years ago
localhost/storagegrid-11.6.0 1.38 GB	API_Gateway	cb480ed37eea	2 years ago

```
[root@podman-example ~]#
```

- Supprimez les images de conteneur pour les versions précédentes de StorageGRID : `podman rmi image id`



Ne supprimez pas les images de conteneur pour la version de StorageGRID que vous exécutez actuellement ou les versions de StorageGRID vers lesquelles vous prévoyez de mettre à niveau.

Exemple:

```
[root@podman-example ~]# podman rmi f5ef895dcad0
Untagged: localhost/storagegrid-11.6.0:Storage_Node
Deleted:
f5ef895dcad0d78d0fd21a07dd132d7c7f65f45d80ee7205a4d615494e44cbb7
[root@podman-example ~]#
```

Effectuer la mise à niveau

Vous pouvez effectuer une mise à niveau vers StorageGRID 11.9 et appliquer le dernier correctif pour cette version en même temps. La page de mise à niveau de StorageGRID fournit le chemin de mise à niveau recommandé et des liens directs vers les pages de téléchargement appropriées.

Avant de commencer

Vous avez examiné toutes les considérations et terminé toutes les étapes de planification et de préparation.

Accéder à la page de mise à niveau de StorageGRID

Dans un premier temps, accédez à la page de mise à niveau de StorageGRID dans le gestionnaire de grille.

Étapes

1. Sign in au Grid Manager à l'aide d'un ["navigateur Web pris en charge"](#) .
2. Sélectionnez **MAINTENANCE > Système > Mise à jour du logiciel**.
3. Dans la mosaïque de mise à niveau de StorageGRID , sélectionnez **Mettre à niveau**.

Sélectionner les fichiers

Le chemin de mise à jour sur la page de mise à niveau de StorageGRID indique les versions principales (par exemple, 11.9.0) et les correctifs (par exemple, 11.9.0.1) que vous devez installer pour obtenir la dernière version de StorageGRID . Vous devez installer les versions et les correctifs recommandés dans l'ordre indiqué.



Si aucun chemin de mise à jour n'est affiché, il est possible 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* > Paramètres**) soit désactivée.

Étapes

1. Pour l'étape **Sélectionner les fichiers**, vérifiez le chemin de mise à jour.
2. Dans la section Télécharger les fichiers, sélectionnez chaque lien **Télécharger** pour télécharger les fichiers requis à partir du site de support NetApp .

Si aucun chemin de mise à jour n'est affiché, accédez à la ["Téléchargements NetApp : StorageGRID"](#) pour déterminer si une nouvelle version ou un correctif est disponible et pour télécharger les fichiers dont vous avez besoin.



Si vous devez télécharger et installer un package RPM ou DEB sur tous les hôtes Linux, vous disposez peut-être déjà des fichiers de mise à niveau et de correctifs StorageGRID répertoriés dans le chemin de mise à jour.

3. Sélectionnez **Parcourir** pour télécharger le fichier de mise à niveau de version sur StorageGRID:
`NetApp_StorageGRID_11.9.0_Software_uniqueID.upgrade`

Une fois le processus de téléchargement et de validation terminé, une coche verte apparaît à côté du nom du fichier.

4. Si vous avez téléchargé un fichier de 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**.

Exécuter des pré-vérifications

L'exécution de pré-vérifications vous permet de détecter et de résoudre tout problème de mise à niveau avant de commencer la mise à niveau de votre grille.

Étapes

1. Pour l'étape **Exécuter les pré-vérifications**, commencez par saisir la phrase secrète de provisionnement de votre grille.
2. Sélectionnez **Télécharger le package 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 Recovery Package vous permet de restaurer le système en cas de panne.

3. Une fois le fichier téléchargé, confirmez que vous pouvez accéder au contenu, y compris le `Passwords.txt` déposer.
4. Copier le fichier téléchargé(`.zip`) vers deux endroits sûrs, sécurisés et séparés.



Le fichier du package de récupération doit être sécurisé car il contient des clés de chiffrement et des mots de passe qui peuvent être utilisés pour obtenir des données à partir du système StorageGRID .

5. Sélectionnez **Exécuter les pré-vérifications** et attendez que les pré-vérifications soient terminées.
6. Passez en revue les détails de chaque pré-vérification signalée et résolvez toutes les erreurs signalées. Voir le "[Guide de résolution de mise à niveau du logiciel StorageGRID](#)" pour la version StorageGRID 11.9.

Vous devez résoudre toutes les erreurs de pré-vérification avant de pouvoir mettre à niveau votre système. Cependant, vous n'avez pas besoin de répondre aux *avertissements* de pré-vérification avant la mise à niveau.



Si vous avez ouvert des ports de pare-feu personnalisés, vous en êtes averti lors de la validation préalable. Vous devez contacter le support technique avant de procéder à la mise à niveau.

7. Si vous avez apporté des modifications de configuration pour résoudre les problèmes signalés, sélectionnez à nouveau **Exécuter les pré-vérifications** pour obtenir des résultats mis à jour.

Si toutes les erreurs ont été résolues, vous êtes invité à démarrer la mise à niveau.

Démarrer la mise à niveau et mettre à niveau le nœud d'administration principal

Lorsque vous démarrez la mise à niveau, les vérifications préalables de mise à niveau sont à nouveau exécutées 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 pas accéder aux autres pages du gestionnaire de grille pendant la mise à niveau du nœud d'administration principal. Les journaux d'audit ne seront pas non plus disponibles.

Étapes

1. Sélectionnez **Démarrer la mise à niveau**.

Un avertissement apparaît pour vous rappeler que vous perdrez temporairement l'accès au gestionnaire de grille.

2. Sélectionnez **OK** pour accepter l'avertissement et démarrer la mise à niveau.
3. Attendez que les vérifications préalables de mise à niveau soient effectuées et que le nœud d'administration principal soit mis à niveau.



Si des erreurs de pré-vérification sont signalées, résolvez-les et sélectionnez à 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 surveiller 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 grille.

4. Si nécessaire, sélectionnez **Continuer** pour accéder à l'étape **Mettre à niveau d'autres nœuds**.

Mettre à niveau d'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 préférerez peut-être mettre à niveau les nœuds du site A au cours d'une session, puis mettre à niveau les nœuds du site B au cours d'une session ultérieure. Si vous choisissez d'effectuer la mise à niveau en plusieurs sessions, sachez que vous ne pourrez pas commencer à utiliser les nouvelles fonctionnalités tant que tous les nœuds n'auront pas été mis à niveau.

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 ou le groupe de nœuds suivant.



Lorsque la mise à niveau démarre sur un nœud de grille, les services sur ce nœud sont arrêtés. Plus tard, le nœud de grille est redémarré. Pour éviter les interruptions de service pour les applications clientes qui communiquent avec le nœud, n'approuvez pas la mise à niveau d'un nœud à moins d'être sûr que ce nœud est prêt à être arrêté et redémarré. Si nécessaire, planifiez une fenêtre de maintenance ou informez 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 la grille et le service de mise à niveau est démarré sur chaque nœud.
 - Une fois la tâche **Démarrer le service de mise à niveau** terminée, la tâche **Mettre à niveau les autres nœuds de grille** démarre et vous êtes invité à télécharger une nouvelle copie du package de récupération.
2. Lorsque vous y êtes invité, saisissez votre mot de passe de provisionnement et téléchargez une nouvelle copie du package 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 Recovery Package vous permet de restaurer le système en cas de panne.

3. Consultez les tableaux d'état pour chaque type de nœud. Il existe des tables pour les nœuds d'administration non principaux, les nœuds de passerelle et les nœuds de stockage.

Un nœud de grille peut être dans l'une de ces étapes 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 les nœuds de grille pour la mise à niveau (ou si vous devez désapprouver les nœuds sélectionnés), utilisez ces instructions :

Tâche	Instruction
Rechercher des nœuds spécifiques à approuver, tels que tous les nœuds d'un site particulier	Saisissez la chaîne de recherche dans le champ Rechercher
Sélectionnez tous les nœuds pour la mise 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 Approuver tout pour le type de nœud 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 Approuver pour le nœud
Reporter la mise à niveau sur tous les nœuds sélectionnés	Sélectionnez Désapprouver tous les nœuds
Reporter la mise à niveau sur tous les nœuds sélectionnés du même type	Sélectionnez le bouton Tout désapprouver pour le type de nœud
Reporter la mise à niveau sur un nœud individuel	Sélectionnez le bouton Ne pas approuver pour le 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 son étape atteint **Arrêt des services**. Le bouton **Ne pas approuver** est désactivé.

- Arrêt du conteneur
- Nettoyage des images Docker
- Mise à niveau des packages du système d'exploitation de base



Lorsqu'un nœud d'appliance atteint cette étape, le logiciel d'installation de l'appliance StorageGRID sur 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'appareils peuvent redémarrer plusieurs fois pour mettre à niveau le micrologiciel et le BIOS.

- Exécution des étapes après le redémarrage
- Démarrage des services
- Fait

6. Répétez **l'étape d'approbation** autant de fois que nécessaire jusqu'à ce que tous les nœuds de la grille aient été mis à niveau.

Mise à niveau complète

Lorsque tous les nœuds de la grille ont terminé les étapes de mise à niveau, la tâche **Mettre à niveau les autres nœuds de la 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 fonctionnalités** est terminée (ce qui se produit rapidement), vous pouvez commencer à utiliser le **"nouvelles fonctionnalités"** dans la version mise à niveau de StorageGRID .
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 11.8 vers 11.9 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 des fonctionnalités de StorageGRID , l'étape de mise à jour de la base de données Cassandra peut prendre plusieurs jours.

3. Une fois la tâche de **Mise à niveau de la base de données** terminée, attendez quelques minutes que les **Étapes finales de mise à niveau** soient terminées.
4. Une fois les **étapes de mise à niveau finales** terminées, la mise à niveau est terminée. La première étape, **Sélectionner les fichiers**, s'affiche à nouveau avec une bannière de réussite verte.
5. Vérifiez que les opérations du réseau sont revenues à la normale :
 - a. Vérifiez que les services fonctionnent normalement et qu'il n'y a pas d'alertes inattendues.
 - b. Confirmez que les connexions client au système StorageGRID fonctionnent comme prévu.

Résoudre les problèmes de mise à niveau

Si quelque chose ne va pas lorsque vous effectuez une mise à niveau, vous pourrez peut-être résoudre le problème vous-même. Si vous ne parvenez pas à résoudre un problème, rassemblez autant d'informations que possible, puis contactez le support technique.

La mise à niveau ne se termine pas

Les sections suivantes décrivent comment récupérer des situations où la mise à niveau a partiellement échoué.

Erreurs de pré-vérification de mise à niveau

Pour détecter et résoudre les problèmes, vous pouvez exécuter manuellement les vérifications préalables de mise à niveau avant de démarrer la mise à niveau réelle. La plupart des erreurs de pré-vérification fournissent des informations sur la manière de résoudre le problème.

Échecs de provisionnement

Si le processus de provisionnement automatique échoue, contactez le support technique.

Le nœud de grille plante ou ne démarre pas

Si un nœud de grille tombe en panne pendant le processus de mise à niveau ou ne parvient pas à démarrer correctement une fois la mise à niveau terminée, contactez le support technique pour enquêter 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 lorsque vous ne mettez pas à niveau un nœud de grille, contactez le support technique.

Erreurs de mise à niveau de la base de données

Si la mise à niveau de la base de données échoue avec une erreur, réessayez la mise à niveau. Si cela échoue à nouveau, contactez le support technique.

Informations connexes

["Vérification de l'état du système avant la mise à niveau du logiciel"](#)

Problèmes d'interface utilisateur

Vous pourriez rencontrer des problèmes avec Grid Manager ou Tenant Manager 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 accédez à une autre page du gestionnaire de grille pendant que le nœud d'administration principal est en cours de mise à niveau, vous pouvez voir plusieurs messages « 503 : Service indisponible » et « Problème de connexion au serveur ». Vous pouvez ignorer ces messages en toute sécurité : ils cesseront d'apparaître dès que le nœud sera mis à niveau.

Si ces messages s'affichent pendant plus d'une heure après le début de la mise à niveau, il se peut qu'un

événement se soit produit qui 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

Il est possible que le gestionnaire de grille ou le gestionnaire de locataires ne répondent pas comme prévu après la mise à niveau du logiciel StorageGRID .

Si vous rencontrez des problèmes avec l'interface Web :

- Assurez-vous que vous utilisez un ["navigateur Web pris en charge"](#) .



La prise en charge du navigateur change généralement pour chaque version de StorageGRID .

- Videz le cache de votre navigateur Web.

La suppression du cache supprime les ressources obsolètes utilisées par la version précédente du logiciel StorageGRID et permet à l'interface utilisateur de fonctionner à nouveau correctement. Pour obtenir des instructions, consultez la documentation de votre navigateur Web.

Messages d'erreur « Vérification de la disponibilité des images Docker »

Lorsque vous essayez de démarrer le processus de mise à niveau, vous pouvez recevoir un message d'erreur indiquant « Les problèmes suivants ont été identifiés par la suite de validation de vérification de la disponibilité des images Docker ». Tous les problèmes doivent être résolus avant de pouvoir terminer la mise à niveau.

Contactez le support technique si vous n'êtes pas sûr des modifications nécessaires pour résoudre les problèmes identifiés.

Message	Cause	Solution
Impossible de déterminer la version de mise à niveau. Fichier d'informations sur la version de mise à niveau {file_path} ne correspond pas au format attendu.	Le package de mise à niveau est corrompu.	Rechargez le package de mise à niveau et réessayez. Si le problème persiste, contactez le support technique.
Fichier d'informations sur la version de mise à niveau {file_path} n'a pas été trouvé. Impossible de déterminer la version de mise à niveau.	Le package de mise à niveau est corrompu.	Rechargez le package de mise à niveau et réessayez. Si le problème persiste, contactez le support technique.
Impossible de déterminer la version de publication actuellement installée sur {node_name} .	Un fichier critique sur le nœud est corrompu.	Contactez le support 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.

Message	Cause	Solution
L'hôte du 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 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 s'exécute, ou les images sont toujours en cours d'importation. Remarque : cette erreur s'applique uniquement aux nœuds exécutés en tant que conteneurs sous Linux.	Vérifiez que les packages RPM ou DEB ont été installés sur tous les hôtes Linux sur lesquels les nœuds sont en cours d'exécution. Assurez-vous que la version est correcte pour le service et le fichier images. Attendez quelques minutes et réessayez. Voir " Linux : installer 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 et réessayez.
Erreur non détectée lors de l'exécution des pré-vérifications. {error_string}	Une erreur inattendue s'est produite.	Attendez quelques minutes et réessayez.

Appliquer le correctif StorageGRID

Procédure de correctif logiciel StorageGRID

Vous devrez peut-être appliquer un correctif à votre système StorageGRID si des problèmes avec le logiciel sont détectés et résolus entre les versions de fonctionnalités.

Les correctifs StorageGRID contiennent des modifications logicielles qui sont rendues disponibles en dehors d'une fonctionnalité ou d'une version de correctif. Les mêmes modifications sont incluses dans une future version. De plus, chaque version de correctif contient un récapitulatif de tous les correctifs précédents dans la version de fonctionnalité ou 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 pendant qu'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 suspendue, vous pouvez appliquer un correctif en toute sécurité. En outre, vous pourrez peut-être appliquer un correctif lors des dernières étapes d'une procédure de mise à niveau de StorageGRID. Consultez les instructions de mise à niveau du logiciel StorageGRID pour plus de détails.

Une fois le correctif téléchargé dans le gestionnaire de grille, il est appliqué automatiquement au nœud d'administration principal. Ensuite, vous pouvez approuver l'application du correctif au reste des nœuds de votre système StorageGRID.

Si un correctif ne parvient pas à être appliqué à un ou plusieurs nœuds, la raison de l'échec apparaît dans la colonne Détails du tableau de progression du correctif. Vous devez résoudre tous les problèmes à l'origine des échecs, puis réessayer l'ensemble du processus. Les nœuds avec une application réussie du correctif seront

ignorés dans les applications ultérieures. Vous pouvez réessayer le processus de correctif en toute sécurité 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 complète.

Bien que les nœuds de grille soient mis à jour avec la nouvelle version du correctif, les modifications réelles d'un correctif peuvent uniquement affecter des services spécifiques sur des types de nœuds spécifiques. Par exemple, un correctif peut uniquement affecter le service LDR sur les nœuds de stockage.

Comment les correctifs sont appliqués pour la récupération 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 des opérations de récupération ou ajoutés dans une extension.

Cependant, si vous devez récupérer le nœud d'administration principal, vous devez installer manuellement la version StorageGRID correcte, puis appliquer le correctif. La version finale de StorageGRID 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 récupération du nœud 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 échoue.
3. Vous redéployez le nœud d'administration principal à l'aide de StorageGRID 11.A.B et effectuez la procédure de récupération.



Comme requis pour correspondre à la version de la grille, vous pouvez utiliser une version mineure lors du déploiement du nœud ; vous n'avez pas besoin de déployer d'abord la version majeure.

4. Vous appliquez ensuite le correctif 11.A.B.y au nœud d'administration principal.

Pour plus d'informations, consultez la section ["Configurer le nœud d'administration principal de remplacement"](#).

Comment votre système est affecté lorsque vous appliquez un correctif

Vous devez comprendre comment votre système StorageGRID sera affecté lorsque vous appliquez un correctif.

Les correctifs de StorageGRID ne sont pas perturbateurs

Le système StorageGRID peut ingérer et récupérer des données à partir des applications clientes tout au long du processus de correctif. Si vous approuvez tous les nœuds du même type pour le correctif (par exemple, les nœuds de stockage), les nœuds sont arrêtés un par un, de sorte qu'il n'y a aucun moment où tous les nœuds de grille ou tous les nœuds de grille d'un certain type sont indisponibles.

Pour permettre une disponibilité continue, assurez-vous que votre politique ILM contient des règles qui spécifient le stockage de plusieurs copies de chaque objet. Vous devez également vous assurer que tous les clients S3 externes sont configurés pour envoyer des requêtes à l'un des éléments suivants :

- Une adresse IP virtuelle de groupe haute disponibilité (HA)

- Un équilibreur de charge tiers à haute disponibilité
- Plusieurs nœuds de passerelle pour chaque client
- Plusieurs nœuds de stockage pour chaque client

Les applications clientes peuvent subir des perturbations à court terme

Le système StorageGRID peut ingérer et récupérer des données à partir d'applications clientes tout au long du processus de correctif logiciel. Cependant, les connexions clientes aux nœuds de passerelle ou aux nœuds de stockage individuels peuvent être temporairement interrompues si le correctif logiciel 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 un 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 le moment où certains nœuds sont mis à jour.



Vous pouvez utiliser plusieurs passerelles et groupes de haute disponibilité (HA) pour fournir un basculement automatique pendant le processus de correctif. Voir les instructions pour "[configuration des groupes de 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 dans un environnement à versions mixtes (certains nœuds de grille exécutant une version antérieure, tandis que d'autres ont été mis à niveau vers une version ultérieure). En général, ces alertes et notifications disparaissent une fois le correctif 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, en spécifiant les sous-réseaux du réseau de grille ou en approuvant les nœuds de grille 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.

Obtenir le matériel nécessaire pour le correctif

Avant d'appliquer un correctif, vous devez obtenir tout le matériel requis.

Article	Remarques
Fichier de correctifs StorageGRID	Vous devez télécharger le fichier de correctif StorageGRID .
• Port réseau • "Navigateur Web pris en charge" • Client SSH (par exemple, PuTTY)	

Article	Remarques
Paquet de relance(.zip) déposer	Avant d'appliquer un correctif, " télécharger le fichier du package de récupération le plus récent " au cas où des problèmes surviendraient pendant le correctif. Ensuite, une fois le correctif appliqué, téléchargez une nouvelle copie du fichier du package de récupération et enregistrez-le dans un endroit sûr. Le fichier de package de récupération mis à jour vous permet de restaurer le système en cas de panne.
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 package de récupération .zip déposer.
Mot de passe d'approvisionnement	La phrase secrète est créée et documentée lors de la première installation du système StorageGRID . La phrase secrète de provisionnement n'est pas répertoriée dans le Passwords .txt déposer.
Documentation connexe	readme.txt`fichier pour le correctif. Ce fichier est inclus sur la page de téléchargement du correctif. Assurez-vous de revoir le `readme fichier soigneusement avant d'appliquer le correctif.

Télécharger le fichier de correctif

Vous devez télécharger le fichier de correctif avant de pouvoir appliquer le correctif.

Étapes

1. Aller à "[Téléchargements NetApp : StorageGRID](#)".
2. Sélectionnez la flèche vers le bas sous **Logiciels disponibles** pour voir une liste des correctifs disponibles au téléchargement.



Les versions des fichiers de correctifs ont la forme : 11.4.x.y.

3. Consultez les modifications incluses dans la mise à jour.



Si vous venez de "[récupéré le nœud d'administration principal](#)" et vous devez appliquer un correctif, sélectionnez la même version de correctif que celle installée sur les autres nœuds de la grille.

- a. Sélectionnez la version du correctif que vous souhaitez télécharger et sélectionnez **Aller**.
- b. Sign in en utilisant le nom d'utilisateur et le mot de passe de votre compte NetApp .
- c. Lisez et acceptez le contrat de licence utilisateur final.

La page de téléchargement de la version que vous avez sélectionnée apparaît.

- d. Télécharger 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 changez pas le nom de ce fichier.



Si vous utilisez un appareil macOS, le fichier de correctif peut être automatiquement enregistré en tant que `.txt` déposer. 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 accueillir le correctif.

1. Sign in 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 du réseau sont connectés au réseau.

Les nœuds connectés ont des coches vertes  sur la page Nœuds.

3. Vérifiez et résolvez toutes les alertes actuelles, 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 pendant qu'une procédure de mise hors service, d'extension ou de récupération est en cours d'exécution.



Si un nœud ou un site ["la procédure de déclassement est suspendue"](#) , vous pouvez appliquer un correctif en toute sécurité. En outre, vous pourrez peut-être appliquer un correctif lors des dernières étapes d'une procédure de mise à niveau de StorageGRID . Voir les instructions pour ["mise à niveau du logiciel StorageGRID"](#) .

Appliquer le correctif

Le correctif est d'abord appliqué automatiquement au nœud d'administration principal. Ensuite, vous devez approuver l'application du correctif aux autres nœuds de grille jusqu'à ce que tous les nœuds exécutent la même version du logiciel. Vous pouvez personnaliser la séquence d'approbation en choisissant d'approuver des nœuds de grille individuels, des groupes de nœuds de grille ou tous les nœuds de grille.

Avant de commencer

- Vous avez examiné le ["considérations pour l'application d'un correctif"](#) .
- Vous disposez de la phrase secrète de provisionnement.
- Vous disposez d'un accès Root ou de l'autorisation Maintenance.

À propos de cette 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 une mise à niveau du logiciel StorageGRID ou une mise à jour du système d'exploitation SANtricity tant que vous n'avez pas terminé le processus de correctif.

Étapes

1. Sign in au Grid Manager à l'aide d'un ["navigateur Web pris en charge"](#).
2. Sélectionnez **MAINTENANCE > Système > Mise à jour du logiciel**.

La page de mise à jour du logiciel apparaît.

Software update

You can upgrade StorageGRID software, apply a hotfix, or upgrade the SANtricity OS software on StorageGRID storage appliances. NetApp recommends you apply the latest hotfix before and after each software upgrade. Some hotfixes are required to prevent data loss.

StorageGRID upgrade Upgrade to the next StorageGRID version and apply the latest hotfix for that version. Upgrade →	StorageGRID hotfix Apply a hotfix to your current StorageGRID software version. Apply hotfix →	SANtricity OS update Update the SANtricity OS software on your StorageGRID storage appliances. Update →

3. Sélectionnez **Appliquer le correctif**.

La page Hotfix StorageGRID s'affiche.

StorageGRID Hotfix

Before starting the hotfix process, you must confirm that there are no active alerts and that all grid nodes are online and available.

When the primary Admin Node is updated, services are stopped and restarted. Connectivity might be interrupted until the services are back online.

Hotfix file

Hotfix file ?

Browse

Passphrase

Provisioning Passphrase ?

Start

4. Sélectionnez le fichier de 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. Une fois le téléchargement terminé, le nom du fichier s'affiche dans le champ Détails.



Ne modifiez pas le nom du fichier car cela fait partie du processus de vérification.

5. Saisissez la phrase secrète 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 temporairement perdue lorsque 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 du correctif sont exécutées.



Si des erreurs sont signalées, résolvez-les, téléchargez à nouveau le fichier de correctif et sélectionnez à nouveau **Démarrer**.

- b. Le tableau de progression de l'installation du correctif apparaît.

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 d'administration, nœuds de passerelle et nœuds de stockage).

- c. La barre de progression atteint la fin, puis le nœud d'administration principal s'affiche comme « Terminé ».

Hotfix Installation Progress

[Approve All](#)
[Remove All](#)

Admin Nodes - 1 out of 1 completed

Search

Site	Name	Progress	Stage	Details	Action
Vancouver	VTC-ADM1-101-191		Complete		

8. Vous pouvez également trier les listes de nœuds de chaque groupe par ordre croissant ou décroissant par **Site**, **Nom**, **Progression**, **Étape** ou **Détails**. Ou saisissez un terme dans la case **Rechercher** pour rechercher des nœuds spécifiques.
9. Approuver les nœuds de grille 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 à moins d'être 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 provoquer des interruptions de service pour les clients qui communiquent avec le nœud.

- Sélectionnez un ou plusieurs boutons **Approuver** pour ajouter un ou plusieurs nœuds individuels à la file d'attente des correctifs.
- Sélectionnez le bouton **Approuver tout** dans chaque groupe pour ajouter tous les nœuds du même type à la file d'attente des correctifs. Si vous avez saisi des critères de recherche dans la case **Rechercher**, 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 regroupement de tables approuve uniquement 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(s) nœud(s) suivant(s).

- 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 des correctifs.



Vous devez terminer le correctif StorageGRID avant de pouvoir démarrer une autre mise à jour logicielle. Si vous ne parvenez pas à effectuer le correctif, contactez le support technique.

- Sélectionnez **Supprimer** ou **Supprimer tout** pour supprimer un nœud ou tous les nœuds de la file d'attente des correctifs.

Lorsque l'étape progresse au-delà de « En file d'attente », le bouton **Supprimer** est masqué et vous ne pouvez plus supprimer le nœud du processus de correctif.

Storage Nodes - 1 out of 9 completed						Approve All	Remove All
Search							
Site	Name	Progress	Stage	Details	Action		
Raleigh	RAL-S1-101-196		Queued			Remove	
Raleigh	RAL-S2-101-197		Complete				
Raleigh	RAL-S3-101-198		Queued			Remove	
Sunnyvale	SVL-S1-101-199		Queued			Remove	
Sunnyvale	SVL-S2-101-93		Waiting for you to approve			Approve	
Sunnyvale	SVL-S3-101-94		Waiting for you to approve			Approve	
Vancouver	VTC-S1-101-193		Waiting for you to approve			Approve	
Vancouver	VTC-S2-101-194		Waiting for you to approve			Approve	
Vancouver	VTC-S3-101-195		Waiting for you to approve			Approve	

10. Attendez que le correctif soit appliqué à chaque nœud de grille approuvé.

Une fois le correctif installé avec succès sur tous les nœuds, le tableau de progression de l'installation du correctif se ferme. Une bannière verte indique la date et l'heure à laquelle le correctif a été effectué.

11. Si le correctif n'a pu être appliqué à aucun nœud, examinez l'erreur pour chaque nœud, résolvez le problème et répétez ces étapes.

La procédure n'est pas terminée tant que le correctif n'est pas appliqué avec succès à tous les nœuds. Vous pouvez réessayer le processus de correctif en toute sécurité autant de fois que nécessaire jusqu'à ce qu'il soit terminé.

Configurer et gérer un système StorageGRID

Administrer StorageGRID

Administrer StorageGRID

Utilisez ces instructions pour configurer et administrer un système StorageGRID .

À propos de ces instructions

Les principales tâches de configuration et d'administration de StorageGRID vous permettent de :

- Utilisez le gestionnaire de grille pour configurer des groupes et des utilisateurs
- Créer des comptes locataires pour permettre aux applications clientes S3 de stocker et de récupérer des objets
- Configurer et gérer les réseaux StorageGRID
- Configurer AutoSupport
- Gérer les paramètres des nœuds

Avant de commencer

- Vous avez une compréhension générale du système StorageGRID .
- Vous avez une connaissance assez détaillée des shells de commande Linux, de la mise en réseau et de la configuration du matériel du serveur.

Démarrer avec Grid Manager

Configuration requise pour le navigateur Web

Vous devez utiliser un navigateur Web pris en charge.

navigateur Web	Version minimale prise en charge
Google Chrome	119
Microsoft Edge	119
Mozilla Firefox	119

Vous devez définir la fenêtre du navigateur à une largeur recommandée.

Largeur du navigateur	Pixels
Minimum	1024
Optimum	1280

Sign in au gestionnaire de grille

Vous accédez à la page de connexion de Grid Manager en saisissant le nom de domaine complet (FQDN) ou l'adresse IP d'un nœud d'administration dans la barre d'adresse d'un navigateur Web pris en charge.

Chaque système StorageGRID comprend un nœud d'administration principal et un nombre quelconque de nœuds d'administration non principaux. Vous pouvez vous connecter au Grid Manager sur n'importe quel nœud d'administration pour gérer le système StorageGRID . Cependant, certaines procédures de maintenance ne peuvent être effectuées qu'à partir du nœud d'administration principal.

Se connecter au groupe HA

Si les nœuds d'administration sont inclus dans un groupe haute disponibilité (HA), vous vous connectez à l'aide de l'adresse IP virtuelle du groupe HA ou d'un nom de domaine complet mappé à l'adresse IP virtuelle. Le nœud d'administration principal doit être sélectionné comme interface principale du groupe, de sorte que lorsque vous accédez au gestionnaire de grille, vous y accédez sur le nœud d'administration principal, sauf si le nœud d'administration principal n'est pas disponible. Voir ["Gérer les groupes de haute disponibilité"](#) .

Utiliser SSO

Les étapes de connexion sont légèrement différentes si ["l'authentification unique \(SSO\) a été configurée"](#) .

Sign in à Grid Manager sur le premier nœud d'administration

Avant de commencer

- Vous avez 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 qui dispose d'au moins une autorisation.
- Vous avez l'URL du Grid Manager :

```
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 HA de nœuds d'administration.

Pour accéder au Grid Manager sur un port autre que le port par défaut pour HTTPS (443), incluez le numéro de port dans l'URL :

```
https://FQDN_or_Admin_Node_IP:port/
```



SSO n'est pas disponible sur le port restreint du Grid Manager. Vous devez utiliser le port 443.

Étapes

1. Lancez un navigateur Web pris en charge.
2. Dans la barre d'adresse du navigateur, saisissez l'URL du gestionnaire de grille.
3. Si une alerte de sécurité s'affiche, installez le certificat à l'aide de l'assistant d'installation du navigateur. Voir ["Gérer les certificats de sécurité"](#) .

4. Sign in au gestionnaire de grille.

L'écran de connexion qui s'affiche dépend de la configuration de l'authentification unique (SSO) pour StorageGRID.

Ne pas utiliser SSO

- a. Entrez votre nom d'utilisateur et votre mot de passe pour le Grid Manager.
- b. Sélectionnez **Connexion**.



The screenshot shows the NetApp StorageGRID Grid Manager login interface. At the top, the NetApp logo is followed by 'StorageGRID®' and 'Grid Manager' in a large font. Below this, there are two input fields: 'Username' and 'Password'. The 'Username' field has a blue border and a vertical cursor. Below the 'Password' field is a blue 'Sign in' button. At the bottom, there are three links: 'Tenant sign in', 'NetApp support', and 'NetApp.com'.

Utilisation de SSO

- Si StorageGRID utilise SSO et que c'est la première fois que vous accédez à l'URL sur ce navigateur :
 - i. Sélectionnez * Sign in*. Vous pouvez laisser le 0 dans le champ Compte.



Sign in

Account

Sign in

[NetApp support](#) | [NetApp.com](#)

- ii. Saisissez vos informations d'identification SSO standard sur la page de connexion SSO de votre organisation. Par exemple:

Sign in with your organizational account

Sign in

- Si StorageGRID utilise SSO et que vous avez déjà accédé au Grid Manager ou à un compte locataire :
 - i. Saisissez **0** (l'ID de compte pour le gestionnaire de grille) ou sélectionnez **Gestionnaire de grille** s'il apparaît dans la liste des comptes récents.

The image shows the NetApp StorageGRID Sign in page. At the top, there is the NetApp logo followed by "StorageGRID®". Below this is the heading "Sign in". Under the heading, there is a section labeled "Recent" with a dropdown menu currently showing "Grid Manager". Below that is a section labeled "Account" with a text input field containing the number "0". At the bottom of the form is a blue button labeled "Sign in". Below the button, there are two links: "NetApp support" and "NetApp.com".

NetApp StorageGRID®

Sign in

Recent

Grid Manager ▼

Account

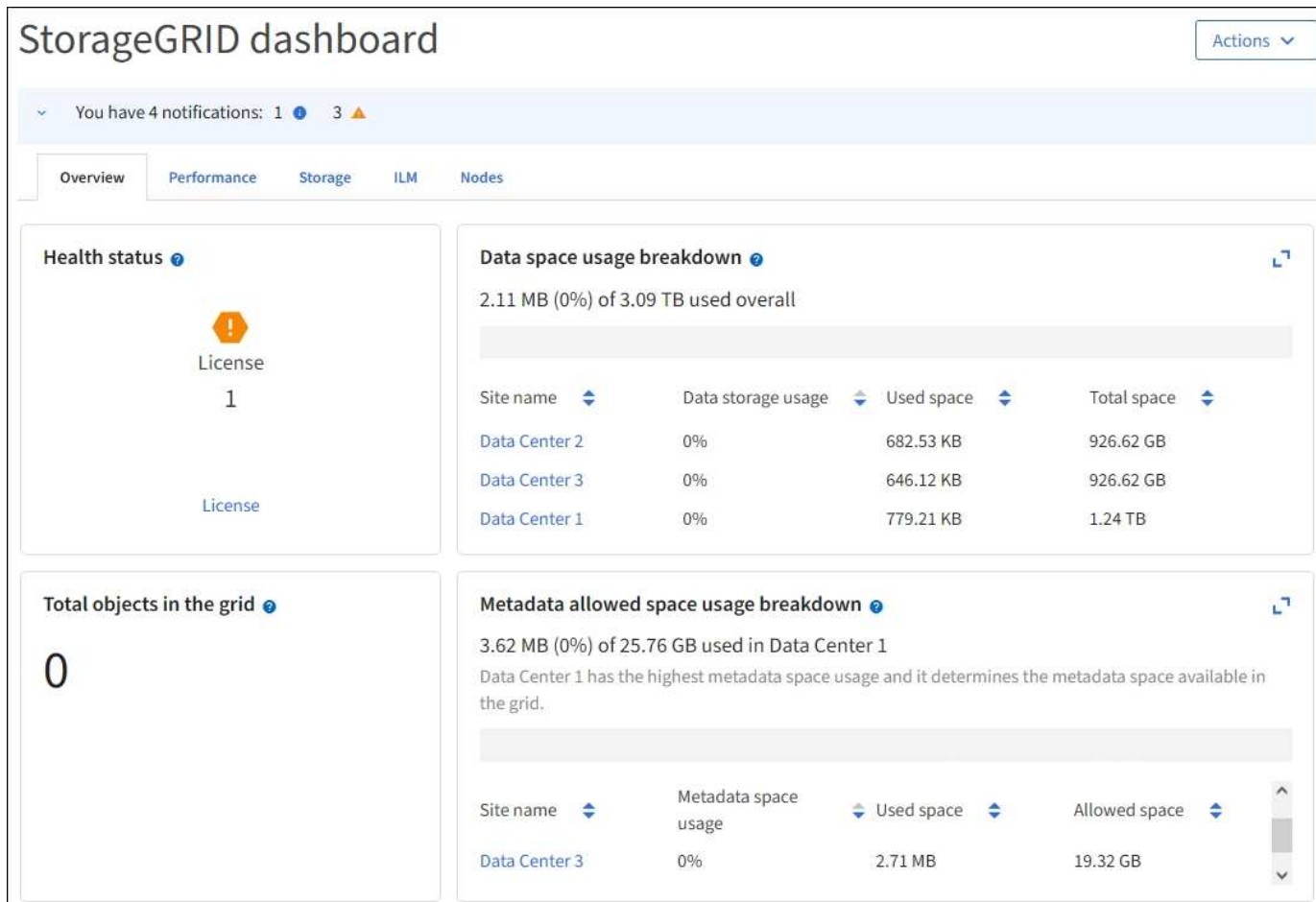
0

Sign in

[NetApp support](#) | [NetApp.com](#)

- ii. Sélectionnez * Sign in*.
- iii. Sign in avec vos informations d'identification SSO standard sur la page de connexion SSO de votre organisation.

Lorsque vous êtes connecté, la page d'accueil du Grid Manager apparaît, qui comprend le tableau de bord. Pour savoir quelles informations sont fournies, consultez "[Afficher et gérer le tableau de bord](#)".



Connectez-vous à un autre nœud d'administration

Suivez ces étapes pour vous connecter à un autre nœud d'administration.

Ne pas utiliser SSO

Étapes

1. Dans la barre d'adresse du navigateur, saisissez le nom de domaine complet ou l'adresse IP de l'autre nœud d'administration. Incluez le numéro de port si nécessaire.
2. Entrez 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 êtes connecté à un nœud d'administration, vous pouvez accéder aux autres nœuds d'administration sans avoir à vous reconnecter.

Étapes

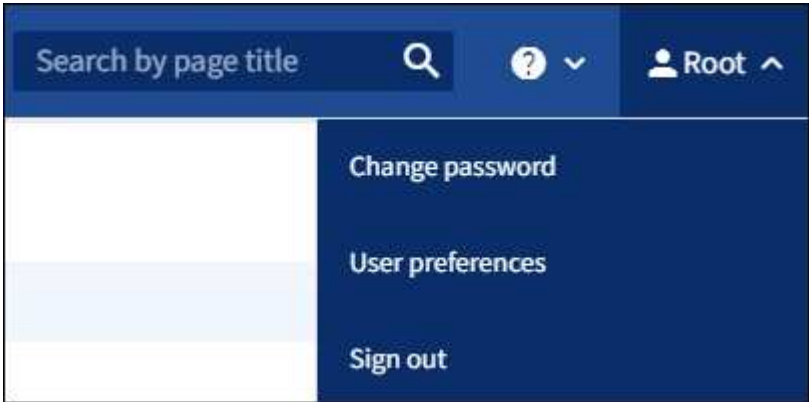
1. Saisissez le nom de domaine complet ou l'adresse IP de l'autre nœud d'administration dans la barre d'adresse du navigateur.
2. Si votre session SSO a expiré, saisissez à nouveau vos informations d'identification.

Déconnectez-vous du gestionnaire de grille

Lorsque vous avez terminé d'utiliser Grid Manager, vous devez vous déconnecter pour garantir que les utilisateurs non autorisés ne peuvent pas accéder au système StorageGRID . La fermeture de votre navigateur peut ne pas vous déconnecter du système, en fonction des paramètres de 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 accédez. La page de connexion StorageGRID s'affiche. Grid Manager est répertorié par défaut dans la liste déroulante Comptes récents et le champ ID de compte affiche 0. Remarque : si l'authentification unique est activée et que vous êtes également connecté au gestionnaire de locataires, vous devez également "se déconnecter du compte locataire" à "se déconnecter de SSO" .

Changez votre mot de passe

Si vous êtes un utilisateur local du 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"](#) .

À propos de cette 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 Grid Manager. Au lieu de cela, vous devez modifier votre mot de passe dans la source d'identité externe, par exemple, Active Directory ou OpenLDAP.

Étapes

1. Dans l'en-tête du Gestionnaire de grille, sélectionnez **votre nom** > **Modifier le mot de passe**.
2. Entrez votre mot de passe actuel.
3. Tapez un nouveau mot de passe.

Votre mot de passe doit contenir au moins 8 et pas plus de 32 caractères. Les mots de passe sont sensibles à la casse.

4. Entrez à nouveau le nouveau mot de passe.
5. Sélectionnez **Enregistrer**.

Afficher les informations de licence StorageGRID

Vous pouvez afficher les informations de licence de votre système StorageGRID, telles que la capacité de stockage maximale de votre grille, chaque fois que nécessaire.

Avant de commencer

Vous êtes connecté au Grid Manager à l'aide d'un ["navigateur Web pris en charge"](#).

À propos de cette tâche

S'il y a un problème avec la licence du logiciel pour ce système StorageGRID, la carte d'état de santé sur le tableau de bord comprend une icône d'état de licence et un lien **Licence**. Le nombre indique le nombre de problèmes liés aux licences.



Étapes

1. Accédez à la page Licence en effectuant l'une des opérations suivantes :
 - Sélectionnez **MAINTENANCE** > **Système** > **Licence**.
 - À partir de la carte d'état de santé du tableau de bord, sélectionnez l'icône d'état de la licence ou le lien **Licence**.

Ce lien apparaît uniquement s'il y a un problème avec la licence.

2. Afficher les détails en lecture seule de la licence actuelle :

- ID système StorageGRID , qui est le numéro d'identification unique de cette installation StorageGRID
- Numéro de série de la licence
- Type de licence, soit **Perpétuelle** soit **Abonnement**
- Capacité de stockage sous licence du réseau
- Capacité de stockage prise en charge
- Date de fin de licence. **N/A** apparaît pour une licence perpétuelle.
- Date de fin du 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 d'assistance après avoir obtenu le fichier de licence. Pour mettre à jour cette valeur, voir "[Mettre à jour les informations de licence StorageGRID](#)". Vous pouvez également consulter la date de fin réelle du contrat à l'aide d'Active IQ.

- Contenu du fichier texte de licence

Mettre à jour les informations de licence StorageGRID

Vous devez mettre à jour les informations de licence de votre système StorageGRID chaque fois que les termes de votre licence changent. Par exemple, vous devez mettre à jour les informations de licence si vous achetez une capacité de stockage supplémentaire pour votre réseau.

Avant de commencer

- Vous disposez d'un nouveau fichier de licence à appliquer à votre système StorageGRID .
- Tu as "[autorisations d'accès spécifiques](#)".
- Vous disposez de la phrase secrète de provisionnement.

Étapes

1. Sélectionnez **MAINTENANCE > Système > Licence**.
2. Dans la section Mettre à jour la licence, sélectionnez **Parcourir**.
3. Localisez et sélectionnez le nouveau fichier de licence(.txt).

Le nouveau fichier de licence est validé et affiché.

4. Saisissez la phrase secrète d'approvisionnement.
5. Sélectionnez **Enregistrer**.

Utiliser la API

Utiliser l'API de gestion de grille

Vous pouvez effectuer des tâches de gestion du système à l'aide de l'API REST Grid Management au lieu de l'interface utilisateur Grid Manager. Par exemple, vous souhaitez peut-être utiliser l'API pour automatiser des opérations ou créer plusieurs

entités, telles que des utilisateurs, plus rapidement.

Ressources de haut niveau

L'API de gestion de grille fournit les ressources de niveau supérieur 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, consultez la section "[Utiliser un compte 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 points de terminaison privés StorageGRID ignorent également la version API de la demande.

Émettre des requêtes API

L'API de gestion de grille utilise la plate-forme 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 de Swagger fournit des détails complets et une documentation pour chaque opération API.

Avant de commencer

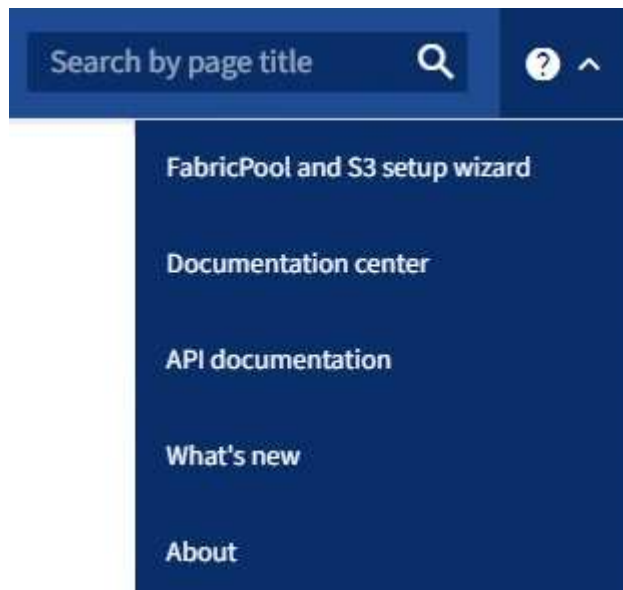
- Vous êtes connecté au Grid Manager à l'aide d'un "[navigateur Web pris en charge](#)".
- Tu as "[autorisations d'accès spécifiques](#)".



Toutes les opérations API que vous effectuez à l'aide de la page Web de documentation API 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. Depuis l'en-tête du gestionnaire de grille, sélectionnez l'icône d'aide et sélectionnez **Documentation API**.



2. Pour effectuer une opération avec l'API privée, sélectionnez **Accéder à la documentation de l'API privée** sur la page API de gestion StorageGRID .

Les API privées sont susceptibles d'être modifiées sans préavis. Les points de terminaison 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 et DELETE.

4. Sélectionnez une action HTTP pour afficher les détails de la demande, y compris l'URL du point de terminaison, une liste de tous les paramètres obligatoires ou facultatifs, un exemple du corps de la demande (si nécessaire) et les réponses possibles.

GET /grid/groups Lists Grid Administrator Groups

Parameters
Try it out

Name	Description
type string (query)	filter by group type Available values : local, federated --
limit integer (query)	maximum number of results Default value : 25 25
marker string (query)	marker-style pagination offset (value is Group's URN) marker - marker-style pagination offset (value
includeMarker boolean (query)	if set, the marker element is also returned --
order string (query)	pagination order (desc requires marker) Available values : asc, desc --

Responses
Response content type application/json

Code	Description
200	successfully retrieved Example Value Model <pre>{ "responseTime": "2021-03-29T14:22:19.673Z", "status": "success", "apiVersion": "3.3", "deprecated": false, "data": [{ "displayName": "Developers",</pre>

- Déterminez si la demande nécessite des paramètres supplémentaires, tels qu'un ID de groupe ou d'utilisateur. Ensuite, obtenez ces valeurs. Vous devrez peut-être d'abord émettre une demande d'API différente pour obtenir les informations dont vous avez besoin.
- Déterminez si vous devez modifier le corps de la demande d'exemple. Si tel est le cas, vous pouvez sélectionner **Modèle** pour connaître les exigences de chaque champ.
- Sélectionnez **Essayer**.
- Fournissez tous les paramètres requis ou modifiez le corps de la demande selon vos besoins.
- Sélectionnez **Exécuter**.
- Consultez le code de réponse pour déterminer si la demande a réussi.

L'API de gestion de grille 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.
- **alert-history** : Opérations sur les alertes résolues.
- **alert-receivers** : Opérations sur les récepteurs de notifications d'alerte (e-mail).
- **alert-rules** : Opérations sur les règles d'alerte.
- **alert-silences** : Opérations sur les silences d'alerte.
- **alertes** : Opérations sur les alertes.
- **audit** : opérations permettant de répertorier et de mettre à jour la configuration de l'audit.
- **auth** : opérations permettant d'effectuer l'authentification de la session utilisateur.

L'API de gestion de grille prend en charge le schéma d'authentification du jeton porteur. 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 avec succès, un jeton de sécurité est renvoyé. Ce jeton doit être fourni dans l'en-tête des requêtes API ultérieures (« `Authorization : Bearer token` »). Le jeton expire après 16 heures.



Si l'authentification unique est activée pour le système StorageGRID, vous devez effectuer différentes étapes pour vous authentifier. Voir « Authentification auprès de l'API si l'authentification unique est activée ».

Consultez « Protection contre la falsification de requêtes intersites » pour obtenir des informations sur l'amélioration de la sécurité de l'authentification.

- **client-certificates** : opérations de configuration des certificats clients 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 versions principales de l'API Grid Management prises en charge par cette version, et vous pouvez désactiver les versions obsolètes de l'API.
- **fonctionnalités désactivées** : opérations permettant d'afficher les fonctionnalités qui pourraient avoir été désactivées.
- **dns-servers** : opérations permettant de lister et de modifier les serveurs DNS externes configurés.
- **drive-details** : opérations sur les lecteurs pour des modèles d'appareils de stockage spécifiques.
- **endpoint-domain-names** : opérations permettant de répertorier et de modifier les noms de domaine de point de terminaison S3.
- **erasure-coding** : Opérations sur les profils d'effacement-codage.
- **expansion** : Opérations sur l'expansion (niveau procédure).
- **expansion-nodes** : opérations sur l'expansion (au niveau du nœud).
- **expansion-sites** : Opérations sur l'extension (au niveau du site).
- **grid-networks** : Opérations permettant de lister et de modifier la liste des réseaux de grille.

- **grid-passwords** : Opérations pour la gestion des mots de passe de la grille.
- **groupes** : opérations de gestion des groupes d'administrateurs de grille locaux et de récupération des groupes d'administrateurs de grille fédérés à partir d'un serveur LDAP externe.
- **identity-source** : opérations permettant de configurer une source d'identité externe et de synchroniser manuellement les informations des groupes fédérés et des utilisateurs.
- **ilm** : Opérations sur la gestion du cycle de vie de l'information (ILM).
- **in-progress-procedures**: Récupère les procédures de maintenance actuellement en cours.
- **licence** : opérations permettant de récupérer et de mettre à jour la licence StorageGRID .
- **logs** : opérations de collecte et de téléchargement des fichiers journaux.v
- **métriques** : opérations sur les métriques StorageGRID , y compris les requêtes de métriques instantanées à un moment donné et les requêtes de métriques de plage sur une plage de temps. L'API Grid Management utilise l'outil de surveillance des systèmes Prometheus comme source de données back-end. Pour plus d'informations sur la construction de requêtes Prometheus, consultez le site Web Prometheus.



Les mesures qui incluent *private* dans leurs noms sont destinés à un usage interne uniquement. Ces mesures sont susceptibles d'être modifiées entre les versions de StorageGRID sans préavis.

- **node-details** : Opérations sur les détails du nœud.
- **node-health** : opérations sur l'état de santé du nœud.
- **node-storage-state** : opérations sur l'état de stockage des nœuds.
- **ntp-servers** : opérations permettant de répertorier ou de mettre à jour les 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 de téléchargement du package de récupération.
- **régions** : opérations permettant d'afficher et de créer des régions.
- **s3-object-lock** : opérations sur les paramètres globaux de verrouillage d'objet S3.
- **server-certificate** : opérations permettant d'afficher et de mettre à jour les certificats du serveur Grid Manager.
- **snmp** : opérations sur la configuration SNMP actuelle.
- **storage-watermarks** : Filigranes des nœuds de stockage.
- **traffic-classes** : opérations pour les politiques de classification du trafic.
- **untrusted-client-network** : opérations sur la configuration du réseau client non approuvé.
- **utilisateurs** : opérations permettant d'afficher et de gérer les utilisateurs de Grid Manager.

Gestion des versions de l'API de gestion de grille

L'API de gestion de grille utilise le contrôle de version pour prendre en charge les mises à niveau sans interruption.

Par exemple, cette URL de demande spécifie la version 4 de l'API.

`https://hostname_or_ip_address/api/v4/authorize`

La version principale de l'API est mise à jour lorsque des modifications sont apportées qui ne sont pas compatibles avec les versions plus anciennes. La version mineure de l'API est mise à jour lorsque des modifications sont apportées qui sont *compatibles* avec les versions plus anciennes. Les modifications compatibles incluent l'ajout de nouveaux points de terminaison ou de nouvelles propriétés.

L'exemple suivant illustre comment la version de l'API est augmentée en fonction du type de modifications apportées.

Type de modification de l'API	Ancienne version	Nouvelle version
Compatible avec les anciennes versions	2,1	2,2
Non compatible avec les anciennes versions	2,1	3,0

Lorsque vous installez le logiciel StorageGRID pour la première fois, seule la version la plus récente de l'API est activée. Cependant, lorsque vous effectuez une mise à niveau vers une nouvelle version de fonctionnalité de StorageGRID, vous continuez à avoir accès à l'ancienne version de l'API pour au moins une version de fonctionnalité de StorageGRID .



Vous pouvez configurer les versions prises en charge. Consultez la section **config** de la documentation de l'API Swagger pour le "[API de gestion de grille](#)" pour plus d'informations. Vous devez désactiver la prise en charge de l'ancienne version après avoir mis à jour tous les clients API pour utiliser la version la plus récente.

Les demandes obsolètes sont marquées comme obsolètes 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 v2 API at POST "/api/v2/authorize"
```

Déterminer quelles versions d'API sont prises en charge dans la version actuelle

Utilisez le GET `/versions` Requête d'API pour renvoyer une liste des versions majeures d'API prises en charge. Cette demande se trouve dans la section **config** de la documentation de l'API Swagger.

```
GET https://{{IP-Address}}/api/versions
{
  "responseTime": "2023-06-27T22:13:50.750Z",
  "status": "success",
  "apiVersion": "4.0",
  "data": [
    2,
    3,
    4
  ]
}
```

Spécifier une version d'API pour une requête

Vous pouvez spécifier la version de l'API à l'aide d'un paramètre de chemin(`/api/v4`) ou un en-tête(`Api-Version: 4`). Si vous fournissez les deux valeurs, la valeur de l'en-tête remplace la valeur du chemin.

```
curl https://[IP-Address]/api/v4/grid/accounts

curl -H "Api-Version: 4" https://[IP-Address]/api/grid/accounts
```

Protection contre la falsification de requêtes intersites (CSRF)

Vous pouvez contribuer à vous protéger contre les attaques de falsification de requête intersite (CSRF) contre StorageGRID en utilisant des jetons CSRF pour améliorer l'authentification qui utilise des cookies. Le gestionnaire de grille et le gestionnaire de locataires activent automatiquement cette fonctionnalité de sécurité ; les autres clients API peuvent choisir de l'activer ou non lorsqu'ils se connectent.

Un attaquant capable de déclencher une requête vers un autre site (par exemple avec un formulaire HTTP POST) peut provoquer l'exécution de certaines requêtes à l'aide des cookies de l'utilisateur connecté.

StorageGRID aide à se protéger contre les attaques CSRF en utilisant des jetons CSRF. Lorsqu'elle 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 fonctionnalité, définissez le `csrfToken` paramètre à `true` lors de 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"
```

Lorsque c'est vrai, un `GridCsrfToken` Le cookie est défini avec une valeur aléatoire pour les connexions au Grid Manager, et le `AccountCsrfToken` le cookie est défini avec une valeur aléatoire pour les connexions au Tenant Manager.

Si le cookie est présent, toutes les requêtes pouvant modifier l'état du système (POST, PUT, PATCH, DELETE) doivent inclure l'un des éléments suivants :

- Le `X-Csrf-Token` en-tête, avec la valeur de l'en-tête définie sur la valeur du cookie de jeton CSRF.
- Pour les points de terminaison qui acceptent un corps codé par formulaire : A `csrfToken` paramètre de corps de requête codé par formulaire.

Consultez la documentation de l'API en ligne pour des exemples et des détails supplémentaires.



Les requêtes qui ont un cookie de jeton CSRF défini appliqueront également l'en-tête « Content-Type : application/json » pour toute requête qui attend un corps de requête JSON comme protection supplémentaire contre les attaques CSRF.

Utiliser l'API si l'authentification unique est activée

Utiliser l'API si l'authentification unique est activée (Active Directory)

Si vous avez ["configuré et activé l'authentification unique \(SSO\)"](#) et que 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.

Sign in 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 qui appartient à un groupe d'utilisateurs StorageGRID .
- Si vous souhaitez accéder à l'API de gestion des locataires, vous connaissez l'ID du compte locataire.

À propos de cette 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, `./debs` pour Ubuntu ou Debian, et `./vsphere`

pour VMware).

- Un exemple de flux de travail de requêtes curl.

Le flux de travail curl peut expirer si vous l'exécutez trop lentement. Vous pourriez voir l'erreur : `A valid SubjectConfirmation was not found on this Response`.



L'exemple de workflow curl ne protège pas le mot de passe contre toute visualisation par d'autres utilisateurs.

Si vous avez un problème d'encodage d'URL, vous pourriez voir l'erreur : `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.
 - Utilisez les requêtes curl. Passez à l'étape 3.
2. Si vous souhaitez utiliser le `storagegrid-ssoauth.py` script, transmettez le script à l'interpréteur Python et exécutez le script.

Lorsque vous y êtes invité, saisissez des valeurs pour les arguments suivants :

- La méthode SSO. Entrez ADFS ou adfs.
- Le nom d'utilisateur SSO
- Le domaine où StorageGRID est installé
- L'adresse de StorageGRID
- L'ID du compte locataire, si vous souhaitez 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 désormais utiliser le jeton pour d'autres requêtes, de la même manière que vous utiliseriez l'API si SSO n'était pas utilisé.

3. Si vous souhaitez utiliser des requêtes curl, utilisez la procédure suivante.
 - a. Déclarez les variables nécessaires à 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, émettez une requête POST à `/api/v3/authorize-saml` et supprimez l'encodage JSON supplémentaire de la réponse.

Cet exemple montre une requête 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 pour cet exemple inclut une URL signée qui est codée en URL, mais elle n'inclut pas la couche de codage JSON supplémentaire.

```
{
  "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. Sauver le SAMLRequest à partir de la réponse à utiliser dans les commandes suivantes.

```
export SAMLREQUEST='fZHLbsIwEEV%2FJTuv7...sSl%2BfQ33cvfwA%3D'
```

- d. Obtenez une URL complète qui inclut l'ID de demande client d'AD FS.

Une option consiste à demander le formulaire de connexion en utilisant 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 la demande du client :

```
<form method="post" id="loginForm" autocomplete="off"
novalidate="novalidate" onKeyPress="if (event && event.keyCode == 13)
Login.submitLoginRequest();" action="/adfs/ls/?
SAMLRequest=fZHRTomwFIZfzhb...UJikvo77sXPw%3D%3D&RelayState=12345&client-request-id=00000000-0000-0000-ee02-0080000000de" >
```

e. Enregistrez l'ID de demande du client à partir de la réponse.

```
export SAMLREQUESTID='00000000-0000-0000-ee02-0080000000de'
```

f. Envoyez vos informations d'identification à l'action du 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=$SAMPLPASSWORD&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 formulaire de publication 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=fZHRTomwFIZfzhb...UJikvo77sXPw%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
```



```
export SAMLResponse='PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4='
```

- j. Utilisation de la sauvegarde SAMLResponse , créer un StorageGRID/api/saml-response demande de génération d'un jeton d'authentification StorageGRID .

Pour RelayState , utilisez l'ID de compte locataire ou utilisez 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 désormais utiliser MYTOKEN pour d'autres demandes, de la même manière que vous utiliseriez 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 Grid Management ou de l'API Tenant Management. Ces instructions s'appliquent si vous utilisez Active Directory comme fournisseur d'identité SSO

À propos de cette 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 porteur StorageGRID valide.

Étapes

1. Pour générer une demande de déconnexion signée, transmettez `cookie "sso=true" à 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%3D",
  "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 rediriger vers StorageGRID.

```
curl --include "$LOGOUT_REQUEST"
```

La réponse 302 est renvoyée. L'emplacement de redirection ne s'applique pas à la déconnexion de l'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 porteur StorageGRID .

La suppression du jeton porteur StorageGRID fonctionne de la même manière que sans SSO. Si `cookie "sso=true" n'est pas 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
```

UN 204 No Content la réponse indique que l'utilisateur est maintenant déconnecté.

```
HTTP/1.1 204 No Content
```

Utiliser l'API si l'authentification unique est activée (Azure)

Si vous avez [configuré et activé l'authentification unique \(SSO\)](#) et vous utilisez Azure comme fournisseur SSO, vous pouvez utiliser deux exemples de scripts pour obtenir un jeton d'authentification valide pour l'API Grid Management ou l'API Tenant Management.

Sign in 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 et le mot de passe SSO d'un utilisateur fédéré qui appartient à un groupe d'utilisateurs StorageGRID .
- Si vous souhaitez accéder à l'API de gestion des locataires, vous connaissez l'ID du compte locataire.

À propos de cette 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, `./debs` pour Ubuntu ou Debian, et `./vsphere` pour VMware).

Pour écrire votre propre intégration d'API avec Azure, consultez le `storagegrid-ssoauth-azure.py` scénario. Le script Python envoie deux requêtes directement à StorageGRID (d'abord pour obtenir le SAMLRequest, puis 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 API, mais cela n'est pas simple. Le module Puppeteer Node.js est utilisé pour récupérer l'interface Azure SSO.

Si vous avez un problème d'encodage d'URL, vous pourriez voir l'erreur : `Unsupported SAML version` .

Étapes

1. Installez les dépendances requises, comme suit :
 - a. Installez Node.js (voir ["https://nodejs.org/en/download/"](https://nodejs.org/en/download/)).

b. Installez les modules Node.js requis (puppeteer et jsdom) :

```
npm install -g <module>
```

2. Transmettez le script Python à l'interpréteur Python pour exécuter le script.

Le script Python appellera ensuite le script Node.js correspondant pour effectuer les interactions Azure SSO.

3. Lorsque vous y êtes invité, saisissez des valeurs pour les arguments suivants (ou transmettez-les à l'aide de paramètres) :

- L'adresse e-mail SSO utilisée pour se connecter à Azure
- L'adresse de StorageGRID
- L'ID du compte locataire, si vous souhaitez accéder à l'API de gestion des locataires

4. Lorsque vous y êtes invité, saisissez le mot de passe et soyez prêt à fournir une autorisation MFA à Azure si nécessaire.

```
c:\Users\user\Documents\azure_sso>py storagegrid-azure-ssoauth.py --sso-email-address user@my-domain.com
--sg-address storagegrid.examp.e.com --tenant-account-id 0
Enter the user's SSO password:
*****

Watch for and approve a 2FA authorization request
*****

StorageGRID Auth Token: {'responseTime': '2021-10-04T21:30:48.807Z', 'status': 'success', 'apiVersion':
'3.4', 'data': '4807d93e-a3df-48f2-9680-906cd255979e'}
```



Le script suppose que l'authentification multifacteur est effectuée à l'aide de Microsoft Authenticator. Vous devrez peut-être modifier le script pour prendre en charge d'autres formes d'authentification multifacteur (comme la saisie d'un code reçu dans un message texte).

Le jeton d'autorisation StorageGRID est fourni dans la sortie. Vous pouvez désormais utiliser le jeton pour d'autres requêtes, de la même manière que vous utiliseriez l'API si SSO n'était pas utilisé.

Utiliser l'API si l'authentification unique est activée (PingFederate)

Si vous avez ["configuré et activé l'authentification unique \(SSO\)"](#) et que vous utilisez PingFederate comme fournisseur SSO, vous devez émettre une série de requêtes API pour obtenir un jeton d'authentification valide pour l'API de gestion de grille ou l'API de gestion des locataires.

Sign in 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 qui appartient à un groupe d'utilisateurs StorageGRID .
- Si vous souhaitez accéder à l'API de gestion des locataires, vous connaissez l'ID du compte locataire.

À propos de cette 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, `./debs` pour Ubuntu ou Debian, et `./vsphere` pour VMware).
- Un exemple de flux de travail de requêtes curl.

Le flux de travail curl peut expirer si vous l'exécutez trop lentement. Vous pourriez voir l'erreur : `A valid SubjectConfirmation was not found on this Response.`



L'exemple de workflow curl ne protège pas le mot de passe contre toute visualisation par d'autres utilisateurs.

Si vous avez un problème d'encodage d'URL, vous pourriez voir l'erreur : `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.
 - Utilisez les requêtes curl. Passez à l'étape 3.
2. Si vous souhaitez utiliser le `storagegrid-ssoauth.py` script, transmettez le script à l'interpréteur Python et exécutez le script.

Lorsque vous y êtes invité, saisissez des valeurs pour les arguments suivants :

- La méthode SSO. Vous pouvez saisir n'importe quelle variante de « pingfederate » (PINGFEDERATE, pingfederate, etc.).
- Le nom d'utilisateur SSO
- Le domaine où StorageGRID est installé. Ce champ n'est pas utilisé pour PingFederate. Vous pouvez le laisser vide ou saisir n'importe quelle valeur.
- L'adresse de StorageGRID
- L'ID du compte locataire, si vous souhaitez 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 désormais utiliser le jeton pour d'autres requêtes, de la même manière que vous utiliseriez l'API si SSO n'était pas utilisé.

3. Si vous souhaitez utiliser des requêtes curl, utilisez la procédure suivante.

- a. Déclarez les variables nécessaires à 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, émettez une requête POST à `/api/v3/authorize-saml` et supprimez l'encodage JSON supplémentaire de la réponse.

Cet exemple montre une requête 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 pour cet exemple inclut une URL signée qui est codée en URL, mais elle n'inclut pas la couche de codage JSON supplémentaire.

```
{
  "apiVersion": "3.0",
  "data": "https://my-pf-baseurl/idp/SSO.saml2?...",
  "responseTime": "2018-11-06T16:30:23.355Z",
  "status": "success"
}
```

- c. Sauver le SAMLRequest à partir de la réponse à utiliser dans les commandes suivantes.

```
export SAMLREQUEST="https://my-pf-baseurl/idp/SSO.saml2?..."
```

- d. Exportez la réponse et le cookie, et faites écho à la réponse :

```
RESPONSE=$(curl -c - "$SAMLREQUEST")
```

```
echo "$RESPONSE" | grep 'input type="hidden" name="pf.adapterId"
id="pf.adapterId"'
```

e. Exportez la valeur « pf.adapterId » et renvoyez la réponse :

```
export ADAPTER='myAdapter'
```

```
echo "$RESPONSE" | grep 'base'
```

f. Exportez la valeur « href » (supprimez la barre oblique /) et affichez 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 les 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. Sauver le SAMLResponse du champ caché :

```
export SAMLResponse='PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4='
```

j. Utilisation de la sauvegarde SAMLResponse , créer un StorageGRID/api/saml-response demande de génération d'un jeton d'authentification StorageGRID .

Pour RelayState , utilisez l'ID de compte locataire ou utilisez 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 désormais utiliser MYTOKEN pour d'autres demandes, de la même manière que vous utiliseriez 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 Grid Management ou de l'API Tenant Management. Ces instructions s'appliquent si vous utilisez PingFederate comme fournisseur d'identité SSO

À propos de cette 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 porteur StorageGRID valide.

Étapes

1. Pour générer une demande de déconnexion signée, transmettez `cookie "sso=true"` à 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 rediriger vers StorageGRID.

```
curl --include "$LOGOUT_REQUEST"
```

La réponse 302 est renvoyée. L'emplacement de redirection ne s'applique pas à la déconnexion de l'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 porteur StorageGRID .

La suppression du jeton porteur StorageGRID fonctionne de la même manière que sans SSO. Si `cookie "sso=true" n'est pas 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
```

UN 204 No Content la réponse indique que l'utilisateur est maintenant déconnecté.

```
HTTP/1.1 204 No Content
```

Désactiver les fonctionnalités avec l'API

Vous pouvez utiliser l'API Grid Management pour désactiver complètement certaines fonctionnalités du système StorageGRID . Lorsqu'une fonctionnalité est désactivée, personne ne peut se voir attribuer d'autorisations pour effectuer les tâches liées à cette fonctionnalité.

À propos de cette tâche

Le système de fonctionnalités désactivées vous permet d'empêcher l'accès à certaines fonctionnalités du système StorageGRID . La désactivation d'une fonctionnalité est le seul moyen d'empêcher l'utilisateur root ou les utilisateurs appartenant à des groupes d'administrateurs avec l'autorisation **Accès root** de pouvoir utiliser cette fonctionnalité.

Pour comprendre comment cette fonctionnalité pourrait être utile, considérez 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 locataires. Pour protéger la sécurité des objets de ses locataires, la société A souhaite s'assurer que ses propres employés ne pourront jamais accéder à un compte locataire après le déploiement du compte.

_L'entreprise A peut atteindre cet objectif en utilisant le système de désactivation des fonctionnalités dans l'API de gestion de la grille. En désactivant complètement la fonctionnalité **Modifier le mot de passe root du locataire** dans le gestionnaire de grille (à la fois l'interface utilisateur et l'API), la société A garantit que les utilisateurs administrateurs, y compris l'utilisateur root et les utilisateurs appartenant à des groupes disposant de l'autorisation **Accès root**, ne peuvent pas modifier le mot de passe de l'utilisateur root d'un compte locataire.

Étapes

1. Accédez à la documentation Swagger pour l'API de gestion de grille. Voir ["Utiliser l'API de gestion de grille"](#).
2. Localisez le point de terminaison Désactiver les fonctionnalités.
3. Pour désactiver une fonctionnalité, telle que Modifier le mot de passe racine du locataire, envoyez un corps à l'API comme ceci :

```
{ "grid": { "changeTenantRootPassword": true } }
```

Une fois la demande terminée, la fonctionnalité Modifier le 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 le message « 403 Forbidden ».

Réactiver les fonctionnalités désactivées

Par défaut, vous pouvez utiliser l'API de gestion de grille pour réactiver une fonctionnalité qui a été désactivée. Cependant, si vous souhaitez empêcher que les fonctionnalités désactivées ne soient réactivées, vous pouvez désactiver la fonctionnalité **activateFeatures** elle-même.



La fonctionnalité **activateFeatures** ne peut pas être réactivée. Si vous décidez de désactiver cette fonctionnalité, sachez que vous perdrez définitivement la possibilité de réactiver toute autre fonctionnalité désactivée. Vous devez contacter le support technique pour restaurer toute fonctionnalité perdue.

Étapes

1. Accédez à la documentation Swagger pour l'API de gestion de grille.
2. Localisez le point de terminaison Désactiver les fonctionnalités.
3. Pour réactiver toutes les fonctionnalités, envoyez un corps à l'API comme ceci :

```
{ "grid": null }
```

Une fois cette demande terminée, toutes les fonctionnalités, y compris la fonctionnalité Modifier le mot de passe racine du locataire, sont réactivées. L'autorisation de gestion **Modifier le mot de passe racine du locataire** apparaît désormais dans l'interface utilisateur, et toute demande d'API qui tente de modifier le mot de passe racine d'un locataire réussira, en supposant que l'utilisateur dispose de l'autorisation de gestion **Accès racine** ou **Modifier le mot de passe racine du locataire**.



L'exemple précédent provoque la réactivation de *toutes* les fonctionnalités désactivées. Si d'autres fonctionnalités ont été désactivées et doivent rester désactivées, vous devez les spécifier explicitement dans la requête PUT. Par exemple, pour réactiver la fonctionnalité Modifier le mot de passe root du locataire et continuer à désactiver l'autorisation de gestion storageAdmin, envoyez cette requête PUT :

```
{ "grid": {"storageAdmin": true} }
```

Contrôler l'accès à StorageGRID

Contrôler l'accès à StorageGRID

Vous contrôlez 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. En option, vous pouvez activer l'authentification unique (SSO), créer des certificats clients et modifier les mots de passe de la grille.

Contrôler l'accès au Grid Manager

Vous déterminez qui peut accéder au Grid Manager et à l'API Grid Management en important des groupes et des utilisateurs à partir d'un service de fédération d'identité ou en configurant des groupes et des utilisateurs locaux.

En utilisant "[fédération d'identité](#)" facilite la mise en place "[groupes](#)" et "[utilisateurs](#)" plus rapide et permet aux utilisateurs de se connecter à StorageGRID à l'aide d'informations d'identification familières. Vous pouvez configurer la fédération d'identité 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 attribuant des rôles différents "[autorisations](#)" à chaque groupe. Par exemple, vous souhaitez peut-être que les utilisateurs d'un groupe puissent gérer les règles ILM et que les utilisateurs d'un autre groupe puissent effectuer des tâches de maintenance. Un utilisateur doit appartenir à au moins un groupe pour accéder au système.

En option, vous pouvez 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 fonctionnalités. Ils ne peuvent apporter aucune modification ni effectuer aucune opération dans Grid Manager ou l'API Grid Management.

Activer l'authentification unique

Le système StorageGRID prend en charge l'authentification unique (SSO) à l'aide de la norme Security Assertion Markup Language 2.0 (SAML 2.0). Après vous "[configurer et activer SSO](#)", tous les utilisateurs doivent être authentifiés par un fournisseur d'identité externe avant de pouvoir accéder au Grid Manager, au Tenant Manager, à l'API Grid Management ou à l'API Tenant Management. Les utilisateurs locaux ne peuvent pas se connecter à StorageGRID.

Modifier la phrase secrète d'approvisionnement

La phrase secrète de provisionnement est requise pour de nombreuses procédures d'installation et de maintenance, ainsi que pour le téléchargement du package de récupération StorageGRID . La phrase secrète est également requise pour télécharger les sauvegardes des informations de topologie de grille et des clés de chiffrement pour le système StorageGRID . Tu peux "[changer la phrase secrète](#)" selon les besoins.

Modifier les mots de passe de la console du nœud

Chaque nœud de votre grille possède un mot de passe de console de nœud unique, dont vous avez besoin pour vous connecter au nœud en tant qu'« admin » via SSH, ou en tant qu'utilisateur root sur une connexion VM/console physique. Au besoin, vous pouvez "[modifier le mot de passe de la console du nœud](#)" pour chaque nœud.

Modifier la phrase secrète de provisionnement

Utilisez cette procédure pour modifier la phrase secrète de provisionnement StorageGRID . La phrase secrète est requise pour les procédures de récupération, d'extension et de maintenance. La phrase secrète est également requise pour télécharger les sauvegardes du package de récupération qui incluent les informations de topologie de grille, les mots de passe de la console du nœud de grille et les clés de chiffrement du système StorageGRID .

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "[navigateur Web pris en charge](#)".
- Vous disposez des autorisations d'accès Maintenance ou Root.
- Vous disposez de la phrase secrète de provisionnement actuelle.

À propos de cette tâche

La phrase secrète de provisionnement est requise pour de nombreuses procédures d'installation et de maintenance, ainsi que pour "[téléchargement du package de récupération](#)". La phrase secrète de provisionnement n'est pas répertoriée dans le `Passwords.txt` déposer. Assurez-vous de documenter la phrase secrète de provisionnement et de la conserver dans un endroit sûr et sécurisé.

Étapes

1. Sélectionnez **CONFIGURATION > Contrôle d'accès > Mots de passe de la grille**.
2. Sous **Modifier la phrase secrète d'approvisionnement**, sélectionnez **Effectuer une modification**.
3. Saisissez votre mot de passe de provisionnement actuel.
4. Entrez la nouvelle phrase secrète. La phrase secrète doit contenir au moins 8 et pas plus de 32 caractères. Les phrases secrètes sont sensibles à la casse.
5. Stockez la nouvelle phrase secrète de provisionnement dans un endroit sûr. Il est nécessaire pour les procédures d'installation, d'extension et de maintenance.

6. Saisissez à nouveau la nouvelle phrase secrète et sélectionnez **Enregistrer**.

Le système affiche une bannière de réussite verte lorsque la modification de la phrase secrète de provisionnement est terminée.

 Provisioning passphrase successfully changed. Go to the [Recovery Package](#) to download a new Recovery Package.

7. Sélectionnez **Pack de récupération**.

8. Saisissez la nouvelle phrase secrète de provisionnement pour télécharger le nouveau package de récupération.



Après avoir modifié la phrase secrète de provisionnement, vous devez immédiatement télécharger un nouveau package de récupération. Le fichier Recovery Package vous permet de restaurer le système en cas de panne.

Modifier les mots de passe de la console du nœud

Chaque nœud de votre grille possède un mot de passe de console de nœud unique, dont vous avez besoin pour vous connecter au nœud. Suivez ces étapes 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 avez le ["Autorisation d'accès de maintenance ou root"](#).
- Vous disposez de la phrase secrète de provisionnement actuelle.

À propos de cette tâche

Utilisez le mot de passe de la console du nœud pour vous connecter à un nœud en tant qu'« administrateur » à l'aide de SSH ou en tant qu'utilisateur root sur une connexion VM/console physique. Le processus de changement de mot de passe de la console du nœud crée de nouveaux mots de passe pour chaque nœud de votre grille et stocke les mots de passe dans un fichier mis à jour. `Passwords.txt` fichier dans le package de récupération. 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 la grille**.
2. Sous **Modifier les mots de passe de la console du nœud**, sélectionnez **Effectuer une modification**.

Saisissez la phrase secrète de provisionnement

Étapes

1. Saisissez la phrase secrète de provisionnement de votre grille.
2. Sélectionnez **Continuer**.

Télécharger le package de récupération actuel

Avant de modifier les mots de passe de la console du nœud, téléchargez le package de récupération actuel. Vous pouvez utiliser les mots de passe de ce fichier si le processus de changement de mot de passe échoue pour un nœud.

Étapes

1. Sélectionnez **Télécharger le package de récupération**.
2. Copier le fichier du package de récupération(`.zip`) vers deux endroits sûrs, sécurisés et séparés.



Le fichier du package de récupération doit être sécurisé car il contient des clés de chiffrement et des mots de passe qui peuvent être utilisés pour obtenir des données à partir du système StorageGRID .

3. Sélectionnez **Continuer**.
4. Lorsque la boîte de dialogue de confirmation s'affiche, sélectionnez **Oui** si vous êtes prêt à commencer à modifier les mots de passe de la console du nœud.

Vous ne pouvez pas annuler ce processus une fois qu'il a commencé.

Modifier 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 récupération est généré qui inclut les nouveaux mots de passe. Ensuite, les mots de passe sont mis à jour sur chaque nœud.

Étapes

1. Attendez que le nouveau package de récupération soit généré, ce qui peut prendre quelques minutes.
2. Sélectionnez **Télécharger un nouveau package de récupération**.
3. Une fois le téléchargement terminé :
 - a. Ouvrez le `.zip` déposer.
 - b. Confirmez que vous pouvez accéder au contenu, y compris le `Passwords.txt` fichier, qui contient les nouveaux mots de passe de la console du nœud.
 - c. Copiez le nouveau fichier du package de récupération(`.zip`) vers deux endroits sûrs, sécurisés et séparés.



N'écrasez pas l'ancien package de récupération.

Le fichier du package de récupération doit être sécurisé car il contient des clés de chiffrement et des mots de passe qui peuvent être utilisés pour obtenir des données à partir 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 du nœud** et attendez que tous les nœuds soient mis à jour avec les nouveaux mots de passe. Cela peut prendre quelques minutes.

Si les mots de passe sont modifiés pour tous les nœuds, une bannière de réussite verte apparaît. Passez à l'étape suivante.

S'il y a une erreur pendant le processus de mise à jour, un message de bannière répertorie le nombre de nœuds dont le mot de passe n'a pas pu être modifié. Le système réessaiera automatiquement le processus sur tout nœud dont le mot de passe n'a pas été modifié. Si le processus se termine et que certains nœuds n'ont toujours pas de mot de passe modifié, le bouton **Réessayer** apparaît.

Si la mise à jour du mot de passe a échoué pour un ou plusieurs nœuds :

- a. Consultez les messages d'erreur répertoriés dans le tableau.
- b. Résoudre les problèmes.
- c. Sélectionnez **Réessayer**.



La nouvelle tentative modifie uniquement les mots de passe de la console du nœud sur les nœuds qui ont échoué lors des tentatives de modification de mot de passe précédentes.

6. Une fois les mots de passe de la console de nœud modifiés pour tous les nœuds, supprimez le [premier package de récupération que vous avez téléchargé](#) .
7. Vous pouvez également utiliser le lien **Pack de récupération** pour télécharger une copie supplémentaire du nouveau package de récupération.

Modifier les mots de passe d'accès SSH pour les nœuds d'administration

La modification des mots de passe d'accès SSH pour les nœuds d'administration met également à jour les ensembles uniques de clés SSH internes pour chaque nœud de la grille. Le nœud d'administration principal utilise ces clés SSH pour accéder aux nœuds à l'aide d'une authentification sécurisée et sans mot de passe.

Utilisez une clé SSH pour vous connecter à un nœud en tant que `admin` ou à l'utilisateur `root` sur une connexion VM ou console physique.

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 de maintenance ou root"](#) .
- Vous disposez de la phrase secrète de provisionnement actuelle.

À propos de cette tâche

Les nouveaux mots de passe d'accès pour les nœuds d'administration et les nouvelles clés internes pour chaque nœud sont stockés dans le `Passwords.txt` fichier dans le package de récupération. Les clés sont répertoriées dans la colonne Mot de passe de ce fichier.

Il existe des mots de passe d'accès SSH distincts pour les clés SSH utilisées pour la communication entre les nœuds. Ceux-ci ne sont pas modifiés par cette procédure.

Accéder à l'assistant

Étapes

1. Sélectionnez **CONFIGURATION > Contrôle d'accès > Mots de passe de la grille**.
2. Sous **Modifier les clés SSH**, sélectionnez **Effectuer une modification**.

Télécharger le package de récupération actuel

Avant de modifier les clés d'accès SSH, téléchargez le package de récupération actuel. Vous pouvez utiliser les clés de ce fichier si le processus de changement de clé échoue pour un nœud.

Étapes

1. Saisissez la phrase secrète de provisionnement de votre grille.
2. Sélectionnez **Télécharger le package de récupération**.
3. Copier le fichier du package de récupération(. zip) vers deux endroits sûrs, sécurisés et séparés.



Le fichier du package de récupération doit être sécurisé car il contient des clés de chiffrement et des mots de passe qui peuvent être utilisés pour obtenir des données à partir du système StorageGRID .

4. Sélectionnez **Continuer**.
5. Lorsque la boîte de dialogue de confirmation apparaît, sélectionnez **Oui** si vous êtes prêt à commencer à modifier les clés d'accès SSH.



Vous ne pouvez pas annuler ce processus une fois qu'il a commencé.

Modifier les clés d'accès SSH

Lorsque le processus de modification des clés d'accès SSH démarre, un nouveau package de récupération est généré qui inclut les nouvelles clés. Ensuite, les clés sont mises à jour sur chaque nœud.

Étapes

1. Attendez que le nouveau package de récupération soit généré, ce qui peut prendre quelques minutes.
2. Lorsque le bouton Télécharger un nouveau package de récupération est activé, sélectionnez **Télécharger un nouveau package de récupération** et enregistrez le nouveau fichier de package de récupération(. zip) vers deux endroits sûrs, sécurisés et séparés.
3. Une fois le téléchargement terminé :
 - a. Ouvrez le . zip déposer.
 - b. Confirmez que vous pouvez accéder au contenu, y compris le `Passwords.txt` fichier, qui contient les nouvelles clés d'accès SSH.
 - c. Copiez le nouveau fichier du package de récupération(. zip) vers deux endroits sûrs, sécurisés et séparés.



N'écrasez pas l'ancien package de récupération.

Le fichier du package de récupération doit être sécurisé car il contient des clés de chiffrement et des mots de passe qui peuvent être utilisés pour obtenir des données à partir du système StorageGRID .

4. Attendez que les clés soient mises à jour sur chaque nœud, ce qui peut prendre quelques minutes.

Si les clés sont modifiées pour tous les nœuds, une bannière de réussite verte apparaît.

En cas d'erreur lors du processus de mise à jour, un message de bannière répertorie le nombre de nœuds dont les clés n'ont pas pu être modifiées. Le système réessaiera automatiquement le processus sur tout

nœud dont la clé n'a pas été modifiée. Si le processus se termine avec certains nœuds n'ayant toujours pas de clé modifiée, le bouton **Réessayer** apparaît.

Si la mise à jour de la clé a échoué pour un ou plusieurs nœuds :

- a. Consultez les messages d'erreur répertoriés dans le tableau.
- b. Résoudre les problèmes.
- c. Sélectionnez **Réessayer**.

La nouvelle tentative modifie uniquement les clés d'accès SSH sur les nœuds qui ont échoué lors des tentatives de modification de clé précédentes.

5. Une fois les clés d'accès SSH modifiées pour tous les nœuds, supprimez le [premier package de récupération que vous avez téléchargé](#) .
6. Vous pouvez également sélectionner **MAINTENANCE > Système > Pack de récupération** pour télécharger une copie supplémentaire du nouveau package de récupération.

Utiliser la fédération d'identité

L'utilisation de la fédération d'identité accélère la configuration des groupes et des utilisateurs et permet aux utilisateurs de se connecter à StorageGRID à l'aide d'informations d'identification familières.

Configurer la fédération d'identité pour Grid Manager

Vous pouvez configurer la fédération d'identité dans Grid Manager si vous souhaitez que les groupes d'administrateurs et les utilisateurs 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"](#) .
- Tu as ["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 qui n'est pas répertorié, contactez le support technique.

- Si vous prévoyez d'utiliser OpenLDAP, vous devez configurer le serveur OpenLDAP. Voir [Directives pour la configuration d'un serveur OpenLDAP](#) .
- Si vous envisagez d'activer l'authentification unique (SSO), vous avez examiné les ["exigences et considérations relatives à l'authentification unique"](#) .
- Si vous prévoyez d'utiliser Transport Layer Security (TLS) pour les communications avec le serveur LDAP, le fournisseur d'identité utilise TLS 1.2 ou 1.3. Voir ["Chiffres pris en charge pour les connexions TLS sortantes"](#) .

À propos de cette tâche

Vous pouvez configurer une source 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'administrateurs. Les utilisateurs des groupes d'administrateurs 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 source 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 locataire](#)" et "[Utiliser un compte locataire](#)" pour plus de détails.

Entrer la configuration

Étapes

1. Sélectionnez **CONFIGURATION > Contrôle d'accès > Fédération d'identité**.
2. Sélectionnez **Activer la fédération d'identité**.
3. Dans la section Type de service LDAP, sélectionnez le type de service LDAP que vous souhaitez configurer.

LDAP service type

Select the type of LDAP service you want to configure.

Active Directory	Azure	OpenLDAP	Other

Sélectionnez **Autre** pour configurer les valeurs d'un serveur LDAP qui utilise Oracle Directory Server.

4. Si vous avez sélectionné **Autre**, remplissez les champs de la section Attributs LDAP. , passez à l'étape suivante.
 - **Nom unique de l'utilisateur** : le 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 utilisateur** : le 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 du groupe** : le 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** : le nom de l'attribut qui contient l'identifiant 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, saisissez les informations de serveur LDAP et de connexion réseau 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** : Le port utilisé pour se connecter au serveur LDAP.



Le port par défaut pour STARTTLS est 389 et le port par défaut pour LDAPS est 636. Cependant, vous pouvez utiliser n'importe quel port à condition que votre pare-feu soit correctement configuré.

- **Nom d'utilisateur** : le 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 de niveau inférieur ou le nom d'utilisateur principal.

L'utilisateur spécifié doit avoir l'autorisation de répertorier les groupes et les utilisateurs et d'accéder aux attributs suivants :

- `sAMAccountName` ou `uid`
- `objectGUID`, `entryUUID`, ou `nsuniqueid`
- `cn`
- `memberOf` ou `isMemberOf`
- **Active Directory**: `objectSid`, `primaryGroupID`, `userAccountControl`, et `userPrincipalName`
- **Azuré**: `accountEnabled` et `userPrincipalName`

- **Mot de passe** : Le mot de passe associé au nom d'utilisateur.



Si vous modifiez le mot de passe à l'avenir, vous devez le mettre à jour sur cette page.

- **DN de base du groupe** : le chemin complet du nom distinctif (DN) d'une sous-arborescence LDAP dans laquelle vous souhaitez 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=example,DC=com`) peuvent être utilisés comme groupes fédérés.



Les valeurs **Nom unique du groupe** doivent être uniques dans le **DN de base du groupe** auquel elles appartiennent.

- **DN de base utilisateur** : le chemin complet du nom distinctif (DN) d'une sous-arborescence LDAP dans laquelle vous souhaitez rechercher des utilisateurs.



Les valeurs **Nom unique de l'utilisateur** doivent être uniques dans le **DN de base de l'utilisateur** auquel elles appartiennent.

- * **Format de nom d'utilisateur de liaison *** (facultatif) : le modèle de nom d'utilisateur par défaut que StorageGRID doit utiliser si le modèle ne peut pas être déterminé automatiquement.

Il est recommandé de fournir le **format de nom d'utilisateur de liaison** car il peut permettre aux utilisateurs de se connecter si StorageGRID ne parvient pas à se lier au compte de service.

Saisissez l'un de ces modèles :

- **Modèle UserPrincipalName (Active Directory et Azure)**: `[USERNAME]@example.com`

- **Modèle de nom de connexion de niveau inférieur (Active Directory et Azure):**

example \ [USERNAME]

- **Modèle de nom distinctif:** CN= [USERNAME] , CN=Users, DC=*example*, DC=com

Incluez [USERNAME] exactement comme écrit.

6. Dans la section Sécurité de la couche de transport (TLS), sélectionnez un paramètre de sécurité.

- **Utiliser 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.
- **Utiliser 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.

- **Utiliser le certificat CA du système d'exploitation** : utilisez le certificat CA Grid par défaut installé sur le système d'exploitation pour sécuriser les connexions.
- **Utiliser un certificat CA 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.

Tester la connexion et enregistrer 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 du nom d'utilisateur de liaison, 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 de connexion réussi » s'affiche si les paramètres de connexion sont valides. Sélectionnez **Enregistrer** pour enregistrer la configuration.
 - Un message « La connexion de test n'a pas pu être établie » s'affiche si les paramètres de connexion ne sont pas valides. Sélectionnez **Fermer**. Ensuite, résolvez tous les problèmes et testez à nouveau la connexion.
3. Si vous avez fourni un format de nom d'utilisateur de liaison, saisissez le nom d'utilisateur et le mot de passe d'un utilisateur fédéré valide.

Par exemple, entrez votre propre nom d'utilisateur et votre mot de passe. N'incluez aucun caractère spécial dans le nom d'utilisateur, tel que @ ou /.

Test Connection

To test the connection and the bind username format, enter the username and password of a federated user. For example, enter your own federated username and password. The test values are not saved.

Test username

The username of a federated user.

Test password

[Cancel](#) [Test Connection](#)

- Un message « Test de connexion réussi » 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 de test ne sont pas valides. Résolvez tous les problèmes et testez à nouveau la connexion.

Forcer la synchronisation avec la source d’identité

Le système StorageGRID synchronise périodiquement les groupes fédérés et les utilisateurs à partir de la source d’identité. Vous pouvez forcer le démarrage de la synchronisation si vous souhaitez activer ou restreindre les autorisations des utilisateurs le plus rapidement possible.

Étapes

1. Accédez à la page Fédération d’identité.
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 la synchronisation de la fédération d’identité** est déclenchée s’il y a un problème de synchronisation des groupes fédérés et des utilisateurs à partir de la source d’identité.

Désactiver la fédération d’identité

Vous pouvez désactiver temporairement ou définitivement la fédération d’identité pour les groupes et les utilisateurs. Lorsque la fédération d’identité est désactivée, il n’y a aucune communication entre StorageGRID et la source d’identité. Cependant, tous les paramètres que vous avez configurés sont conservés, ce qui vous permet de réactiver facilement la fédération d’identité à l’avenir.

À propos de cette tâche

Avant de désactiver la fédération d’identité, vous devez tenir compte des points suivants :

- Les utilisateurs fédérés ne pourront pas se connecter.
- Les utilisateurs fédérés actuellement connectés conserveront 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 la source d'identité n'aura pas lieu et les alertes ne seront pas générées pour les comptes qui n'ont pas été synchronisés.
- La case à cocher **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 d'authentification unique doit être **Désactivé** avant de pouvoir désactiver la fédération d'identité. Voir ["Désactiver l'authentification unique"](#) .

Étapes

1. Accédez à la page Fédération d'identité.
2. Décochez la case **Activer la fédération d'identité**.

Directives pour la configuration d'un serveur OpenLDAP

Si vous souhaitez utiliser un serveur OpenLDAP pour la fédération d'identité, vous devez configurer des paramètres spécifiques sur le serveur OpenLDAP.



Pour les sources 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 toutes les clés S3 de l'utilisateur ou supprimez l'utilisateur de tous les groupes.

Superpositions Memberof et refint

Les superpositions memberof et refint doivent être activées. Pour plus d'informations, consultez les instructions relatives à la maintenance de l'appartenance à un groupe inversé dans <http://www.openldap.org/doc/admin24/index.html>["Documentation OpenLDAP : Guide de l'administrateur version 2.4"] .

Indexage

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.

Consultez les informations sur la maintenance de l'appartenance à un groupe inversé dans <http://www.openldap.org/doc/admin24/index.html>["Documentation OpenLDAP : Guide de l'administrateur version 2.4"] .

Gérer les groupes d'administrateurs

Vous pouvez créer des groupes d'administrateurs pour gérer les autorisations de sécurité d'un ou plusieurs utilisateurs administrateurs. Les utilisateurs doivent appartenir à un groupe pour avoir accès au système StorageGRID .

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un ["navigateur Web pris en charge"](#) .
- Tu as ["autorisations d'accès spécifiques"](#) .
- Si vous prévoyez d'importer un groupe fédéré, vous avez configuré la fédération d'identité et le groupe fédéré existe déjà dans la source d'identité configurée.

Créer un groupe d'administrateurs

Les groupes d'administrateurs vous permettent de déterminer quels utilisateurs peuvent accéder à quelles fonctionnalités et opérations dans Grid Manager et l'API Grid Management.

Accéder à l'assistant

Étapes

1. Sélectionnez **CONFIGURATION > Contrôle d'accès > Groupes d'administrateurs**.
2. Sélectionnez **Créer un 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 de la source 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, « Utilisateurs de maintenance » ou « Administrateurs ILM ».
3. Saisissez 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. Saisissez le nom du groupe que vous souhaitez importer, exactement tel qu'il apparaît dans la source d'identité configurée.
 - 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 le **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 peuvent

uniquement afficher 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 apporter aucune modification ni effectuer aucune opération dans Grid Manager ou l'API 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 aura un accès en lecture seule à tous les paramètres et fonctionnalités sélectionnés.

2. Sélectionnez un ou plusieurs **"autorisations du groupe administrateur"** .

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 un 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 de détails.

2. Sélectionnez **Créer un groupe** et **Terminer**.

Afficher et modifier les groupes d'administrateurs

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 sur 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 correspondant au groupe. b. Sélectionnez Actions > Afficher les détails du groupe .	Sélectionnez le nom du groupe dans le tableau.

Tâche	Menu Actions	Page de détails
Modifier le nom d'affichage (groupes locaux uniquement)	a. Cochez la case correspondant au groupe. b. Sélectionnez Actions > Modifier le nom du groupe . c. Entrez le nouveau nom. d. Sélectionnez Enregistrer les modifications .	a. Sélectionnez le nom du groupe pour afficher les détails. b. Sélectionnez l'icône d'édition  . c. Entrez le nouveau nom. d. Sélectionnez Enregistrer les modifications .
Modifier le mode d'accès ou les autorisations	a. Cochez la case correspondant au groupe. b. Sélectionnez Actions > Afficher les détails du groupe . c. Vous pouvez également modifier le mode d'accès du groupe. d. En option, sélectionnez ou désélectionnez " autorisations du groupe administrateur ". e. Sélectionnez Enregistrer les modifications .	a. Sélectionnez le nom du groupe pour afficher les détails. b. Vous pouvez également modifier le mode d'accès du groupe. c. En option, sélectionnez ou désélectionnez " autorisations du groupe administrateur ". d. Sélectionnez Enregistrer les modifications .

Dupliquer un groupe

Étapes

1. Cochez la case correspondant au groupe.
2. Sélectionnez **Actions > Dupliquer le groupe**.
3. Complétez l'assistant de duplication de groupe.

Supprimer un groupe

Vous pouvez supprimer un groupe d'administrateurs lorsque vous souhaitez supprimer le groupe du système et supprimer toutes les autorisations associées au groupe. La suppression d'un groupe d'administrateurs supprime tous les utilisateurs du groupe, mais ne supprime pas les utilisateurs.

Étapes

1. Depuis la page Groupes, cochez la case correspondant à chaque groupe que vous souhaitez supprimer.
2. Sélectionnez **Actions > Supprimer le groupe**.
3. Sélectionnez **Supprimer les groupes**.

Autorisations du groupe d'administrateurs

Lors de la création de groupes d'utilisateurs administrateurs, vous sélectionnez une ou plusieurs autorisations pour contrôler l'accès à des fonctionnalités spécifiques du gestionnaire de grille. Vous pouvez ensuite affecter chaque utilisateur à un ou plusieurs de ces groupes d'administrateurs pour déterminer les tâches que cet utilisateur peut

effectuer.

Vous devez attribuer au moins une autorisation à chaque groupe ; sinon, les utilisateurs appartenant à ce groupe ne pourront pas se connecter au gestionnaire de grille ou à l'API de gestion de grille.

Par défaut, tout utilisateur appartenant à un groupe disposant d'au moins une autorisation peut effectuer les tâches suivantes :

- Sign in au gestionnaire de grille
- Afficher le tableau de bord
- Afficher les pages Nœuds
- Afficher les alertes actuelles et résolues
- Modifier leur propre mot de passe (utilisateurs locaux uniquement)
- Consultez 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 peuvent uniquement afficher les paramètres et fonctionnalités associés. Si un utilisateur appartient à plusieurs groupes et qu'un groupe est défini sur **Lecture seule**, l'utilisateur aura un accès en lecture seule à tous les paramètres et fonctionnalités sélectionnés.

Les sections suivantes décrivent les autorisations que vous pouvez attribuer lors de la création ou de la modification d'un groupe d'administrateurs. Toute fonctionnalité non explicitement mentionnée nécessite l'autorisation **Accès root**.

Accès root

Cette autorisation donne accès à toutes les fonctionnalités d'administration du réseau.

Modifier le mot de passe root du locataire

Cette autorisation donne accès à l'option **Modifier le mot de passe root** sur la page Locataires, vous permettant de contrôler qui peut modifier le mot de passe de l'utilisateur root 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 **Modifier le mot de passe root**, attribuez également l'autorisation **Comptes locataires**.

Configuration de la page de topologie de grille

Cette autorisation donne accès aux onglets de configuration sur la page **SUPPORT > Outils > Topologie de grille**.



La page Topologie de grille est obsolète et sera supprimée dans une prochaine version.

ILM

Cette autorisation donne accès aux options de menu **ILM** suivantes :

- Règles
- Politiques
- Balises de politique
- Piscines de stockage
- Niveaux de stockage
- Régions
- Recherche de métadonnées d'objet



Les utilisateurs doivent disposer des autorisations **Autre configuration de grille** et **Configuration de la page de topologie de grille** pour gérer les niveaux de stockage.

Entretien

Les utilisateurs doivent disposer de l'autorisation Maintenance pour utiliser ces options :

- **CONFIGURATION > Contrôle d'accès:**
 - Mots de passe de la grille
- **CONFIGURATION > Réseau:**
 - Noms de domaine de point de terminaison S3
- **ENTRETIEN > Tâches:**
 - Déclassement
 - Expansion
 - Vérification de l'existence de l'objet
 - Récupération
- **ENTRETIEN > Système :**
 - Paquet de relance
 - Mise à jour du logiciel
- **SUPPORT > Outils:**
 - Journaux

Les utilisateurs qui ne disposent pas de l'autorisation Maintenance peuvent afficher, mais pas modifier, ces pages :

- **ENTRETIEN > Réseau :**
 - serveurs DNS
 - Réseau de grille
 - Serveurs NTP
- **ENTRETIEN > Système :**
 - Licence
- **CONFIGURATION > Réseau:**
 - Noms de domaine de point de terminaison 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.

Requête de métriques

Cette autorisation donne accès à :

- **SUPPORT > Outils > Page Métriques**
- Requêtes de métriques Prometheus personnalisées à l'aide de la section **Metrics** de l'API Grid Management
- Cartes de tableau de bord Grid Manager contenant des métriques

Recherche de métadonnées d'objet

Cette autorisation donne accès à la page **ILM > Recherche de métadonnées d'objet**.

Autre configuration de grille

Cette autorisation donne accès à des options de configuration de grille supplémentaires.



Pour voir ces options supplémentaires, les utilisateurs doivent également disposer de l'autorisation **Configuration de la page de topologie de grille**.

- **ILM:**
 - Niveaux de stockage
- **CONFIGURATION > Système:**
- **SOUTIEN > Autre :**
 - Coût du lien

Administrateur d'appareils de stockage

Cette autorisation prévoit :

- Accès au gestionnaire de système SANtricity E-Series sur les appliances de stockage via Grid Manager.
- La possibilité d'effectuer des tâches de dépannage et de maintenance sur l'onglet Gérer les lecteurs pour les appareils qui prennent en charge ces opérations.

Comptes locataires

Cette autorisation donne la possibilité de :

- Accédez à la page Locataires, où vous pouvez créer, modifier et supprimer des comptes locataires

- Afficher les politiques de classification du trafic existantes
- Afficher 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'administrateurs locaux pour déterminer les fonctionnalités 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"](#).
- Tu as ["autorisations d'accès spécifiques"](#).

Créer un utilisateur local

Vous pouvez créer un ou plusieurs utilisateurs locaux et affecter chaque utilisateur à un ou plusieurs groupes locaux. Les autorisations du groupe contrôlent les fonctionnalités de Grid Manager et de l'API Grid Management auxquelles l'utilisateur peut accéder.

Vous ne pouvez créer que des utilisateurs locaux. Utilisez la source d'identité externe pour gérer les utilisateurs et les groupes fédérés.

Le gestionnaire de grille comprend un utilisateur local prédéfini, nommé « root ». Vous ne pouvez pas supprimer l'utilisateur root.



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 administrateurs**.
2. Sélectionnez **Créer un utilisateur**.

Entrez 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. Si vous le souhaitez, sélectionnez **Oui** si cet utilisateur ne doit pas avoir accès au Grid Manager ou à l'API Grid Management.
3. Sélectionnez **Continuer**.

Affecter à des groupes

Étapes

1. Vous pouvez également affecter 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 "[Gérer les groupes d'administrateurs](#)" pour plus de détails.

2. Sélectionnez **Créer un utilisateur** et sélectionnez **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 la source d'identité externe pour gérer les utilisateurs fédérés.

- Pour afficher les informations de base de tous les utilisateurs locaux et fédérés, consultez le tableau sur la page Utilisateurs.
- Pour afficher tous les détails d'un utilisateur spécifique, modifier un utilisateur local ou changer 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 gestionnaire de grille.



Les utilisateurs locaux peuvent modifier leurs propres mots de passe à l'aide de l'option **Modifier le mot de passe** dans la bannière du gestionnaire de grille.

Tâche	Menu Actions	Page de détails
Afficher les détails de l'utilisateur	a. Cochez la case correspondant à 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 correspondant à l'utilisateur. b. Sélectionnez Actions > Modifier le nom complet . c. Entrez le nouveau nom. d. Sélectionnez Enregistrer les modifications .	a. Sélectionnez le nom de l'utilisateur pour afficher les détails. b. Sélectionnez l'icône d'édition  . c. Entrez le nouveau nom. d. Sélectionnez Enregistrer les modifications .

Tâche	Menu Actions	Page de détails
Refuser ou autoriser l'accès à StorageGRID	a. Cochez la case correspondant à 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 gestionnaire de grille ou à l'API de gestion de grille, ou sélectionnez Non pour autoriser l'utilisateur à 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 gestionnaire de grille ou à l'API de gestion de grille, ou sélectionnez Non pour autoriser l'utilisateur à se connecter. d. Sélectionnez Enregistrer les modifications.
Changer le mot de passe (utilisateurs locaux uniquement)	a. Cochez la case correspondant à l'utilisateur. b. Sélectionnez Actions > Afficher les détails de l'utilisateur. c. Sélectionnez l'onglet Mot de passe. d. Entrez un nouveau mot de passe. e. Sélectionnez Modifier le mot de passe.	a. Sélectionnez le nom de l'utilisateur pour afficher les détails. b. Sélectionnez l'onglet Mot de passe. c. Entrez un nouveau mot de passe. d. Sélectionnez Modifier le mot de passe.
Changer de groupe (utilisateurs locaux uniquement)	a. Cochez la case correspondant à 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 du 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 du 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 correspondant à l'utilisateur.

2. Sélectionnez **Actions** > **Dupliquer l'utilisateur**.
3. Complétez l'assistant de duplication d'utilisateur.

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. Depuis la page Utilisateurs, cochez la case correspondant à chaque utilisateur que vous souhaitez supprimer.
2. Sélectionnez **Actions** > **Supprimer l'utilisateur**.
3. Sélectionnez **Supprimer l'utilisateur**.

Utiliser l'authentification unique (SSO)

Configurer l'authentification unique

Lorsque l'authentification unique (SSO) est activée, les utilisateurs ne peuvent accéder au gestionnaire de grille, au gestionnaire de locataires, à l'API de gestion de grille ou à l'API de gestion de locataires que si leurs informations d'identification sont autorisées à l'aide du processus de connexion SSO mis en œuvre par votre organisation. Les utilisateurs locaux ne peuvent pas se connecter à StorageGRID.

Comment fonctionne l'authentification unique

Le système StorageGRID prend en charge l'authentification unique (SSO) à l'aide de la norme Security Assertion Markup Language 2.0 (SAML 2.0).

Avant d'activer l'authentification unique (SSO), vérifiez comment les processus de connexion et de déconnexion StorageGRID sont affectés lorsque SSO est activé.

Sign in lorsque SSO est activé

Lorsque SSO est activé et que vous vous connectez à StorageGRID, vous êtes redirigé vers la page SSO de votre organisation pour valider vos informations d'identification.

Étapes

1. Saisissez le nom de domaine complet ou l'adresse IP de n'importe quel nœud d'administration StorageGRID dans un navigateur Web.

La page de Sign in StorageGRID s'affiche.

- Si c'est la première fois que vous accédez à l'URL sur ce navigateur, vous êtes invité à saisir un identifiant de compte :



Sign in

Account

Sign in

[NetApp support](#) | [NetApp.com](#)

- 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 :



Tenant Manager

Recent

Account

Sign in

[NetApp support](#) | [NetApp.com](#)



La page de Sign in StorageGRID ne s'affiche pas lorsque vous saisissez l'URL complète d'un compte 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 organisation, où vous pouvez [connectez-vous avec 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 **Gestionnaire de grille** s'il apparaît dans la liste des comptes récents.
- Pour accéder au gestionnaire de locataires, saisissez l'ID de compte locataire à 20 chiffres ou sélectionnez un locataire par son nom s'il apparaît dans la liste des comptes récents.

3. Sélectionner * Sign in*

StorageGRID vous redirige vers la page de connexion SSO de votre organisation. Par exemple:

Sign in with your organizational account

someone@example.com

Password

Sign in

4. Sign in avec vos identifiants SSO.

Si vos informations d'identification SSO sont correctes :

- a. Le fournisseur d'identité (IdP) 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 Grid Manager ou au Tenant Manager, selon le compte que vous avez sélectionné.



Si le compte de service est inaccessible, vous pouvez toujours vous connecter, à condition que vous soyez un utilisateur existant appartenant à un groupe fédéré avec des autorisations d'accès StorageGRID.

5. Vous pouvez également accéder à d'autres nœuds d'administration ou accéder au gestionnaire de grille ou au gestionnaire de locataires, si vous disposez des autorisations adéquates.

Vous n'avez pas besoin de ressaisir vos identifiants SSO.

Déconnectez-vous lorsque SSO est activé

Lorsque SSO est activé pour StorageGRID, ce qui se passe lorsque vous vous déconnectez dépend de ce à quoi vous êtes connecté et de l'endroit d'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 Sign in 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 à ces interfaces utilisateur plus rapidement à l'avenir.

Si vous êtes connecté à...	Et vous vous déconnectez de...	Vous êtes déconnecté de...
Gestionnaire de grille sur un ou plusieurs nœuds d'administration	Gestionnaire de grille sur n'importe quel nœud d'administration	Gestionnaire de grille sur tous les nœuds d'administration Remarque : si vous utilisez Azure pour l'authentification unique, la déconnexion 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
Gestionnaire de réseau et gestionnaire de locataires	Gestionnaire de grille	Le gestionnaire de grille uniquement. Vous devez également vous déconnecter du gestionnaire de locataires 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 sur plusieurs sessions de navigateur, vous devez vous déconnecter de toutes les sessions de navigateur séparément.

Exigences et considérations relatives à l'authentification unique

Avant d'activer l'authentification unique (SSO) pour un système StorageGRID, examinez les exigences et les considérations.

Exigences relatives aux fournisseurs d'identité

StorageGRID prend en charge les fournisseurs d'identité SSO (IdP) suivants :

- Service de fédération Active Directory (AD FS)
- Azure Active Directory (Azure AD)
- PingFédéré

Vous devez configurer la fédération d'identité pour votre système StorageGRID avant de pouvoir configurer un fournisseur d'identité SSO. Le type de service LDAP que vous utilisez pour la fédération d'identité 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 • Azuré • PingFédéré
Azuré	Azuré

Exigences AD FS

Vous pouvez utiliser l'une des versions suivantes d'AD FS :

- Windows Server 2022 AD FS
- Windows Server 2019 AD FS
- Windows Server 2016 AD FS



Windows Server 2016 devrait utiliser le "[Mise à jour KB3201845](#)" , ou supérieur.

Exigences supplémentaires

- Sécurité de la couche transport (TLS) 1.2 ou 1.3
- Microsoft .NET Framework, version 3.5.1 ou supérieure

Considérations pour Azure

Si vous utilisez Azure comme type SSO et que les utilisateurs ont des noms d'utilisateur principaux qui n'utilisent pas sAMAccountName comme préfixe, des problèmes de connexion peuvent survenir si StorageGRID perd sa connexion avec le serveur LDAP. Pour permettre aux utilisateurs de se connecter, vous devez restaurer la connexion au serveur LDAP.

Exigences relatives aux certificats de serveur

Par défaut, StorageGRID utilise un certificat d'interface de gestion sur chaque nœud d'administration pour sécuriser l'accès au gestionnaire de grille, au gestionnaire de locataires, à l'API de gestion de grille et à l'API de gestion de locataires. Lorsque vous configurez des approbations de parties de confiance (AD FS), des applications d'entreprise (Azure) ou des connexions de fournisseurs de services (PingFederate) pour StorageGRID, vous utilisez le certificat du serveur comme certificat de signature pour les demandes StorageGRID .

Si vous ne l'avez pas déjà fait "[configuré un certificat personnalisé pour l'interface de gestion](#)" , tu devrais 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 parties de confiance StorageGRID , les applications d'entreprise ou les connexions SP .



L'utilisation du certificat de serveur par défaut d'un nœud d'administration dans une connexion de confiance, une application d'entreprise ou un SP n'est pas recommandée. 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 récupéré, vous devez mettre à jour l'approbation de la partie de confiance, l'application d'entreprise ou la connexion SP avec le nouveau certificat.

Vous pouvez accéder au certificat du serveur d'un nœud d'administration en vous connectant à l'interpréteur de commandes du nœud et en accédant à l' `/var/local/mgmt-api` annuaire. Un certificat de serveur personnalisé est nommé `custom-server.crt` . Le certificat de serveur par défaut du nœud est nommé `server.crt` .

Exigences portuaires

L'authentification unique (SSO) n'est pas disponible sur les ports restreints Grid Manager ou Tenant Manager. Vous devez utiliser le port HTTPS par défaut (443) si vous souhaitez que les utilisateurs s'authentifient avec l'authentification unique. Voir "[Contrôler l'accès au pare-feu externe](#)".

Confirmer 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 gestionnaire de grille et au gestionnaire de locataires pour tous les comptes de locataires existants.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "[navigateur Web pris en charge](#)".
- Tu as "[autorisations d'accès spécifiques](#)".
- Vous avez déjà configuré la fédération d'identité.

Étapes

1. S'il existe des comptes locataires existants, confirmez qu'aucun des locataires n'utilise sa propre source d'identité.



Lorsque vous activez SSO, une source d'identité configurée dans le gestionnaire de locataires est remplacée par la source d'identité configurée dans le gestionnaire de grille. Les utilisateurs appartenant à la source d'identité du locataire ne pourront plus se connecter à moins qu'ils ne disposent d'un compte auprès de la source d'identité Grid Manager.

- a. Sign in au gestionnaire de locataires pour chaque compte locataire.
 - b. Sélectionnez **GESTION DES ACCÈS > Fédération d'identité**.
 - c. Vérifiez que la case à cocher **Activer la fédération d'identité** n'est pas sélectionnée.
 - d. Si tel est le cas, confirmez que tous les groupes fédérés susceptibles d'être utilisés pour ce compte locataire ne sont plus nécessaires, décochez la case et sélectionnez **Enregistrer**.
2. Confirmer qu'un utilisateur fédéré peut accéder au gestionnaire de grille :
 - a. Depuis le Gestionnaire de grille, sélectionnez **CONFIGURATION > Contrôle d'accès > Groupes d'administrateurs**.
 - b. Assurez-vous qu'au moins un groupe fédéré a été importé à partir de la source d'identité Active Directory et que l'autorisation d'accès racine lui a été attribuée.
 - c. Se déconnecter.

- d. Confirmez que vous pouvez vous reconnecter au gestionnaire de grille en tant qu'utilisateur du groupe fédéré.
3. S'il existe des comptes locataires existants, confirmez qu'un utilisateur fédéré disposant d'une autorisation d'accès root peut se connecter :
 - a. Depuis le gestionnaire de grille, sélectionnez **LOCATAIRES**.
 - b. Sélectionnez le compte locataire, puis sélectionnez **Actions > Modifier**.
 - c. Dans l'onglet Entrer les détails, sélectionnez **Continuer**.
 - d. Si la case à cocher **Utiliser sa propre source d'identité** est sélectionnée, décochez la case et sélectionnez **Enregistrer**.

Edit the tenant

Enter details — 2 Select permissions

Select permissions

Select the permissions for this tenant account.

☐ Allow platform services ?

☐ Use own identity source ?

☐ Allow S3 Select ?

La page Locataire apparaît.

- a. Sélectionnez le compte locataire, sélectionnez * Sign in* et connectez-vous au compte locataire en tant qu'utilisateur root local.
- b. Depuis le gestionnaire de locataires, sélectionnez **GESTION DES ACCÈS > Groupes**.
- c. Assurez-vous qu'au moins un groupe fédéré du gestionnaire de grille s'est vu attribuer l'autorisation d'accès racine pour ce locataire.
- d. Se déconnecter.
- e. Confirmez que vous pouvez vous reconnecter au locataire en tant qu'utilisateur du groupe fédéré.

Informations connexes

- ["Exigences et considérations relatives à l'authentification unique"](#)
- ["Gérer les groupes d'administrateurs"](#)
- ["Utiliser un compte 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 l'authentification unique activée, vous pouvez revenir au mode sandbox chaque fois que vous devez modifier ou retester la configuration.

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 root"](#) .
- Vous avez configuré la fédération d'identité pour votre système StorageGRID .
- Pour le type de service LDAP de fédération d'identité, vous avez sélectionné Active Directory ou Azure, en fonction du fournisseur d'identité SSO que vous prévoyez d'utiliser.

Type de service LDAP configuré	Options pour le fournisseur d'identité SSO
Active Directory	• Active Directory • Azuré • PingFédéré
Azuré	Azuré

À propos de cette 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. À son tour, le fournisseur d'identité SSO renvoie une réponse d'authentification à StorageGRID, indiquant si la demande d'authentification a réussi. Pour des demandes réussies :

- La réponse d'Active Directory ou de 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 sur les demandes d'authentification des utilisateurs, vous devez configurer certains paramètres dans StorageGRID. Ensuite, vous devez utiliser le logiciel du fournisseur d'identité SSO pour créer une approbation de partie 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 SSO.

Le mode Sandbox facilite l'exécution de cette configuration aller-retour et permet de tester tous vos paramètres avant d'activer 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 > Authentification unique**.

La page d'authentification unique s'affiche, avec l'option **Désactivé** sélectionnée.

Single Sign-on

You can enable single sign-on (SSO) if you want an external identity provider (IdP) to authorize all user access to StorageGRID. To start, enable [identity federation](#) and confirm that at least one federated user has Root Access permission to the Grid Manager and to the Tenant Manager for any existing tenant accounts. Next, select Sandbox Mode to configure, save, and then test your SSO settings. After verifying the connections, select Enabled and click Save to start using SSO.

SSO status  ☒ Disabled ☐ Sandbox Mode ☐ Enabled

Save



Si les options d'état SSO n'apparaissent pas, confirmez que vous avez configuré le fournisseur d'identité comme source d'identité fédérée. Voir "[Exigences et considérations relatives à l'authentification unique](#)".

2. Sélectionnez **Mode Sandbox**.

La section Fournisseur d'identité apparaît.

Entrez les détails du fournisseur d'identité

Étapes

1. Sélectionnez le **type SSO** dans la liste déroulante.
2. Remplissez les champs de la section Fournisseur d'identité en fonction du type SSO que vous avez sélectionné.

Active Directory

- a. Saisissez le **Nom du service de fédération** pour le fournisseur d'identité, exactement tel qu'il apparaît dans Active Directory Federation Service (AD FS).



Pour localiser le nom du service de fédération, accédez au Gestionnaire de serveur Windows. Sélectionnez **Outils > Gestion AD FS**. Dans le menu Action, sélectionnez **Modifier les propriétés du service de fédération**. Le nom du service de fédération est affiché dans le deuxième champ.

- b. Spécifiez quel certificat TLS sera utilisé pour sécuriser la connexion lorsque le fournisseur d'identité envoie des informations de configuration SSO en réponse aux demandes StorageGRID .

- **Utiliser le certificat CA du système d'exploitation** : utilisez le certificat CA par défaut installé sur le système d'exploitation pour sécuriser la connexion.
- **Utiliser un certificat CA personnalisé** : utilisez un certificat CA 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**.

- **Ne pas utiliser TLS** : N'utilisez pas de certificat TLS pour sécuriser la connexion.



Si vous modifiez le certificat CA, immédiatement "[redémarrer le service mgmt-api sur les nœuds d'administration](#)" et tester une connexion SSO réussie dans le Grid Manager.

- c. Dans la section Partie de confiance, spécifiez l'**identifiant de la partie de confiance** pour StorageGRID. Cette valeur contrôle le nom que vous utilisez pour chaque approbation de partie de confiance dans AD FS.

- Par exemple, si votre grille 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 grille comprend plusieurs nœuds d'administration, incluez la chaîne [HOSTNAME] dans l'identifiant. Par exemple : SG-[HOSTNAME] . Cela génère un tableau qui affiche l'identifiant de la partie de confiance pour chaque nœud d'administration de votre système, en fonction du nom d'hôte du nœud.



Vous devez créer une approbation de partie de confiance pour chaque nœud d'administration de votre système StorageGRID . Le fait de disposer d'une partie de confiance pour chaque nœud d'administration garantit que les utilisateurs peuvent se connecter et se déconnecter en toute sécurité de n'importe quel nœud d'administration.

- d. Sélectionnez **Enregistrer**.

Une coche verte apparaît sur le bouton **Enregistrer** pendant quelques secondes.

Save

Azuré

- a. Spécifiez quel certificat TLS sera utilisé pour sécuriser la connexion lorsque le fournisseur d'identité envoie des informations de configuration SSO en réponse aux demandes StorageGRID .

- **Utiliser le certificat CA du système d'exploitation** : utilisez le certificat CA par défaut installé sur le système d'exploitation pour sécuriser la connexion.
- **Utiliser un certificat CA personnalisé** : utilisez un certificat CA 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**.

- **Ne pas utiliser TLS** : N'utilisez pas de certificat TLS pour sécuriser la connexion.



Si vous modifiez le certificat CA, immédiatement "[redémarrer le service mgmt-api sur les nœuds d'administration](#)" et tester une connexion SSO réussie dans le Grid Manager.

- b. Dans la section Application d'entreprise, spécifiez le **Nom de l'application d'entreprise** pour StorageGRID. Cette valeur contrôle le nom que vous utilisez pour chaque application d'entreprise dans Azure AD.

- Par exemple, si votre grille 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 grille comprend plusieurs nœuds d'administration, incluez la chaîne [HOSTNAME] dans l'identifiant. Par exemple : SG-[HOSTNAME] . Cela génère un tableau qui affiche un nom d'application d'entreprise pour chaque nœud d'administration de votre système, en fonction du nom d'hôte du nœud.



Vous devez créer une application d'entreprise pour chaque nœud d'administration de votre système StorageGRID . Disposer d'une application d'entreprise pour chaque nœud d'administration garantit que les utilisateurs peuvent se connecter et se déconnecter en toute sécurité de n'importe quel nœud d'administration.

- c. Suivez les étapes dans "[Créer des applications d'entreprise dans Azure AD](#)" pour créer une application d'entreprise pour chaque nœud d'administration répertorié dans le tableau.
- d. 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 la fédération** correspondant dans StorageGRID.
- e. 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 **Enregistrer** pendant quelques secondes.



PingFédéré

- a. Spécifiez quel certificat TLS sera utilisé pour sécuriser la connexion lorsque le fournisseur d'identité envoie des informations de configuration SSO en réponse aux demandes StorageGRID .

- **Utiliser le certificat CA du système d'exploitation** : utilisez le certificat CA par défaut installé sur le système d'exploitation pour sécuriser la connexion.
- **Utiliser un certificat CA personnalisé** : utilisez un certificat CA 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**.

- **Ne pas utiliser TLS** : N'utilisez pas de certificat TLS pour sécuriser la connexion.



Si vous modifiez le certificat CA, immédiatement "[redémarrer le service mgmt-api sur les nœuds d'administration](#)" et tester une connexion SSO réussie dans le Grid Manager.

- b. Dans la section Fournisseur de services (SP), 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 grille 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 grille comprend plusieurs nœuds d'administration, incluez la chaîne [HOSTNAME] dans l'identifiant. Par exemple : SG- [HOSTNAME] . Cela génère un tableau qui affiche l'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 . Disposer d'une connexion SP pour chaque nœud d'administration garantit que les utilisateurs peuvent se connecter et se déconnecter en toute sécurité de n'importe quel nœud d'administration.

- c. Spécifiez l'URL des métadonnées de la fédération pour chaque nœud d'administration dans le champ **URL des métadonnées de la fédération**.

Utilisez le format suivant :

```
https://<Federation Service  
Name>:<port>/pf/federation_metadata.ping?PartnerSpId=<SP  
Connection ID>
```

- d. Sélectionnez **Enregistrer**.

Une coche verte apparaît sur le bouton **Enregistrer** pendant quelques secondes.

Save 

Configurer les approbations des parties de confiance, les applications d'entreprise ou les connexions SP

Lorsque la configuration est enregistrée, l'avis de confirmation du mode Sandbox apparaît. Cet avis confirme que le mode sandbox est désormais activé et fournit des instructions générales.

StorageGRID peut rester en mode sandbox aussi longtemps que nécessaire. Cependant, lorsque le **Mode Sandbox** est sélectionné sur la page d'authentification unique, l'authentification unique est désactivée pour tous les utilisateurs de StorageGRID . Seuls les utilisateurs locaux peuvent se connecter.

Suivez ces étapes pour configurer les approbations des parties de confiance (Active Directory), compléter les applications d'entreprise (Azure) ou configurer les connexions SP (PingFederate).

Active Directory

Étapes

1. Accédez aux services de fédération Active Directory (AD FS).
2. Créez une ou plusieurs approbations de partie de confiance pour StorageGRID, en utilisant chaque identifiant de partie de confiance indiqué dans le tableau de la page d'authentification unique StorageGRID .

Vous devez créer une approbation pour chaque nœud d'administration affiché dans le tableau.

Pour obtenir des instructions, rendez-vous sur "[Créer des approbations de parties de confiance dans AD FS](#)" .

Azuré

Étapes

1. Depuis la page d'authentification unique du nœud d'administration auquel vous êtes actuellement connecté, sélectionnez le bouton pour télécharger et enregistrer les métadonnées SAML.
2. Ensuite, pour tous les autres nœuds d'administration de votre grille, répétez ces étapes :
 - a. Sign in au nœud.
 - b. Sélectionnez **CONFIGURATION > Contrôle d'accès > Authentification unique**.
 - c. Téléchargez et enregistrez les métadonnées SAML pour ce nœud.
3. Accédez au portail Azure.
4. Suivez les étapes dans "[Créer des applications d'entreprise dans Azure AD](#)" pour télécharger le fichier de métadonnées SAML pour chaque nœud d'administration dans son application d'entreprise Azure correspondante.

PingFédéré

Étapes

1. Depuis la page d'authentification unique du nœud d'administration auquel vous êtes actuellement connecté, sélectionnez le bouton pour télécharger et enregistrer les métadonnées SAML.
2. Ensuite, pour tous les autres nœuds d'administration de votre grille, répétez ces étapes :
 - a. Sign in au nœud.
 - b. Sélectionnez **CONFIGURATION > Contrôle d'accès > Authentification unique**.
 - c. Téléchargez et enregistrez les métadonnées SAML pour ce nœud.
3. Accédez à PingFederate.
4. "[Créer une ou plusieurs connexions de fournisseur de services \(SP\) pour StorageGRID](#)" . Utilisez l'ID de connexion SP pour chaque nœud d'administration (affiché 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 indiqué 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. À partir de la page d'authentification unique StorageGRID , recherchez le lien dans le message du mode Sandbox.

L'URL est dérivée de la valeur que vous avez saisie dans le champ **Nom du service de fédération**.

Sandbox mode

Sandbox mode is currently enabled. Use this mode to configure relying party trusts and to confirm that single sign-on (SSO) and single logout (SLO) are correctly configured for the StorageGRID system.

1. Use Active Directory Federation Services (AD FS) to create relying party trusts for StorageGRID. Create one trust for each Admin Node, using the relying party identifier(s) shown below.
2. Go to your identity provider's sign-on page: <https://ad2016.saml.sgws/adfs/ls/idpinitiatedsignon.htm>
3. From this page, sign in to each StorageGRID relying party trust. If the SSO operation is successful, StorageGRID displays a page with a success message. Otherwise, an error message is displayed.

When you have confirmed SSO for each of the relying party trusts and you are ready to enforce the use of SSO for StorageGRID, change the SSO Status to Enabled, and click Save.

2. Sélectionnez le lien ou copiez et collez l'URL dans un navigateur pour accéder à la page de connexion de votre fournisseur d'identité.
3. Pour confirmer que vous pouvez utiliser SSO pour vous connecter à StorageGRID, sélectionnez * Sign in à l'un des sites suivants*, sélectionnez l'identifiant de la partie de confiance pour votre nœud d'administration principal et sélectionnez * Sign in*.

You are not signed in.

☐ Sign in to this site.

☒ Sign in to one of the following sites:

SG-DC1-ADM1

Sign in

4. Entrez votre nom d'utilisateur et votre mot de passe fédérés.
 - Si les opérations de connexion et de déconnexion SSO réussissent, 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. Résolvez 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.

Azuré

Étapes

1. Accédez à la page d'authentification unique dans le portail Azure.
2. Sélectionnez **Tester cette application**.
3. Saisissez les informations d'identification d'un utilisateur fédéré.
 - Si les opérations de connexion et de déconnexion SSO réussissent, 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. Résolvez 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.

PingFédéré

Étapes

1. À partir de la page d'authentification unique StorageGRID , sélectionnez le premier lien dans le message du mode Sandbox.

Sélectionnez et testez un lien à la fois.

Sandbox mode

Sandbox mode is currently enabled. Use this mode to configure service provider (SP) connections and to confirm that single sign-on (SSO) and single logout (SLO) are correctly configured for the StorageGRID system.

1. Use Ping Federate to create SP connections for StorageGRID. Create one SP connection for each Admin Node, using the relying party identifier(s) shown below.
2. Test SSO and SLO by selecting the link for each Admin Node:
 - [https://\[redacted\]/idp/startSSO.ping?PartnerSpId=SG-DC1-ADM1-106-69](https://[redacted]/idp/startSSO.ping?PartnerSpId=SG-DC1-ADM1-106-69)
 - [https://\[redacted\]/idp/startSSO.ping?PartnerSpId=SG-DC2-ADM1-106-73](https://[redacted]/idp/startSSO.ping?PartnerSpId=SG-DC2-ADM1-106-73)
3. StorageGRID displays a success or error message for each test.

When you have confirmed SSO for each SP connection and you are ready to enforce the use of SSO for StorageGRID, change the SSO Status to Enabled, and select **Save**.

2. Saisissez les informations d'identification d'un utilisateur fédéré.
 - Si les opérations de connexion et de déconnexion SSO réussissent, 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. Résolvez le problème, effacez les cookies du navigateur et réessayez.
3. Sélectionnez le lien suivant pour vérifier la connexion SSO pour chaque nœud d'administration de votre grille.

Si vous voyez un message indiquant que la page a expiré, sélectionnez le bouton **Retour** dans votre navigateur et soumettez à nouveau vos informations d'identification.

Activer l'authentification unique

Une fois que vous avez confirmé que vous pouvez utiliser SSO pour vous connecter à chaque nœud d'administration, vous pouvez activer SSO pour l'ensemble de votre système StorageGRID .



Lorsque SSO est activé, tous les utilisateurs doivent utiliser SSO pour accéder au gestionnaire de grille, au gestionnaire de locataires, à l'API de gestion de grille et à l'API de gestion de locataires. Les utilisateurs locaux ne peuvent plus accéder à StorageGRID.

Étapes

1. Sélectionnez **CONFIGURATION > Contrôle d'accès > Authentification unique**.
2. Modifiez le statut SSO sur **Activé**.
3. Sélectionnez **Enregistrer**.
4. Lisez 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 (un utilisateur d'un groupe fédéré qui a été importé dans StorageGRID) ou déconnectez-vous du portail Azure avant de tenter de vous connecter à StorageGRID.

Créer des approbations de parties de confiance dans AD FS

Vous devez utiliser les services de fédération Active Directory (AD FS) pour créer une approbation de partie de confiance pour chaque nœud d'administration de votre système. Vous pouvez créer des approbations de parties de confiance à l'aide de commandes PowerShell, en important des métadonnées SAML à partir de StorageGRID ou en saisissant les données manuellement.

Avant de commencer

- Vous avez configuré l'authentification unique pour StorageGRID et vous avez sélectionné **AD FS** comme type d'authentification unique.
- Le **mode Sandbox** est sélectionné sur la page d'authentification unique dans Grid Manager. Voir "[Utiliser le mode sandbox](#)".
- Vous connaissez le nom de domaine complet (ou l'adresse IP) et l'identifiant de la partie de confiance pour chaque nœud d'administration de votre système. Vous pouvez trouver ces valeurs dans le tableau détaillé des nœuds d'administration sur la page d'authentification unique StorageGRID .



Vous devez créer une approbation de partie de confiance pour chaque nœud d'administration de votre système StorageGRID . Le fait de disposer d'une partie de confiance pour chaque nœud d'administration garantit que les utilisateurs peuvent se connecter et se déconnecter en toute sécurité de n'importe quel nœud d'administration.

- Vous avez de l'expérience dans la création d'approbations de parties de confiance dans AD FS ou vous avez accès à la documentation Microsoft AD FS.
- Vous utilisez le composant logiciel enfichable Gestion AD FS et vous appartenez au groupe Administrateurs.
- Si vous créez manuellement l'approbation de partie de confiance, vous disposez du certificat personnalisé qui a été téléchargé pour l'interface de gestion StorageGRID ou vous savez comment vous connecter à un nœud d'administration à partir de l'interpréteur de commandes.

À propos de cette 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. Consultez la documentation Microsoft AD FS si vous avez des questions.

Créer une approbation de partie de confiance à l'aide de Windows PowerShell

Vous pouvez utiliser Windows PowerShell pour créer rapidement une ou plusieurs approbations de parties de confiance.

Étapes

1. Dans le menu Démarrer de Windows, sélectionnez avec le bouton droit de la souris l'icône PowerShell et sélectionnez **Exécuter en tant qu'administrateur**.
2. À l'invite de commande PowerShell, entrez la commande suivante :

```
Add-AdfsRelyingPartyTrust -Name "Admin_Node_Identifer" -MetadataURL
"https://Admin_Node_FQDN/api/saml-metadata"
```

- Pour *Admin_Node_Identifier*, saisissez l'identifiant de la partie de confiance pour le nœud d'administration, exactement tel qu'il apparaît sur la page d'authentification unique. Par exemple : SG-DC1-ADM1 .
- Pour *Admin_Node_FQDN*, entrez le nom de domaine complet pour le même nœud d'administration. (Si nécessaire, vous pouvez utiliser l'adresse IP du nœud à la place. Cependant, si vous saisissez une adresse IP ici, sachez que vous devez mettre à jour ou recréer cette approbation de partie de confiance si cette adresse IP change un jour.)

3. Dans le Gestionnaire de serveur Windows, sélectionnez **Outils > Gestion AD FS**.

L'outil de gestion AD FS apparaît.

4. Sélectionnez **AD FS > Approbations de parties de confiance**.

La liste des fiduciaires de parties utilisatrices s'affiche.

5. Ajoutez une politique de contrôle d'accès à la nouvelle approbation de partie de confiance créée :
 - a. Localisez la fiducie de partie de confiance que vous venez de créer.
 - b. Cliquez avec le bouton droit sur l'approbation et sélectionnez **Modifier la politique de contrôle d'accès**.
 - c. Sélectionnez une politique de contrôle d'accès.
 - d. Sélectionnez **Appliquer**, puis **OK**
6. Ajoutez une politique d'émission de réclamation à la fiducie de partie utilisatrice nouvellement créée :

- a. Localisez la fiducie de partie de confiance que vous venez de créer.
- b. Cliquez avec le bouton droit sur la fiducie et sélectionnez **Modifier la politique d'émission de réclamation**.
- c. Sélectionnez **Ajouter une règle**.
- d. Sur la page Sélectionner un modèle de règle, sélectionnez **Envoyer les attributs LDAP en tant que revendications** dans la liste, puis sélectionnez **Suivant**.
- e. Sur la page Configurer la règle, entrez un nom d'affichage pour cette règle.

Par exemple, **ObjectGUID vers Name ID** ou **UPN vers Name ID**.

- f. Pour le magasin d'attributs, sélectionnez **Active Directory**.
 - g. Dans la colonne Attribut LDAP de la table de mappage, saisissez **objectGUID** ou sélectionnez **User-Principal-Name**.
 - h. Dans la colonne Type de réclamation sortante de la table de mappage, sélectionnez **ID de nom** dans la liste déroulante.
 - i. Sélectionnez **Terminer**, puis **OK**.
7. Confirmez que les métadonnées ont été importées avec succès.
 - a. Cliquez avec le bouton droit sur l'approbation de la partie de confiance pour ouvrir ses propriétés.
 - b. Confirmez que les champs des onglets **Points de terminaison**, **Identifiants** et **Signature** sont renseignés.

Si les métadonnées sont manquantes, confirmez que l'adresse des métadonnées de la Fédération est correcte ou saisissez les valeurs manuellement.

8. Répétez ces étapes pour configurer une approbation de partie de confiance pour tous les nœuds d'administration de votre système StorageGRID .
9. Une fois que vous avez terminé, revenez à StorageGRID et testez toutes les approbations des parties de confiance pour confirmer qu'elles sont correctement configurées. Voir "[Utiliser le mode Sandbox](#)" pour les instructions.

Créer une approbation de partie de confiance en important des métadonnées de fédération

Vous pouvez importer les valeurs de chaque partie de confiance en accédant aux métadonnées SAML pour chaque nœud d'administration.

Étapes

1. Dans le Gestionnaire de serveur Windows, sélectionnez **Outils**, puis **Gestion AD FS**.
2. Sous Actions, sélectionnez **Ajouter une approbation de partie de confiance**.
3. Sur la page d'accueil, choisissez **Réclamations prises en compte**, puis sélectionnez **Démarrer**.
4. Sélectionnez **Importer des données sur la partie utilisatrice publiées en ligne ou sur un réseau local**.
5. Dans **Adresse des métadonnées de la fédération (nom d'hôte ou URL)**, saisissez l'emplacement des métadonnées SAML pour ce nœud d'administration :

`https://Admin_Node_FQDN/api/saml-metadata`

Pour *Admin_Node_FQDN*, entrez le nom de domaine complet pour le même nœud d'administration. (Si nécessaire, vous pouvez utiliser l'adresse IP du nœud à la place. Cependant, si vous saisissez une

adresse IP ici, sachez que vous devez mettre à jour ou recréer cette approbation de partie de confiance si cette adresse IP change un jour.)

6. Terminez l'assistant d'approbation de partie de confiance, enregistrez l'approbation de partie de confiance et fermez l'assistant.



Lors de la saisie du nom d'affichage, utilisez l'identifiant de la partie de confiance pour le nœud d'administration, exactement tel qu'il apparaît sur la page d'authentification unique dans le gestionnaire de grille. Par exemple : SG-DC1-ADM1 .

7. Ajouter une règle de revendication :

- a. Cliquez avec le bouton droit sur la fiducie et sélectionnez **Modifier la politique d'émission de réclamation**.
- b. Sélectionnez **Ajouter une règle**:
- c. Sur la page Sélectionner un modèle de règle, sélectionnez **Envoyer les attributs LDAP en tant que revendications** dans la liste, puis sélectionnez **Suivant**.
- d. Sur la page Configurer la règle, entrez un nom d'affichage pour cette règle.

Par exemple, **ObjectGUID vers Name ID** ou **UPN vers Name ID**.

- e. Pour le magasin d'attributs, sélectionnez **Active Directory**.
 - f. Dans la colonne Attribut LDAP de la table de mappage, saisissez **objectGUID** ou sélectionnez **User-Principal-Name**.
 - g. Dans la colonne Type de réclamation sortante de la table de mappage, sélectionnez **ID de nom** dans la liste déroulante.
 - h. Sélectionnez **Terminer**, puis **OK**.
8. Confirmez que les métadonnées ont été importées avec succès.
 - a. Cliquez avec le bouton droit sur l'approbation de la partie de confiance pour ouvrir ses propriétés.
 - b. Confirmez que les champs des onglets **Points de terminaison**, **Identifiants** et **Signature** sont renseignés.

Si les métadonnées sont manquantes, confirmez que l'adresse des métadonnées de la Fédération est correcte ou saisissez les valeurs manuellement.

9. Répétez ces étapes pour configurer une approbation de partie de confiance pour tous les nœuds d'administration de votre système StorageGRID .
10. Une fois que vous avez terminé, revenez à StorageGRID et testez toutes les approbations des parties de confiance pour confirmer qu'elles sont correctement configurées. Voir "[Utiliser le mode Sandbox](#)" pour les instructions.

Créer manuellement une fiducie de partie utilisatrice

Si vous choisissez de ne pas importer les données des approbations de partie de confiance, vous pouvez saisir les valeurs manuellement.

Étapes

1. Dans le Gestionnaire de serveur Windows, sélectionnez **Outils**, puis **Gestion AD FS**.
2. Sous Actions, sélectionnez **Ajouter une approbation de partie de confiance**.

3. Sur la page d'accueil, choisissez **Réclamations prises en compte**, puis sélectionnez **Démarrer**.
4. Sélectionnez **Saisir manuellement les données sur la partie de confiance**, puis sélectionnez **Suivant**.
5. Complétez l'assistant d'approbation de partie de confiance :

- a. Saisissez un nom d'affichage pour ce nœud d'administration.

Par souci de cohérence, utilisez l'identifiant de partie de confiance pour le nœud d'administration, exactement tel qu'il apparaît sur la page d'authentification unique dans le gestionnaire de grille. 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 point de terminaison du service SAML pour le nœud 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. Cependant, si vous saisissez une adresse IP ici, sachez que vous devez mettre à jour ou recréer cette approbation de partie de confiance si cette adresse IP change un jour.)

- e. Sur la page Configurer les identifiants, spécifiez l'identifiant de la partie de confiance pour le même nœud d'administration :

Admin_Node_Identifier

Pour *Admin_Node_Identifier*, saisissez l'identifiant de la partie de confiance pour le nœud d'administration, exactement tel qu'il apparaît sur la page d'authentification unique. Par exemple : SG-DC1-ADM1 .

- f. Vérifiez les paramètres, enregistrez l'approbation de la partie de confiance et fermez l'assistant.

La boîte de dialogue Modifier la politique d'émission de réclamation s'affiche.



Si la boîte de dialogue n'apparaît pas, cliquez avec le bouton droit sur la fiducie et sélectionnez **Modifier la politique d'émission de réclamation**.

6. Pour démarrer l'assistant de règle de revendication, sélectionnez **Ajouter une règle** :
 - a. Sur la page Sélectionner un modèle de règle, sélectionnez **Envoyer les attributs LDAP en tant que revendications** dans la liste, puis sélectionnez **Suivant**.
 - b. Sur la page Configurer la règle, entrez un nom d'affichage pour cette règle.

Par exemple, **ObjectGUID vers Name ID** ou **UPN vers Name ID**.

- c. Pour le magasin d'attributs, sélectionnez **Active Directory**.
- d. Dans la colonne Attribut LDAP de la table de mappage, saisissez **objectGUID** ou sélectionnez **User-Principal-Name**.
- e. Dans la colonne Type de réclamation sortante de la table de mappage, sélectionnez **ID de nom** dans la liste déroulante.

- f. Sélectionnez **Terminer**, puis **OK**.
7. Cliquez avec le bouton droit sur l'approbation de la partie de confiance pour ouvrir ses propriétés.
8. Dans l'onglet **Points de terminaison**, configurez le point de terminaison pour la déconnexion unique (SLO) :
 - a. Sélectionnez **Ajouter SAML**.
 - b. Sélectionnez **Type de point de terminaison > Déconnexion SAML**.
 - c. Sélectionnez **Liaison > Redirection**.
 - d. Dans le champ **URL de confiance**, saisissez l'URL utilisée pour la déconnexion unique (SLO) de ce nœud 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. Cependant, si vous saisissez une adresse IP ici, sachez que vous devez mettre à jour ou recréer cette approbation de partie de confiance si cette adresse IP change un jour.)

- a. Sélectionnez **OK**.
9. Dans l'onglet **Signature**, spécifiez le certificat de signature pour cette approbation de partie de confiance :
 - a. Ajoutez le certificat personnalisé :
 - Si vous disposez du certificat de gestion personnalisé que vous avez téléchargé sur StorageGRID, sélectionnez ce certificat.
 - Si vous n'avez pas le certificat personnalisé, connectez-vous au nœud d'administration, accédez à la `/var/local/mgmt-api` répertoire du nœud Admin et ajoutez le `custom-server.crt` fichier de certificat.



Utilisation du certificat par défaut du nœud d'administration(`server.crt`) n'est pas recommandé. Si le nœud d'administration échoue, le certificat par défaut sera régénéré lorsque vous récupérerez le nœud et vous devrez mettre à jour l'approbation de la partie 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 approbation de partie de confiance pour tous les nœuds d'administration de votre système StorageGRID .
11. Une fois que vous avez terminé, revenez à StorageGRID et testez toutes les approbations des parties de confiance pour confirmer qu'elles sont correctement configurées. Voir "[Utiliser le mode sandbox](#)" pour les instructions.

Créer des 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 l'authentification unique pour StorageGRID et vous avez sélectionné **Azure** comme type d'authentification unique.
- Le **mode Sandbox** est sélectionné sur la page d'authentification unique dans Grid Manager. Voir "[Utiliser le mode sandbox](#)".
- Vous disposez du **nom de l'application d'entreprise** pour chaque nœud 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. Disposer d'une application d'entreprise pour chaque nœud d'administration garantit que les utilisateurs peuvent se connecter et se déconnecter en toute sécurité de 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 disposez de l'un des rôles suivants dans le compte Azure : administrateur général, administrateur d'applications cloud, administrateur d'applications ou propriétaire du principal du service.

Accéder à Azure AD

Étapes

1. Connectez-vous à la "[Portail Azure](#)".
2. Accéder à "[Azure Active Directory](#)".
3. Sélectionner "[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 pour créer une application d'entreprise pour chaque nœud d'administration. Vous copiez les URL de métadonnées de fédération depuis Azure et les collez dans les champs **URL de métadonnées de fédération** correspondants sur la page d'authentification unique StorageGRID.

Étapes

1. Répétez les étapes suivantes pour chaque nœud d'administration.
 - a. Dans le volet Applications Azure Enterprise, sélectionnez **Nouvelle application**.
 - b. Sélectionnez **Créer votre propre application**.
 - c. Pour le nom, saisissez le **Nom de l'application d'entreprise** que vous avez copié à partir du tableau des détails du nœud d'administration sur la page d'authentification 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 **Commencer** dans le **2. Configurer l'authentification unique** ou sélectionner le lien **Authentification unique** dans la marge de gauche.
 - g. Sélectionnez la case **SAML**.
 - h. Copiez l'**URL des métadonnées de la fédération d'applications**, que vous pouvez trouver sous **Étape 3 Certificat de signature SAML**.

- i. Accédez à la page d'authentification unique StorageGRID et collez l'URL dans le champ **URL des métadonnées de la fédération** qui correspond au **nom de l'application d'entreprise** que vous avez utilisé.
2. Après avoir 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'authentification 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. Sign in à StorageGRID à partir du nœud d'administration.
 - b. Sélectionnez **CONFIGURATION > Contrôle d'accès > Authentification unique**.
 - c. Sélectionnez le bouton pour télécharger les métadonnées SAML pour ce nœud d'administration.
 - d. Enregistrez le fichier que vous téléchargerez dans Azure AD.

Télécharger les métadonnées SAML vers chaque application d'entreprise

Après avoir téléchargé un fichier de métadonnées SAML pour chaque nœud d'administration StorageGRID , effectuez les étapes suivantes dans Azure AD :

Étapes

1. Revenez au portail Azure.
2. Répétez ces étapes 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 les affectations séparément).
 - c. Accédez à la page d'authentification unique.
 - 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 sélectionnez **X** pour fermer le volet. Vous êtes redirigé vers la page Configurer l'authentification unique avec SAML.
3. Suivez les étapes dans "[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 nœud d'administration de votre système. Pour accélérer le processus, vous importerez les métadonnées SAML depuis StorageGRID.

Avant de commencer

- Vous avez configuré l'authentification unique pour StorageGRID et vous avez sélectionné **Ping Federate** comme type d'authentification unique.
- Le **mode Sandbox** est sélectionné sur la page d'authentification unique dans Grid Manager. Voir "[Utiliser le mode sandbox](#)".
- Vous disposez de l'*ID de connexion SP * pour chaque nœud d'administration de votre système. Vous pouvez trouver ces valeurs dans le tableau détaillé des nœuds d'administration sur la page d'authentification unique StorageGRID .
- Vous avez téléchargé les **métadonnées SAML** pour chaque nœud d'administration de votre système.
- Vous avez de l'expérience dans la création de connexions SP dans PingFederate Server.
- Vous avez
le https://docs.pingidentity.com/pingfederate/latest/administrators_reference_guide/pf_administrators_reference_guide.html ["Guide de référence de l'administrateur"] pour le serveur PingFederate. La documentation de PingFederate fournit des instructions et des explications détaillées étape par étape.
- Vous avez le "[Autorisation d'administrateur](#)" pour le serveur PingFederate.

À propos de cette 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 pour votre version.

Prérequis complets 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 lorsque vous configurerez les connexions SP .

Créer un magasin de données

Si vous ne l'avez 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 d'identité](#)" dans StorageGRID.

- **Type** : Répertoire (LDAP)
- **Type LDAP** : Active Directory
- **Nom de l'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 vous ne l'avez pas déjà fait, créez un validateur d'informations d'identification de mot de passe.

- **Type** : Validateur d'informations d'identification de mot de passe de nom d'utilisateur LDAP
- **Magasin de données** : sélectionnez le magasin de données que vous avez créé.
- **Base de recherche** : saisissez les informations de LDAP (par exemple, DC=saml,DC=sgws).
- **Filtre de recherche** : sAMAccountName=\${username}
- **Portée** : Sous-arbre

Créer une instance d'adaptateur IdP

Si vous ne l'avez pas déjà fait, créez une instance d'adaptateur IdP.

Étapes

1. Accédez à **Authentification > Intégration > Adaptateurs IdP**.
2. Sélectionnez **Créer une nouvelle instance**.
3. Dans l'onglet Type, sélectionnez **Adaptateur IdP de formulaire HTML**.
4. Dans l'onglet Adaptateur IdP, sélectionnez **Ajouter une nouvelle ligne à « Validateurs d'informations d'identification »**.
5. Sélectionnez le [validateur d'informations d'identification de mot de passe](#) tu as créé.
6. Dans l'onglet Attributs de l'adaptateur, sélectionnez l'attribut **username** pour **Pseudonyme**.
7. Sélectionnez **Enregistrer**.

Créer ou importer un certificat de signature

Si vous ne l'avez pas déjà fait, créez ou importez le certificat de signature.

Étapes

1. Accédez à **Sécurité > Clés et certificats 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 que vous avez téléchargées à partir de StorageGRID pour le nœud d'administration. Le fichier de métadonnées contient de nombreuses 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 et se déconnecter en toute sécurité de n'importe quel nœud. Utilisez ces instructions pour créer la première connexion SP. Ensuite, allez à [Créer des connexions SP supplémentaires](#) pour créer toutes les connexions supplémentaires dont vous avez besoin.

Choisissez le type de connexion SP

Étapes

1. Accédez à **Applications > Intégration > *Connexions SP ***.
2. Sélectionnez **Créer une connexion**.
3. Sélectionnez **Ne pas utiliser de modèle pour cette connexion**.
4. Sélectionnez **Profils SSO du navigateur** et **SAML 2.0** comme protocole.

Importer les métadonnées SP

Étapes

1. Dans l'onglet Importer des 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. Consultez le résumé des métadonnées et les informations fournies dans l'onglet Informations générales.

L'ID d'entité du partenaire et le nom de connexion sont définis sur l'ID de connexion StorageGRID SP . (par exemple, 10.96.105.200-DC1-ADM1-105-200). L'URL de base est l'IP du nœud d'administration StorageGRID .

4. Sélectionnez **Suivant**.

Configurer l'authentification unique du navigateur IdP

Étapes

1. Dans l'onglet SSO du navigateur, sélectionnez **Configurer SSO du navigateur**.
2. Dans l'onglet Profils SAML, sélectionnez les options * SP-initiated SSO*, * SP-initial SLO*, **IdP-initiated SSO** et **IdP-initiated SLO**.
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.

Instance d'adaptateur de carte

Étapes

1. Dans l'onglet Mappage de la source d'authentification, sélectionnez **Mapper une nouvelle instance d'adaptateur**.
2. Dans l'onglet Instance de l'adaptateur, sélectionnez l'[instance d'adaptateur](#) tu as 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 d'utilisateur, sélectionnez **Ajouter une source d'attribut**.
5. Dans l'onglet Magasin de données, fournissez une description et sélectionnez l'option [magasin de données](#) tu as ajouté.
6. Dans l'onglet Recherche d'annuaire LDAP :
 - Saisissez le **DN de base**, qui doit correspondre exactement à la valeur que vous avez saisie dans StorageGRID pour le serveur LDAP.
 - Pour la portée de la recherche, sélectionnez **Sous-arbre**.
 - Pour la classe d'objet racine, recherchez et ajoutez l'un de ces attributs : **objectGUID** ou **userPrincipalName**.
7. Dans l'onglet Types de codage d'attribut binaire LDAP, sélectionnez **Base64** pour l'attribut **objectGUID**.
8. Dans l'onglet Filtre LDAP, saisissez **sAMAccountName=\${username}**.
9. Dans l'onglet Exécution du contrat d'attribut, sélectionnez **LDAP (attribut)** dans la liste déroulante Source et sélectionnez **objectGUID** ou **userPrincipalName** dans la liste déroulante Valeur.
10. Vérifiez puis enregistrez la source de l'attribut.

11. Dans l'onglet Source d'attribut Failsave, sélectionnez **Annuler la transaction SSO**.
12. Consultez le résumé et sélectionnez **Terminé**.
13. Sélectionnez **Terminé**.

Configurer les paramètres du protocole

Étapes

1. Dans l'onglet * Connexion SP * > * SSO du navigateur* > * Paramètres du protocole*, sélectionnez * Configurer les paramètres du protocole*.
2. Dans l'onglet URL du service consommateur d'assertions, 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 de terminaison).
3. Dans l'onglet URL du service SLO, acceptez les valeurs par défaut, qui ont été importées à partir des métadonnées SAML StorageGRID (**REDIRECT** pour la liaison et `/api/saml-logout` pour l'URL du point de terminaison).
4. Dans l'onglet Liaisons SAML autorisées, décochez **ARTIFACT** et **SOAP**. Seuls **POST** et **REDIRECT** sont obligatoires.
5. Dans l'onglet Politique de signature, laissez les cases à cocher **Exiger que les demandes d'authentification soient signées** et **Toujours signer l'assertion** sélectionnées.
6. Dans l'onglet Politique de chiffrement, sélectionnez **Aucun**.
7. Consultez le résumé et sélectionnez **Terminé** pour enregistrer les paramètres du protocole.
8. Consultez le résumé et sélectionnez **Terminé** 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. Sélectionnez le [certificat de signature](#) 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 du certificat de signature, qui ont été importées à partir des métadonnées SAML StorageGRID.
5. Consultez les écrans récapitulatifs et sélectionnez **Enregistrer** pour enregistrer la connexion SP.

Créer des connexions SP supplémentaires

Vous pouvez copier la première connexion SP pour créer les connexions SP dont vous avez besoin pour chaque nœud d'administration de votre grille. Vous téléchargez de nouvelles métadonnées pour chaque copie.



Les connexions SP pour 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 la signature et de l'URL de réponse SLO.

Étapes

1. Sélectionnez **Action** > **Copier** pour créer une copie de la connexion SP initiale pour chaque nœud

d'administration supplémentaire.

2. Saisissez l'ID de connexion et le nom de connexion pour la copie, puis sélectionnez **Enregistrer**.
3. Choisissez le fichier de métadonnées correspondant au nœud d'administration :
 - a. Sélectionnez **Action > Mettre à jour avec les métadonnées**.
 - b. Sélectionnez **Choisir un fichier** et téléchargez les métadonnées.
 - c. Sélectionnez **Suivant**.
 - d. Sélectionnez **Enregistrer**.
4. Résoudre l'erreur due à l'attribut inutilisé :
 - a. Sélectionnez la nouvelle connexion.
 - b. Sélectionnez **Configurer l'authentification unique du navigateur > Configurer la création d'assertions > 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 d'identité.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un ["navigateur Web pris en charge"](#).
- Tu as ["autorisations d'accès spécifiques"](#).

Étapes

1. Sélectionnez **CONFIGURATION > Contrôle d'accès > Authentification unique**.

La page d'authentification unique s'affiche.

2. Sélectionnez l'option **Désactivé**.
3. Sélectionnez **Enregistrer**.

Un message d'avertissement apparaît indiquant que les utilisateurs locaux pourront désormais se connecter.

4. Sélectionnez **OK**.

La prochaine fois que vous vous connectez à StorageGRID, la page de Sign in à StorageGRID s'affiche et vous devez saisir le nom d'utilisateur et le mot de passe d'un utilisateur StorageGRID local ou fédéré.

Désactiver et réactiver temporairement l'authentification unique pour un nœud d'administration

Vous ne pourrez peut-être pas vous connecter au Grid Manager si le système d'authentification unique (SSO) tombe en panne. Dans ce cas, vous pouvez désactiver et réactiver temporairement SSO pour un nœud d'administration. Pour désactiver puis réactiver SSO, vous devez accéder à l'interpréteur de commandes du nœud.

Avant de commencer

- Tu as "autorisations d'accès spécifiques" .
- Vous avez le `Passwords.txt` déposer.
- Vous connaissez le mot de passe de l'utilisateur root local.

À propos de cette tâche

Après avoir désactivé SSO pour un nœud d'administration, vous pouvez vous connecter au gestionnaire de grille en tant qu'utilisateur root local. Pour sécuriser votre système StorageGRID , vous devez utiliser l'interpréteur de commandes 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 des autres nœuds d'administration de la grille. La case à cocher **Activer SSO** sur la page Authentification unique dans le Gestionnaire de grille reste sélectionnée et tous les paramètres SSO existants sont conservés, sauf si vous les mettez à jour.

Étapes

1. Connectez-vous à un nœud d'administration :

- Entrez la commande suivante : `ssh admin@Admin_Node_IP`
- Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.
- Entrez la commande suivante pour passer en root : `su -`
- Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.

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 SSO.

Un message indique que l'authentification unique est désactivée sur le nœud.

4. À partir d'un navigateur Web, accédez au gestionnaire de grille sur le même nœud d'administration.

La page de connexion de Grid Manager s'affiche désormais car SSO a été désactivé.

5. Sign in avec le nom d'utilisateur root et le mot de passe de l'utilisateur root local.

6. Si vous avez désactivé temporairement SSO parce que vous deviez corriger la configuration SSO :

- Sélectionnez **CONFIGURATION > Contrôle d'accès > Authentification unique**.
- Modifiez les paramètres SSO incorrects ou obsolètes.
- Sélectionnez **Enregistrer**.

La sélection de **Enregistrer** sur la page d'authentification unique réactive automatiquement l'authentification unique pour l'ensemble de la grille.

7. Si vous avez désactivé temporairement SSO parce que vous aviez besoin d'accéder au Grid Manager pour une autre raison :

- a. Effectuez la ou les tâches que vous devez effectuer.
- b. Sélectionnez **Déconnexion** et fermez le gestionnaire de grille.
- c. Réactiver SSO sur le nœud d'administration. Vous pouvez effectuer l'une des étapes 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 SSO.

Un message indique que l'authentification unique est activée sur le nœud.

- ° Redémarrer le nœud de grille : `reboot`

8. À partir d'un navigateur Web, accédez au gestionnaire de grille à partir du même nœud d'administration.
9. Confirmez que la page de Sign in StorageGRID s'affiche et que vous devez saisir vos informations d'identification SSO pour accéder au Grid Manager.

Utiliser la fédération de grille

Qu'est-ce que la fédération de réseau ?

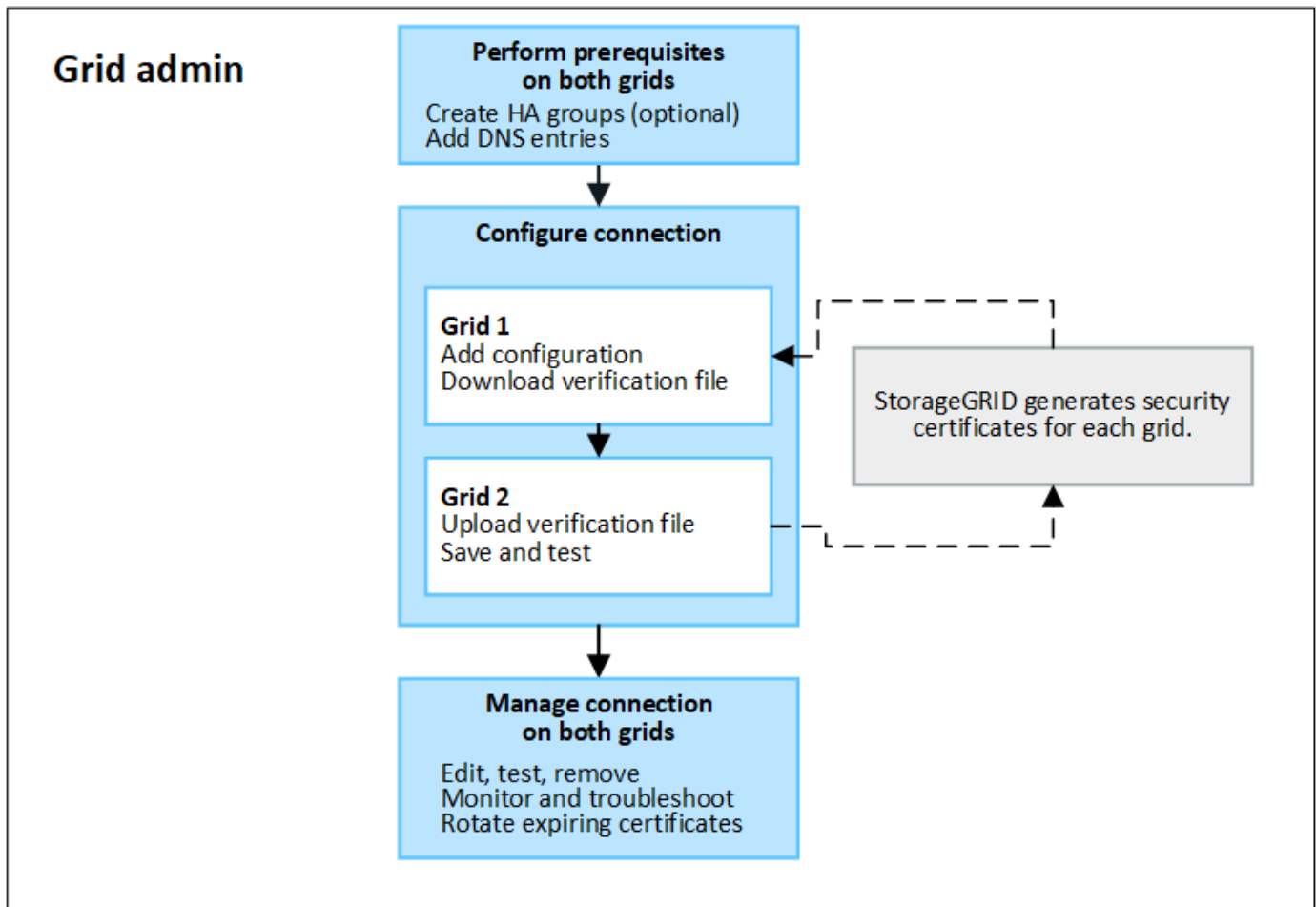
Vous pouvez utiliser la fédération de grille pour cloner des locataires et répliquer leurs objets entre deux systèmes StorageGRID pour la reprise après sinistre.

Qu'est-ce qu'une connexion à une fédération de réseau ?

Une connexion de fédération de grille est une connexion bidirectionnelle, fiable et sécurisée entre les nœuds d'administration et de passerelle dans deux systèmes StorageGRID .

Workflow pour la fédération de grilles

Le diagramme de flux de travail résume les étapes de configuration d'une connexion de fédération de grille entre deux grilles.



Considérations et exigences relatives aux connexions de fédérations de réseaux

- Les grilles utilisées pour la fédération de grilles doivent exécuter des versions de StorageGRID qui sont soit identiques, soit ne présentant pas plus d'une différence de version majeure entre elles.

Pour plus de détails sur les exigences de version, reportez-vous à la ["Notes de version"](#).

- Une grille peut avoir une ou plusieurs connexions de fédération de grilles à d'autres grilles. Chaque connexion de fédération de grille est indépendante de toutes les autres connexions. Par exemple, si la grille 1 a une connexion avec la grille 2 et une deuxième connexion avec la grille 3, il n'y a pas de connexion implicite entre la grille 2 et la grille 3.
- Les connexions de la 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 des grilles.
- Au moins une connexion à une fédération de grille doit exister avant de pouvoir utiliser ["clone de compte"](#) ou ["réplication inter-réseaux"](#).

Exigences en matière de 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 de grille sur l'autre grille composée de nœuds d'administration, de nœuds de passerelle ou des deux.
- La meilleure pratique consiste à se connecter ["groupes de haute disponibilité \(HA\)"](#) des nœuds de

passerelle et d'administration sur chaque grille. L'utilisation de groupes HA permet de garantir que les connexions de la fédération de grille resteront en ligne si les nœuds deviennent indisponibles. Si l'interface active de l'un des groupes HA échoue, 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 seul nœud d'administration ou nœud de passerelle. Si le nœud devient indisponible, la connexion à la fédération de grille deviendra également indisponible.
- "[Réplication inter-réseaux](#)" des objets nécessite que les nœuds de stockage de chaque grille puissent accéder aux nœuds d'administration et de passerelle configurés sur l'autre grille. Pour chaque grille, confirmez que tous les nœuds de stockage disposent d'une route à bande passante élevée vers les nœuds d'administration ou les nœuds de passerelle utilisés pour la connexion.

Utiliser les noms de domaine complets 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. Ensuite, créez les entrées DNS appropriées, comme suit :

- Le nom de domaine complet (FQDN) de Grid 1 mappé à une ou plusieurs adresses IP virtuelles (VIP) pour les groupes HA de Grid 1 ou à l'adresse IP d'un ou plusieurs nœuds d'administration ou de passerelle de Grid 1.
- Le FQDN de Grid 2 mappé à une ou plusieurs adresses VIP pour Grid 2 ou à l'adresse IP d'un ou plusieurs nœuds d'administration ou de passerelle dans Grid 2.

Lorsque vous utilisez plusieurs entrées DNS, les demandes d'utilisation de la connexion sont équilibrées, comme suit :

- Les entrées DNS qui correspondent aux adresses VIP de plusieurs groupes HA sont équilibrées entre les nœuds actifs des groupes HA.
- Les entrées DNS qui correspondent aux adresses IP de plusieurs nœuds d'administration ou nœuds de passerelle sont équilibrées en charge entre les nœuds mappés.

Exigences portuaires

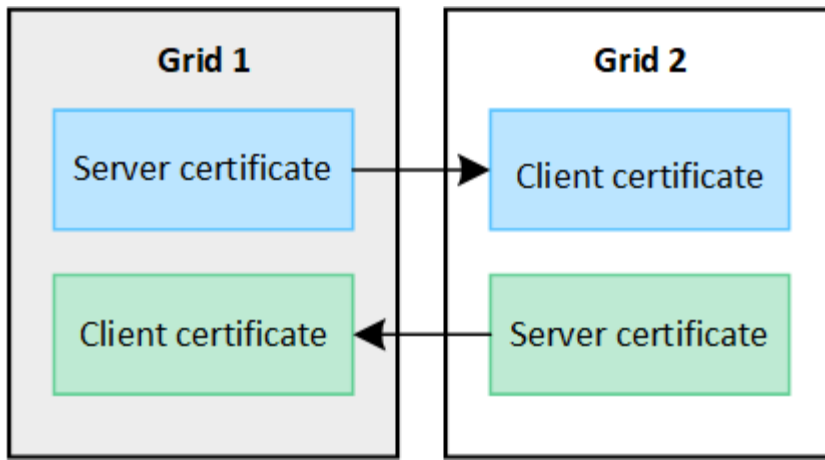
Lors de la création d'une connexion de fédération de grille, vous pouvez spécifier n'importe quel numéro de port inutilisé compris entre 23 000 et 23 999. Les deux réseaux de cette connexion utiliseront le même port.

Vous devez vous assurer qu'aucun nœud de l'une ou l'autre 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 serveur et client pour authentifier et crypter les informations envoyées de la grille 1 à la grille 2
- Certificats serveur et client pour authentifier et crypter les informations envoyées de la grille 2 à la grille 1



Par défaut, les certificats sont valables 730 jours (2 ans). Lorsque ces certificats approchent de leur date d'expiration, l'alerte **Expiration du certificat de fédération de grille** vous rappelle de faire pivoter les certificats, ce que vous pouvez faire à l'aide du gestionnaire de grille.



Si les certificats à l'une ou l'autre extrémité de la connexion expirent, la connexion cessera de fonctionner. La réplication des données sera en attente jusqu'à ce que les certificats soient mis à jour.

Apprendre encore plus

- ["Créer des connexions de fédération de grille"](#)
- ["Gérer les connexions de la fédération de réseau"](#)
- ["Résoudre les erreurs de fédération de grille"](#)

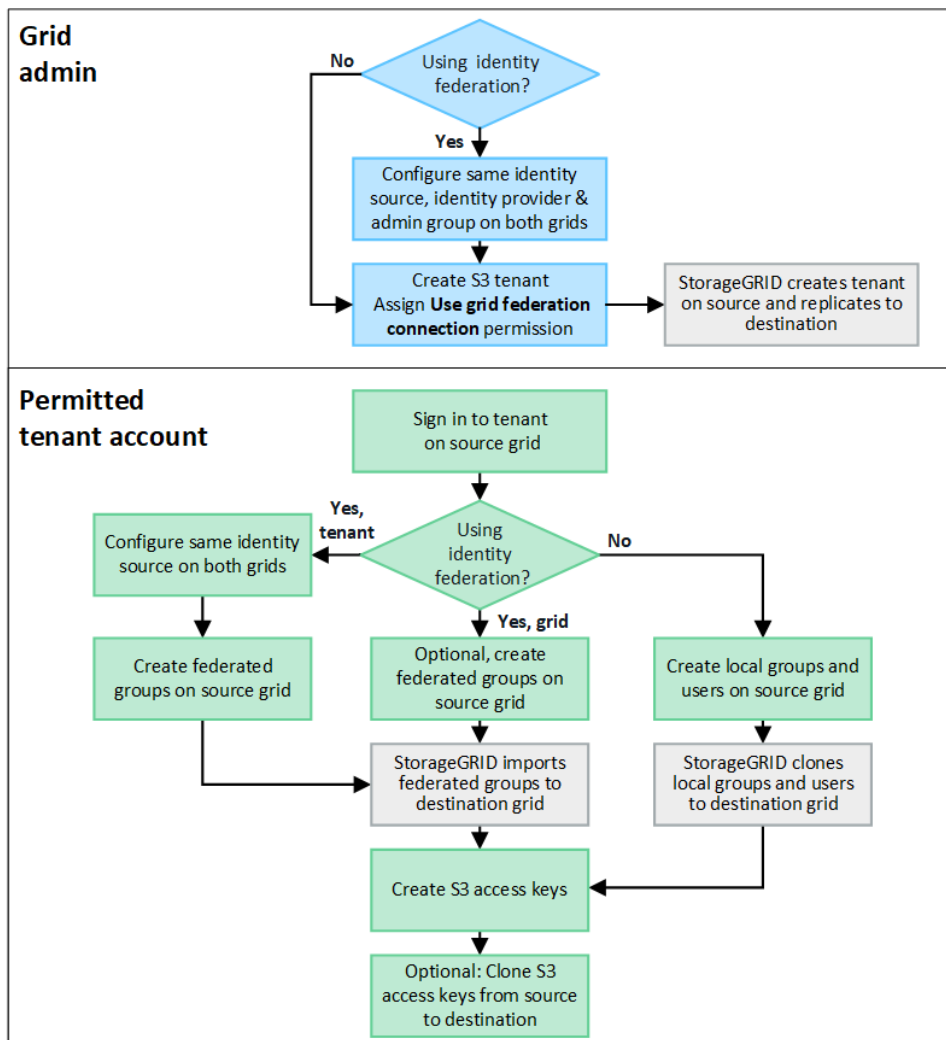
Qu'est-ce que le clonage de compte ?

Le clonage de compte est la réplication automatique d'un compte de locataire, de groupes de locataires, d'utilisateurs de locataires et, éventuellement, de clés d'accès S3 entre les systèmes StorageGRID d'un ["connexion à la fédération de réseau"](#).

Le clonage de compte est requis pour ["réplication inter-réseaux"](#). Le clonage des informations de compte d'un système StorageGRID source vers un système StorageGRID de destination garantit que les utilisateurs et les groupes de locataires peuvent accéder aux compartiments et objets correspondants sur l'une ou l'autre grille.

Flux de travail pour le clonage de compte

Le diagramme de flux de travail montre les étapes que les administrateurs de grille et les locataires autorisés effectueront pour configurer le clonage de compte. Ces étapes sont effectuées après la ["la connexion à la fédération de grille est configurée"](#).



Flux de travail d'administration de la grille

Les étapes effectuées par les administrateurs de grille dépendent du fait que les systèmes StorageGRID du "connexion à la fédération de réseau" utilisent l'authentification unique (SSO) ou la fédération d'identité.

Configurer SSO pour le clonage 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 locataire 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 la même source d'identité pour les deux grilles. Voir ["Utiliser la fédération d'identité"](#) .
2. Configurez le même fournisseur d'identité SSO (IdP) pour les deux grilles. Voir ["Configurer l'authentification unique"](#) .
3. ["Créer le même groupe d'administrateurs"](#) sur les deux grilles en important le même groupe fédéré.

Lorsque vous créez le locataire, vous sélectionnez ce groupe pour disposer de l'autorisation d'accès racine initiale pour les comptes de locataire source et de destination.



Si ce groupe d'administrateurs n'existe pas sur les deux grilles avant la création du locataire, le locataire n'est pas répliqué vers la destination.

Configurer la fédération d'identité au niveau de la grille pour le clonage de compte (facultatif)

Si l'un des systèmes StorageGRID utilise la fédération d'identité sans SSO, les deux grilles doivent utiliser la fédération d'identité. Avant de créer les comptes de locataire 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 la même source d'identité pour les deux grilles. Voir ["Utiliser la fédération d'identité"](#) .
2. En option, si un groupe fédéré dispose d'une autorisation d'accès racine initiale pour les comptes locataires source et de destination, ["créer le même groupe d'administrateurs"](#) 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 locataire 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 root initiale pour les deux comptes, spécifiez un mot de passe pour l'utilisateur root local.

Créer un compte locataire S3 autorisé

Après avoir configuré éventuellement SSO ou la fédération d'identité, un administrateur de grille exécute ces étapes pour déterminer quels locataires peuvent répliquer des objets de bucket vers d'autres systèmes StorageGRID .

Étapes

1. Déterminez la grille que vous souhaitez utiliser comme grille source du locataire pour les opérations de clonage de compte.

La grille sur laquelle le locataire est créé à l'origine est appelée *grille source* du locataire. La grille sur laquelle le locataire est répliqué est appelée *grille de destination* du locataire.

2. Sur cette grille, créez un nouveau compte locataire S3 ou modifiez un compte existant.
3. Attribuer l'autorisation **Utiliser la connexion à la fédération de grille**.
4. Si le compte locataire doit gérer ses propres utilisateurs fédérés, attribuez l'autorisation **Utiliser sa propre source d'identité**.

Si cette autorisation est attribuée, les comptes de locataire source et de destination doivent configurer la même source d'identité avant de créer des groupes fédérés. Les groupes fédérés ajoutés au locataire source ne peuvent pas être clonés vers le locataire de destination, sauf si les deux grilles utilisent la même source d'identité.

5. Sélectionnez une connexion de fédération de grille spécifique.
6. Enregistrez le locataire nouveau ou modifié.

Lorsqu'un nouveau locataire avec l'autorisation **Utiliser la connexion à la fédération de grille** est enregistré, StorageGRID crée automatiquement une réplique de ce locataire sur l'autre grille, comme suit :

- Les deux comptes locataires ont le même ID de compte, le même nom, le même quota de stockage et

les mêmes autorisations attribuées.

- Si vous avez sélectionné un groupe fédéré pour disposer de l'autorisation d'accès racine pour le locataire, ce groupe est cloné sur le locataire de destination.
- Si vous avez sélectionné un utilisateur local pour disposer de l'autorisation d'accès root pour le locataire, cet utilisateur est cloné sur le locataire de destination. Cependant, le mot de passe de cet utilisateur n'est pas cloné.

Pour plus de détails, consultez la section ["Gérer les locataires autorisés pour la fédération de réseau"](#) .

Flux de travail des comptes locataires autorisés

Une fois qu'un locataire avec l'autorisation **Utiliser la connexion à la fédération de grille** est répliqué sur la grille de destination, les comptes de locataire autorisés peuvent effectuer ces étapes pour cloner des groupes de locataires, des utilisateurs et des clés d'accès S3.

Étapes

1. Sign in au compte locataire sur la grille source du locataire.
2. Si cela est autorisé, configurez l'identification de la fédération sur les comptes locataires 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 vers le locataire de destination, mais aucun clonage n'a lieu de la destination vers la source.

4. Créer des clés d'accès S3.
5. Vous pouvez également cloner les clés d'accès S3 du locataire source vers le locataire de destination.

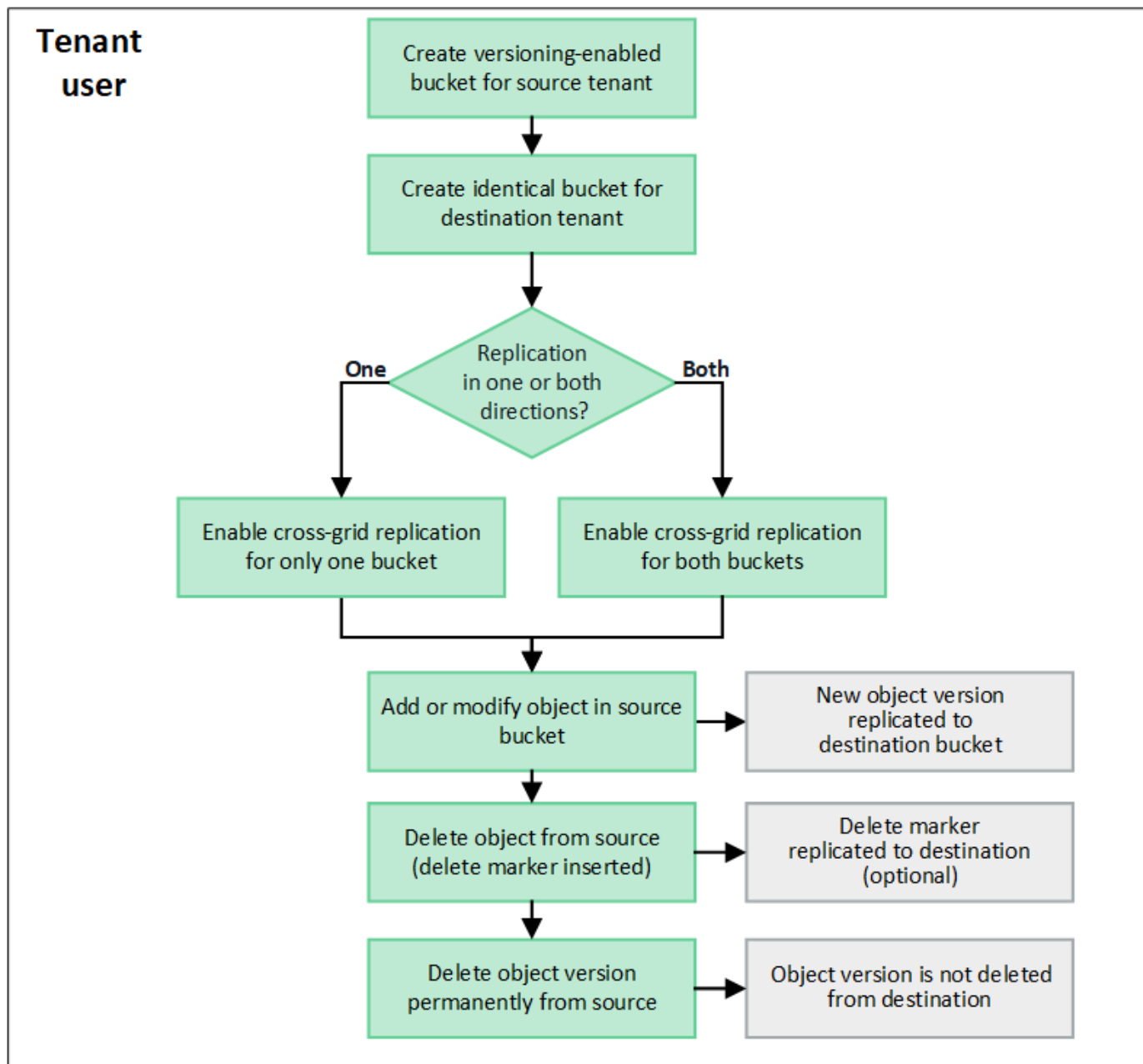
Pour plus de détails sur le flux de travail du compte locataire autorisé et pour savoir comment les groupes, les utilisateurs et les clés d'accès S3 sont clonés, consultez ["Cloner des groupes de locataires et des utilisateurs"](#) et ["Cloner les clés d'accès S3 à l'aide de l'API"](#) .

Qu'est-ce que la réplication inter-réseau ?

La réplication inter-grille est la réplication automatique d'objets entre des buckets S3 sélectionnés dans deux systèmes StorageGRID connectés dans un ["connexion à la fédération de réseau"](#) . ["Clonage de compte"](#) est nécessaire pour la réplication inter-grille.

Flux de travail pour la réplication inter-grille

Le diagramme de flux de travail résume les étapes de configuration de la réplication inter-grille entre les buckets sur deux grilles.



Exigences pour la réplication inter-réseaux

Si un compte locataire dispose de l'autorisation **Utiliser la connexion à la fédération de grille** pour utiliser une ou plusieurs ["connexions de fédération de réseau"](#), un utilisateur locataire avec l'autorisation d'accès root peut créer des buckets identiques dans les comptes locataires correspondants sur chaque grille. Ces seaux :

- Doit avoir le même nom mais peut avoir des régions différentes
- Doit avoir le contrôle de version activé
- Le verrouillage d'objet S3 doit être désactivé
- Doit être vide

Une fois les deux buckets créés, la réplication inter-grille peut être configurée pour l'un ou les deux buckets.

Apprendre encore plus

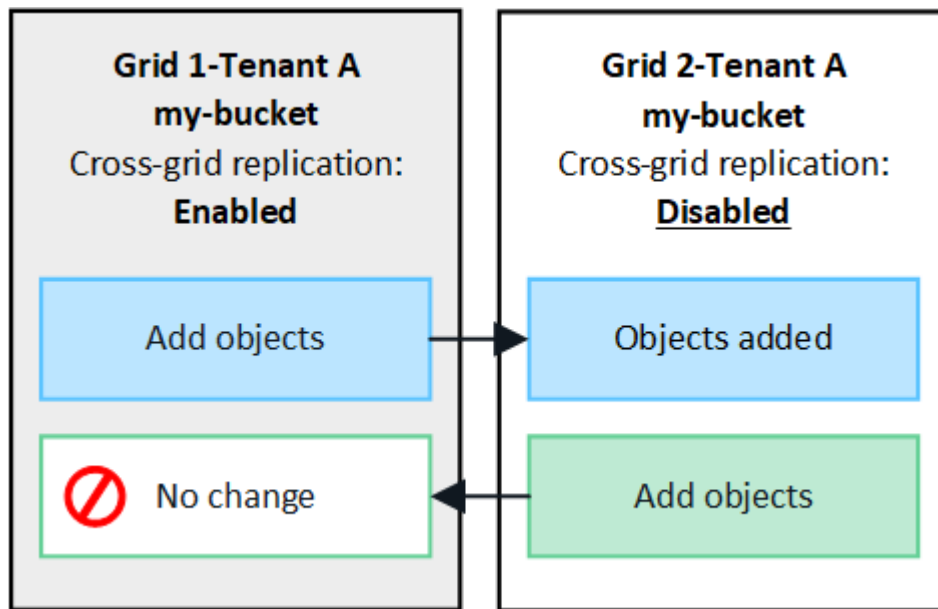
["Gérer la réplication inter-réseaux"](#)

Comment fonctionne la réplication inter-réseaux

La réplication inter-grille peut être configurée pour se produire dans une direction ou dans les deux directions.

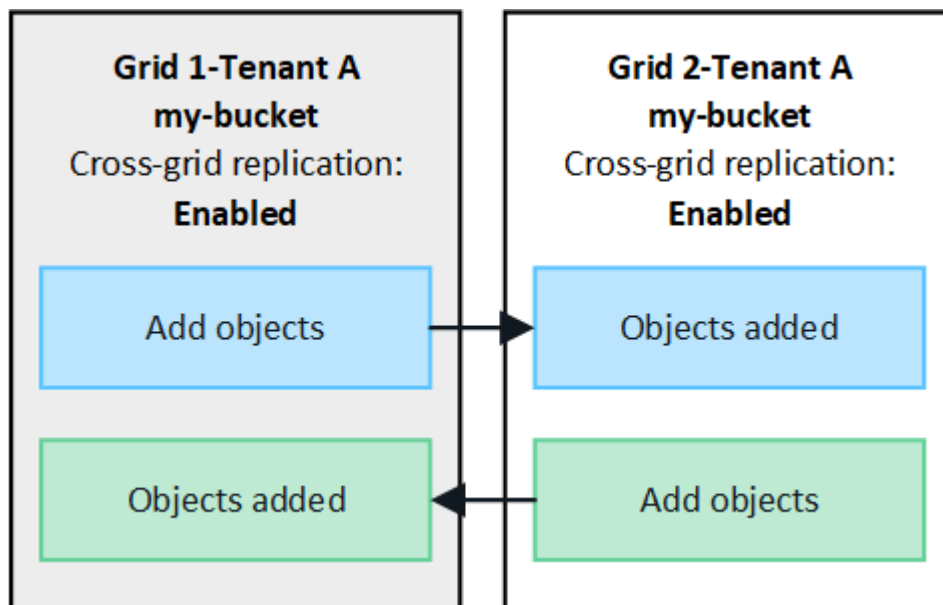
Réplication dans une direction

Si vous activez la réplication inter-grille pour un bucket sur une seule grille, les objets ajoutés à ce bucket (le bucket source) sont répliqués vers le bucket correspondant sur l'autre grille (le bucket de destination). Cependant, les objets ajoutés au bucket de destination ne sont pas répliqués vers la source. Dans la figure, la réplication inter-grille 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-grille pour le même bucket sur les deux grilles, les objets ajoutés à l'un des buckets sont répliqués sur l'autre grille. Dans la figure, la réplication inter-grille 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 bucket pour lequel la réplication inter-grille est activée, ce qui suit se produit :

1. StorageGRID réplique automatiquement l'objet du bucket source vers le bucket de destination. Le temps nécessaire pour effectuer cette opération de réplication en arrière-plan dépend de plusieurs facteurs, notamment du nombre d'autres opérations de réplication en attente.

Le client S3 peut vérifier l'état de réplication d'un objet en émettant une requête `GetObject` ou `HeadObject`. La réponse inclut un StorageGRID spécifique `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 `GetObject` ou `HeadObject`. La réponse inclut un StorageGRID spécifique `x-ntap-sg-cgr-replication-status` en-tête de réponse, qui aura l'une des valeurs suivantes :

Grille	État de réplication
Source	• TERMINÉ : La réplication a réussi pour toutes les connexions au réseau. • EN ATTENTE : L'objet n'a pas été répliqué sur au moins une connexion au réseau. • ÉCHEC : La réplication n'est en attente pour aucune connexion au réseau et au moins une a échoué avec une panne permanente. Un 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 les politiques ILM actives de chaque grille pour gérer les objets, comme il le ferait pour tout autre objet. Par exemple, l'objet A sur la grille 1 peut être stocké sous forme de deux copies répliquées et conservées pour toujours, tandis que la copie de l'objet A qui a été répliquée sur la grille 2 peut être stockée à l'aide du codage 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 du gestionnaire de locataires sélectionne le "[Supprimer les objets dans le bucket](#)" option permettant de supprimer tous les objets d'un bucket.
- Le bucket a une configuration de 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 bucket, de l'expiration du cycle de vie du bucket ou de l'expiration du placement ILM, l'objet répliqué n'est jamais supprimé de l'autre grille dans une connexion de fédération de grille. Cependant, les marqueurs de suppression ajoutés au bucket source par les suppressions du client S3 peuvent éventuellement être répliqués vers le bucket de destination.

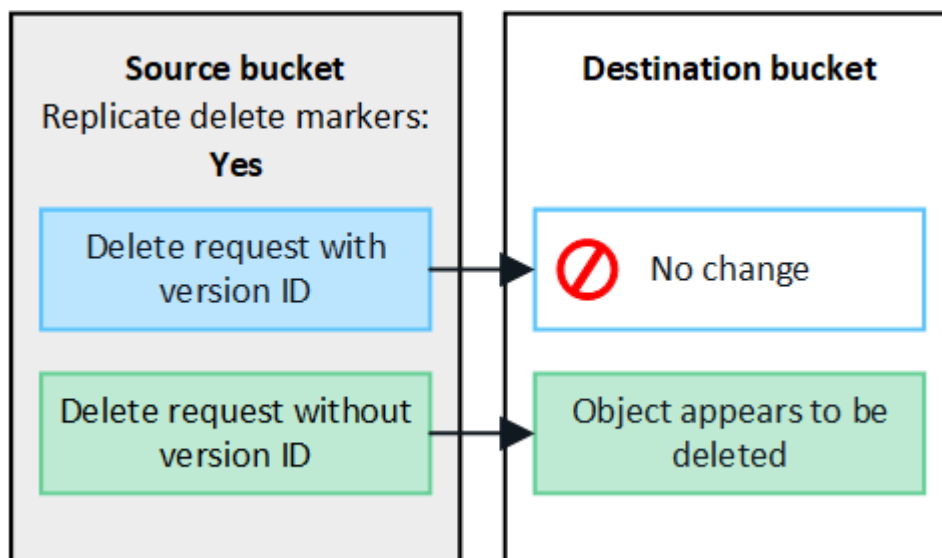
Pour comprendre ce qui se passe lorsqu'un client S3 supprime des objets d'un bucket pour lequel la réplication inter-grille est activée, examinez comment les clients S3 suppriment des objets des buckets pour lesquels le contrôle de version est activé, comme suit :

- 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 bucket.
- 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 bucket. Le marqueur de suppression oblige StorageGRID à agir comme si l'objet avait été supprimé :
 - Une requête `GetObject` sans ID de version échouera avec `404 No Object Found`
 - Une demande `GetObject` avec un ID de version valide réussira et renverra la version de l'objet demandée.

Lorsqu'un client S3 supprime un objet d'un bucket pour lequel la réplication inter-grille 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-grille pour le bucket :
 - Si vous choisissez de répliquer les marqueurs de suppression (par défaut), un marqueur de suppression est ajouté au bucket source et répliqué vers le bucket 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 bucket source mais n'est pas répliqué dans le bucket de destination. En effet, les objets supprimés sur la grille source ne sont pas supprimés sur la grille de destination.

Dans la figure, **Répliquer les marqueurs de suppression** était défini sur **Oui** lorsque "[la réplication inter-réseau a été activée](#)". Les demandes de suppression pour le bucket source qui incluent un ID de version ne supprimeront pas les objets du bucket de destination. Les demandes de suppression pour le bucket source qui n'incluent pas d'ID de version sembleront supprimer des objets dans le bucket de destination.





Si vous souhaitez que les suppressions d'objets restent synchronisées entre les grilles, créez des [Configurations du cycle de vie S3](#) pour les seaux sur les deux grilles.

Comment les objets chiffrés sont répliqués

Lorsque vous utilisez la réplication inter-grille pour répliquer des objets entre des grilles, vous pouvez chiffrer des objets individuels, utiliser le chiffrement de compartiment par défaut ou configurer le chiffrement à l'échelle de la grille. Vous pouvez ajouter, modifier ou supprimer les paramètres de chiffrement par défaut du bucket ou de la grille avant ou après avoir activé la réplication inter-grille pour un bucket.

Pour chiffrer des objets individuels, vous pouvez utiliser SSE (chiffrement côté serveur avec clés gérées par StorageGRID) lors de l'ajout des objets au bucket source. Utilisez le `x-amz-server-side-encryption` en-tête de demande et spécifiez `AES256`. Voir ["Utiliser 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'ingestion échouera.

Pour utiliser le cryptage par défaut pour un bucket, utilisez une requête `PutBucketEncryption` et définissez le `SSEAlgorithm` paramètre à `AES256`. Le chiffrement au niveau du bucket s'applique à tous les objets ingérés sans le `x-amz-server-side-encryption` en-tête de requête. Voir ["Opérations sur les godets"](#).

Pour utiliser le chiffrement au niveau de la grille, définissez l'option **Chiffrement des objets stockés** sur **AES-256**. Le chiffrement au niveau de la grille s'applique à tous les objets qui ne sont pas chiffrés au niveau du bucket ou qui sont ingérés sans le `x-amz-server-side-encryption` en-tête de requête. Voir ["Configurer les options réseau et objet"](#).



SSE ne prend pas en charge AES-128. Si l'option **Cryptage d'objet stocké** 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. Au lieu de cela, l'objet répliqué utilisera le bucket par défaut de la destination ou le paramètre de chiffrement au niveau de la grille, s'il est disponible.

Lors de la détermination de la manière de chiffrer les objets sources, StorageGRID applique ces règles :

1. Utilisez le `x-amz-server-side-encryption` ingérer l'en-tête, s'il est présent.
2. Si aucun en-tête d'ingestion n'est présent, utilisez le paramètre de chiffrement par défaut du bucket, s'il est configuré.
3. Si aucun paramètre de bucket n'est configuré, utilisez le paramètre de chiffrement à l'échelle de la grille, s'il est configuré.
4. Si un paramètre à l'échelle de la grille n'est pas présent, ne cryptez pas l'objet source.

Lors de la détermination de la manière de chiffrer les objets répliqués, StorageGRID applique ces règles dans cet ordre :

1. Utilisez le même cryptage que l'objet source, sauf si cet objet utilise le cryptage AES-128.
2. Si l'objet source n'est pas chiffré ou s'il utilise AES-128, utilisez le paramètre de chiffrement par défaut du bucket de destination, s'il est configuré.
3. Si le bucket de destination ne dispose pas d'un paramètre de chiffrement, utilisez le paramètre de chiffrement à l'échelle de la grille de destination, s'il est configuré.
4. Si un paramètre à l'échelle de la grille n'est pas présent, ne cryptez pas l'objet de destination.

PutObjectTagging et DeleteObjectTagging ne sont pas pris en charge

Les requêtes PutObjectTagging et DeleteObjectTagging ne sont pas prises en charge pour les objets dans les buckets pour lesquels la réplication inter-grille est activée.

Si un client S3 émet une requête PutObjectTagging ou DeleteObjectTagging, 501 Not Implemented est retourné. 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 sur une autre grille, le paramètre **Taille maximale du segment (CONFIGURATION > Système > Options de stockage)** de la grille source sera utilisé sur les deux grilles. Par exemple, supposons que la taille maximale du segment pour la grille source soit de 1 Go, tandis que la taille maximale du segment de la grille de destination soit de 50 Mo. Si vous ingérez un objet de 2 Go sur la grille source, cet objet est enregistré sous forme de 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 du segment de cette grille est de 50 Mo.

Comparer la réplication inter-grille et la réplication CloudMirror

Lorsque vous commencez à utiliser la fédération de grille, examinez les similitudes et les différences entre "réplication inter-réseaux" et le "Service de réplication StorageGRID CloudMirror".

	Réplication inter-réseaux	Service de réplication CloudMirror
Quel est le but principal ?	Un système StorageGRID agit comme un système de reprise après sinistre. Les objets d'un bucket peuvent être répliqués entre les grilles dans une ou les deux directions.	Permet à un locataire de répliquer automatiquement des objets d'un bucket dans StorageGRID (source) vers un bucket 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 souvent traitée ultérieurement dans le cloud.
Comment est-il configuré ?	1. Configurer une connexion de fédération de grille entre deux grilles. 2. Ajoutez de nouveaux comptes locataires, qui sont automatiquement clonés sur l'autre grille. 3. Ajoutez de nouveaux groupes de locataires et utilisateurs, qui sont également clonés. 4. Créez des buckets correspondants sur chaque grille et activez la réplication inter-grille dans une ou les deux directions.	1. Un utilisateur locataire configure la réplication CloudMirror en définissant un point de terminaison CloudMirror (adresse IP, informations d'identification, etc.) à l'aide du gestionnaire de locataires ou de l'API S3. 2. Tout bucket appartenant à ce compte locataire peut être configuré pour pointer vers le point de terminaison CloudMirror.

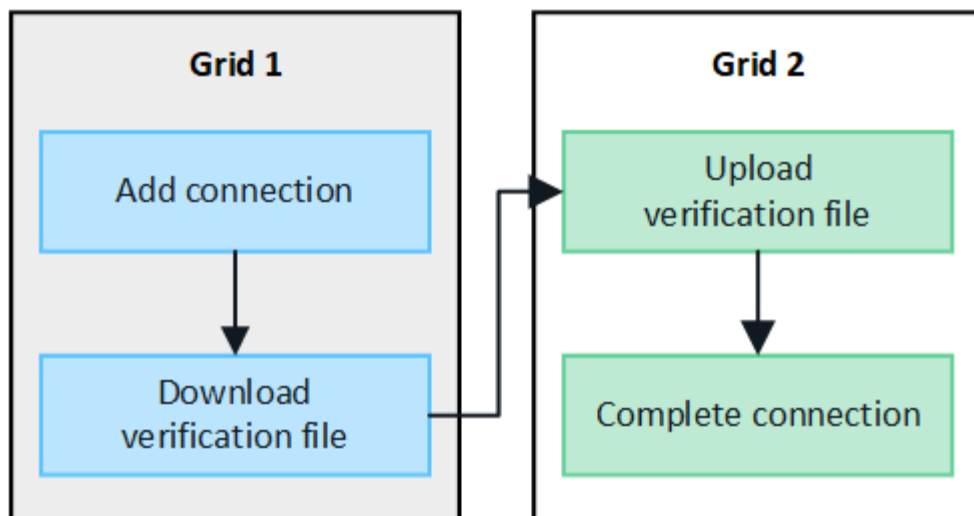
	Réplication inter-réseaux	Service de réplication CloudMirror
Qui est responsable de sa mise en place ?	• Un administrateur de grille configure la connexion et les locataires. • Les utilisateurs locataires configurent les groupes, les utilisateurs, les clés et les buckets.	Généralement, un utilisateur locataire.
Quelle est la destination ?	Un bucket S3 correspondant et identique sur l'autre système StorageGRID dans la connexion de fédération de grille.	• Toute infrastructure S3 compatible (y compris Amazon S3). • Plateforme Google Cloud (GCP)
La gestion des versions d'objets est-elle requise ?	Oui, le contrôle de version des objets doit être activé pour les buckets source et de destination.	Non, la réplication CloudMirror prend en charge toute combinaison de buckets versionnés et non versionnés sur la source et la destination.
Qu'est-ce qui provoque le déplacement des objets vers la destination ?	Les objets sont automatiquement répliqués lorsqu'ils sont ajoutés à un bucket pour lequel la réplication inter-grille est activée.	Les objets sont automatiquement répliqués lorsqu'ils sont ajoutés à un bucket qui a été configuré avec un point de terminaison CloudMirror. Les objets qui existaient dans le bucket source avant que le bucket ne soit configuré avec le point de terminaison CloudMirror ne sont pas répliqués, sauf s'ils sont modifiés.
Comment les objets sont-ils répliqués ?	La réplication inter-grille crée des objets versionnés et réplique l'ID de version du bucket source vers le bucket de destination. Cela permet de maintenir l'ordre des versions sur les deux grilles.	La réplication CloudMirror ne nécessite pas de buckets avec contrôle de version activé. CloudMirror ne peut donc conserver l'ordre d'une clé que dans un site. Il n'y a aucune garantie que la commande soit maintenue pour les demandes concernant un objet sur un site différent.
Que faire si un objet ne peut pas être répliqué ?	L'objet est mis en file d'attente pour la réplication, sous réserve des limites de stockage des métadonnées.	L'objet est mis en file d'attente pour la réplication, sous réserve des limites des services de la plateforme (voir "Recommandations pour l'utilisation des services de la plateforme").
Les métadonnées système de l'objet sont-elles répliquées ?	Oui, lorsqu'un objet est répliqué sur l'autre grille, ses métadonnées système sont également répliquées. Les métadonnées seront identiques sur les deux grilles.	Non, lorsqu'un objet est répliqué dans le bucket externe, ses métadonnées système sont mises à jour. Les métadonnées différeront selon les emplacements, en fonction du moment d'ingestion et du comportement de l'infrastructure S3 indépendante.

	Réplication inter-réseaux	Service de réplication CloudMirror
Comment les objets sont-ils récupérés ?	Les applications peuvent récupérer ou lire des objets en adressant une requête au bucket sur l'une ou l'autre grille.	Les applications peuvent récupérer ou lire des objets en adressant une demande à StorageGRID ou à la destination S3. Par exemple, supposons que vous utilisiez la réplication CloudMirror pour mettre en miroir des objets vers une organisation partenaire. Le partenaire peut utiliser ses propres applications pour lire ou mettre à jour des objets directement depuis la destination S3. L'utilisation de StorageGRID n'est pas requise.
Que se passe-t-il si un objet est supprimé ?	• Les demandes de suppression qui incluent un ID de version ne sont jamais répliquées sur la grille de destination. • Les demandes de suppression qui n'incluent pas d'ID de version ajoutent un marqueur de suppression au bucket source, qui peut éventuellement être répliqué vers la grille de destination. • Si la réplication inter-grille 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 version des buckets source et de destination (qui n'ont pas besoin d'être identiques) : • Si les deux buckets sont versionnés, une demande de suppression ajoutera un marqueur de suppression aux deux emplacements. • Si seul le bucket source est versionné, une demande de suppression ajoutera un marqueur de suppression à la source mais pas à la destination. • Si aucun des deux compartiments n'est versionné, une demande de suppression supprimera l'objet de la source mais pas de la destination. De même, les objets du bucket 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 de l'objet.

Comme le montre la figure, la création d'une connexion de fédération de grille comprend des étapes sur les deux grilles. Vous ajoutez la connexion sur une grille et la complétez sur l'autre grille. Vous pouvez commencer à partir de l'une ou l'autre grille.



Avant de commencer

- Vous avez examiné le "[considérations et exigences](#)" pour configurer les connexions de fédération de grille.
- Si vous prévoyez d'utiliser des noms de domaine entièrement qualifiés (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 dispose des entrées appropriées.
- Vous utilisez un "[navigateur Web pris en charge](#)".
- Vous disposez de l'autorisation d'accès root et de la phrase secrète de provisionnement pour les deux grilles.

Ajouter une connexion

Effectuez ces étapes sur l'un des deux systèmes StorageGRID .

Étapes

1. Sign in au gestionnaire de grille à partir du nœud d'administration principal sur l'une ou l'autre grille.
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'un des éléments suivants : • Le FQDN de la grille à laquelle vous êtes actuellement connecté • Une adresse VIP d'un groupe HA sur cette grille • Une adresse IP d'un nœud d'administration ou d'un nœud de passerelle sur cette grille. L'IP peut se trouver sur n'importe quel réseau que la grille de destination peut atteindre.

Champ	Description
Port	Le port que vous souhaitez utiliser pour cette connexion. Vous pouvez saisir n'importe quel numéro de port inutilisé compris entre 23 000 et 23 999. Les deux réseaux de cette connexion utiliseront le même port. Vous devez vous assurer qu'aucun nœud de l'une ou l'autre grille n'utilise ce port pour d'autres connexions.
Jours de validité du certificat pour cette grille	Le 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 de 730 jours (2 ans), mais vous pouvez saisir n'importe quelle valeur comprise entre 1 et 762 jours. StorageGRID génère automatiquement des certificats client et serveur pour chaque grille lorsque vous enregistrez la connexion.
Mot de passe d'approvisionnement pour cette grille	La phrase secrète de provisionnement pour la grille à laquelle vous êtes connecté.
FQDN ou IP pour l'autre grille	L'un des éléments suivants : • Le FQDN du réseau auquel vous souhaitez vous connecter • Une adresse VIP d'un groupe HA sur l'autre grille • Une adresse IP d'un nœud d'administration ou d'un nœud de passerelle sur l'autre grille. L'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 établie sur l'autre grille, vous ne pouvez plus télécharger le fichier de vérification à partir de l'une ou l'autre des grilles.

7. Localisez le fichier téléchargé(*connection-name.grid-federation*), et enregistrez-le dans un endroit sûr.



Ce fichier contient des secrets (masqués comme *) et d'autres détails sensibles et doivent être stockés et transmis en toute sécurité.

8. Sélectionnez **Fermer** pour revenir à la page de la fédération Grid.

9. Confirmez que la nouvelle connexion est affichée et que son **Statut de connexion** est **En attente de connexion**.

10. Fournir le *connection-name.grid-federation* fichier à l'administrateur de la grille pour l'autre grille.

Connexion complète

Effectuez ces étapes sur le système StorageGRID auquel vous vous connectez (l'autre grille).

Étapes

1. Sign in au gestionnaire de grille 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 qui a été 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 de validité pour les certificats de sécurité de cette grille. L'entrée **Jours de validité du certificat** correspond par défaut à la valeur que vous avez saisie dans 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 ou l'autre extrémité de la connexion expirent, la connexion cessera de fonctionner et les répliquions seront en attente jusqu'à ce que les certificats soient mis à jour.

6. Saisissez la phrase secrète 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 est répertoriée sur la page de la fédération Grid. Le **statut de connexion** sera **Connecté**.

Si un message d'erreur apparaît, corrigez les problèmes. Voir "[Résoudre les erreurs de fédération de grille](#)".

8. Accédez à la page de la fédération Grid sur la première grille et actualisez le navigateur. Confirmez que le **statut de connexion** est désormais **Connecté**.
9. Une fois la connexion établie, supprimez en toute sécurité toutes les copies du fichier de vérification.

Si vous modifiez cette connexion, un nouveau fichier de vérification sera créé. Le fichier original ne peut pas être réutilisé.

Après avoir terminé

- Passez en revue les considérations pour "[gestion des locataires autorisés](#)".
- "[Créer un ou plusieurs nouveaux comptes locataires](#)", attribuez l'autorisation **Utiliser la connexion à la 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 normales de surveillance StorageGRID.
- "[Dépanner la connexion](#)", y compris la résolution des alertes et des erreurs liées au clonage de compte et à la répliquion inter-grille.

Gérer les connexions de la fédération de réseau

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 des locataires et la suppression des connexions inutilisées.

Avant de commencer

- Vous êtes connecté au gestionnaire de grille sur l'une ou l'autre grille à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous avez le ["Autorisation d'accès root"](#) pour la grille à laquelle vous êtes connecté.

Modifier une connexion à une fédération de grille

Vous pouvez modifier une connexion de fédération de grille en vous connectant au nœud d'administration principal sur l'une ou l'autre des grilles de la connexion. Après avoir apporté des modifications à la première grille, vous devez télécharger un nouveau fichier de vérification et le charger sur l'autre grille.



Pendant que la connexion est en cours de modification, les demandes de clonage de compte ou de réplication inter-grille continueront d'utiliser les paramètres de connexion existants. Toutes les modifications que vous apportez à la première grille sont enregistrées localement mais ne sont pas utilisées tant qu'elles n'ont pas été téléchargées sur la deuxième grille, enregistrées et testées.

Commencer à éditer la connexion

Étapes

1. Sign in au gestionnaire de grille à partir du nœud d'administration principal sur l'une ou l'autre grille.
2. Sélectionnez **NODES** et confirmez que tous les autres nœuds d'administration de votre système sont en ligne.



Lorsque vous modifiez une connexion de fédération de grille, StorageGRID tente d'enregistrer un fichier de « 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 apparaît 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** sur la page de fédération de grille ou sur la page de détails d'une connexion spécifique. Voir ["Créer des connexions de fédération de grille"](#) pour quoi entrer.

Menu Actions

- a. Sélectionnez le bouton radio pour 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 secrète 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, accédez à 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 la fédération Grid.
10. Confirmez que le **statut de 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 **En attente de modification**.

11. Fournir le *connection-name.grid-federation* fichier à l'administrateur de la grille pour l'autre grille.

Terminer la modification de la connexion

Terminez la modification de la connexion en téléchargeant le fichier de vérification sur l'autre grille.

Étapes

1. Sign in au gestionnaire de grille 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 qui a été téléchargé à partir de la première grille.
5. Saisissez la phrase secrète 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 apparaît. Examinez le message et résolvez les problèmes éventuels.

7. Fermez l'assistant pour revenir à la page de fédération de grille.
8. Confirmez que le **statut de connexion** est **Connecté**.
9. Accédez à la page de la fédération Grid sur la première grille et actualisez le navigateur. Confirmez que le **statut de connexion** est désormais **Connecté**.
10. Une fois la connexion établie, supprimez en toute sécurité toutes les copies du fichier de vérification.

Tester une connexion à une fédération de grille

Étapes

1. Sign in au gestionnaire de grille à partir du nœud d'administration principal.
2. Sélectionnez **CONFIGURATION > Système > Fédération de grille**.
3. Testez la connexion en utilisant le menu **Actions** sur la page de fédération Grid ou la page de détails d'une connexion spécifique.

Menu Actions

- a. Sélectionnez le bouton radio pour 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 réseaux sont connectés et communiquent normalement.
Erreur	La connexion est dans un état d'erreur. Par exemple, un certificat a expiré ou une valeur de configuration n'est plus valide.
En attente de modification	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 dans l'autre grille.
En attente de connexion	Vous avez configuré la connexion sur cette grille, mais la connexion n'a pas été établie sur l'autre grille. Téléchargez le fichier de vérification 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 réseau ou d'un nœud hors ligne.

- Si l'état de la connexion est **Erreur**, résolvez tous les problèmes. Ensuite, sélectionnez à nouveau **Tester la connexion** pour confirmer que le problème a été résolu.

Faire tourner les certificats de connexion

Chaque connexion à la fédération de grille utilise quatre certificats SSL générés automatiquement pour sécuriser la connexion. Lorsque les deux certificats de chaque grille approchent de leur date d'expiration, l'alerte **Expiration du certificat de fédération de grille** vous rappelle de faire pivoter les certificats.



Si les certificats à l'une ou l'autre extrémité de la connexion expirent, la connexion cessera de fonctionner et les répliquions seront en attente jusqu'à ce que les certificats soient mis à jour.

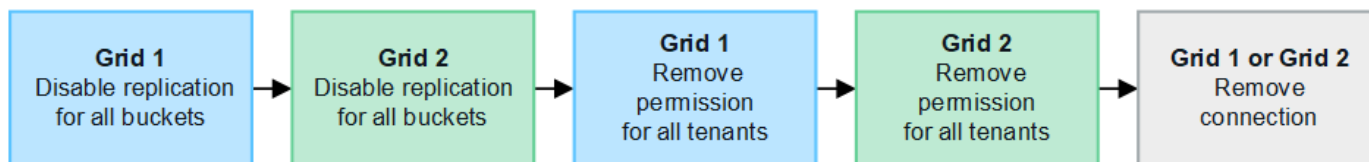
Étapes

- Sign in au gestionnaire de grille à partir du nœud d'administration principal sur l'une ou l'autre grille.
- Sélectionnez **CONFIGURATION > Système > Fédération de grille**.
- À partir de l'un ou l'autre onglet de la page de fédération Grid, sélectionnez le nom de la connexion pour afficher ses détails.
- Sélectionnez l'onglet **Certificats**.
- Sélectionnez **Faire tourner les certificats**.
- Spécifiez combien de jours les nouveaux certificats doivent être valides.
- Saisissez la phrase secrète de provisionnement pour la grille à laquelle vous êtes connecté.
- Sélectionnez **Faire tourner les certificats**.
- 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.

Supprimer une connexion à une fédération de grille

Vous pouvez supprimer une connexion de fédération de grille de l'une ou l'autre 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 utilisée par aucun locataire sur l'une ou l'autre grille.



Avant de supprimer une connexion, notez les points suivants :

- La suppression d'une connexion ne supprime aucun élément qui a déjà été copié entre les grilles. Par exemple, les utilisateurs, groupes et objets locataires qui existent sur les deux grilles ne sont supprimés d'aucune des deux grilles lorsque l'autorisation du locataire est supprimée. Si vous souhaitez supprimer ces éléments, vous devez les supprimer manuellement des deux grilles.
- Lorsque vous supprimez une connexion, la répliquion de tous les objets en attente de répliquion (ingérés mais pas encore répliqués sur l'autre grille) échouera définitivement.

Désactiver la réplication pour tous les compartiments locataires

Étapes

1. À partir de l'une ou l'autre 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 des locataires.
5. Si des locataires sont répertoriés, demandez à tous les locataires de "[désactiver la réplication inter-grille](#)" pour tous leurs buckets sur les deux grilles de la connexion.



Vous ne pouvez pas supprimer l'autorisation **Utiliser la connexion à la fédération de grille** si la réplication inter-grille est activée pour l'un des compartiments de locataire. Chaque compte locataire doit désactiver la réplication inter-grille pour ses buckets sur les deux grilles.

Supprimer l'autorisation pour chaque locataire

Une fois la réplication inter-grille désactivée pour tous les compartiments de locataire, supprimez l'autorisation **Utiliser la fédération de grille** 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 à la fédération de grille** de chaque locataire. Voir "[Gérer les locataires autorisés](#)".
4. Répétez ces étapes pour les locataires autorisés sur l'autre grille.

Supprimer la connexion

Étapes

1. Lorsqu'aucun locataire sur l'une ou l'autre des grilles 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 à la fédération de grille est désormais supprimée des deux grilles.
 - Si la connexion ne peut pas être supprimée (par exemple, elle est toujours utilisée ou il y a une erreur de connexion), un message d'erreur s'affiche. Vous pouvez effectuer l'une des opérations suivantes :
 - Résoudre l'erreur (recommandé). Voir "[Résoudre les erreurs de fédération de grille](#)".
 - Retirer la connexion par la force. Voir la section suivante.

Supprimer une connexion à une fédération de grille de force

Si nécessaire, vous pouvez forcer la suppression d'une connexion qui n'a pas le statut **Connecté**.

La suppression forcée supprime uniquement la connexion du réseau local. 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 apparaît. Cette connexion à la fédération de grille ne peut plus être utilisée. Cependant, les buckets locataires peuvent toujours avoir la réplication inter-grille activée et certaines copies d'objets peuvent avoir déjà été répliquées entre les grilles de 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 de réseau

Vous pouvez autoriser les comptes de locataire S3 à utiliser une connexion de fédération de grille entre deux systèmes StorageGRID . Lorsque les locataires sont autorisés à utiliser une connexion, des étapes spéciales sont nécessaires 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 ou l'autre grille à l'aide d'un ["navigateur Web pris en charge"](#) .
- Vous avez le ["Autorisation d'accès root"](#) pour la grille à laquelle vous êtes connecté.
- Tu as ["créé une connexion à une fédération de grille"](#) entre deux grilles.
- Vous avez examiné les flux de travail pour ["clone de compte"](#) et ["réplication inter-réseaux"](#) .
- 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 clonage de compte"](#) .

Créer un locataire autorisé

Si vous souhaitez autoriser un compte locataire nouveau ou existant à utiliser une connexion de fédération de grille pour le clonage de compte et la réplication inter-grille, suivez les instructions générales pour ["créer un nouveau locataire S3"](#) ou ["modifier un compte locataire"](#) et notez ce qui suit :

- Vous pouvez créer le locataire à partir de l'une ou l'autre grille de la connexion. La grille sur laquelle un locataire est créé est la *grille source du locataire*.
- Le statut de la connexion doit être **Connecté**.
- Lorsque le locataire est créé ou modifié pour activer l'autorisation **Utiliser la connexion à la fédération de grille**, puis enregistré sur la première grille, un locataire identique est automatiquement répliqué sur l'autre grille. La grille sur laquelle le locataire est répliqué est la *grille de destination du locataire*.
- Les locataires des deux grilles auront le même identifiant de compte à 20 chiffres, le même nom, la même description, le même quota et les mêmes autorisations. 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 apparaîtra 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.



Avant qu'un utilisateur root local puisse se connecter au locataire répliqué sur la grille de destination, un administrateur de grille pour cette grille doit ["changer le mot de passe de l'utilisateur root local"](#) .

- Une fois que le locataire nouveau ou modifié est disponible sur les deux grilles, les utilisateurs du locataire peuvent effectuer ces opérations :
 - À partir de la grille source du locataire, créez des groupes et des utilisateurs locaux, qui sont automatiquement clonés vers la grille de destination du locataire. Voir ["Cloner des groupes de locataires et des utilisateurs"](#) .
 - Créez de nouvelles clés d'accès S3, qui peuvent éventuellement être clonées sur la grille de destination du locataire. Voir ["Cloner les clés d'accès S3 à l'aide de l'API"](#) .
 - Créez des buckets identiques sur les deux grilles de la connexion et activez la réplication inter-grille dans une direction ou dans les deux directions. Voir ["Gérer la réplication inter-réseaux"](#) .

Afficher un locataire autorisé

Vous pouvez voir les détails d'un locataire autorisé à utiliser une connexion de fédération de grille.

Étapes

1. Sélectionnez **LOCATAIRES**.
2. Depuis la page Locataires, 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 sur une autre grille. Si vous modifiez ou supprimez ce locataire, vos modifications ne seront pas synchronisées avec l'autre grille.

Tenants > tenant A for grid federation

tenant A for grid federation

Tenant ID: 0899 6970 1700 0930 0009 

Protocol: S3

Object count: 0

Quota utilization: —

Logical space used: 0 bytes

Quota: —

Description: this tenant was created on Grid 1

[Sign in](#) [Edit](#) [Actions](#) ▾

 This tenant has been cloned to another grid. If you edit or delete this tenant, your changes will not be synced to the other grid.

[Space breakdown](#) [Allowed features](#) [Grid federation](#)

[Remove permission](#) [Clear error](#)  Displaying one result

Connection name	Connection status	Remote grid hostname	Last error
 Grid 1 to Grid 2	 Connected	10.96.106.230	Check for errors

3. Sélectionnez éventuellement l'onglet **Fédération de grille** pour "[surveiller la connexion à la fédération du réseau](#)".

Modifier un locataire autorisé

Si vous devez modifier un locataire disposant de l'autorisation **Utiliser la connexion à la fédération de grille**, suivez les instructions générales pour "[modifier un compte locataire](#)" et notez ce qui suit :

- Si un locataire dispose de l'autorisation **Utiliser la connexion à la fédération de grille**, vous pouvez modifier les détails du locataire à partir de l'une ou l'autre des grilles de la connexion. Cependant, les modifications que vous apportez ne seront pas copiées sur l'autre grille. Si vous souhaitez conserver les détails du locataire synchronisés entre les grilles, vous devez effectuer les mêmes modifications sur les deux grilles.
- Vous ne pouvez pas effacer l'autorisation **Utiliser la connexion à la fédération de grille** lorsque vous modifiez un locataire.
- Vous ne pouvez pas sélectionner une connexion de fédération de grille différente lorsque vous modifiez un locataire.

Supprimer un locataire autorisé

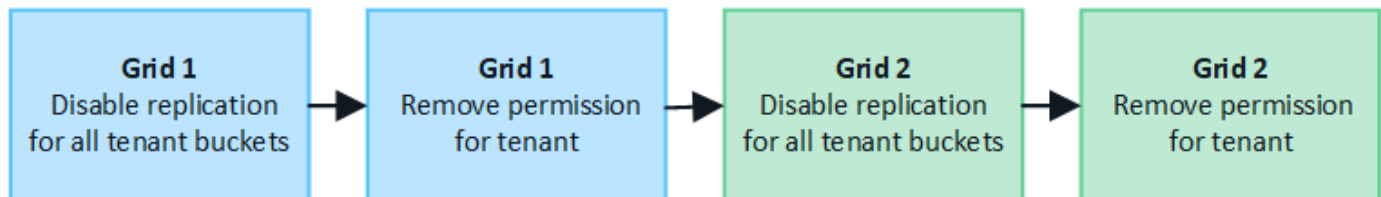
Si vous devez supprimer un locataire disposant de l'autorisation **Utiliser la connexion à la fédération de grille**, suivez les instructions générales pour ["suppression d'un compte locataire"](#) et notez ce qui suit :

- Avant de pouvoir supprimer le locataire d'origine sur la grille source, vous devez supprimer tous les buckets du compte sur la grille source.
- Avant de pouvoir supprimer le locataire cloné sur la grille de destination, vous devez supprimer tous les buckets du compte sur la grille de destination.
- Si vous supprimez le locataire d'origine ou cloné, le compte ne peut plus être utilisé pour la réplication inter-grille.
- Si vous supprimez le locataire d'origine sur la grille source, tous les groupes de locataires, utilisateurs ou clés qui ont été clonés sur 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 buckets.
- Si vous supprimez le locataire cloné sur la grille de destination, des erreurs de clonage se produiront 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 à la fédération de grille avant de supprimer le locataire de cette grille.

Supprimer l'autorisation Utiliser la connexion à 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 à une fédération de réseau, notez les points suivants :

- Vous ne pouvez pas supprimer l'autorisation **Utiliser la connexion à la fédération de grille** si la réplication inter-grille est activée pour l'un des buckets du locataire. Le compte locataire doit d'abord désactiver la réplication inter-grille pour tous ses buckets.
- La suppression de l'autorisation **Utiliser la connexion à la fédération de grille** ne supprime aucun élément qui a déjà été répliqué entre les grilles. Par exemple, les utilisateurs, groupes et objets locataires qui existent sur les deux grilles ne sont supprimés d'aucune des deux grilles lorsque l'autorisation du locataire est supprimée. Si vous souhaitez supprimer ces éléments, vous devez les supprimer manuellement des deux grilles.
- Si vous souhaitez réactiver cette autorisation avec la même connexion de fédération de grille, supprimez d'abord ce locataire sur la grille de destination ; sinon, la réactivation de cette autorisation entraînera une erreur.



La réactivation de l'autorisation **Utiliser la connexion à la fédération de grille** fait de la grille locale la grille source et déclenche le clonage vers la grille distante spécifiée par la connexion à la fédération de grille sélectionnée. Si le compte locataire existe déjà sur la grille distante, le clonage entraînera une erreur de conflit.

Avant de commencer

- Vous utilisez un ["navigateur Web pris en charge"](#) .
- Vous avez le ["Autorisation d'accès root"](#) pour les deux grilles.

Désactiver la réplication pour les compartiments locataires

Dans un premier temps, désactivez la réplication inter-grille pour tous les buckets locataires.

Étapes

1. À partir de l'une ou l'autre 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 ["désactiver la réplication inter-grille"](#) pour tous leurs buckets sur les deux grilles de la connexion.



Vous ne pouvez pas supprimer l'autorisation **Utiliser la connexion à la fédération de grille** si la réplication inter-grille est activée pour l'un des compartiments de locataire. Le locataire doit désactiver la réplication inter-grille pour ses buckets sur les deux grilles.

Supprimer l'autorisation du locataire

Une fois la réplication inter-grille désactivée pour les buckets de locataire, vous pouvez supprimer l'autorisation du locataire d'utiliser la connexion de fédération de grille.

Étapes

1. Sign in au gestionnaire de grille à partir du nœud d'administration principal.
2. Supprimez l'autorisation de la page de la fédération Grid ou de la page Locataires.

Page de la fédération Grid

- 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 correspondant au locataire.
- d. Sélectionnez **Supprimer l'autorisation**.

Page des locataires

- a. Sélectionnez **LOCATAIRES**.
- b. Sélectionnez le nom du locataire pour afficher la page de détails.
- c. Dans l'onglet **Fédération de grille**, sélectionnez le bouton radio pour la connexion.
- d. Sélectionnez **Supprimer l'autorisation**.

3. Vérifiez les avertissements dans la boîte de dialogue de confirmation et sélectionnez **Supprimer**.
 - Si l'autorisation peut être supprimée, vous revenez à la page de détails et un message de réussite s'affiche. Ce locataire ne peut plus utiliser la connexion à la fédération de grille.

- Si la réplication inter-grille est toujours activée pour un ou plusieurs buckets de locataires, une erreur s'affiche.

 **Remove permission to use grid federation connection** 

Are you sure you want to prevent **Tenant A** from performing account sync and cross-grid replication using grid federation connection **Grid 1-Grid 2**?

- Removing this permission does not delete any items that have already been copied to the other grid.
- After removing this permission for the tenant on this grid, go to the other grid and remove the permission for the corresponding tenant account.

 Connection '5427cbf8-0dd0-4b83-a2c8-e5e23cc49cc5' is used by bucket 'my-cgr-bucket' for cross-grid replication, so it can't be removed. From Tenant Manager, remove the cross-grid configuration from the tenant bucket and retry.

 Using **Force remove** removes the tenant's permission to use the grid federation connection even if tenant buckets still have cross-grid replication enabled. When the permission is removed, data in these buckets can no longer be copied between the grids.

Cancel Force remove Remove

Vous pouvez effectuer l'une des opérations suivantes :

- (Recommandé.) Sign in au gestionnaire de locataires et désactivez la réplication pour chacun des compartiments du locataire. Voir "[Gérer la réplication inter-réseaux](#)". Ensuite, répétez les étapes pour supprimer l'autorisation **Utiliser la connexion au réseau**.
 - Supprimer l'autorisation par la force. Voir la section suivante.
4. Accédez à l'autre grille et répétez ces étapes pour supprimer l'autorisation du même locataire sur l'autre grille.

Supprimer l'autorisation de 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-grille est activée pour les buckets de locataire.

Avant de retirer l'autorisation d'un locataire par la force, notez les considérations générales pour [supprimer l'autorisation](#) ainsi que ces considérations supplémentaires :

- Si vous supprimez de force l'autorisation **Utiliser la connexion à la fédération de grille**, 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 bucket de destination, vous devez également supprimer l'autorisation du locataire sur l'autre grille.
- Tous les objets ingérés dans le bucket source après avoir supprimé l'autorisation **Utiliser la connexion à la fédération de grille** ne seront jamais répliqués dans le bucket de destination.

Étapes

1. Sign in 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 sa page de détails.
4. Dans l'onglet * Locataires autorisés *, sélectionnez le bouton radio correspondant au locataire.
5. Sélectionnez **Supprimer l'autorisation**.
6. Vérifiez les avertissements dans la boîte de dialogue de confirmation et sélectionnez **Forcer la suppression**.

Un message de réussite apparaît. Ce locataire ne peut plus utiliser la connexion à la 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 locataire sur l'autre grille. Par exemple, vous devez répéter ces étapes sur l'autre grille pour empêcher les objets en cours d'atteindre le bucket de destination.

Résoudre les erreurs de fédération de grille

Vous devrez peut-être résoudre les alertes et les erreurs liées aux connexions de fédération de grille, au clonage de compte et à la réplication inter-grille.

Alertes et erreurs de connexion à la fédération de grille

Vous pourriez recevoir des alertes ou rencontrer des erreurs avec vos connexions à la fédération de réseau.

Après avoir apporté des modifications pour résoudre un problème de connexion, testez la connexion pour vous assurer que l'état de la connexion revient à **Connecté**. Pour les instructions, voir ["Gérer les connexions de la fédération de réseau"](#).

Alerte d'échec de connexion à la fédération de réseau

Problème

L'alerte **Échec de la connexion à la 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 sur la page Grid Federation pour les deux grilles. Confirmez que toutes les valeurs sont correctes. Voir ["Gérer les connexions de la fédération de réseau"](#).
2. Vérifiez les certificats utilisés pour la connexion. Assurez-vous qu'il n'y a pas d'alertes concernant les certificats de fédération de grille expirés et que les détails de chaque certificat sont valides. Consultez les instructions pour la rotation des certificats de connexion dans ["Gérer les connexions de la fédération de réseau"](#).

3. Confirmez que tous les nœuds d'administration et de passerelle des deux grilles sont en ligne et disponibles. Résolvez toutes 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, confirmez que le serveur DNS est en ligne et disponible. Voir ["Qu'est-ce que la fédération de réseau ?"](#) pour les exigences de mise en réseau, d'adresse IP et de DNS.

Alerte d'expiration du certificat de la fédération de réseau

Problème

L'alerte **Expiration du certificat de la 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

Consultez les instructions pour la rotation des certificats de connexion dans ["Gérer les connexions de la fédération de réseau"](#).

Erreur lors de la modification d'une connexion à une fédération de grille

Problème

Lors de la modification d'une connexion à une fédération de grille, le message d'avertissement suivant s'affiche lorsque vous sélectionnez **Enregistrer et tester** : « Échec de la création d'un fichier de configuration candidat sur un ou plusieurs nœuds. »

Détails

Lorsque vous modifiez une connexion de fédération de grille, StorageGRID tente d'enregistrer un fichier de « configuration candidate » 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. Confirmez que tous les nœuds d'administration de cette grille sont en ligne.
3. Si des nœuds sont hors ligne, remettez-les en ligne et essayez à nouveau de modifier la connexion.

Erreurs de clonage de compte

Impossible de se connecter à un compte locataire cloné

Problème

Vous ne pouvez pas vous connecter à un compte 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 de la grille source du locataire vers la grille de destination du locataire, le mot de passe que vous avez défini pour l'utilisateur root local du locataire n'est pas cloné. De même, lorsqu'un locataire crée des utilisateurs locaux sur sa grille source, les mots de passe des utilisateurs locaux ne sont pas clonés sur la grille de destination.

Actions recommandées

Avant que l'utilisateur root puisse se connecter à la grille de destination du locataire, un administrateur de grille doit d'abord [changer le mot de passe de l'utilisateur root local](#) sur la grille de destination.

Avant 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 les instructions, voir [Gérer les utilisateurs locaux](#) dans les instructions d'utilisation du Tenant Manager.

Locataire créé sans clone

Problème

Vous voyez le message « Locataire créé sans clone » après avoir créé un nouveau locataire avec l'autorisation **Utiliser la connexion à la fédération de grille**.

Détails

Ce problème peut se produire si les mises à jour de l'état de la connexion sont retardées, ce qui peut entraîner l'affichage d'une connexion défectueuse comme **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 à la fédération de grille](#).
2. Suivez les instructions pour tester une connexion à une fédération de grille dans [Gérer les connexions de la fédération de réseau](#) pour confirmer que le problème a été résolu.
3. Dans la grille source du locataire, sélectionnez **LOCATAIRES**.
4. Localisez le compte locataire qui n'a pas pu être cloné.
5. Sélectionnez le nom du locataire pour afficher la page de détails.
6. Sélectionnez **Réessayer le clonage du compte**.

Tenants > test

test

Tenant ID: 0040 2213 8117 4859 6503

Protocol: S3

Object count: 0

Quota utilization: —

Logical space used: 0 bytes

Quota: —

Sign in

Edit

Actions

Tenant account could not be cloned to the other grid.
Reason: Internal server error. The server encountered an error and could not complete your request. Try again. If the problem persists, contact support. Internal Server Error

Retry account clone

Si l'erreur a été résolue, le compte locataire sera désormais cloné sur l'autre grille.

Dernière erreur affichée pour la connexion ou le locataire

Problème

Quand "[visualisation d'une connexion à une fédération de grille](#)" (ou quand "[gérer les locataires autorisés](#)" (pour une connexion), vous remarquez une erreur dans la colonne **Dernière erreur** sur la page des détails de la connexion. Par exemple:

Grid 1 - Grid 2

Local hostname (this grid): 10.96.130.64
Port: 23000
Remote hostname (other grid): 10.96.130.76
Connection status: Connected

[Edit](#) [Download file](#) [Test connection](#) [Remove](#)

Permitted tenants

Certificates

[Remove permission](#) [Clear error](#)

Displaying one result

Tenant name	Last error
Tenant A	2022-12-22 16:19:20 MST Cross-grid replication has encountered an error. Failed to send cross-grid replication request from source bucket 'my-bucket' to destination bucket 'my-bucket'. Error code: DestinationRequestError. Detail: InvalidBucketState. Confirm that the source and destination buckets have object versioning enabled and S3 Object Lock disabled. (logID 13916508109026943924) Check for errors

Détails

Pour chaque connexion de fédération de grille, la colonne **Dernière erreur** affiche l'erreur la plus récente survenue, le cas échéant, lors de la réplication des données d'un locataire sur l'autre grille. Cette colonne affiche uniquement la dernière erreur de réplication inter-grille survenue ; les erreurs précédentes qui auraient pu se produire ne seront pas affichées. Une erreur dans cette colonne peut se produire pour l'une des raisons suivantes :

- La version de l'objet source n'a pas été trouvée.
- Le bucket source n'a pas été trouvé.
- Le bucket de destination a été supprimé.
- Le bucket de destination a été recréé par un compte différent.
- Le contrôle de version du bucket de destination est suspendu.
- Le bucket de destination a été recréé par le même compte mais n'est désormais plus versionné.

Actions recommandées

Si un message d'erreur apparaît dans la colonne **Dernière erreur**, procédez comme suit :

1. Relisez le texte du message.
2. Effectuez toutes les actions recommandées. Par exemple, si le contrôle de version a été suspendu sur le bucket de destination pour la réplication inter-grille, réactivez le contrôle de version pour ce bucket.
3. Sélectionnez la connexion ou le compte locataire dans le tableau.
4. Sélectionnez **Effacer l'erreur**.
5. Sélectionnez **Oui** pour effacer le message et mettre à jour l'état du système.
6. Attendez 5 à 6 minutes, puis ingérez un nouvel objet dans le seau. 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 du message avant d'ingérer un nouvel objet.



Une fois l'erreur corrigée, une nouvelle **Dernière erreur** peut apparaître si des objets sont ingérés dans un autre compartiment qui comporte également une erreur.

7. Pour déterminer si des objets n'ont pas pu être répliqués en raison de l'erreur de compartiment, consultez ["Identifier et réessayer les opérations de réplication ayant échoué"](#).

Alerte d'échec permanent de réplication inter-réseau

Problème

L'alerte **Échec permanent de la réplication inter-réseau** a été déclenchée.

Détails

Cette alerte indique que les objets locataires ne peuvent pas être répliqués entre les buckets sur deux grilles pour une raison qui nécessite l'intervention de l'utilisateur pour être résolue. Cette alerte est généralement provoquée par une modification du bucket source ou de destination.

Actions recommandées

1. Sign in à la grille où l'alerte a été déclenchée.
2. Accédez à **CONFIGURATION > Système > Fédération de grille** et recherchez le nom de connexion répertorié dans l'alerte.
3. Dans l'onglet Locataires autorisés, regardez la colonne **Dernière erreur** pour déterminer quels comptes de locataire présentent des erreurs.
4. Pour en savoir plus sur l'échec, consultez les instructions dans ["Surveiller les connexions de la fédération de réseau"](#) pour examiner les mesures de réplication inter-réseaux.
5. Pour chaque compte locataire concerné :
 - a. Voir les instructions dans ["Surveiller l'activité des locataires"](#) pour confirmer que le locataire n'a pas dépassé son quota sur la grille de destination pour la réplication inter-grille.
 - 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 à Tenant Manager sur les deux grilles afin de pouvoir comparer la liste des compartiments.
7. Pour chaque bucket pour lequel la réplication inter-grille est activée, confirmez les éléments suivants :

- Il existe un bucket correspondant pour le même locataire sur l'autre grille (vous devez utiliser le nom exact).
- Les deux buckets ont le contrôle de version des objets activé (le contrôle de version ne peut pas être suspendu sur l'une ou l'autre des grilles).
- Le verrouillage d'objet S3 est désactivé pour les deux buckets.
- Aucun des deux compartiments n'est dans l'état **Suppression d'objets : lecture seule**.

8. Pour confirmer que le problème a été résolu, consultez les instructions dans "[Surveiller les connexions de la fédération de réseau](#)" pour examiner les mesures de réplication inter-grille ou effectuez ces étapes :

- Retournez à la page de la fédération Grid.
- Sélectionnez le locataire concerné et sélectionnez **Effacer l'erreur** dans la colonne **Dernière erreur**.
- Sélectionnez **Oui** pour effacer le message et mettre à jour l'état du système.
- Attendez 5 à 6 minutes, puis ingérez un nouvel objet dans le seau. 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 du message avant d'ingérer un nouvel objet.



Il faudra peut-être jusqu'à un jour pour que l'alerte disparaisse une fois résolue.

- Aller 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 réessayer la réplication si nécessaire.

Alerte d'indisponibilité des ressources de réplication inter-réseau

Problème

L'alerte **Ressource de réplication inter-grille indisponible** a été déclenchée.

Détails

Cette alerte indique que des demandes de réplication inter-grille sont en attente car une ressource n'est pas disponible. Par exemple, il peut y avoir une erreur réseau.

Actions recommandées

- Surveillez l'alerte pour voir si le problème se résout de lui-même.
- Si le problème persiste, déterminez si l'une des grilles présente une alerte **Échec de connexion à la fédération de grille** pour la même connexion ou une alerte **Impossible de communiquer avec le nœud** pour un nœud. Cette alerte pourrait être résolue lorsque vous résolvez ces alertes.
- Pour en savoir plus sur l'échec, consultez les instructions dans "[Surveiller les connexions de la fédération de réseau](#)" pour examiner les mesures de réplication inter-réseaux.
- Si vous ne parvenez pas à résoudre l'alerte, contactez le support technique.

La réplication inter-grille 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 inter-grille**, 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 inter-grille** indique que les objets locataires ne peuvent pas être répliqués entre les buckets sur deux grilles pour une raison qui nécessite l'intervention de l'utilisateur pour être résolue. Cette alerte est généralement provoquée par une modification du bucket source ou de destination. Pour plus de détails, consultez la section "[Résoudre les erreurs de fédération de grille](#)".

Déterminer 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 \(demande de réplication inter-réseau\)](#)" messages. Ce message est ajouté au journal lorsque StorageGRID ne parvient pas à répliquer un objet, un objet en plusieurs parties ou à supprimer un marqueur dans le bucket 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 root.
- Vous avez le `Passwords.txt` déposer.
- Vous connaissez l'adresse IP du nœud d'administration principal.

Étapes

1. Connectez-vous au nœud d'administration principal :

- a. Entrez la commande suivante : `ssh admin@primary_Admin_Node_IP`
- b. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.
- c. Entrez la commande suivante pour passer en root : `su -`
- d. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.

Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

2. Recherchez les messages CGRR dans le journal d'audit et utilisez l'outil `audit-explain` pour formater les résultats.

Par exemple, cette commande recherche 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 ressembleront à cet exemple, qui comporte des entrées pour six messages CGRR. Dans l'exemple, toutes les demandes de réplication inter-grille ont renvoyé une erreur générale car l'objet n'a pas pu être répliqué. Les trois premières erreurs concernent les opérations de « réplication d'objet » et les trois dernières erreurs concernent les opérations de « réplication de marqueur de suppression ».

```

CGRR Cross-Grid Replication Request tenant:50736445269627437748
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:50736445269627437748
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:50736445269627437748
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:50736445269627437748
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 inter-réseau CGRR	Le nom de la demande
locataire	L'identifiant du compte du locataire
connexion	L'ID de la connexion à la fédération de grille
opération	Le type d'opération de réplication qui était tentée : • répliquer l'objet • répliquer supprimer le marqueur • répliquer un objet en plusieurs parties
seau	Le nom du bucket
objet	Le nom de l'objet
version	L'ID de version de l'objet

Champ	Description
erreur	Le type d'erreur. Si la réplication inter-grille échoue, l'erreur est « Erreur générale ».

Réessayer les réplications ayant échoué

Après avoir généré une liste d'objets et supprimé les marqueurs qui n'ont pas été répliqués dans le compartiment de destination et résolu les problèmes sous-jacents, vous pouvez réessayer la réplication de deux manières :

- Réingérez chaque objet dans le bucket 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 **Accéder à la documentation de l'API privée**.



Les points de terminaison de l'API StorageGRID marqués « Privé » sont susceptibles d'être modifiés sans préavis. Les points de terminaison privés StorageGRID ignorent également la version API de la demande.

3. Dans la section **cross-grid-replication-advanced**, sélectionnez le point de terminaison suivant :

```
POST /private/cross-grid-replication-retry-failed
```

4. Sélectionnez **Essayer**.
5. Dans la zone de texte **body**, remplacez l'exemple d'entrée pour **versionID** par un ID de version du fichier audit.log qui correspond à une demande de réplication inter-grille ayant échoué.

Assurez-vous de conserver les guillemets doubles autour de la chaîne.

6. Sélectionnez **Exécuter**.
7. Confirmez que le code de réponse du serveur est **204**, indiquant que l'objet ou le marqueur de suppression a été marqué comme en attente de réplication inter-grille 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 tentatives de réplication

Vous devez surveiller les opérations de nouvelle tentative de réplication pour vous assurer qu'elles se terminent.



La réplication d'un objet ou d'un marqueur de suppression sur l'autre grille peut prendre plusieurs heures, voire plus.

Vous pouvez surveiller les opérations de nouvelle tentative de deux manières :

- Utiliser un S3 ["HeadObject"](#) ou ["Obtenir l'objet"](#) demande. La réponse inclut le StorageGRID spécifique `x-ntap-sg-cgr-replication-status` en-tête de réponse, qui aura l'une des valeurs suivantes :

Grille	État de réplication
Source	• TERMINÉ : La réplication a réussi. • EN ATTENTE : L'objet n'a pas encore été répliqué. • ÉCHEC : La réplication a échoué avec un échec permanent. Un 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 point de terminaison suivant :

```
GET /private/cross-grid-replication-object-status/{id}
```

2. Sélectionnez **Essayer**.
3. Dans la section Paramètres, entrez l'ID de version que vous avez utilisé dans le `cross-grid-replication-retry-failed` demande.
4. Sélectionnez **Exécuter**.
5. Confirmez que le code de réponse du serveur est **200**.
6. Vérifiez l'état de 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 un échec permanent. Un utilisateur doit résoudre l'erreur.

Gérer la sécurité

Gérer la sécurité

Vous pouvez configurer divers paramètres de sécurité à partir du Grid Manager pour contribuer à sécuriser votre système StorageGRID .

Gérer le cryptage

StorageGRID fournit plusieurs options pour crypter les données. Tu devrais ["examiner les méthodes de cryptage disponibles"](#) pour déterminer ceux qui répondent à vos exigences en matière de protection des données.

Gérer les certificats

Tu peux ["configurer et gérer les certificats du serveur"](#) utilisé pour les connexions HTTP ou les certificats clients utilisés pour authentifier l'identité d'un client ou d'un utilisateur auprès du serveur.

Configurer les serveurs de gestion de clés

En utilisant un ["serveur de gestion de clés"](#) vous permet de protéger les données StorageGRID même si un appareil est retiré du centre de données. Une fois les volumes de l'apppliance chiffrés, vous ne pouvez accéder à aucune donnée sur l'apppliance, sauf si le nœud peut communiquer avec le KMS.



Pour utiliser la gestion des clés de chiffrement, vous devez activer le paramètre **Chiffrement de nœud** pour chaque appliance lors de l'installation, avant que l'apppliance ne soit ajoutée à la grille.

Gérer les paramètres de proxy

Si vous utilisez des services de plateforme S3 ou des pools de stockage cloud, vous pouvez configurer un ["serveur proxy de stockage"](#) entre les nœuds de stockage et les points de terminaison S3 externes. Si vous envoyez des packages AutoSupport via HTTPS ou HTTP, vous pouvez configurer un ["serveur proxy d'administration"](#) entre les nœuds d'administration et le support technique.

Contrôler les 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 au niveau du ["pare-feu externe"](#). Vous pouvez également contrôler l'accès réseau à chaque nœud en configurant son ["pare-feu interne"](#). Vous pouvez empêcher l'accès sur tous les ports, sauf ceux nécessaires à votre déploiement.

Examiner les méthodes de chiffrement StorageGRID

StorageGRID fournit plusieurs options pour crypter les données. Vous devez examiner les méthodes disponibles pour déterminer celles qui répondent à vos exigences en matière de protection des données.

Le tableau fournit un résumé de haut niveau des méthodes de chiffrement disponibles dans StorageGRID.

Option de cryptage	Comment ça marche	S'applique à
Serveur de gestion de clés (KMS) dans Grid Manager	Toi "configurer un serveur de gestion de clés" pour le site StorageGRID et "activer le chiffrement des nœuds pour l'apppliance" . Ensuite, un nœud d'appareil se connecte au KMS pour demander une clé de chiffrement de clé (KEK). Cette clé crypte et décrypte la clé de cryptage des données (DEK) sur chaque volume.	Nœuds d'appareils pour lesquels le chiffrement de nœud est activé lors de l'installation. Toutes les données de l'appareil sont protégées contre toute perte physique ou suppression du centre de données. Remarque : la gestion des clés de chiffrement avec un KMS est uniquement prise en charge pour les nœuds de stockage et les appliances de services.

Option de cryptage	Comment ça marche	S'applique à
Page de chiffrement de lecteur dans le programme d'installation de l'appliance StorageGRID	Si l'appareil contient des lecteurs prenant en charge le chiffrement matériel, vous pouvez définir une phrase secrète de lecteur lors de l'installation. Lorsque vous définissez une phrase secrète de lecteur, il est impossible pour quiconque de récupérer des données valides à partir de lecteurs qui ont été supprimés du système, à moins de connaître la phrase secrète. Avant de commencer l'installation, accédez à Configurer le matériel > Chiffrement de lecteur pour définir une phrase secrète de lecteur qui s'applique à tous les lecteurs à chiffrement automatique gérés par StorageGRID dans un nœud.	Appareils contenant des lecteurs à chiffrement automatique. Toutes les données sur les disques sécurisés sont protégées contre toute perte physique ou suppression du centre de données. Le chiffrement des lecteurs ne s'applique pas aux lecteurs gérés par SANtricity. Si vous disposez d'un dispositif de stockage avec des lecteurs à chiffrement automatique et des contrôleurs SANtricity, vous pouvez activer la sécurité des lecteurs dans SANtricity.
Pilotez la sécurité dans SANtricity System Manager	Si la fonctionnalité Drive Security est activée pour votre appliance StorageGRID, vous pouvez utiliser " Gestionnaire de système SANtricity " pour créer et gérer la clé de sécurité. La clé est nécessaire pour accéder aux données sur les lecteurs sécurisés.	Appareils de stockage dotés de lecteurs à chiffrement complet du disque (FDE) ou de lecteurs à chiffrement automatique. Toutes les données sur les disques sécurisés sont protégées contre toute perte physique ou suppression du centre de données. Ne peut pas être utilisé avec certains appareils de stockage ou avec des appareils de service.
Chiffrement des objets stockés	Vous activez le " Chiffrement des objets stockés " option dans le gestionnaire de grille. Lorsque cette option est activée, tous les nouveaux objets qui ne sont pas chiffrés au niveau du bucket ou au niveau de l'objet sont chiffrés lors de l'ingestion.	Données d'objet S3 nouvellement ingérées. Les objets stockés existants ne sont pas chiffrés. Les métadonnées des objets et autres données sensibles ne sont pas chiffrées.

Option de cryptage	Comment ça marche	S'applique à
Chiffrement du compartiment S3	Vous émettez une demande PutBucketEncryption pour activer le chiffrement du bucket. Tous les nouveaux objets qui ne sont pas chiffrés au niveau de l'objet sont chiffrés lors de l'ingestion.	Données d'objet S3 nouvellement ingérées uniquement. Le chiffrement doit être spécifié pour le bucket. Les objets de bucket existants ne sont pas chiffrés. Les métadonnées des objets et autres données sensibles ne sont pas chiffrées. "Opérations sur les godets"
Chiffrement côté serveur d'objets S3 (SSE)	Vous émettez une requête S3 pour stocker un objet et incluez le x-amz-server-side-encryption-en-tête de requête.	Données d'objet S3 nouvellement ingérées uniquement. Le cryptage doit être spécifié pour l'objet. Les métadonnées des objets et autres données sensibles ne sont pas chiffrées. StorageGRID gère les clés. "Utiliser le cryptage côté serveur"
Chiffrement côté serveur d'objets S3 avec clés fournies par le client (SSE-C)	Vous émettez une requête 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 nouvellement ingérées uniquement. Le cryptage doit être spécifié pour l'objet. Les métadonnées des objets et autres données sensibles ne sont pas chiffrées. Les clés sont gérées en dehors de StorageGRID. "Utiliser le cryptage côté serveur"
Chiffrement de volume externe ou de banque de données	Vous utilisez une méthode de chiffrement en dehors de StorageGRID pour chiffrer un volume ou une banque de données entière, si votre plate-forme de déploiement la prend en charge.	Toutes les données d'objet, métadonnées et données de configuration système, en supposant que chaque volume ou banque de données soit chiffré. Une méthode de cryptage externe permet un contrôle plus strict des algorithmes et des clés de cryptage. Peut être combiné avec les autres méthodes répertoriées.

Option de cryptage	Comment ça marche	S'applique à
Chiffrement d'objets en dehors de StorageGRID	Vous utilisez une méthode de chiffrement en dehors de StorageGRID pour chiffrer les données et les métadonnées des objets avant qu'elles ne soient ingérées dans StorageGRID.	Données d'objet et métadonnées uniquement (les données de configuration du système ne sont pas chiffrées). Une méthode de cryptage externe permet un contrôle plus strict des algorithmes et des clés de cryptage. Peut être combiné avec les autres méthodes répertoriées. "Amazon Simple Storage Service - Guide de l'utilisateur : Protection des données à l'aide du chiffrement côté client"

Utiliser plusieurs méthodes de cryptage

Selon vos besoins, vous pouvez utiliser plusieurs méthodes de cryptage à la fois. Par exemple:

- Vous pouvez utiliser un KMS pour protéger les nœuds de l'appliance et également utiliser la fonction de sécurité du lecteur dans SANtricity System Manager pour « doublement crypter » les données sur les lecteurs à chiffrement automatique dans les mêmes appliances.
- Vous pouvez utiliser un KMS pour sécuriser les données sur les nœuds de l'appliance et également utiliser l'option de chiffrement des objets stockés pour chiffrer tous les objets lorsqu'ils sont ingérés.

Si seule une petite partie de vos objets nécessite un chiffrement, envisagez plutôt de contrôler le chiffrement au niveau du bucket ou de l'objet individuel. L'activation de plusieurs niveaux de cryptage entraîne un coût supplémentaire en termes de performances.

Gérer les certificats

Gérer les certificats de sécurité

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 sont utilisés pour établir des connexions sécurisées entre les clients et les serveurs, authentifiant l'identité d'un serveur auprès de ses clients et fournissant un chemin de communication sécurisé pour les données. Le serveur et le client disposent chacun d'une copie du certificat.
- **Les certificats clients** authentifient l'identité d'un client ou d'un utilisateur auprès du serveur, offrant une authentification plus sécurisée que les mots de passe seuls. Les certificats clients ne cryptent 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 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 (comme le point de terminaison de l'équilibreur de charge) ou comme client pour d'autres connexions (comme le service de réplication CloudMirror).

Certificat Grid CA par défaut

StorageGRID inclut une autorité de certification (CA) intégrée qui génère un certificat CA Grid interne lors de l'installation du système. Le certificat Grid CA est utilisé, par défaut, pour sécuriser le trafic StorageGRID interne. Une autorité de certification (CA) externe peut émettre des certificats personnalisés entièrement conformes aux politiques de sécurité des informations de votre organisation. Bien que vous puissiez utiliser le certificat Grid CA pour un environnement hors production, 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 CA personnalisés 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 répondre aux ["directives 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 regroupement de certificats d'autorité de certification).



StorageGRID inclut également des certificats d'autorité de certification du système d'exploitation qui sont les mêmes 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 CA du système d'exploitation.

Les variantes des types de certificats serveur et client sont implémentées de plusieurs manières. Vous devez disposer de tous les certificats nécessaires à votre configuration StorageGRID spécifique avant de configurer le système.

Accéder aux certificats de sécurité

Vous pouvez accéder aux informations sur tous les certificats StorageGRID dans un seul emplacement, ainsi qu'aux liens vers le flux de travail de configuration pour chaque certificat.

Étapes

1. Depuis le Gestionnaire de grille, sélectionnez **CONFIGURATION > Sécurité > Certificats**.

Certificates

View and manage the certificates that secure HTTPS connections between StorageGRID and external clients, such as S3 or Swift, and external servers, such as a key management server (KMS).

Global

Grid CA

Client

Load balancer endpoints

Tenants

Other

The StorageGRID certificate authority ("grid CA") generates and signs two global certificates during installation. The management interface certificate on Admin Nodes secures the management interface. The S3 and Swift API certificate on Storage and Gateway Nodes secures client access. You should replace each default certificate with your own custom certificate signed by an external certificate authority.

Name	Description	Type ⓘ	Expiration date ⓘ ⌵
Management interface certificate	Secures the connection between client web browsers and the Grid Manager, Tenant Manager, Grid Management API, and Tenant Management API.	Custom	Jun 4th, 2022
S3 and Swift API certificate	Secures the connections between S3 and Swift clients and Storage Nodes or between clients and the deprecated CLB service on Gateway Nodes. You can optionally use this certificate for a load balancer endpoint as well.	Custom	Jun 4th, 2022

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 pouvez accéder à un onglet si vous avez le ["autorisation appropriée"](#) .

- **Global** : Sécurise l'accès à StorageGRID à partir des navigateurs Web et des 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 de terminaison de l'équilibreur de charge** : sécurise les connexions entre les clients S3 et l'équilibreur de charge StorageGRID .
- *** Locataires *** : sécurise les connexions aux serveurs de fédération d'identité ou des points de terminaison de service de la plateforme 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 à StorageGRID à partir des navigateurs Web et des clients API S3 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 d'interface de gestion](#): Sécurise les connexions du navigateur Web client aux interfaces de gestion StorageGRID .
- [Certificat API S3](#):Sécurise les connexions API client aux nœuds de stockage, aux nœuds d'administration et aux nœuds de passerelle, que les applications client S3 utilisent pour télécharger et charger des données d'objet.

Les informations sur les certificats globaux installés incluent :

- **Nom** : Nom du certificat avec lien pour gérer le certificat.
- **Description**
- **Type** : Personnalisé ou par défaut. + Vous devez toujours utiliser un certificat personnalisé pour améliorer la sécurité du réseau.
- **Date d'expiration** : Si vous utilisez le certificat par défaut, aucune date d'expiration n'est affichée.

Tu peux:

- Remplacez les certificats par défaut par des certificats personnalisés signés par une autorité de certification externe pour améliorer la sécurité de la grille :
 - ["Remplacer le certificat d'interface de gestion généré par StorageGRID par défaut"](#)utilisé pour les connexions Grid Manager et Tenant Manager.
 - ["Remplacer le certificat API S3"](#)utilisé pour les connexions au nœud de stockage et au point de terminaison de l'équilibreur de charge (facultatif).
- ["Restaurer le certificat d'interface de gestion par défaut"](#) .
- ["Restaurer le certificat API S3 par défaut"](#) .
- ["Utiliser un script pour générer un nouveau certificat d'interface de gestion auto-signé"](#) .
- Copiez ou téléchargez le ["certificat d'interface de gestion"](#) ou ["Certificat API S3"](#) .

Grille CA

Le [Certificat Grid CA](#) , généré par l'autorité de certification StorageGRID lors de l'installation de StorageGRID , sécurise tout le trafic interne de StorageGRID .

Les informations du certificat incluent la date d'expiration du certificat et le contenu du certificat.

Tu peux [copier ou télécharger le certificat Grid CA](#) , mais tu ne peux pas le changer.

Client

[Certificats clients](#), généré par une autorité de certification externe, sécurise les connexions entre les outils de surveillance externes et la base de données StorageGRID Prometheus.

La table des certificats comporte 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.

Tu peux:

- ["Téléchargez ou générez un nouveau certificat client."](#)
- Sélectionnez un nom de certificat pour afficher les détails du certificat où vous pouvez :
 - ["Modifier le nom du certificat client."](#)
 - ["Définissez l'autorisation d'accès Prometheus."](#)
 - ["Téléchargez et remplacez le certificat client."](#)
 - ["Copiez ou téléchargez le certificat client."](#)
 - ["Supprimer le certificat client."](#)
- Sélectionnez **Actions** pour rapidement ["modifier"](#), ["attacher"](#), ou ["retirer"](#) un certificat client. Vous pouvez sélectionner jusqu'à 10 certificats clients et les supprimer simultanément en utilisant **Actions > Supprimer**.

Points de terminaison de l'équilibreur de charge

[Certificats de point de terminaison d'équilibrage de charge](#) sécurisez les connexions entre les clients S3 et le service StorageGRID Load Balancer sur les nœuds de passerelle et les nœuds d'administration.

La table des points de terminaison de l'équilibreur de charge comporte une ligne pour chaque point de terminaison de l'équilibreur de charge configuré et indique si le certificat API S3 global ou un certificat de point de terminaison de l'équilibreur de charge personnalisé est utilisé pour le point de terminaison. La date d'expiration de chaque certificat est également affichée.



Les modifications apportées à un certificat de point de terminaison peuvent prendre jusqu'à 15 minutes pour être appliquées à tous les nœuds.

Tu peux:

- ["Afficher un point de terminaison d'équilibrage de charge"](#), y compris les détails de son certificat.
- ["Spécifiez un certificat de point de terminaison d'équilibrage de charge pour FabricPool."](#)
- ["Utiliser le certificat API S3 global"](#) au lieu de générer un nouveau certificat de point de terminaison d'équilibrage de charge.

Locataires

Les locataires peuvent utiliser [certificats de serveur de fédération d'identité](#) ou [certificats de point de terminaison de service de plateforme](#) pour sécuriser leurs connexions avec StorageGRID.

La table des locataires comporte une ligne pour chaque locataire et indique si chaque locataire est autorisé à utiliser sa propre source d'identité ou ses propres services de plateforme.

Tu peux:

- ["Sélectionnez un nom de locataire pour vous connecter au gestionnaire de locataires"](#)
- ["Sélectionnez un nom de locataire pour afficher les détails de la fédération d'identité du locataire"](#)
- ["Sélectionnez un nom de locataire pour afficher les détails des services de la plateforme locataire"](#)
- ["Spécifier un certificat de point de terminaison de service de plateforme lors de la création du point de terminaison"](#)

Autre

StorageGRID utilise d'autres certificats de sécurité à des fins spécifiques. Ces certificats sont répertoriés par leur nom fonctionnel. D'autres certificats de sécurité incluent :

- [Certificats Cloud Storage Pool](#)
- [Certificats de notification d'alerte par courrier électronique](#)
- [Certificats de serveur syslog externes](#)
- [Certificats de connexion à la fédération de réseau](#)
- [Certificats de fédération d'identité](#)
- [Certificats du serveur de gestion de clés \(KMS\)](#)
- [Certificats d'authentification unique](#)

Les informations indiquent le type de certificat utilisé par une fonction ainsi que les dates d'expiration de ses certificats serveur et 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 des autres certificats que si vous disposez des droits d'accès. ["autorisation appropriée"](#) .

Tu peux:

- ["Spécifier un certificat de pool de stockage cloud pour S3, C2S S3 ou Azure"](#)
- ["Spécifier un certificat pour les notifications d'alerte par e-mail"](#)
- ["Utiliser un certificat pour un serveur syslog externe"](#)
- ["Faire pivoter les certificats de connexion à la fédération de réseau"](#)
- ["Afficher et modifier un certificat de fédération d'identité"](#)
- ["Télécharger les certificats du serveur de gestion des clés \(KMS\) et du client"](#)
- ["Spécifier manuellement un certificat SSO pour une approbation de partie de confiance"](#)

Détails du certificat de sécurité

Chaque type de certificat de sécurité est décrit ci-dessous, avec des liens vers les instructions de mise en œuvre.

Certificat d'interface de gestion

Type de certificat	Description	Emplacement de navigation	Détails
Serveur	Authentifie la connexion entre les navigateurs Web clients et l'interface de gestion StorageGRID , permettant aux utilisateurs d'accéder à Grid Manager et Tenant Manager sans avertissements de sécurité. Ce certificat authentifie également les connexions à l'API Grid Management et à l'API Tenant Management. 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 sélectionnez Certificat d'interface de gestion	"Configurer les certificats de l'interface de gestion"

Certificat API S3

Type de certificat	Description	Emplacement de navigation	Détails
Serveur	Authentifie les connexions client S3 sécurisées à un nœud de stockage et aux points de terminaison de l'équilibreur de charge (facultatif).	CONFIGURATION > Sécurité > Certificats , sélectionnez l'onglet Global , puis sélectionnez Certificat API S3	"Configurer les certificats API S3"

Certificat Grid CA

Voir le [Description du certificat Grid CA par défaut](#) .

Certificat 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. • Permet une surveillance sécurisée de StorageGRID à l'aide d'outils externes.	CONFIGURATION > Sécurité > Certificats puis sélectionnez l'onglet Client	"Configurer les certificats clients"

Certificat de point de terminaison de l'équilibreur de charge

Type de certificat	Description	Emplacement de navigation	Détails
Serveur	Authentifie la connexion entre les clients S3 et le service d'équilibrage de charge StorageGRID 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 point de terminaison d'équilibreur de charge. Les applications clientes utilisent le certificat d'équilibrage de charge lors de la connexion à StorageGRID pour enregistrer et récupérer les données d'objet. Vous pouvez également utiliser une version personnalisée du global Certificat API S3 certificat pour 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 point de terminaison 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 StorageGRID .	CONFIGURATION > Réseau > Points de terminaison de l'équilibreur de charge	• "Configurer les points de terminaison de l'équilibreur de charge" • "Créer un point de terminaison d'équilibrage de charge pour FabricPool"

Certificat de point de terminaison du pool de stockage cloud

Type de certificat	Description	Emplacement de navigation	Détails
Serveur	Authentifie la connexion d'un pool de stockage cloud StorageGRID vers un emplacement de stockage externe, tel que S3 Glacier ou le stockage Microsoft Azure Blob. Un certificat différent est requis pour chaque type de fournisseur de cloud.	ILM > Pools de stockage	"Créer un pool de stockage cloud"

Certificat de notification d'alerte par courrier électronique

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 Transport Layer Security (TLS), vous devez spécifier le certificat d'autorité de certification du serveur de messagerie. • Spécifiez un certificat client uniquement si le serveur de messagerie SMTP requiert des certificats clients pour l'authentification.	ALERTES > Configuration de la messagerie électronique	"Configurer des 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 enregistre 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 > Serveur d'audit et syslog	"Utiliser un serveur syslog externe"

Certificat de connexion à la fédération de réseau

Type de certificat	Description	Emplacement de navigation	Détails
Serveur et client	Authentifiez et cryptez 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 tourner les certificats de connexion"

Certificat de fédération d'identité

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 d'identité, qui permet aux groupes d'administrateurs et aux utilisateurs d'être gérés par un système externe.	CONFIGURATION > Contrôle d'accès > Fédération d'identité	"Utiliser la fédération d'identité"

Certificat du serveur de gestion de clés (KMS)

Type de certificat	Description	Emplacement de navigation	Détails
Serveur et client	Authentifie la connexion entre StorageGRID et un serveur de gestion de clés externe (KMS), qui fournit des clés de chiffrement aux nœuds de l'appliance StorageGRID .	CONFIGURATION > Sécurité > Serveur de gestion des clés	"Ajouter un serveur de gestion de clés (KMS)"

Certificat de point de terminaison des services de plateforme

Type de certificat	Description	Emplacement de navigation	Détails
Serveur	Authentifie la connexion du service de plateforme StorageGRID à une ressource de stockage S3.	Gestionnaire de locataires > STOCKAGE (S3) > Points de terminaison des services de plateforme	"Créer un point de terminaison des services de plateforme" "Modifier le point de terminaison des services de la plateforme"

Certificat d'authentification unique (SSO)

Type de certificat	Description	Emplacement de navigation	Détails
Serveur	Authentifie la connexion entre les services de fédération d'identité, tels que les services de fédération Active Directory (AD FS) et StorageGRID qui sont utilisés pour les demandes d'authentification unique (SSO).	CONFIGURATION > Contrôle d'accès > Authentification unique	"Configurer l'authentification unique"

Exemples de certificats

Exemple 1 : service d'équilibrage de charge

Dans cet exemple, StorageGRID agit comme serveur.

1. Vous configurez un point de terminaison d'équilibrage de charge et téléchargez ou générez un certificat de serveur dans StorageGRID.
2. Vous configurez une connexion client S3 au point de terminaison de l'équilibreur de charge et téléchargez le même certificat sur le 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 avec une signature basée sur la clé privée.
5. Le client vérifie ce certificat en comparant la signature du serveur à la signature sur sa copie du certificat. Si les signatures correspondent, le client démarre une session en utilisant la même clé publique.
6. Le client envoie des données d'objet à StorageGRID.

Exemple 2 : Serveur de gestion de clés externe (KMS)

Dans cet exemple, StorageGRID agit en tant que client.

1. À l'aide d'un logiciel de gestion de clés externe, vous configurez StorageGRID en tant que client KMS et obtenez un certificat de serveur signé par une autorité de certification, un certificat client public et la clé privée du certificat client.
2. À l'aide du gestionnaire de grille, 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 demande 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 en utilisant la connexion validée.

Types de certificats de serveur pris en charge

Le système StorageGRID prend en charge les certificats personnalisés chiffrés avec RSA ou ECDSA (Elliptic Curve Digital Signature Algorithm).



Le type de chiffrement de la politique de sécurité doit correspondre au type de certificat du serveur. Par exemple, les chiffrements RSA nécessitent des certificats RSA et les chiffrements ECDSA nécessitent des certificats ECDSA. Voir "[Gérer les certificats de sécurité](#)". Si vous configurez une politique de sécurité personnalisée qui n'est pas compatible avec le certificat du serveur, vous pouvez "[revenir temporairement à la politique de sécurité par défaut](#)".

Pour plus d'informations sur la manière dont StorageGRID sécurise les connexions client, consultez "[Sécurité pour les clients S3](#)".

Configurer les certificats de l'interface de gestion

Vous pouvez remplacer le certificat d'interface de gestion par défaut par un seul certificat personnalisé qui permet aux utilisateurs d'accéder au gestionnaire de grille et au gestionnaire de locataires sans rencontrer d'avertissements de sécurité. Vous pouvez également revenir au certificat d'interface de gestion par défaut ou en générer un nouveau.

À propos de cette tâche

Par défaut, chaque nœud d'administration reçoit un certificat signé par l'autorité de certification de la grille. Ces certificats signés par une autorité de certification peuvent être remplacés par un seul certificat d'interface de gestion personnalisé commune et la clé privée correspondante.

Étant donné qu'un seul certificat d'interface de gestion personnalisé est utilisé pour tous les nœuds d'administration, vous devez spécifier le certificat comme certificat générique ou multi-domaine si les clients doivent vérifier le nom d'hôte lors de la connexion au gestionnaire de grille et au gestionnaire de locataires. 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 (CA) que vous utilisez, les utilisateurs peuvent également avoir besoin d'installer le certificat Grid CA dans le navigateur Web qu'ils utiliseront pour accéder au Grid Manager et au Tenant Manager.



Pour garantir que les opérations ne sont pas perturbées 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 voir quand le certificat actuel expire en sélectionnant **CONFIGURATION > Sécurité > Certificats** et en regardant la date d'expiration du certificat de l'interface de gestion dans l'onglet Global.



Si vous accédez au Grid Manager ou au Tenant Manager 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'une des situations suivantes se produit :

- Votre certificat d'interface de gestion personnalisée expire.
- [Toi revenir d'un certificat d'interface de gestion personnalisé au certificat de serveur par défaut .](#)

Ajouter un certificat d'interface de gestion personnalisé

Pour ajouter un certificat d'interface de gestion personnalisé, vous pouvez fournir votre propre certificat ou en générer un à l'aide du gestionnaire de grille.

Étapes

1. Sélectionnez **CONFIGURATION > Sécurité > Certificats**.
2. Dans l'onglet **Global**, sélectionnez **Certificat d'interface de gestion**.
3. Sélectionnez **Utiliser un certificat personnalisé**.
4. Téléchargez 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** : Le fichier de certificat de serveur personnalisé (codé PEM).
- **Clé privée du certificat** : Le fichier de clé privée du certificat du serveur personnalisé(. key).



Les clés privées EC doivent être de 224 bits ou plus. Les clés privées RSA doivent être de 2 048 bits ou plus.

- **CA bundle** : un fichier facultatif unique contenant les certificats de chaque autorité de certification émettrice intermédiaire (CA). Le fichier doit contenir chacun des fichiers de certificat CA codés en PEM, concaténés dans l'ordre de la chaîne de certificats.

c. Développez **Détails du certificat** pour voir 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 bundle CA** pour enregistrer le bundle 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 **Copier le certificat PEM** ou **Copier le bundle CA PEM** pour copier le contenu du certificat afin de le coller ailleurs.

d. Sélectionnez **Enregistrer**. + Le certificat d'interface de gestion personnalisé est utilisé pour toutes les nouvelles connexions ultérieures au Grid Manager, au Tenant Manager, à l'API Grid Manager ou à l'API Tenant Manager.

Générer un certificat

Générer les fichiers de certificat du serveur.



La meilleure pratique pour un environnement de production consiste à utiliser un certificat d'interface de gestion personnalisé signé par une autorité de certification externe.

a. Sélectionnez **Générer un certificat**.

b. Spécifiez les informations du certificat :

Champ	Description
Nom de domaine	Un ou plusieurs noms de domaine entièrement qualifiés à inclure dans le certificat. Utilisez un * comme caractère générique pour représenter plusieurs noms de domaine.

Champ	Description
propriété intellectuelle	Une ou plusieurs adresses IP à inclure dans le certificat.
Sujet (facultatif)	Sujet 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 adresse IP comme nom commun du sujet (CN).
Jours de validité	Nombre de jours après la création pendant lesquels le certificat expire.
Ajouter des extensions d'utilisation de clés	Si cette option est sélectionnée (par défaut et recommandé), les extensions d'utilisation de clé et d'utilisation de clé étendue sont ajoutées au certificat généré. Ces extensions définissent l'objectif de la clé contenue dans le certificat. Remarque : laissez cette case à cocher sélectionnée, sauf si vous rencontrez des problèmes de connexion avec des clients plus anciens lorsque les certificats incluent ces extensions.

c. Sélectionnez **Générer**.

d. Sélectionnez **Détails du certificat** pour voir 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 afin de le coller ailleurs.

e. Sélectionnez **Enregistrer**. + Le certificat d'interface de gestion personnalisé est utilisé pour toutes les nouvelles connexions ultérieures au Grid Manager, au Tenant Manager, à l'API Grid Manager ou à l'API Tenant Manager.

5. Actualisez la page pour vous assurer que le navigateur Web est à jour.



Après avoir téléchargé ou généré un nouveau certificat, prévoyez jusqu'à un jour pour que les alertes d'expiration de certificat associées disparaissent.

6. Une fois que vous avez ajouté un certificat d'interface de gestion personnalisé, la page Certificat d'interface de gestion affiche des informations détaillées sur les certificats en cours d'utilisation. + Vous pouvez télécharger ou copier le certificat PEM selon vos besoins.

Restaurer le certificat d'interface de gestion par défaut

Vous pouvez revenir à l'utilisation du certificat d'interface de gestion par défaut pour les connexions Grid

Étapes

1. Sélectionnez **CONFIGURATION > Sécurité > Certificats**.
2. Dans l'onglet **Global**, sélectionnez **Certificat d'interface de gestion**.
3. Sélectionnez **Utiliser le certificat par défaut**.

Lorsque vous restaurez le certificat d'interface de gestion par défaut, les fichiers de certificat de serveur personnalisé que vous avez configurés sont supprimés et ne peuvent pas être récupérés à partir du système. Le certificat d'interface de gestion par défaut est utilisé pour toutes les nouvelles connexions client ultérieures.

4. Actualisez la page pour vous assurer que le navigateur Web est à jour.

Utiliser 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

- Tu as "[autorisations d'accès spécifiques](#)".
- Vous avez le `Passwords.txt` déposer.

À propos de cette 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. Entrez la commande suivante : `ssh admin@primary_Admin_Node_IP`
 - b. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.
 - c. Entrez la commande suivante pour passer en root : `su -`
 - d. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.

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`.
- Ensemble `--type` à `management` pour configurer le certificat d'interface de gestion, qui est utilisé par Grid Manager et Tenant Manager.
- Par défaut, les certificats générés sont valables 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 lorsque `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 risque de rejeter le certificat.

```
$ sudo make-certificate --domains *.ui.storagegrid.example.com --type  
management --days 720
```

La sortie résultante contient le certificat public nécessaire à votre client API de gestion.

4. Sélectionnez et copiez le certificat.

Incluez les balises BEGIN et END dans votre sélection.

5. Déconnectez-vous de l'interpréteur de commandes. `$ exit`

6. Confirmer que le certificat a été configuré :

- a. Accéder au gestionnaire de grille.
- b. Sélectionnez **CONFIGURATION > Sécurité > Certificats**
- c. Dans l'onglet **Global**, sélectionnez **Certificat d'interface de gestion**.

7. Configurez votre client de gestion pour utiliser le certificat public que vous avez copié. Inclure les balises BEGIN et END.

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 **Certificat d'interface de gestion**.
3. Sélectionnez l'onglet **Serveur** ou **Pack CA**, puis téléchargez ou copiez le certificat.

Télécharger le fichier de certificat ou le bundle CA

Téléchargez le certificat ou le bundle CA .pem déposer. Si vous utilisez un ensemble d'autorités de certification facultatif, chaque certificat de l'ensemble s'affiche dans son propre sous-onglet.

- a. Sélectionnez **Télécharger le certificat** ou **Télécharger le bundle CA**.

Si vous téléchargez un bundle CA, tous les certificats des onglets secondaires du bundle CA sont téléchargés sous forme de fichier unique.

- 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 ou le bundle CA PEM

Copiez le texte du certificat pour le coller ailleurs. Si vous utilisez un ensemble d'autorités de certification facultatif, chaque certificat de l'ensemble s'affiche dans son propre sous-onglet.

- a. Sélectionnez **Copier le certificat PEM** ou **Copier le bundle CA PEM**.

Si vous copiez un bundle d'autorités de certification, tous les certificats des onglets secondaires du bundle d'autorités de certification 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`

Configurer les certificats API S3

Vous pouvez remplacer ou restaurer le certificat de serveur utilisé pour les connexions client S3 aux nœuds de stockage ou aux points de terminaison de l'équilibreur de charge. Le certificat de serveur personnalisé de remplacement est spécifique à votre organisation.



Les détails Swift ont été supprimés de cette version du site de documentation. Voir ["StorageGRID 11.8 : Configurer les certificats API S3 et Swift"](#) .

À propos de cette tâche

Par défaut, chaque nœud de stockage reçoit un certificat de serveur X.509 signé par l'autorité de certification de la grille. Ces certificats signés par une 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 certificat générique ou multi-domaine si les clients doivent vérifier le nom d'hôte lors de la connexion au point de terminaison de stockage. Définissez le certificat personnalisé de sorte qu'il corresponde à tous les nœuds de stockage de la grille.

Une fois la configuration sur le serveur terminée, vous devrez peut-être également installer le certificat Grid CA

dans le client API S3 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 perturbées par un certificat de serveur défaillant, l'alerte **Expiration du certificat de serveur global pour l'API S3** est déclenchée lorsque le certificat du serveur racine est sur le point d'expirer. Si nécessaire, vous pouvez voir quand le certificat actuel expire en sélectionnant **CONFIGURATION > Sécurité > Certificats** et en regardant la date d'expiration du certificat API S3 dans l'onglet Global.

Vous pouvez télécharger ou générer un certificat API S3 personnalisé.

Ajouter un certificat API S3 personnalisé

Étapes

1. Sélectionnez **CONFIGURATION > Sécurité > Certificats**.
2. Dans l'onglet **Global**, sélectionnez **Certificat API S3**.
3. Sélectionnez **Utiliser un certificat personnalisé**.
4. Téléchargez 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** : Le fichier de certificat de serveur personnalisé (codé PEM).
- **Clé privée du certificat** : Le fichier de clé privée du certificat du serveur personnalisé(. key).



Les clés privées EC doivent être de 224 bits ou plus. Les clés privées RSA doivent être de 2 048 bits ou plus.

- **CA bundle** : un fichier facultatif unique contenant les certificats de chaque autorité de certification émettrice intermédiaire. Le fichier doit contenir chacun des fichiers de certificat CA codés 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 personnalisé qui a été 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 bundle CA** pour enregistrer le bundle 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 **Copier le certificat PEM** ou **Copier le bundle CA PEM** pour copier le contenu du certificat afin de le coller ailleurs.

d. Sélectionnez **Enregistrer**.

Le certificat de serveur personnalisé est utilisé pour les nouvelles connexions client S3 ultérieures.

Générer un certificat

Générer les fichiers de certificat du serveur.

a. Sélectionnez **Générer un certificat**.

b. Spécifiez les informations du certificat :

Champ	Description
Nom de domaine	Un ou plusieurs noms de domaine entièrement qualifiés à inclure dans le certificat. Utilisez un * comme caractère générique pour représenter plusieurs noms de domaine.
propriété intellectuelle	Une ou plusieurs adresses IP à inclure dans le certificat.

Champ	Description
Sujet (facultatif)	Sujet 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 adresse IP comme nom commun du sujet (CN).
Jours de validité	Nombre de jours après la création pendant lesquels le certificat expire.
Ajouter des extensions d'utilisation de clés	Si cette option est sélectionnée (par défaut et recommandé), les extensions d'utilisation de clé et d'utilisation de clé étendue sont ajoutées au certificat généré. Ces extensions définissent l'objectif de la clé contenue dans le certificat. Remarque : laissez cette case à cocher sélectionnée, sauf si vous rencontrez des problèmes de connexion avec des clients plus anciens lorsque les certificats incluent ces extensions.

c. Sélectionnez **Générer**.

d. Sélectionnez **Détails du certificat** pour afficher les métadonnées et le PEM du certificat API S3 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 afin de le coller ailleurs.

e. Sélectionnez **Enregistrer**.

Le certificat de serveur personnalisé est utilisé pour les nouvelles connexions client S3 ultérieures.

5. Sélectionnez un onglet pour afficher les métadonnées du certificat de serveur StorageGRID par défaut, d'un certificat signé par une autorité de certification qui a été téléchargé ou d'un certificat personnalisé qui a été généré.



Après avoir téléchargé ou généré un nouveau certificat, prévoyez jusqu'à un jour pour que les alertes d'expiration de certificat associées disparaissent.

6. Actualisez la page pour vous assurer que le navigateur Web est à jour.

7. Après avoir ajouté un certificat API S3 personnalisé, la page de certificat API S3 affiche des informations détaillées sur le certificat API S3 personnalisé en cours d'utilisation. + Vous pouvez télécharger ou copier le certificat PEM selon vos besoins.

Restaurer le certificat API S3 par défaut

Vous pouvez revenir à l'utilisation du certificat API S3 par défaut pour les connexions client S3 aux nœuds de stockage. Cependant, vous ne pouvez pas utiliser le certificat API S3 par défaut pour un point de terminaison d'équilibreur de charge.

Étapes

1. Sélectionnez **CONFIGURATION > Sécurité > Certificats**.
2. Dans l'onglet **Global**, sélectionnez **Certificat API S3**.
3. Sélectionnez **Utiliser le certificat par défaut**.

Lorsque vous restaurez la version par défaut du certificat API S3 global, les fichiers de certificat de serveur personnalisés que vous avez configurés sont supprimés et ne peuvent pas être récupérés à partir du système. Le certificat API S3 par défaut sera utilisé pour les nouvelles connexions client S3 ultérieures aux nœuds de stockage.

4. Sélectionnez **OK** pour confirmer l'avertissement et restaurer le certificat API S3 par défaut.

Si vous disposez de l'autorisation d'accès racine et que le certificat API S3 personnalisé a été utilisé pour les connexions aux points de terminaison de l'équilibreur de charge, une liste des points de terminaison de l'équilibreur de charge qui ne seront plus accessibles à l'aide du certificat API S3 par défaut s'affiche. Aller à ["Configurer les points de terminaison de l'équilibreur de charge"](#) pour modifier ou supprimer les points de terminaison affectés.

5. Actualisez la page pour vous assurer que le navigateur Web est à jour.

Téléchargez ou copiez le certificat API S3

Vous pouvez enregistrer ou copier le contenu du certificat API S3 pour l'utiliser ailleurs.

Étapes

1. Sélectionnez **CONFIGURATION > Sécurité > Certificats**.
2. Dans l'onglet **Global**, sélectionnez **Certificat API S3**.
3. Sélectionnez l'onglet **Serveur** ou **Pack CA**, puis téléchargez ou copiez le certificat.

Télécharger le fichier de certificat ou le bundle CA

Téléchargez le certificat ou le bundle CA .pem déposer. Si vous utilisez un ensemble d'autorités de certification facultatif, chaque certificat de l'ensemble s'affiche dans son propre sous-onglet.

- a. Sélectionnez **Télécharger le certificat** ou **Télécharger le bundle CA**.

Si vous téléchargez un bundle CA, tous les certificats des onglets secondaires du bundle CA sont téléchargés sous forme de fichier unique.

- 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 ou le bundle CA PEM

Copiez le texte du certificat pour le coller ailleurs. Si vous utilisez un ensemble d'autorités de certification facultatif, chaque certificat de l'ensemble s'affiche dans son propre sous-onglet.

- a. Sélectionnez **Copier le certificat PEM** ou **Copier le bundle CA PEM**.

Si vous copiez un bundle d'autorités de certification, tous les certificats des onglets secondaires du bundle d'autorités de certification 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 connexes

- ["Utiliser l'API REST S3"](#)
- ["Configurer les noms de domaine des points de terminaison S3"](#)

Copier le certificat Grid CA

StorageGRID utilise une autorité de certification interne (CA) 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"](#) .
- Tu as ["autorisations d'accès spécifiques"](#) .

À propos de cette tâche

Si un certificat de serveur personnalisé a été configuré, les applications clientes doivent vérifier le serveur à l'aide du certificat de serveur personnalisé. Ils ne doivent pas copier le certificat CA du système StorageGRID .

Étapes

1. Sélectionnez **CONFIGURATION** > **Sécurité** > **Certificats** puis sélectionnez l'onglet **Grid CA**.

2. Dans la section **Certificat PEM**, téléchargez ou copiez le certificat.

Télécharger le fichier de certificat

Télécharger le certificat .pem déposer.

- Sélectionnez **Télécharger le 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`

Copie du certificat PEM

Copiez le texte du certificat pour le coller ailleurs.

- Sélectionnez **Copier le certificat PEM**.
- Collez le certificat copié dans un éditeur de texte.
- Enregistrez le fichier texte avec l'extension .pem .

Par exemple : `storagegrid_certificate.pem`

Configurer les certificats StorageGRID pour FabricPool

Pour les clients S3 qui effectuent une validation stricte du nom d'hôte et ne prennent pas en charge la désactivation de la validation stricte du nom d'hôte, tels que les clients ONTAP utilisant FabricPool, vous pouvez générer ou télécharger un certificat de serveur lorsque vous configurez le point de terminaison de l'équilibreur de charge.

Avant de commencer

- Tu as "[autorisations d'accès spécifiques](#)" .
- Vous êtes connecté au Grid Manager à l'aide d'un "[navigateur Web pris en charge](#)" .

À propos de cette tâche

Lorsque vous créez un point de terminaison d'équilibrage de charge, vous pouvez générer un certificat de serveur auto-signé ou télécharger un certificat signé par une autorité de certification (CA) 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 renouvelés sans interruption. Ils sont également plus sécurisés car ils offrent une meilleure protection contre les attaques de type « man-in-the-middle ».

Les étapes suivantes fournissent des directives générales pour les clients S3 qui utilisent FabricPool. Pour des informations et des procédures plus détaillées, voir "[Configurer StorageGRID pour FabricPool](#)" .

Étapes

- Vous pouvez également configurer un groupe de haute disponibilité (HA) à utiliser par FabricPool .
- Créez un point de terminaison d'équilibrage de charge S3 à utiliser par FabricPool .

Lorsque vous créez un point de terminaison d'équilibrage de charge HTTPS, vous êtes invité à télécharger

votre certificat de serveur, votre clé privée de certificat et votre ensemble d'autorités de certification facultatif.

3. Attachez StorageGRID en tant que niveau cloud dans ONTAP.

Spécifiez le port du point de terminaison de l'équilibreur de charge et le nom de domaine complet utilisé dans le certificat CA que vous avez téléchargé. Ensuite, fournissez le certificat CA.



Si une autorité de certification intermédiaire a émis le certificat StorageGRID, vous devez fournir le certificat de l'autorité de certification intermédiaire. Si le certificat StorageGRID a été émis directement par l'autorité de certification racine, vous devez fournir le certificat de l'autorité de certification racine.

Configurer les certificats clients

Les certificats clients permettent aux clients externes autorisés d'accéder à la base de données StorageGRID Prometheus, offrant ainsi un moyen sécurisé aux outils externes de surveiller 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 du Grid Manager et copier les informations du certificat sur l'outil externe.

Voir "[Gérer les certificats de sécurité](#)" et "[Configurer des certificats de serveur personnalisés](#)".



Pour garantir que les opérations ne sont pas perturbées par un certificat de serveur défaillant, l'alerte **Expiration des certificats clients configurés sur la page Certificats** est déclenchée lorsque ce certificat de serveur est sur le point d'expirer. Si nécessaire, vous pouvez voir quand le certificat actuel expire en sélectionnant **CONFIGURATION > Sécurité > Certificats** et en regardant la date d'expiration du certificat client dans l'onglet Client.



Si vous utilisez un serveur de gestion de clés (KMS) pour protéger les données sur des nœuds d'appliance spécialement configurés, consultez les informations spécifiques sur "[téléchargement d'un certificat client KMS](#)".

Avant de commencer

- Vous disposez de l'autorisation d'accès root.
- 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 d'interface de gestion StorageGRID, vous disposez de l'autorité de certification, du certificat client et de la clé privée utilisés pour configurer le certificat d'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 sauvegardée ou enregistrée au moment de sa création. Si vous ne disposez pas de 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 clients

Pour ajouter le certificat client, utilisez l'une de ces procédures :

- [Certificat d'interface de gestion déjà configuré](#)
- [Certificat client émis par l'AC](#)
- [Certificat généré à partir de 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, d'un certificat client et d'une clé privée fournis par le client.

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 métriques Prometheus à l'aide de votre outil de surveillance externe, sélectionnez **Autoriser Prometheus**.
5. Sélectionnez **Continuer**.
6. Pour l'étape **Joindre les certificats**, téléchargez le certificat de l'interface de gestion.
 - a. Sélectionnez **Télécharger le certificat**.
 - b. Sélectionnez **Parcourir** 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 PEM du certificat.
 - Sélectionnez **Copier le certificat PEM** pour copier le contenu du certificat afin de le coller ailleurs.
 - c. Sélectionnez **Créer** pour enregistrer le certificat dans le gestionnaire de grille.

Le nouveau certificat apparaît dans l'onglet Client.

7. [Configurer un outil de surveillance externe](#), comme Grafana.

Certificat client émis par l'AC

Utilisez cette procédure pour ajouter un certificat client administrateur si aucun certificat d'interface de gestion n'a été configuré et que vous prévoyez d'ajouter un certificat client pour Prometheus qui utilise un certificat client émis par une autorité de certification et une clé privée.

Étapes

1. Effectuez les étapes pour ["configurer 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 métriques Prometheus à l'aide de votre outil de surveillance externe, sélectionnez **Autoriser Prometheus**.
6. Sélectionnez **Continuer**.
7. Pour l'étape **Joindre les certificats**, téléchargez le certificat client, la clé privée et les fichiers du bundle CA :
 - a. Sélectionnez **Télécharger le certificat**.
 - b. Sélectionnez **Parcourir** et sélectionnez le certificat client, la clé privée et les fichiers groupés de l'autorité de certification(.pem).
 - Sélectionnez **Détails du certificat client** pour afficher les métadonnées du certificat et le PEM du certificat.
 - Sélectionnez **Copier le certificat PEM** pour copier le contenu du certificat afin de le coller ailleurs.
 - c. Sélectionnez **Créer** pour enregistrer le certificat dans le gestionnaire de grille.

Les nouveaux certificats apparaissent dans l'onglet Client.

8. [Configurer un outil de surveillance externe](#), comme Grafana.

Certificat généré à partir de Grid Manager

Utilisez cette procédure pour ajouter un certificat client administrateur si aucun certificat d'interface de gestion n'a été configuré et que vous prévoyez d'ajouter un certificat client pour Prometheus qui utilise la fonction de génération de 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 métriques 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 du certificat :
 - **Sujet** (facultatif) : sujet X.509 ou nom distinctif (DN) du propriétaire du certificat.
 - **Jours de validité** : Le nombre de jours pendant lesquels le certificat généré est valide, à compter du moment où il est généré.
 - **Ajouter des extensions d'utilisation de clé** : si cette option est sélectionnée (par défaut et recommandé), les extensions d'utilisation de clé et 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 à cocher sélectionnée, sauf si vous rencontrez des problèmes de connexion avec des clients plus anciens lorsque les certificats incluent ces extensions.

8. Sélectionnez **Générer**.

9. Sélectionnez **Détails du certificat client** pour afficher les métadonnées du certificat et le PEM du certificat.



Vous ne pourrez pas afficher la clé privée du certificat après avoir fermé la boîte de dialogue. Copiez ou téléchargez la clé dans un emplacement sûr.

- Sélectionnez **Copier le certificat PEM** pour copier le contenu du certificat afin de 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 du certificat afin de la coller ailleurs.
- Sélectionnez **Télécharger la clé privée** pour enregistrer la clé privée sous forme de 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 dans 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 un certificat personnalisé**.

14. Téléchargez les fichiers `certificate.pem` et `private_key.pem` depuis le [détails du certificat client](#) étape. Il n'est pas nécessaire de télécharger le bundle CA.

- Sélectionnez **Télécharger le certificat** puis sélectionnez **Continuer**.
- Téléchargez chaque fichier de certificat (`.pem`).
- Sélectionnez **Enregistrer** pour enregistrer le certificat dans le gestionnaire de grille.

Le nouveau certificat apparaît sur la page des certificats de l'interface de gestion.

15. [Configurer un outil de surveillance externe](#), comme Grafana.

Configurer un outil de surveillance externe

Étapes

1. Configurez les paramètres suivants sur votre outil de surveillance externe, tel que Grafana.

- Nom:** Saisissez un nom pour la connexion.

StorageGRID ne nécessite pas ces informations, mais vous devez fournir un nom pour tester la connexion.

- URL:** Saisissez le nom de domaine ou l'adresse IP du nœud d'administration. Spécifiez HTTPS et le port 9091.

Par exemple : `https://admin-node.example.com:9091`

c. Activez **TLS Client Auth** et **Avec certificat CA**.

d. Sous Détails d'authentification TLS/SSL, copiez et collez : +

- L'interface de gestion du certificat CA vers **CA Cert**
- Le certificat client de **Client Cert**
- La clé privée de **Clé client**

e. **ServerName**: saisissez le nom de domaine du nœud d'administration.

ServerName 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 pouvez désormais accéder aux métriques Prometheus depuis StorageGRID avec votre outil de surveillance externe.

Pour plus d'informations sur les mesures, consultez le ["instructions pour la surveillance de StorageGRID"](#).

Modifier les certificats clients

Vous pouvez modifier un certificat client administrateur pour changer son nom, activer ou désactiver l'accès à 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 que vous souhaitez modifier.

3. Sélectionnez **Modifier** puis sélectionnez **Modifier le nom et l'autorisation**

4. Entrez un nom de certificat.

5. Pour accéder aux métriques Prometheus à l'aide de votre outil de surveillance externe, sélectionnez **Autoriser Prometheus**.

6. Sélectionnez **Continuer** pour enregistrer le certificat dans le gestionnaire de grille.

Le certificat mis à jour s'affiche dans l'onglet Client.

Joindre un nouveau certificat client

Vous pouvez 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 que vous souhaitez modifier.
3. Sélectionnez **Modifier** puis sélectionnez une option de modification.

Télécharger le certificat

Copiez le texte du certificat pour le coller ailleurs.

- a. Sélectionnez **Télécharger le certificat** puis sélectionnez **Continuer**.
- b. Télécharger le nom du certificat client(.pem).

Sélectionnez **Détails du certificat client** pour afficher les métadonnées du certificat et le PEM du certificat.

- 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 afin de 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.

Générer un certificat

Générez le texte du certificat à coller ailleurs.

- a. Sélectionnez **Générer un certificat**.
- b. Spécifiez les informations du certificat :

- **Sujet** (facultatif) : sujet X.509 ou nom distinctif (DN) du propriétaire du certificat.
- **Jours de validité** : Le nombre de jours pendant lesquels le certificat généré est valide, à compter du moment où il est généré.
- **Ajouter des extensions d'utilisation de clé** : si cette option est sélectionnée (par défaut et recommandé), les extensions d'utilisation de clé et 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 à cocher sélectionnée, sauf si vous rencontrez des problèmes de connexion avec des clients plus anciens lorsque les certificats incluent ces extensions.

- c. Sélectionnez **Générer**.
- d. Sélectionnez **Détails du certificat client** pour afficher les métadonnées du certificat et le PEM du certificat.



Vous ne pourrez pas afficher la clé privée du certificat après avoir fermé la boîte de dialogue. Copiez ou téléchargez la clé dans un emplacement sûr.

- Sélectionnez **Copier le certificat PEM** pour copier le contenu du certificat afin de 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 du certificat afin de la coller ailleurs.
- Sélectionnez **Télécharger la clé privée** pour enregistrer la clé privée sous forme de 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 dans l'onglet Client.

Télécharger ou copier les certificats clients

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.

Télécharger le fichier de certificat

Télécharger le certificat `.pem` déposer.

- 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

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 clients

Si vous n'avez plus besoin d'un certificat client administrateur, vous pouvez le supprimer.

Étapes

1. Sélectionnez **CONFIGURATION > Sécurité > Certificats** puis sélectionnez l'onglet **Client**.
2. Sélectionnez le certificat que vous souhaitez 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**.

Une fois un certificat supprimé, les clients qui ont utilisé le certificat doivent spécifier un nouveau certificat client pour accéder à la base de données StorageGRID Prometheus.

Configurer les paramètres de sécurité

Gérer la politique TLS et SSH

La politique TLS et SSH détermine les protocoles et chiffrements utilisés pour établir des connexions TLS sécurisées avec les applications clientes et des connexions SSH sécurisées aux services StorageGRID internes.

La politique de sécurité contrôle la manière dont TLS et SSH chiffrent les données en mouvement. En général, utilisez la politique 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 les chiffrements dans ces politiques.

Avant de commencer

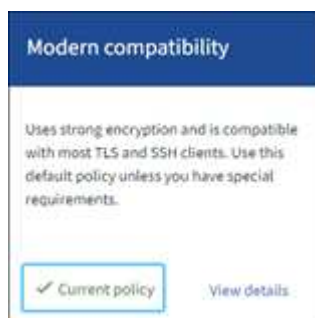
- Vous êtes connecté au Grid Manager à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous avez le ["Autorisation d'accès root"](#).

Sélectionnez une politique de sécurité

Étapes

1. Sélectionnez **CONFIGURATION > Sécurité > Paramètres de sécurité**.

L'onglet **Politiques TLS et SSH** affiche les politiques disponibles. La politique actuellement active est indiquée par une coche verte sur la vignette de la politique.



2. Consultez les tuiles pour en savoir plus sur les politiques disponibles.

Politique	Description
Compatibilité moderne (par défaut)	Utilisez la politique par défaut si vous avez besoin d'un cryptage fort et à moins que vous n'ayez des exigences particulières. Cette politique est compatible avec la plupart des clients TLS et SSH.
Compatibilité héritée	Utilisez cette politique si vous avez besoin d'options de compatibilité supplémentaires pour les clients plus anciens. Les options supplémentaires de cette politique peuvent la rendre moins sécurisée que la politique de compatibilité moderne.
Critères communs	Utilisez cette politique si vous avez besoin d'une certification Critères communs.
FIPS strict	Utilisez cette politique si vous avez besoin d'une certification Common Criteria et devez utiliser le module de sécurité cryptographique NetApp 3.0.8 pour les connexions client externes aux points de terminaison de l'équilibreur de charge, au gestionnaire de locataires et au gestionnaire de grille. L'utilisation de cette politique peut réduire les performances. Remarque : après avoir sélectionné cette politique, tous les nœuds doivent être "redémarré de manière continue" pour activer le module de sécurité cryptographique NetApp . Utilisez Maintenance > Redémarrage progressif pour lancer et surveiller les redémarrages.
Coutume	Créez une politique personnalisée si vous devez appliquer vos propres chiffrements.

3. Pour voir les détails sur les chiffrements, les protocoles et les algorithmes de chaque politique, sélectionnez **Afficher les détails**.

4. Pour modifier la politique actuelle, sélectionnez **Utiliser la politique**.

Une coche verte apparaît à côté de **Politique actuelle** sur la vignette de la politique.

Créer une politique de sécurité personnalisée

Vous pouvez créer une politique personnalisée si vous devez appliquer vos propres chiffrements.

Étapes

1. À partir de la vignette de la politique la plus similaire à la politique personnalisée que vous souhaitez créer, sélectionnez **Afficher les détails**.
2. Sélectionnez **Copier dans le presse-papiers**, puis sélectionnez **Annuler**.



3. Dans la mosaïque **Politique personnalisée**, sélectionnez **Configurer et utiliser**.
4. Collez le JSON que vous avez copié et apportez les modifications nécessaires.
5. Sélectionnez **Utiliser la politique**.

Une coche verte apparaît à côté de **Politique actuelle** sur la mosaïque Politique personnalisée.

6. Vous pouvez également sélectionner **Modifier la configuration** pour apporter d'autres modifications à la nouvelle politique personnalisée.

Revenir temporairement à la politique de sécurité par défaut

Si vous avez configuré une politique de sécurité personnalisée, vous ne pourrez peut-être pas vous connecter au Grid Manager si la politique TLS configurée est incompatible avec la ["certificat de serveur configuré"](#).

Vous pouvez revenir temporairement à la politique de sécurité par défaut.

Étapes

1. Connectez-vous à un nœud d'administration :
 - a. Entrez la commande suivante : `ssh admin@Admin_Node_IP`
 - b. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.
 - c. Entrez la commande suivante pour passer en root : `su -`
 - d. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.

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 au gestionnaire de grille sur le même nœud d'administration.
4. Suivez les étapes dans [Sélectionnez une politique de sécurité](#) pour configurer à nouveau la politique.

Configurer la sécurité du réseau et des objets

Vous pouvez configurer la sécurité du réseau et des objets pour chiffrer les objets stockés, pour empêcher certaines requêtes S3 ou pour autoriser les connexions client aux nœuds de stockage à utiliser HTTP au lieu de HTTPS.

Chiffrement des objets stockés

Le chiffrement des objets stockés permet le chiffrement de toutes les données d'objets lorsqu'elles sont ingérées via S3. Par défaut, les objets stockés ne sont pas chiffrés, mais vous pouvez choisir de crypter les objets à l'aide de l'algorithme de chiffrement AES-128 ou AES-256. Lorsque vous activez le paramètre, tous les objets nouvellement ingérés sont chiffrés, mais aucune modification n'est apportée 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 d'objet stocké s'applique uniquement aux objets S3 qui n'ont pas été chiffrés par un chiffrement au niveau du bucket ou au niveau de l'objet.

Pour plus de détails sur les méthodes de chiffrement StorageGRID, voir ["Examiner les méthodes de chiffrement StorageGRID"](#).

Empêcher la 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.

API REST S3

- Requête DeleteBucket
- Toute demande de modification des données d'un objet existant, des métadonnées définies par l'utilisateur ou du balisage d'un objet S3

Activer HTTP pour les connexions aux nœuds 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 non productive.

Utilisez HTTP pour les connexions aux nœuds de stockage uniquement si les clients S3 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 (car vous pouvez ["configurer chaque point de terminaison de l'équilibreur de charge"](#) (utiliser soit HTTP soit HTTPS)).

Voir ["Résumé : Adresses IP et ports pour les connexions client"](#) pour savoir quels ports les clients S3 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 root.

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 **Aucun** (par défaut) si vous ne souhaitez pas que les objets stockés soient chiffrés, ou sélectionnez **AES-128** ou **AES-256** pour chiffrer les objets stockés.
4. Sélectionnez éventuellement **Empêcher la modification du client** si vous souhaitez empêcher les clients S3 d'effectuer des demandes spécifiques.



Si vous modifiez ce paramètre, l'application du nouveau paramètre prendra environ une minute. La valeur configurée est mise en cache pour les performances et la mise à l'échelle.

5. Sélectionnez éventuellement **Activer HTTP pour les connexions aux nœuds de stockage** si les clients se connectent directement aux nœuds de stockage et que vous souhaitez utiliser des connexions HTTP.



Soyez prudent lorsque vous activez HTTP pour une grille de production car les requêtes seront envoyées non chiffrées.

6. Sélectionnez **Enregistrer**.

Modifier les paramètres de sécurité de l'interface

Les paramètres de sécurité de l'interface vous permettent de contrôler si les utilisateurs sont déconnectés s'ils sont inactifs pendant plus de la durée spécifiée et si une trace de pile est incluse dans les réponses d'erreur d'API.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un ["navigateur Web pris en charge"](#).
- Tu as ["Autorisation d'accès root"](#).

À propos de cette tâche

La page **Paramètres de sécurité** inclut les paramètres **Délai d'inactivité du navigateur** et **Trace de la pile de l'API de gestion**.

Délai d'inactivité du navigateur

Indique combien de temps le navigateur d'un utilisateur peut être inactif avant que l'utilisateur ne soit déconnecté. La valeur par défaut est de 15 minutes.

Le délai d'inactivité du navigateur est également contrôlé par les éléments suivants :

- Un minuteur StorageGRID distinct et non configurable, inclus pour la sécurité du système. 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'expiration 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 SSO est activé et que le navigateur d'un utilisateur expire, l'utilisateur doit ressaisir ses informations d'identification SSO pour accéder à nouveau à StorageGRID. Voir ["Configurer l'authentification unique"](#)

Trace de pile de l'API de gestion

Contrôle si une trace de pile est renvoyée dans les réponses d'erreur de l'API Grid Manager et Tenant Manager.

Cette option est désactivée par défaut, mais vous souhaitez peut-être activer cette fonctionnalité pour un environnement de test. En général, vous devez laisser la trace de pile désactivée dans les environnements de production pour éviter de révéler les détails internes du logiciel lorsque des erreurs d'API se produisent.

Étapes

1. Sélectionnez **CONFIGURATION > Sécurité > Paramètres de sécurité**.
2. Sélectionnez l'onglet **Interface**.
3. Pour modifier le paramètre de délai d'inactivité du navigateur :
 - a. Développez l'accordéon.
 - b. Pour modifier le délai d'expiration, spécifiez une valeur comprise entre 60 secondes et 7 jours. Le délai d'expiration par défaut est de 15 minutes.
 - c. Pour désactiver cette fonctionnalité, décochez la case.
 - d. Sélectionnez **Enregistrer**.

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.

4. Pour modifier le paramètre de la trace de la pile de l'API de gestion :
 - a. Développez l'accordéon.
 - b. Cochez la case pour renvoyer une trace de pile dans les réponses d'erreur de l'API Grid Manager et Tenant Manager.



Laissez la trace de pile désactivée dans les environnements de production pour éviter de révéler les détails internes du logiciel lorsque des erreurs d'API se produisent.

- c. Sélectionnez **Enregistrer**.

Configurer les serveurs de gestion de clés

Qu'est-ce qu'un serveur de gestion de clés (KMS) ?

Un serveur de gestion de 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 d'interopérabilité de gestion de clés (KMIP).

StorageGRID prend en charge uniquement certains serveurs de gestion de clés. Pour obtenir la liste des produits et versions pris en charge, utilisez le "[Outil de matrice d'interopérabilité NetApp \(IMT\)](#)".

Vous pouvez utiliser un ou plusieurs serveurs de gestion de clés pour gérer les clés de chiffrement de nœud pour tous les nœuds d'appliance StorageGRID dont le paramètre **Chiffrement de nœud** est activé lors de l'installation. L'utilisation de serveurs de gestion de clés avec ces nœuds d'appliance vous permet de protéger vos données même si une appliance est supprimée du centre de données. Une fois les volumes de l'appliance

chiffrés, vous ne pouvez accéder à aucune donnée sur l’appliance, sauf si le nœud peut communiquer avec le KMS.



StorageGRID ne crée ni ne gère les clés externes utilisées pour chiffrer et déchiffrer les nœuds de l’appliance. Si vous prévoyez d’utiliser un serveur de gestion de clés externe pour protéger les données StorageGRID , vous devez comprendre comment configurer ce serveur et comment gérer les clés de chiffrement. L’exécution des tâches de gestion des clés dépasse le cadre de ces instructions. Si vous avez besoin d’aide, consultez la documentation de votre serveur de gestion de clés ou contactez le support technique.

Configuration KMS et appliance

Avant de pouvoir utiliser un serveur de gestion de clés (KMS) pour 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 se déroule automatiquement.

L’organigramme montre les étapes de haut niveau pour utiliser un KMS pour sécuriser les données StorageGRID sur les nœuds de l’appliance.

L’organigramme montre la configuration de KMS et la configuration de l’appliance se déroulant en parallèle ; cependant, vous pouvez configurer les serveurs de gestion de clés avant ou après avoir activé le chiffrement des nœuds pour les nouveaux nœuds de l’appliance, en fonction de vos besoins.

Configurer le serveur de gestion des clés (KMS)

La configuration d’un serveur de gestion de clés comprend les étapes de haut niveau suivantes.

Étape	Se référer à
Accédez au logiciel KMS et ajoutez un client pour StorageGRID à chaque KMS ou cluster KMS.	"Configurer StorageGRID en tant que client dans le KMS"
Obtenez les informations requises pour le client StorageGRID sur le KMS.	"Configurer StorageGRID en tant que client dans le KMS"
Ajoutez le KMS au Grid Manager, attribuez-le à un site unique ou à un groupe de sites par défaut, téléchargez les certificats requis et enregistrez la configuration KMS.	"Ajouter un serveur de gestion de clés (KMS)"

Installer l’appareil

La configuration d’un nœud d’appareil pour l’utilisation de KMS comprend les étapes de haut niveau suivantes.

1. Au cours de l’étape de configuration matérielle de l’installation de l’appliance, utilisez le programme d’installation de l’appliance StorageGRID pour activer le paramètre **Chiffrement de nœud** pour l’appliance.



Vous ne pouvez pas activer le paramètre **Chiffrement de nœud** après l'ajout d'un appareil à la grille, et vous ne pouvez pas utiliser la gestion des clés externes pour les appareils sur lesquels 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 de données aléatoire (DEK) est attribuée à chaque volume d'appareil, comme suit :
 - Les DEK sont utilisés pour crypter les données sur chaque volume. Ces clés sont générées à l'aide du chiffrement de disque Linux Unified Key Setup (LUKS) dans le système d'exploitation de l'appliance et ne peuvent pas être modifiées.
 - Chaque DEK individuel est chiffré par une clé de chiffrement à clé principale (KEK). La KEK initiale est une clé temporaire qui crypte les DEK jusqu'à ce que l'appareil puisse se connecter au KMS.
3. Ajoutez le nœud de l'appliance à StorageGRID.

Voir "[Activer le cryptage des nœuds](#)" pour plus de détails.

Processus de cryptage de gestion des clés (se produit automatiquement)

Le chiffrement de gestion des clés comprend les étapes de haut niveau suivantes qui sont exécutées automatiquement.

1. Lorsque vous installez un dispositif sur lequel le chiffrement de nœud est activé dans la grille, 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 sur l'appliance continuent d'être chiffrées 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'appareil utilise la configuration KMS pour se connecter au KMS et demander une clé de chiffrement.
3. Le KMS envoie une clé de chiffrement à l'appareil. La nouvelle clé du KMS remplace la KEK temporaire et est désormais utilisée pour chiffrer et déchiffrer les DEK pour les volumes de l'appliance.



Toutes les données qui existent avant que le nœud de l'appareil chiffré ne se connecte au KMS configuré sont chiffrées avec une clé temporaire. Toutefois, les volumes de l'appareil ne doivent pas être considérés comme protégés contre le retrait du centre de données tant que la clé temporaire n'est pas remplacée par la clé de chiffrement KMS.

4. Si l'appareil est sous tension ou redémarré, il se reconnecte au KMS pour demander la clé. La clé, qui est enregistrée dans la mémoire volatile, ne peut pas survivre à une panne de courant ou à un redémarrage.

Considérations et exigences relatives à l'utilisation d'un serveur de gestion de clés

Avant de configurer un serveur de gestion de clés externe (KMS), vous devez comprendre les considérations et les exigences.

Quelle version de KMIP est prise en charge ?

StorageGRID prend en charge la version 1.4 de KMIP.

"[Spécification du protocole d'interopérabilité de gestion des clés version 1.4](#)"

Quelles sont les considérations relatives au réseau ?

Les paramètres du pare-feu réseau doivent permettre à chaque nœud d'appareil de communiquer via le port utilisé pour les communications du protocole KMIP (Key Management Interoperability Protocol). Le port KMIP par défaut est 5696.

Vous devez vous assurer que chaque nœud d'appliance qui utilise le chiffrement de nœud dispose d'un accès réseau au KMS ou au cluster KMS que vous avez configuré pour le site.

Quelles versions de TLS sont prises en charge ?

Les communications entre les nœuds de l'appliance et le KMS configuré utilisent des connexions TLS sécurisées. StorageGRID peut prendre en charge le protocole TLS 1.2 ou TLS 1.3 lorsqu'il établit des connexions KMIP à un cluster KMS ou KMS, en fonction de ce que le KMS prend en charge et de ce qu'il prend en charge. "[Politique TLS et SSH](#)" vous utilisez.

StorageGRID négocie le protocole et le chiffrement (TLS 1.2) ou la suite de chiffrement (TLS 1.3) avec le KMS lorsqu'il établit la connexion. Pour voir quelles versions de protocole et quels chiffrements/suites de chiffrement sont disponibles, consultez le `tlsOutbound` section de la politique TLS et SSH active de la grille (**CONFIGURATION > Sécurité Paramètres de sécurité**).

Quels appareils sont pris en charge ?

Vous pouvez utiliser un serveur de gestion de clés (KMS) pour gérer les clés de chiffrement de tout dispositif StorageGRID de votre grille sur lequel le paramètre **Chiffrement de nœud** est activé. Ce paramètre ne peut être activé que pendant l'étape de configuration matérielle de l'installation de l'appliance à l'aide du programme d'installation de l'appliance StorageGRID .



Vous ne pouvez pas activer le chiffrement des nœuds après l'ajout d'un appareil à la grille, et vous ne pouvez pas utiliser la gestion des clés externes pour les appareils sur lesquels le chiffrement des nœuds n'est pas activé.

Vous pouvez utiliser le KMS configuré pour les appliances StorageGRID et les nœuds d'appliance.

Vous ne pouvez pas utiliser le KMS configuré pour les nœuds basés sur des logiciels (non-appliances), y compris les suivants :

- Nœuds déployés en tant que machines virtuelles (VM)
- Nœuds déployés dans des moteurs de conteneurs sur des hôtes Linux

Les nœuds déployés sur ces autres plates-formes peuvent utiliser le chiffrement en dehors de StorageGRID au niveau de la banque de données ou du disque.

Quand dois-je configurer les serveurs de gestion de clés ?

Pour une nouvelle installation, vous devez généralement configurer un ou plusieurs serveurs de gestion de clés dans Grid Manager avant de créer des locataires. Cet ordre garantit que les nœuds sont protégés avant que des données d'objet ne soient stockées sur eux.

Vous pouvez configurer les serveurs de gestion de clés dans Grid Manager avant ou après l'installation des nœuds de l'appliance.

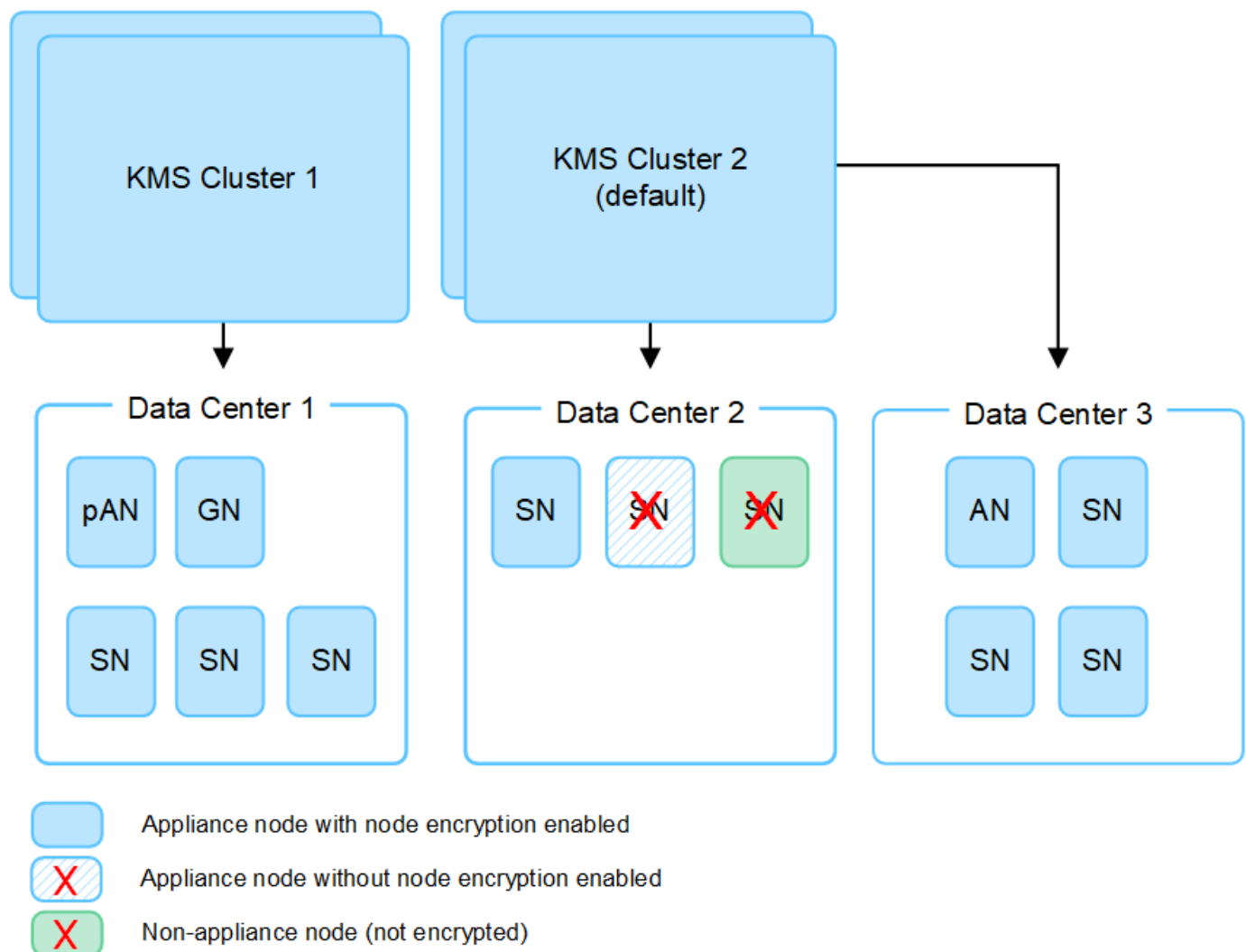
De combien de serveurs de gestion de clés ai-je besoin ?

Vous pouvez configurer un ou plusieurs serveurs de gestion de clés externes pour fournir des clés de chiffrement aux nœuds d'appliance de votre système StorageGRID . Chaque KMS fournit une clé de chiffrement unique aux nœuds de l'appliance StorageGRID sur un site unique ou sur un groupe de sites.

StorageGRID prend en charge l'utilisation de clusters KMS. Chaque cluster KMS contient plusieurs serveurs de gestion de 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 elle améliore les capacités de basculement d'une configuration haute disponibilité.

Par exemple, supposons que votre système StorageGRID dispose de trois sites de centre de données. Vous pouvez configurer un cluster KMS pour fournir une clé à tous les nœuds d'appliance du centre de données 1 et un deuxième cluster KMS pour fournir une clé à tous les nœuds d'appliance de tous les autres sites. Lorsque vous ajoutez le deuxième cluster KMS, vous pouvez configurer un KMS par défaut pour Data Center 2 et Data Center 3.

Notez que vous ne pouvez pas utiliser un KMS pour les nœuds non-appliance ou pour les nœuds d'appliance dont le paramètre **Chiffrement de nœud** n'a pas été activé lors de l'installation.



Que se passe-t-il lorsqu'une clé est tournée ?

En tant que bonne pratique de sécurité, vous devez périodiquement ["faire pivoter la clé de cryptage"](#) utilisé par chaque KMS configuré.

Lorsque la nouvelle version de clé sera disponible :

- Il est automatiquement distribué aux nœuds d'appareils chiffrés sur le ou les sites associés au KMS. La distribution devrait avoir lieu dans l'heure qui suit la rotation de la clé.
- Si le nœud de l'appareil chiffré est hors ligne lorsque la nouvelle version de clé est distribuée, le nœud recevra la nouvelle clé dès son 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 **Échec 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 pour résoudre cette alerte.

Puis-je réutiliser un nœud d'appareil après l'avoir chiffré ?

Si vous devez installer un dispositif chiffré dans un autre système StorageGRID , vous devez d'abord mettre hors service le nœud de grille pour déplacer les données d'objet vers un autre nœud. Ensuite, vous pouvez utiliser le programme d'installation de l'appliance StorageGRID pour ["effacer la configuration KMS"](#) . La suppression de la configuration KMS désactive le paramètre **Chiffrement de nœud** et supprime l'association entre le nœud de l'appliance et la configuration KMS pour le site StorageGRID .



Sans accès à la clé de cryptage KMS, toutes les données restantes sur l'appareil ne sont plus accessibles et sont verrouillées de manière permanente.

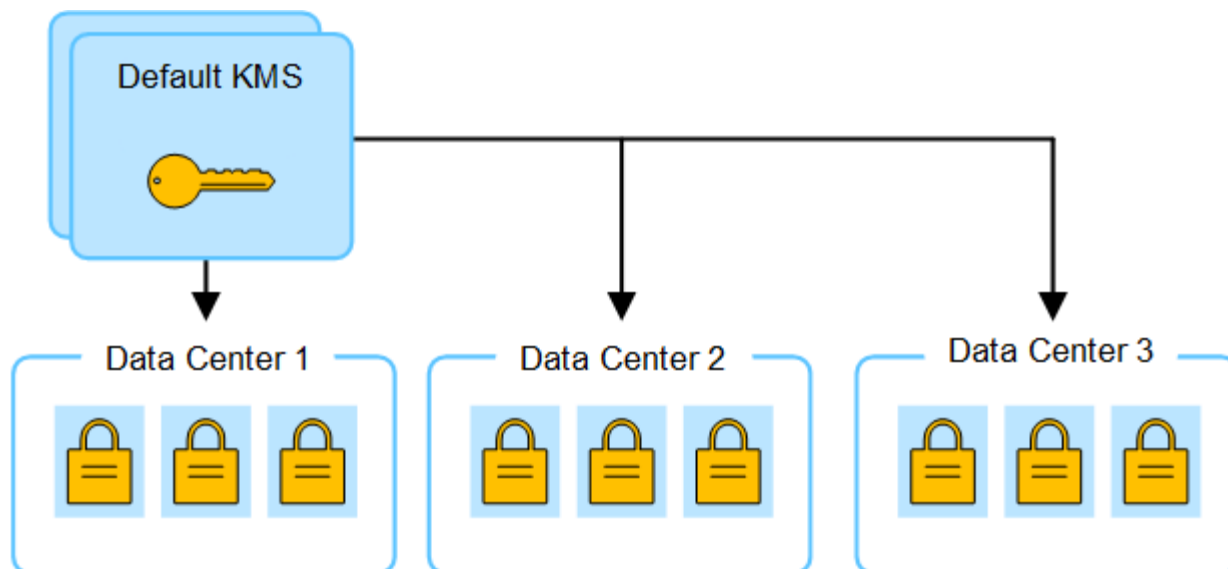
Considérations relatives à la modification du KMS d'un site

Chaque serveur de gestion de clés (KMS) ou cluster KMS fournit une clé de chiffrement à tous les nœuds d'appliance sur un site unique ou sur 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 à un autre.

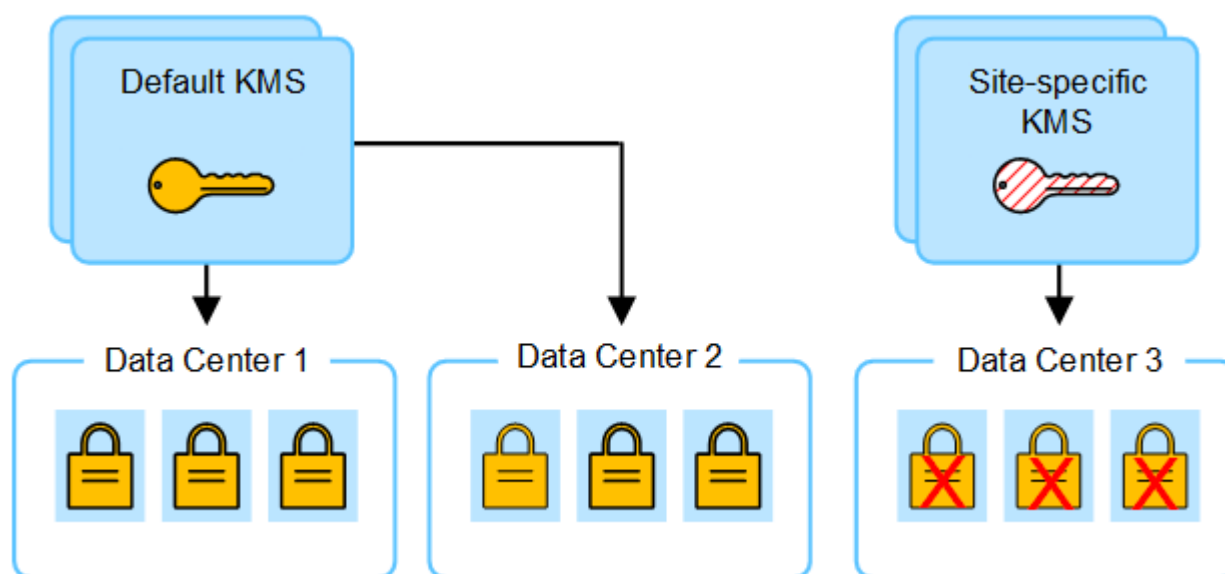
Si vous modifiez le KMS utilisé pour un site, vous devez vous assurer que les nœuds d'appliance précédemment chiffrés sur ce site peuvent être déchiffrés à l'aide de la clé stockée sur le nouveau KMS. Dans certains cas, vous devrez peut-être copier la version actuelle de la clé de chiffrement du KMS d'origine vers le nouveau KMS. Vous devez vous assurer que le KMS dispose de la clé correcte pour déchiffrer les nœuds d'appliance chiffrés sur le site.

Par exemple:

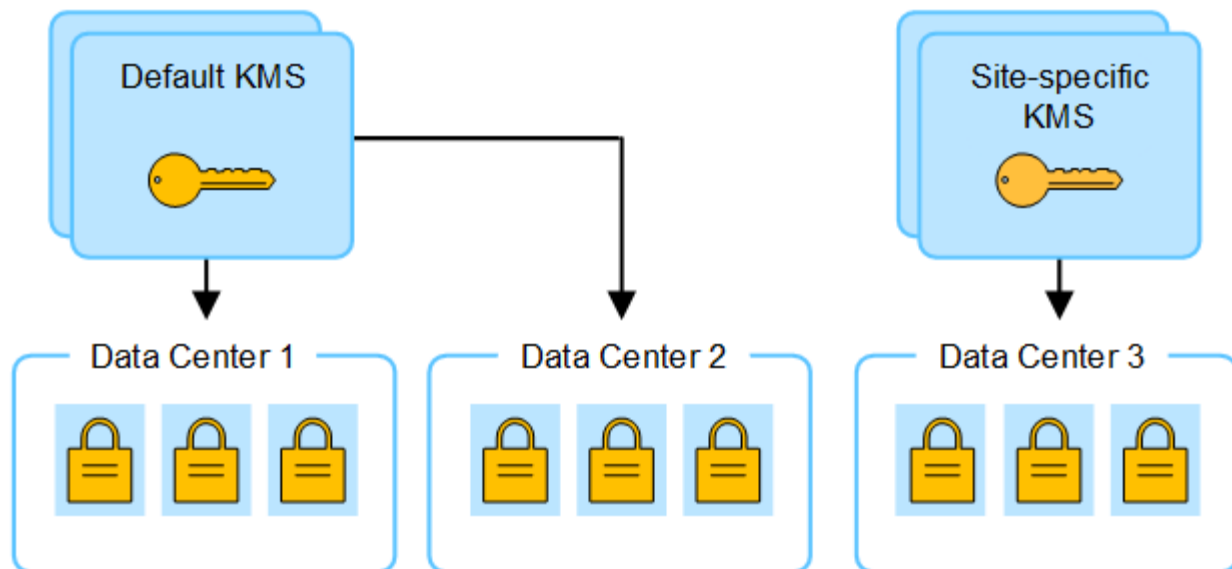
1. Vous configurez initialement un KMS par défaut qui s'applique à tous les sites qui ne disposent pas d'un KMS dédié.
2. Une fois le KMS enregistré, tous les nœuds d'appliance dont le paramètre **Chiffrement de nœud** est activé se connectent au KMS et demandent la clé de chiffrement. Cette clé est utilisée pour crypter les nœuds de l'appliance sur tous les sites. Cette même clé doit également être utilisée pour décrypter ces appareils.



3. Vous décidez d'ajouter un KMS spécifique au site pour un site (Data Center 3 sur la figure). Cependant, étant donné que les nœuds de l'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 déchiffrer les nœuds de ce site.



4. Pour résoudre le problème, copiez la version actuelle de la clé de chiffrement du KMS par défaut vers le nouveau KMS. (Techniquement, vous copiez la clé d'origine sur 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 déchiffrer les nœuds de l'appliance dans le centre de données 3, afin qu'il puisse être enregistré dans StorageGRID.



Cas d'utilisation pour modifier le KMS utilisé pour un site

Le tableau résume les étapes requises pour les cas les plus courants de modification du KMS d'un site.

Cas d'utilisation pour modifier le KMS d'un site	Étapes requises
Vous disposez d'une ou plusieurs entrées KMS spécifiques au site et vous souhaitez utiliser l'une d'entre elles comme KMS par défaut.	Modifier le KMS spécifique au site. Dans le champ Gère les clés pour, sélectionnez Sites non gérés par un autre KMS (KMS par défaut). Le KMS spécifique au site sera désormais utilisé comme KMS par défaut. Cela s'appliquera à tous les sites qui ne disposent pas d'un KMS dédié. "Modifier un serveur de gestion de clés (KMS)"
Vous disposez d'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.	- Si les nœuds de l'appliance sur le 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 du KMS par défaut vers un nouveau KMS. - À l'aide du gestionnaire de grille, ajoutez le nouveau KMS et sélectionnez le site. "Ajouter un serveur de gestion de clés (KMS)"
Vous souhaitez que le KMS d'un site utilise un serveur différent.	- Si les nœuds d'appareils du site ont déjà été chiffrés par le KMS existant, utilisez le logiciel KMS pour copier la version actuelle de la clé de chiffrement du KMS existant vers le nouveau KMS. - À l'aide du gestionnaire de grille, modifiez la configuration KMS existante et entrez le nouveau nom d'hôte ou la nouvelle adresse IP. "Ajouter un serveur de gestion de clés (KMS)"

Configurer StorageGRID en tant que client dans le KMS

Vous devez configurer StorageGRID en tant que client pour chaque serveur de gestion

de clés externe ou cluster KMS avant de pouvoir ajouter le KMS à StorageGRID.



Ces instructions s'appliquent à Thales CipherTrust Manager et Hashicorp Vault. Pour obtenir la liste des produits et versions pris en charge, utilisez le "[Outil de matrice d'interopérabilité NetApp \(IMT\)](#)".

Étapes

1. À partir du logiciel KMS, créez un client StorageGRID pour chaque KMS ou cluster KMS que vous prévoyez d'utiliser.

Chaque KMS gère une clé de chiffrement unique pour les nœuds d'appliances StorageGRID sur un seul site ou sur un groupe de sites.

2. Créez une clé en utilisant l'une des deux méthodes suivantes :
 - Utilisez la page de gestion des clés de votre produit KMS. Créez une clé de chiffrement AES pour chaque KMS ou cluster KMS.

La clé de chiffrement doit être de 2 048 bits ou plus et doit être exportable.

- Demandez à StorageGRID de créer la clé. Vous serez invité à tester et à enregistrer après "[téléchargement de certificats clients](#)".

3. Enregistrez les informations suivantes pour chaque KMS ou cluster 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 chiffrement dans le KMS.

4. Pour chaque KMS ou cluster KMS, obtenez un certificat de serveur signé par une autorité de certification (CA) ou un ensemble de certificats contenant chacun des fichiers de certificat CA codés 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 codé en base 64 (Privacy Enhanced Mail) PEM.
- Le champ Nom alternatif du sujet (SAN) de chaque certificat de serveur doit inclure le nom de domaine complet (FQDN) ou l'adresse IP auquel StorageGRID se connectera.



Lorsque vous configurez le KMS dans StorageGRID, vous devez saisir les mêmes noms de domaine complets ou adresses IP dans le champ **Nom d'hôte**.

- Le certificat du serveur doit correspondre au certificat utilisé par l'interface KMIP du KMS, qui utilise généralement le port 5696.

5. Obtenez le certificat client public émis à StorageGRID par le KMS externe et la clé privée du certificat client.

Le certificat client permet à StorageGRID de s'authentifier auprès du KMS.

Ajouter un serveur de gestion de clés (KMS)

Vous utilisez l'assistant du serveur de gestion de clés StorageGRID pour ajouter chaque KMS ou cluster KMS.

Avant de commencer

- Vous avez examiné le ["considérations et exigences relatives à l'utilisation d'un serveur de gestion de clés"](#) .
- Tu as ["configuré StorageGRID en tant que client dans le KMS"](#) , et vous disposez des informations requises pour chaque KMS ou cluster KMS.
- Vous êtes connecté au Grid Manager à l'aide d'un ["navigateur Web pris en charge"](#) .
- Vous avez le ["Autorisation d'accès root"](#) .

À propos de cette 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, tous les appareils chiffrés par nœud dans la grille seront chiffrés 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 du KMS par défaut vers le nouveau KMS. Voir ["Considérations relatives à la modification du KMS d'un site"](#) pour plus de détails.

Étape 1 : Détails KMS

À l'étape 1 (Détails KMS) de l'assistant Ajouter un serveur de gestion de clés, vous fournissez des détails sur le KMS ou le cluster KMS.

Étapes

1. Sélectionnez **CONFIGURATION > Sécurité > Serveur de gestion des clés**.

La page du serveur de gestion des clés s'affiche avec l'onglet Détails de configuration sélectionné.

2. Sélectionnez **Créer**.

L'étape 1 (détails KMS) de l'assistant Ajouter un serveur de gestion de clés s'affiche.

3. Saisissez les informations suivantes pour le KMS et le client StorageGRID que vous avez configuré dans ce KMS.

Champ	Description
Nom du KMS	Un nom descriptif pour vous aider à identifier ce KMS. Doit comporter entre 1 et 64 caractères.
Nom de la clé	L'alias de clé exact pour le client StorageGRID dans le KMS. Doit comporter entre 1 et 255 caractères. Remarque : si vous n'avez pas créé de clé à l'aide de votre produit KMS, vous serez invité à demander à StorageGRID de créer la clé.

Champ	Description
Gère les clés pour	Le site StorageGRID qui sera associé à ce KMS. Si possible, vous devez configurer 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. • Sélectionnez un site si ce KMS doit gérer 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 ne disposent pas d'un KMS dédié et à tous les sites que vous ajouterez dans les extensions ultérieures. Remarque : une erreur de validation se produit lorsque vous enregistrez la configuration KMS si vous sélectionnez un site qui était précédemment chiffré par le KMS par défaut mais que vous n'avez pas fourni la version actuelle de la clé de chiffrement d'origine au nouveau KMS.
Port	Le port utilisé par le serveur KMS pour les communications du protocole d'interopérabilité de gestion de clés (KMIP). 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 Nom alternatif du sujet (SAN) du certificat du serveur doit inclure le nom de domaine complet ou l'adresse IP que vous saisissez 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 du serveur) de l'assistant Ajouter un serveur de gestion de clés, vous téléchargez le certificat du serveur (ou le groupe de certificats) pour le KMS. Le certificat du serveur permet au KMS externe de s'authentifier auprès de StorageGRID.

Étapes

1. À partir de l'**Étape 2 (Télécharger le certificat du serveur)**, accédez à l'emplacement du certificat de serveur ou du groupe de certificats enregistré.
2. Téléchargez le fichier de certificat.

Les métadonnées du certificat du serveur apparaissent.



Si vous avez téléchargé un ensemble de certificats, les métadonnées de chaque certificat apparaissent sur son propre onglet.

3. Sélectionnez **Continuer**.

Étape 3 : Télécharger les certificats clients

À l'étape 3 (Télécharger les certificats clients) de l'assistant Ajouter un serveur de gestion de 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. À partir de l'**Étape 3 (Télécharger les certificats clients)**, accédez à l'emplacement du certificat client.
2. Téléchargez le fichier de certificat client.

Les métadonnées du certificat client apparaissent.

3. Accédez à l'emplacement de la clé privée du certificat client.
4. Téléchargez le fichier de clé privée.
5. Sélectionnez **Tester et enregistrer**.

Si une clé n'existe pas, vous êtes invité à demander à StorageGRID d'en créer une.

Les connexions entre le serveur de gestion des clés et les nœuds de l'appliance sont testées. Si toutes les connexions sont valides et que la clé correcte est trouvée sur le KMS, le nouveau serveur de gestion de clés est ajouté au tableau sur la page Serveur de gestion de clés.



Immédiatement après avoir ajouté un KMS, l'état du certificat sur la page Serveur de gestion des clés apparaît comme Inconnu. Il faudra peut-être jusqu'à 30 minutes à StorageGRID pour obtenir le statut réel de chaque certificat. Vous devez actualiser votre navigateur Web pour voir l'état actuel.

6. Si un message d'erreur s'affiche lorsque vous sélectionnez **Tester et enregistrer**, vérifiez les détails du message, puis sélectionnez **OK**.

Par exemple, vous pouvez recevoir une erreur 422 : Entité non traitable 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 ne teste pas la connexion externe de chaque appareil à ce KMS. En cas de problème avec la configuration, vous ne pourrez peut-être pas redémarrer les nœuds de l'appliance dont le chiffrement de nœud est activé sur le site concerné. Vous risquez de perdre l'accès à vos données jusqu'à ce que les problèmes soient résolus.

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.

Gérer un KMS

La gestion d'un serveur de gestion de clés (KMS) implique l'affichage ou la modification

des détails, la gestion des certificats, l’affichage des nœuds chiffrés et la suppression d’un KMS lorsqu’il n’est plus nécessaire.

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 requise](#) .

Afficher les détails du KMS

Vous pouvez afficher des informations sur chaque serveur de gestion de clés (KMS) dans votre système StorageGRID , y compris les détails des clés et l’état actuel des certificats serveur et client.

Étapes

1. Sélectionnez **CONFIGURATION > Sécurité > Serveur de gestion des clés**.

La page du serveur de gestion des clés apparaît et affiche les informations suivantes :

- L’onglet Détails de configuration répertorie tous les serveurs de gestion de clés configurés.
 - L’onglet Nœuds chiffrés répertorie tous les nœuds pour lesquels le chiffrement de nœud est activé.
2. Pour afficher les détails d’un KMS spécifique et effectuer des opérations sur ce KMS, sélectionnez le nom du KMS. La page de détails du KMS répertorie les informations suivantes :

Champ	Description
Gère les clés pour	Le 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 de clés, le nom de domaine complet ou l’adresse IP des deux serveurs sont répertoriés. S’il existe plus de deux serveurs de gestion de 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 de 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, sélectionnez un KMS et sélectionnez Modifier ou Actions > Modifier .

3. Sélectionnez un onglet sur la page des détails du KMS pour afficher les informations suivantes :

Langue	Champ	Description
Détails clés	Nom de la clé	L’alias de clé pour le client StorageGRID dans le KMS.

Langue	Champ	Description
Clé UID	L'identifiant unique de la dernière version de la clé.	Dernière modification
La date et l'heure de la dernière version de la clé.	Certificat de serveur	Métadonnées
Les métadonnées du certificat, telles que le numéro de série, la date et l'heure d'expiration et le PEM du certificat.	Certificat PEM	Le contenu du fichier PEM (privacy enhanced mail) pour le certificat.
Certificat client	Métadonnées	Les métadonnées du certificat, telles que le numéro de série, la date et l'heure d'expiration et le PEM du certificat.

4. Aussi souvent que l'exigent les pratiques de sécurité de votre organisation, sélectionnez **Rotate key** ou utilisez le logiciel KMS pour créer une nouvelle version de la clé.

Lorsque la rotation des clés est réussie, les champs UID de la clé et Dernière modification sont mis à jour.



Si vous faites pivoter la clé de chiffrement à l'aide du logiciel KMS, faites-la pivoter de la dernière version utilisée de la clé vers une nouvelle version de la même clé. Ne tournez pas vers une clé entièrement différente.

N'essayez jamais de faire pivoter une clé en modifiant le nom de la clé (alias) pour le KMS. StorageGRID exige que toutes les versions de clés précédemment utilisées (ainsi que toutes les futures) soient accessibles depuis le KMS avec le même alias de clé. Si vous modifiez l'alias de clé d'un KMS configuré, StorageGRID risque de ne pas être en mesure de déchiffrer vos données.

Gérer les certificats

Résolvez rapidement tout problème de certificat de serveur ou de client. Si possible, remplacez les certificats avant leur expiration.



Vous devez résoudre tout problème de certificat dès que possible pour maintenir l'accès aux données.

Étapes

1. Sélectionnez **CONFIGURATION > Sécurité > Serveur de gestion des clés**.
2. Dans le tableau, regardez la valeur d'expiration du certificat pour chaque KMS.
3. Si l'expiration du certificat pour un KMS est inconnue, attendez jusqu'à 30 minutes, puis actualisez votre navigateur Web.

4. Si la colonne Expiration du certificat indique qu'un certificat a expiré ou est sur le point d'expirer, sélectionnez le KMS pour accéder à la page des détails du KMS.
 - a. Sélectionnez **Certificat de serveur** et vérifiez la valeur du champ « Expire le ».
 - b. Pour remplacer le certificat, sélectionnez **Modifier le certificat** pour télécharger un nouveau certificat.
 - c. Répétez ces sous-étapes et sélectionnez **Certificat client** au lieu de Certificat serveur.
5. Lorsque les alertes **Expiration du certificat KMS CA**, **Expiration du certificat client KMS** et **Expiration du certificat serveur KMS** sont déclenchées, notez la description de chaque alerte et effectuez les actions recommandées.

Il faudra peut-être jusqu'à 30 minutes à StorageGRID pour obtenir les mises à jour concernant l'expiration du certificat. Actualisez votre navigateur Web pour voir les valeurs actuelles.



Si vous obtenez le statut **L'état du certificat du serveur est inconnu**, assurez-vous que votre KMS permet d'obtenir un certificat de serveur sans nécessiter de certificat client.

Afficher les nœuds chiffrés

Vous pouvez afficher des informations sur les nœuds d'appliance de votre système StorageGRID sur lesquels le paramètre **Chiffrement de nœud** est activé.

Étapes

1. Sélectionnez **CONFIGURATION > Sécurité > Serveur de gestion des clés**.

La page Serveur de gestion des clés s'affiche. L'onglet Détails de configuration affiche tous les serveurs de gestion de clés qui ont été configurés.

2. En haut de la page, sélectionnez l'onglet **Nœuds chiffrés**.

L'onglet Nœuds chiffrés répertorie les nœuds d'appliance de votre système StorageGRID pour lesquels le paramètre **Chiffrement de nœud** est activé.

3. Consultez les informations du tableau pour chaque nœud d'appareil.

Colonne	Description
Nom du nœud	Le nom du nœud de l'appareil.
Type de nœud	Le type de nœud : Stockage, Admin ou Passerelle.
Site	Le nom du site StorageGRID sur lequel le nœud est installé.
Nom du KMS	Le nom descriptif du KMS utilisé pour le nœud. Si aucun KMS n'est répertorié, sélectionnez l'onglet Détails de configuration pour ajouter un KMS. "Ajouter un serveur de gestion de clés (KMS)"

Colonne	Description
Clé UID	L'ID unique de la clé de chiffrement utilisée pour chiffrer et déchiffrer les données sur le nœud de l'appliance. Pour afficher l'UID d'une clé entière, sélectionnez le texte. Un tiret (--) indique que l'UID de la clé est inconnu, probablement en raison d'un problème de connexion entre le nœud de l'appliance et le KMS.
Statut	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 la connexion après les modifications de la configuration KMS peut prendre plusieurs minutes. Remarque : actualisez votre navigateur Web pour voir les nouvelles valeurs.

4. Si la colonne Statut indique un problème KMS, résolvez le problème immédiatement.

Pendant les opérations KMS normales, le statut sera **Connecté à KMS**. Si un nœud est déconnecté du réseau, l'état de connexion du nœud est affiché (Administrativement hors service ou Inconnu).

D'autres messages d'état correspondent aux alertes StorageGRID portant les mêmes noms :

- Échec du chargement de la configuration KMS
- Erreur de connectivité KMS
- Nom de la clé de chiffrement KMS introuvable
- Échec de la rotation de la clé de chiffrement KMS
- La clé KMS n'a pas réussi à déchiffrer un volume d'appareil
- KMS n'est pas configuré

Effectuez les actions recommandées pour ces alertes.



Vous devez résoudre tout problème immédiatement pour garantir que vos données sont entièrement protégées.

Modifier un KMS

Vous devrez peut-être modifier la configuration d'un serveur de gestion de clés, par exemple, si un certificat est sur le point d'expirer.

Avant de commencer

- Si vous envisagez de mettre à jour le site sélectionné pour un KMS, vous avez examiné les "[considérations pour modifier le KMS d'un site](#)".
- Vous êtes connecté au Grid Manager à l'aide d'un "[navigateur Web pris en charge](#)".
- Vous avez le "[Autorisation d'accès root](#)".

Étapes

1. Sélectionnez **CONFIGURATION > Sécurité > Serveur de gestion des clés**.

La page Serveur de gestion des clés apparaît et affiche tous les serveurs de gestion des clés qui ont été configurés.

- Sélectionnez le KMS que vous souhaitez modifier, puis sélectionnez **Actions > Modifier**.

Vous pouvez également modifier un KMS en sélectionnant le nom du KMS dans le tableau et en sélectionnant **Modifier** sur la page des détails du KMS.

- Vous pouvez également mettre à jour les détails de l'**Étape 1 (Détails KMS)** de l'assistant Modifier un serveur de gestion de clés.

Champ	Description
Nom du KMS	Un nom descriptif pour vous aider à identifier ce KMS. Doit comporter entre 1 et 64 caractères.
Nom de la clé	L'alias de clé exact pour le client StorageGRID dans le KMS. Doit comporter entre 1 et 255 caractères. Vous n'avez besoin de modifier le nom de la clé que 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.
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 du protocole d'interopérabilité de gestion de clés (KMIP). 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 Nom alternatif du sujet (SAN) du certificat du serveur doit inclure le nom de domaine complet ou l'adresse IP que vous saisissez ici. Dans le cas contraire, StorageGRID ne pourra pas se connecter au KMS ou à tous les serveurs d'un cluster KMS.

- Si vous configurez un cluster KMS, sélectionnez **Ajouter un autre nom d'hôte** pour ajouter un nom d'hôte pour chaque serveur du cluster.
- Sélectionnez **Continuer**.

L'étape 2 (Télécharger le certificat du serveur) de l'assistant Modifier un serveur de gestion de clés s'affiche.

6. Si vous devez remplacer le certificat du serveur, sélectionnez **Parcourir** et téléchargez le nouveau fichier.
7. Sélectionnez **Continuer**.

L'étape 3 (Télécharger les certificats clients) de l'assistant Modifier un serveur de gestion de 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'appareil chiffrés sur les sites concernés sont testées. Si toutes les connexions de nœuds sont valides et que la clé correcte est trouvée sur le KMS, le serveur de gestion de clés est ajouté au tableau sur la page Serveur de gestion de clés.

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 non traitable 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 ne teste pas la connexion externe de chaque appareil à ce KMS. En cas de problème avec la configuration, vous ne pourrez peut-être pas redémarrer les nœuds de l'appliance dont le chiffrement de nœud est activé sur le site concerné. Vous risquez de perdre l'accès à vos données jusqu'à ce que les problèmes soient résolus.

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.

Supprimer un serveur de gestion de clés (KMS)

Vous souhaitez peut-être supprimer un serveur de gestion de clés dans certains cas. Par exemple, vous souhaitez peut-être supprimer un KMS spécifique à un site si vous avez mis le site hors service.

Avant de commencer

- Vous avez examiné le ["considérations et exigences relatives à l'utilisation d'un serveur de gestion de clés"](#) .
- Vous êtes connecté au Grid Manager à l'aide d'un ["navigateur Web pris en charge"](#) .
- Vous avez le ["Autorisation d'accès root"](#) .

À propos de cette tâche

Vous pouvez supprimer un KMS dans ces cas :

- Vous pouvez supprimer un KMS spécifique à un site si le site a été mis hors service ou si le site n'inclut aucun nœud d'appliance avec le chiffrement de nœud activé.
- Vous pouvez supprimer le KMS par défaut si un KMS spécifique au site existe déjà pour chaque site disposant de nœuds d'appliance avec chiffrement de nœud activé.

Étapes

1. Sélectionnez **CONFIGURATION > Sécurité > Serveur de gestion des clés**.

La page Serveur de gestion des clés apparaît et affiche tous les serveurs de gestion des clés qui ont été configurés.

2. Sélectionnez le KMS que vous souhaitez supprimer, puis sélectionnez **Actions > Supprimer**.

Vous pouvez également supprimer un KMS en sélectionnant le nom du KMS dans le tableau et en sélectionnant **Supprimer** sur la page des détails du KMS.

3. Confirmez que ce qui suit est vrai :

- Vous supprimez un KMS spécifique au site pour un site qui ne possède aucun nœud d'appliance avec le chiffrement de nœud activé.
- Vous supprimez le KMS par défaut, mais un KMS spécifique au site existe déjà pour chaque site avec chiffrement de nœud.

4. Sélectionnez **Oui**.

La configuration KMS est supprimée.

Gérer les paramètres de proxy

Configurer le 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 points de terminaison S3 externes. Par exemple, vous pourriez avoir besoin d'un proxy non transparent pour permettre l'envoi de messages de services de plateforme à des points de terminaison externes, tels qu'un point de terminaison sur Internet.



Les paramètres de proxy de stockage configurés ne s'appliquent pas aux points de terminaison des services de la plateforme Kafka.

Avant de commencer

- Tu as ["autorisations d'accès spécifiques"](#) .
- Vous êtes connecté au Grid Manager à l'aide d'un ["navigateur Web pris en charge"](#) .

À propos de cette tâche

Vous pouvez configurer les paramètres d'un seul proxy de stockage.

Étapes

1. Sélectionnez **CONFIGURATION > Sécurité > Paramètres proxy**.
2. Dans l'onglet **Stockage**, cochez la case **Activer le proxy de stockage**.
3. Sélectionnez le protocole pour le proxy de stockage.
4. Entrez le nom d'hôte ou l'adresse IP du serveur proxy.
5. Si vous le souhaitez, saisissez le port utilisé pour vous connecter au serveur proxy.

Laissez ce champ vide pour utiliser 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 points de terminaison 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 pour prendre effet.

7. Vérifiez les paramètres de votre serveur proxy pour vous assurer que les messages liés au service de la plateforme provenant de StorageGRID ne seront pas bloqués.
8. Si vous devez désactiver un proxy de stockage, décochez la case et sélectionnez **Enregistrer**.

Configurer les paramètres du proxy d'administration

Si vous envoyez des packages AutoSupport via HTTP ou HTTPS, vous pouvez configurer un serveur proxy non transparent entre les nœuds d'administration et le support technique (AutoSupport).

Pour plus d'informations sur AutoSupport, voir ["Configurer AutoSupport"](#) .

Avant de commencer

- Tu as ["autorisations d'accès spécifiques"](#) .
- Vous êtes connecté au Grid Manager à l'aide d'un ["navigateur Web pris en charge"](#) .

À propos de cette tâche

Vous pouvez configurer les paramètres pour un seul proxy administrateur.

Étapes

1. Sélectionnez **CONFIGURATION > Sécurité > Paramètres proxy**.

La page Paramètres du proxy s'affiche. Par défaut, Stockage est sélectionné dans le menu des onglets.

2. Sélectionnez l'onglet **Admin**.
3. Cochez la case **Activer le proxy administrateur**.
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 un nom d'utilisateur et un mot de passe pour le serveur proxy.

Laissez ces champs vides si votre serveur proxy ne nécessite pas de nom d'utilisateur ou de mot de passe.

7. Sélectionnez l'une des options suivantes :

- Si vous souhaitez sécuriser la connexion au proxy administrateur, sélectionnez **Vérifier le certificat proxy**. Téléchargez un bundle CA pour vérifier l'authenticité des certificats SSL présentés par le serveur proxy d'administration.



AutoSupport à la demande, AutoSupport de la série E via StorageGRID et la détermination du chemin de mise à jour sur la page de mise à niveau de StorageGRID ne fonctionneront pas si un certificat proxy est vérifié.

Une fois le bundle CA téléchargé, ses métadonnées s'affichent.

- Si vous ne souhaitez pas valider les certificats lors de la communication avec le serveur proxy d'administration, sélectionnez **Ne pas vérifier le certificat proxy**.

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 pour prendre effet.

9. Si vous devez désactiver le proxy d'administration, décochez la case **Activer le proxy d'administration**, puis sélectionnez **Enregistrer**.

Contrôler les pare-feu

Contrôler l'accès au 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 sur les nœuds d'administration StorageGRID en ouvrant ou en fermant des ports spécifiques au niveau du pare-feu externe. Par exemple, vous souhaitez peut-être empêcher les locataires de se connecter au 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, consultez ["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 de l'API de gestion peuvent accéder au gestionnaire de grille, à l'API de gestion de grille, au gestionnaire de locataires et à l'API de gestion de locataires. Remarque : le port 443 est également utilisé pour certains trafics internes.
8443	Port Grid Manager restreint sur les nœuds d'administration	• Les navigateurs Web et les clients de l'API de gestion peuvent accéder au Grid Manager et à l'API de gestion de grille à l'aide de HTTPS. • Les navigateurs Web et les clients de l'API de gestion ne peuvent pas accéder au gestionnaire de locataires ni à l'API de gestion des locataires. • Les demandes de contenu interne seront rejetées.

Port	Description	Si le port est ouvert...
9443	Port du gestionnaire de locataires restreint sur les nœuds d'administration	• Les navigateurs Web et les clients de l'API de gestion peuvent accéder au gestionnaire de locataires et à l'API de gestion des locataires à l'aide de HTTPS. • Les navigateurs Web et les clients de l'API de gestion ne peuvent pas accéder au gestionnaire de grille ou à l'API de gestion de grille. • Les demandes de contenu interne seront rejetées.



L'authentification unique (SSO) n'est pas disponible sur les ports restreints Grid Manager ou Tenant Manager. Vous devez utiliser le port HTTPS par défaut (443) si vous souhaitez que les utilisateurs s'authentifient avec l'authentification unique.

Informations connexes

- ["Sign in au gestionnaire de grille"](#)
- ["Créer un compte locataire"](#)
- ["Communications externes"](#)

Gérer les contrôles du pare-feu interne

StorageGRID inclut 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 que vous effectuez 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 spécifier si un nœud approuve le trafic entrant provenant du réseau client.

Les paramètres de cet onglet remplacent les paramètres de l'onglet Gérer l'accès externe.

- Un nœud avec un réseau client non approuvé acceptera uniquement les connexions sur les ports de point de terminaison de l'équilibreur de charge configurés sur ce nœud (points de terminaison globaux, d'interface de nœud et de type de nœud).
- Les ports de point de terminaison de l'équilibreur de charge *sont les seuls ports ouverts* sur les réseaux clients non approuvés, quels que soient les paramètres de l'onglet Gérer les réseaux externes.

- Lorsqu'ils sont approuvés, tous les ports ouverts sous l'onglet Gérer l'accès externe sont accessibles, ainsi que tous les points de terminaison d'équilibrage de charge ouverts sur le réseau client.



Les paramètres que vous définissez sur un onglet peuvent affecter les modifications d'accès que vous effectuez sur un autre onglet. Assurez-vous de vérifier les paramètres de tous les onglets pour vous assurer que votre réseau se comporte comme vous l'attendez.

Pour configurer les contrôles du pare-feu interne, voir ["Configurer les contrôles du pare-feu"](#) .

Pour plus d'informations sur les pare-feu externes et la sécurité du réseau, consultez ["Contrôler l'accès au 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 auxquelles l'accès aux ports de grille fermés est accordé. 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-grille). Ces deux onglets peuvent souvent être utilisés ensemble pour personnaliser l'accès réseau exact dont vous avez besoin pour autoriser votre grille.



Les adresses IP privilégiées n'ont pas d'accès au port de grille interne par défaut.

Exemple 1 : Utiliser un hôte de saut pour les tâches de maintenance

Supposons que vous souhaitiez utiliser un hôte de saut (un hôte renforcé en termes de sécurité) pour l'administration du réseau. Vous pouvez utiliser ces étapes générales :

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, sauf si leur adresse IP a 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 saut pour effectuer des tâches de maintenance sur votre réseau de manière plus sécurisée.

Exemple 2 : Verrouiller les ports sensibles

Supposons que vous souhaitiez 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 l'accès à tous les ports attribués pour accéder à Grid Manager et Tenant Manager (les ports prédéfinis sont 443 et 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.

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'où provient la demande.

Exemple 3 : 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, pour bloquer le trafic client HTTP S3, vous utiliseriez le bouton bascule de l'onglet Gérer l'accès externe pour bloquer le port 18084.

Onglet Réseaux de clients non approuvés

Si vous utilisez un réseau client, vous pouvez contribuer à sécuriser StorageGRID contre les attaques hostiles en acceptant le trafic client entrant uniquement sur les points de terminaison explicitement configurés.

Par défaut, le réseau client sur chaque nœud de grille est *fiable*. Autrement dit, par défaut, StorageGRID approuve les connexions entrantes vers chaque nœud de grille sur tous les [ports externes disponibles](#).

Vous pouvez réduire la menace d'attaques hostiles sur votre système StorageGRID en spécifiant que le réseau client sur chaque nœud doit être *non fiable*. Si le réseau client d'un nœud n'est pas approuvé, le nœud accepte uniquement les connexions entrantes sur les ports explicitement configurés comme points de terminaison d'équilibrage de charge. Voir ["Configurer les points de terminaison de l'équilibreur de charge"](#) et ["Configurer les contrôles du pare-feu"](#).

Exemple 1 : le nœud de passerelle accepte uniquement les requêtes HTTPS S3

Supposons que vous souhaitiez qu'un nœud de passerelle refuse tout le trafic entrant sur le réseau client, à l'exception des requêtes HTTPS S3. Vous effectueriez ces étapes générales :

1. De la ["Points de terminaison de l'équilibreur de charge"](#) page, configurez un point de terminaison d'équilibrage de charge pour S3 via HTTPS sur le port 443.
2. Dans la page de contrôle du pare-feu, sélectionnez Non approuvé pour spécifier que le réseau client sur le nœud de passerelle n'est pas approuvé.

Une fois votre configuration enregistrée, tout le trafic entrant sur le réseau client du nœud de passerelle est supprimé, à l'exception des requêtes HTTPS S3 sur le port 443 et des requêtes d'écho ICMP (ping).

Exemple 2 : Le nœud de stockage envoie des demandes de services de la 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 vers ce nœud de stockage sur le réseau client. Vous effectueriez cette étape générale :

- Dans l'onglet Réseaux clients non approuvés de la page de contrôle du pare-feu, indiquez que le réseau client sur le nœud de stockage n'est pas approuvé.

Une fois votre configuration enregistrée, le nœud de stockage n'accepte plus aucun trafic entrant sur le réseau client, mais il continue d'autoriser les demandes sortantes vers les destinations des 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 de Grid Manager uniquement sur un sous-réseau spécifique. Vous effectuerez les étapes suivantes :

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 approuvé.
3. Lorsque vous créez un point de terminaison d'équilibrage de charge d'interface de gestion, entrez le port et sélectionnez l'interface de gestion à laquelle le port accédera.
4. Sélectionnez **Oui** pour le réseau client non approuvé.
5. Utilisez l'onglet Gérer l'accès externe pour bloquer tous les ports externes (avec ou sans adresses IP privilégiées définies pour les hôtes en dehors de ce sous-réseau).

Une fois votre configuration enregistrée, seuls les hôtes du sous-réseau que vous avez spécifié peuvent accéder au gestionnaire de grille. 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](#) .
- Tu as [autorisations d'accès spécifiques](#) .
- Vous avez examiné les informations contenues dans ["Gérer les contrôles du pare-feu"](#) et ["Directives de mise en réseau"](#) .
- Si vous souhaitez qu'un nœud d'administration ou un nœud de passerelle accepte le trafic entrant uniquement sur des points de terminaison explicitement configurés, vous avez défini les points de terminaison de l'équilibreur de charge.



Lors de la modification de la configuration du réseau client, les connexions client existantes peuvent échouer si les points de terminaison de l'équilibreur de charge n'ont pas été configurés.

À propos de cette tâche

StorageGRID inclut un pare-feu interne sur chaque nœud qui vous permet d'ouvrir ou de fermer certains des ports sur les nœuds de votre grille. Vous pouvez utiliser les onglets de contrôle du pare-feu pour ouvrir ou fermer les ports ouverts par défaut sur le réseau de grille, le réseau d'administration et le réseau client. Vous pouvez également créer une liste d'adresses IP privilégiées pouvant accéder aux ports de grille fermés. Si vous utilisez un réseau client, vous pouvez spécifier si un nœud approuve le trafic entrant provenant du réseau client et vous pouvez configurer l'accès de ports spécifiques sur le réseau client.

Limiter le nombre de ports ouverts aux adresses IP en dehors de votre réseau à ceux qui sont absolument nécessaires améliore la sécurité de votre réseau. 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, y compris des exemples, consultez ["Gérer les contrôles du pare-feu"](#) .

Pour plus d'informations sur les pare-feu externes et la sécurité du réseau, consultez ["Contrôler l'accès au pare-feu externe"](#) .

Contrôles du pare-feu d'accès

Étapes

1. Sélectionnez **CONFIGURATION > Sécurité > Contrôle du pare-feu**.

Les trois onglets de cette page sont décrits dans "[Gérer les contrôles du 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 que vous apportez 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 les paramètres de l'onglet Gérer l'accès externe.

Les adresses IP privilégiées et les sous-réseaux n'ont pas d'accès au réseau interne par défaut. De plus, les points de terminaison de l'équilibreur de charge et les ports supplémentaires ouverts dans l'onglet Liste d'adresses privilégiées sont accessibles même s'ils sont 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 auquel vous souhaitez accorder l'accès aux ports fermés.
2. Vous pouvez également sélectionner **Ajouter une autre adresse IP ou un autre sous-réseau en notation CIDR** pour ajouter des clients privilégiés supplémentaires.



Ajoutez le moins d'adresses possible à la liste privilégiée.

3. Si vous le souhaitez, sélectionnez ***Autoriser les adresses IP privilégiées à accéder aux ports internes de StorageGRID ***. Voir "[Ports internes StorageGRID](#)".



Cette option supprime certaines protections pour les services internes. Laissez-le désactivé si possible.

4. Sélectionnez **Enregistrer**.

Gérer les accès externes

Lorsqu'un port est fermé dans l'onglet Gérer l'accès externe, le port n'est pas accessible par une adresse IP non-grille, sauf si vous ajoutez 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 avec tous les ports externes (ports accessibles par défaut par les nœuds non-grille) pour les nœuds de votre grille.
2. Configurez les ports que vous souhaitez ouvrir et fermer à l'aide des options suivantes :
 - Utilisez le bouton bascule à côté 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 443 ou 8443 de Grid Manager, 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 sur le côté droit du tableau pour vous assurer d'avoir visualisé tous les ports disponibles. Utilisez le champ de recherche pour trouver les paramètres de n'importe quel port externe en saisissant un numéro de port. Vous pouvez saisir un numéro de port partiel. Par exemple, si vous entrez un **2**, tous les ports dont le nom contient la chaîne « 2 » sont affichés.

3. Sélectionnez **Enregistrer**

Réseau de clients non fiables

Si le réseau client d'un nœud n'est pas approuvé, le nœud accepte uniquement le trafic entrant sur les ports configurés comme points de terminaison d'équilibrage 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 des 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 que vous effectuez 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 la valeur par défaut du nouveau nœud, spécifiez le paramètre par défaut à utiliser lorsque de nouveaux nœuds sont ajoutés à la grille dans le cadre d'une procédure d'extension.
 - **Fiable** (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 dans votre système StorageGRID .

3. Utilisez les options suivantes pour sélectionner les nœuds qui doivent autoriser les connexions client uniquement sur les points de terminaison d'équilibrage de charge explicitement configurés ou sur des ports sélectionnés supplémentaires :

- Sélectionnez **Ne pas faire confiance aux nœuds affichés** pour ajouter tous les nœuds affichés dans le tableau à la liste des réseaux clients non approuvés.
- Sélectionnez **Faire confiance aux nœuds affichés** pour supprimer tous les nœuds affichés dans le tableau de la liste Réseau client non approuvé.
- Utilisez le bouton bascule à côté de chaque nœud pour définir le réseau client comme approuvé ou non approuvé pour le nœud sélectionné.

Par exemple, vous pouvez sélectionner **Ne pas faire confiance aux nœuds affichés** pour ajouter tous les nœuds à la liste des réseaux clients non approuvés, puis utiliser le bouton bascule à côté d'un nœud individuel pour ajouter ce nœud unique à la liste des réseaux clients approuvés.



Utilisez la barre de défilement sur le côté droit du tableau pour vous assurer d'avoir visualisé tous les nœuds disponibles. Utilisez le champ de recherche pour trouver les paramètres de n'importe quel nœud en saisissant le nom du nœud. Vous pouvez saisir un nom partiel. Par exemple, si vous entrez un **GW**, tous les nœuds dont le nom contient la chaîne « GW » sont affichés.

4. Sélectionnez **Enregistrer**.

Les nouveaux paramètres du pare-feu sont immédiatement appliqués et mis en œuvre. Les connexions client existantes peuvent échouer si les points de terminaison de l'équilibreur de charge n'ont pas été configurés.

Gérer les locataires

Que sont les comptes locataires ?

Un compte locataire vous permet d'utiliser l'API REST Simple Storage Service (S3) pour stocker et récupérer des objets dans un système StorageGRID .



Les détails Swift ont été supprimés de cette version du site de documentation. Voir ["StorageGRID 11.8 : Gérer les locataires"](#) .

En tant qu'administrateur de grille, vous créez et gérez les comptes locataires que les clients S3 utilisent pour stocker et récupérer des objets.

Chaque compte locataire dispose de groupes fédérés ou locaux, d'utilisateurs, de compartiments S3 et d'objets.

Les comptes locataires peuvent être utilisés pour séparer les objets stockés par différentes entités. Par exemple, plusieurs comptes locataires peuvent être utilisés pour l'un ou l'autre de ces cas d'utilisation :

- **Cas d'utilisation d'entreprise** : si vous administrez un système StorageGRID dans une application d'entreprise, vous souhaitez peut-être séparer le stockage d'objets de la grille par les différents services de votre organisation. Dans ce cas, vous pouvez créer des comptes locataires pour le service marketing,

le service d'assistance client, le service des ressources humaines, etc.



Si vous utilisez le protocole client S3, vous pouvez utiliser des buckets S3 et des stratégies de bucket pour séparer les objets entre les services d'une entreprise. Vous n'avez pas besoin d'utiliser des comptes locataires. Voir les instructions de mise en œuvre "[Buckets S3 et politiques de buckets](#)" pour plus d'informations.

- **Cas d'utilisation du fournisseur de services** : si vous administrez un système StorageGRID en tant que fournisseur de services, vous pouvez séparer le stockage d'objets de la grille par les différentes entités qui loueront le stockage sur votre grille. Dans ce cas, vous créeriez des comptes locataires pour la société A, la société B, la société C, etc.

Pour plus d'informations, consultez la section "[Utiliser un compte locataire](#)".

Comment créer un compte locataire ?

Utilisez le gestionnaire de grille pour créer un compte locataire. Lorsque vous créez un compte locataire, vous spécifiez les informations suivantes :

- Informations de base, notamment le nom du locataire, le type de client (S3) et le quota de stockage facultatif.
- Autorisations pour le compte locataire, par exemple si le compte locataire peut utiliser les services de la plateforme S3, configurer sa propre source d'identité, utiliser S3 Select ou utiliser une connexion de fédération de grille.
- L'accès root initial pour le locataire, selon que le système StorageGRID utilise des groupes et des utilisateurs locaux, une fédération d'identité ou une authentification unique (SSO).

De plus, vous pouvez activer le paramètre de verrouillage d'objet S3 pour le système StorageGRID si les comptes de locataire S3 doivent se conformer aux exigences réglementaires. Lorsque le verrouillage d'objet S3 est activé, tous les comptes de locataire S3 peuvent créer et gérer des compartiments conformes.

À quoi sert Tenant Manager ?

Après avoir créé le compte locataire, les utilisateurs locataires peuvent se connecter au gestionnaire de locataires pour effectuer des tâches telles que les suivantes :

- Configurer la fédération d'identité (sauf si la source d'identité est partagée avec la grille)
- Gérer les groupes et les utilisateurs
- Utiliser la fédération de grille pour le clonage de compte et la réplication inter-grille
- Gérer les clés d'accès S3
- Créer et gérer des buckets S3
- Utiliser les services de la plateforme S3
- Utiliser S3 Select
- Surveiller l'utilisation du stockage



Bien que les utilisateurs de locataires S3 puissent créer et gérer des clés d'accès et des compartiments S3 avec Tenant Manager, ils doivent utiliser une application cliente S3 pour ingérer et gérer des objets. Voir "[Utiliser l'API REST S3](#)" pour plus de détails.

Créer un compte locataire

Vous devez créer au moins un compte locataire pour contrôler l'accès au stockage dans votre système StorageGRID .

Les étapes de création d'un compte locataire varient selon que ["fédération d'identité"](#) et ["authentification unique"](#) sont configurés et si le compte Grid Manager que vous utilisez pour créer le compte locataire appartient à un groupe d'administrateurs avec l'autorisation d'accès root.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un ["navigateur Web pris en charge"](#) .
- Vous avez le ["Accès root ou autorisation des comptes locataires"](#) .
- Si le compte locataire doit utiliser la source d'identité configurée pour le gestionnaire de grille et que vous souhaitez accorder l'autorisation d'accès racine pour le compte locataire à un groupe fédéré, vous devez importer ce groupe fédéré dans le gestionnaire de grille. Vous n'avez pas besoin d'attribuer des autorisations Grid Manager à ce groupe d'administrateurs. Voir ["Gérer les groupes d'administrateurs"](#) .
- Si vous souhaitez autoriser un locataire S3 à cloner des données de compte et à répliquer des objets de compartiment sur une autre grille à l'aide d'une connexion de fédération de grille :
 - Tu as ["configuré la connexion à la fédération de grille"](#) .
 - Le statut de la connexion est **Connecté**.
 - Vous disposez de l'autorisation d'accès root.
 - Vous avez examiné les considérations relatives à ["gérer les locataires autorisés pour la fédération du réseau"](#) .
 - Si le compte locataire doit utiliser la source d'identité configurée pour Grid Manager, vous avez importé le même groupe fédéré dans Grid Manager sur les deux grilles.

Lorsque vous créez le locataire, vous sélectionnez ce groupe pour disposer de l'autorisation d'accès racine initiale pour les comptes de locataire source et de destination.



Si ce groupe d'administrateurs n'existe pas sur les deux grilles avant la création du locataire, le locataire n'est pas répliqué vers la destination.

Accéder à l'assistant

Étapes

1. Sélectionnez **LOCATAIRES**.
2. Sélectionnez **Créer**.

Entrez les détails

Étapes

1. Saisissez les détails du locataire.

Champ	Description
Nom	Un nom pour le compte locataire. Les noms des locataires n'ont pas besoin d'être uniques. Lorsque le compte locataire est créé, il reçoit un identifiant 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, utilisez éventuellement ce champ pour vous aider à identifier quel est le locataire source et quel est le locataire de destination. Par exemple, cette description pour un locataire créé sur la grille 1 apparaîtra également pour le locataire répliqué sur 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 ou Swift. Remarque : la prise en charge des applications clientes Swift est obsolète et sera supprimée dans une prochaine version.
Quota de stockage (facultatif)	Si vous souhaitez que ce locataire dispose d'un quota de stockage, une valeur numérique pour le quota et les unités.

2. Sélectionnez **Continuer**.

Sélectionner les autorisations

Étapes

1. Vous pouvez également sélectionner les autorisations de base que vous souhaitez attribuer à ce locataire.



Certaines de ces autorisations ont des exigences supplémentaires. Pour plus de détails, sélectionnez l'icône d'aide pour chaque autorisation.

Autorisation	Si sélectionné...
Autoriser les services de la plateforme	Le locataire peut utiliser les services de la plateforme S3 tels que CloudMirror. Voir " Gérer les services de plateforme pour les comptes locataires S3 ".
Utiliser sa propre source d'identité	Le locataire peut configurer et gérer sa propre source d'identité pour les groupes et utilisateurs fédérés. Cette option est désactivée si vous avez " SSO configuré " pour votre système StorageGRID.
Autoriser la sélection S3	Le locataire peut émettre des requêtes API S3 SelectObjectContent pour filtrer et récupérer les données d'objet. Voir "Gérer S3 Select pour les comptes locataires". Important : les demandes 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.

2. Vous pouvez également sélectionner les autorisations avancées que vous souhaitez accorder à ce locataire.

Autorisation	Si sélectionné...
Connexion à la fédération de réseau	Le locataire peut utiliser une connexion de fédération de grille, qui : • Fait en sorte que ce locataire et tous les groupes de locataires et utilisateurs ajoutés au compte soient clonés de cette grille (la <i>grille source</i>) vers l'autre grille de la connexion sélectionnée (la <i>grille de destination</i>). • Permet à ce locataire de configurer la réplication inter-grille entre les buckets correspondants sur chaque grille. Voir "Gérer les locataires autorisés pour la fédération de réseau".
Verrouillage d'objet S3	Autoriser le locataire à utiliser des fonctionnalités spécifiques de S3 Object Lock : • Définir la période de conservation maximale définit la durée pendant laquelle les nouveaux objets ajoutés à ce bucket doivent être conservés, à compter du moment où ils sont ingérés. • Le mode de conformité autorisé empêche les utilisateurs d'écraser ou de supprimer les versions d'objets protégées pendant la période de conservation.

3. Sélectionnez **Continuer**.

Définir l'accès root et créer un locataire

Étapes

1. Définissez l'accès root pour le compte locataire, selon que votre système StorageGRID utilise la fédération d'identité, l'authentification unique (SSO) ou les deux.

Option	Fais ceci
Si la fédération d'identité n'est pas activée	Spécifiez le mot de passe à utiliser lors de la connexion au locataire en tant qu'utilisateur root local.
Si la fédération d'identité est activée	a. Sélectionnez un groupe fédéré existant pour disposer de l'autorisation d'accès root pour le locataire. b. Vous pouvez également spécifier le mot de passe à utiliser lors de la connexion au locataire en tant qu'utilisateur root local.
Si la fédération d'identité et l'authentification unique (SSO) sont activées	Sélectionnez un groupe fédéré existant pour disposer de l'autorisation d'accès root pour le locataire. Aucun utilisateur local ne peut se connecter.

2. Sélectionnez **Créer un locataire**.

Un message de réussite s'affiche et le nouveau locataire est répertorié sur la page Locataires. Pour savoir

comment afficher les détails des locataires et surveiller leur activité, consultez ["Surveiller l'activité des locataires"](#) .



L'application des paramètres du locataire sur la grille peut prendre 15 minutes ou plus en fonction de la connectivité réseau, de l'état du nœud et des opérations Cassandra.

3. Si vous avez sélectionné l'autorisation **Utiliser la connexion à la fédération de grille** pour le locataire :

- a. Confirmez qu'un locataire identique a été répliqué sur l'autre grille dans la connexion. Les locataires des deux grilles auront le même identifiant de compte à 20 chiffres, le même nom, la même description, le même quota et les mêmes autorisations.



Si vous voyez le message d'erreur « Locataire créé sans clone », reportez-vous aux instructions de ["Résoudre 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, ["changer le mot de passe de l'utilisateur root local"](#) pour le locataire répliqué.



Un utilisateur root local ne peut pas se connecter à Tenant Manager sur la grille de destination tant que le mot de passe n'est pas modifié.

Sign in au locataire (facultatif)

Si nécessaire, vous pouvez vous connecter au nouveau locataire maintenant pour terminer la configuration, ou vous pouvez vous connecter au locataire ultérieurement. Les étapes de connexion dépendent du fait que vous soyez connecté au Grid Manager à l'aide du port par défaut (443) ou d'un port restreint. Voir ["Contrôler l'accès au pare-feu externe"](#) .

Sign in maintenant

Si vous utilisez...	Fais ceci...
Port 443 et vous définissez un mot de passe pour l'utilisateur root local	1. Sélectionnez * Sign in en tant que root*. Lorsque vous vous connectez, des liens s'affichent pour configurer les buckets, la fédération d'identité, les groupes et les utilisateurs. 2. Sélectionnez les liens pour configurer le compte locataire. Chaque lien ouvre la page correspondante dans le gestionnaire de locataires. Pour compléter la page, voir le "instructions d'utilisation des comptes locataires" .
Port 443 et vous n'avez pas défini de mot de passe pour l'utilisateur root local	Sélectionnez * Sign in* et saisissez les informations d'identification d'un utilisateur dans le groupe fédéré d'accès racine.

Si vous utilisez...	Fais ceci...
Un port restreint	1. Sélectionnez Terminer 2. Sélectionnez Restreint dans le tableau Locataire pour en savoir plus sur l'accès à ce compte locataire. L'URL du Tenant Manager a ce format : <pre>https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id/</pre> ◦ `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'identifiant de compte unique du locataire

Sign in plus tard

Si vous utilisez...	Faites l'une de ces choses...
Port 443	• Depuis le Gestionnaire de grille, sélectionnez LOCATAIRES, puis sélectionnez * Sign in* à droite du nom du locataire. • Saisissez l'URL du locataire dans un navigateur Web : <pre>https://FQDN_or_Admin_Node_IP/?accountId=20-digit-account-id/</pre> ◦ `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'identifiant de compte unique du locataire
Un port restreint	• Depuis le gestionnaire de grille, sélectionnez LOCATAIRES, puis Restreint. • Saisissez l'URL du locataire dans un navigateur Web : <pre>https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id</pre> ◦ `FQDN_or_Admin_Node_IP` est un nom de domaine complet ou l'adresse IP d'un nœud d'administration ◦ `port` est le port restreint réservé aux locataires ◦ `20-digit-account-id` est l'identifiant de compte unique du locataire

Configurer le locataire

Suivez les instructions dans "[Utiliser un compte locataire](#)" pour gérer les groupes de locataires et les utilisateurs, les clés d'accès S3, les buckets, les services de plateforme, le clonage de compte et la réplication inter-grille.

Modifier le compte locataire

Vous pouvez modifier un compte locataire pour modifier le nom d’affichage, le quota de stockage ou les autorisations du locataire.



Si un locataire dispose de l’autorisation **Utiliser la connexion à la fédération de grille**, vous pouvez modifier les détails du locataire à partir de l’une ou l’autre des grilles de la connexion. Cependant, toutes les modifications que vous apportez sur une grille de la connexion ne seront pas copiées sur l’autre grille. Si vous souhaitez que les détails du locataire soient exactement synchronisés entre les grilles, effectuez les mêmes modifications sur les deux grilles. Voir ["Gérer les locataires autorisés pour la connexion à la fédération de réseau"](#).

Avant de commencer

- Vous êtes connecté au Grid Manager à l’aide d’un ["navigateur Web pris en charge"](#).
- Vous avez le ["Accès root ou autorisation des comptes locataires"](#).



L’application des paramètres du locataire sur la grille peut prendre 15 minutes ou plus en fonction de la connectivité réseau, de l’état du nœud et des opérations Cassandra.

Étapes

1. Sélectionnez **LOCATAIRES**.

Tenants							
View information for each tenant account. Depending on the timing of ingests, network connectivity, and node status, the usage data shown might be out of date. To view more recent values, select the tenant name.							
Create	Export to CSV	Actions ▾	Search tenants by name or ID		Displaying 5 results		
☐	Name ? ↕	Logical space used ? ↕	Quota utilization ? ↕	Quota ? ↕	Object count ? ↕	Sign in/Copy URL ?	
☐	Tenant 01	2.00 GB	10%	20.00 GB	100	→ 📄	
☐	Tenant 02	85.00 GB	85%	100.00 GB	500	→ 📄	
☐	Tenant 03	500.00 TB	50%	1.00 PB	10,000	→ 📄	
☐	Tenant 04	475.00 TB	95%	500.00 TB	50,000	→ 📄	
☐	Tenant 05	5.00 GB	—	—	500	→ 📄	

2. Localisez le compte locataire que vous souhaitez modifier.

Utilisez le champ de recherche pour rechercher un locataire par nom ou par ID de locataire.

3. Sélectionnez le locataire. Vous pouvez effectuer l’une des opérations suivantes :
 - Cochez la case correspondant au locataire, puis sélectionnez **Actions > Modifier**.
 - Sélectionnez le nom du locataire pour afficher la page de détails et sélectionnez **Modifier**.
4. Vous pouvez également modifier les valeurs de ces champs :

- **Nom**
- **Description**
- **Quota de stockage**

5. Sélectionnez **Continuer**.

6. Sélectionnez ou effacez les autorisations pour le compte locataire.

- Si vous désactivez les **services de plateforme** pour un locataire qui les utilise déjà, les services qu'il a configurés pour ses compartiments S3 cesseront de fonctionner. Aucun message d'erreur n'est envoyé au locataire. Par exemple, si le locataire a configuré la réplication CloudMirror pour un bucket S3, il peut toujours stocker des objets dans le bucket, mais les copies de ces objets ne seront plus effectuées dans le bucket S3 externe qu'il a configuré comme point de terminaison. Voir "[Gérer les services de plateforme pour les comptes locataires S3](#)".
- Modifiez le paramètre **Utiliser sa propre source d'identité** pour déterminer si le compte de locataire utilisera sa propre source d'identité ou la source d'identité configurée pour le gestionnaire de grille.

Si **Utiliser sa propre source d'identité** est :

- Désactivé et sélectionné, le locataire a déjà activé sa propre source d'identité. Un locataire doit désactiver sa source d'identité avant de pouvoir utiliser la source d'identité configurée pour Grid Manager.
- Désactivé et non sélectionné, SSO est activé pour le système StorageGRID . Le locataire doit utiliser la source d'identité qui a été configurée pour le gestionnaire de grille.
- Sélectionnez ou désactivez l'autorisation **Autoriser la sélection S3** selon vos besoins. Voir "[Gérer S3 Select pour les comptes locataires](#)".
- Pour supprimer l'autorisation **Utiliser la connexion à la fédération de grille** :
 - Sélectionnez l'onglet **Fédération de grille**.
 - Sélectionnez **Supprimer l'autorisation**.
- Pour ajouter l'autorisation **Utiliser la connexion à la fédération de grille** :
 - Sélectionnez l'onglet **Fédération de grille**.
 - Cochez la case **Utiliser la connexion à la fédération de grille**.
 - Vous pouvez également sélectionner **Cloner les utilisateurs et groupes locaux existants** pour les cloner sur la grille distante. Si vous le souhaitez, vous pouvez arrêter le clonage en cours ou réessayer le clonage si certains utilisateurs ou groupes locaux n'ont pas pu être clonés après la fin de la dernière opération de clonage.
- Pour définir une période de conservation maximale ou autoriser le mode de conformité :



Le verrouillage d'objet S3 doit être activé sur la grille avant de pouvoir utiliser ces paramètres.

- Sélectionnez l'onglet **Verrouillage d'objet S3**.
- Pour **Définir la période de conservation maximale**, saisissez une valeur et sélectionnez la période dans le menu déroulant.
- Pour **Autoriser le mode de conformité**, cochez la case.

Modifier le mot de passe de l'utilisateur root local du locataire

Vous devrez peut-être modifier le mot de passe de l'utilisateur root local d'un locataire si l'utilisateur root est exclu du compte.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un ["navigateur Web pris en charge"](#).
- Tu as ["autorisations d'accès spécifiques"](#).

À propos de cette tâche

Si l'authentification unique (SSO) est activée pour votre système StorageGRID, l'utilisateur root local ne peut pas se connecter au compte locataire. Pour effectuer des tâches d'utilisateur root, les utilisateurs doivent appartenir à un groupe fédéré disposant de l'autorisation d'accès root pour le locataire.

Étapes

1. Sélectionnez **LOCATAIRES**.

Tenants							
View information for each tenant account. Depending on the timing of ingests, network connectivity, and node status, the usage data shown might be out of date. To view more recent values, select the tenant name.							
Create	Export to CSV	Actions ▾	Search tenants by name or ID		Displaying 5 results		
☐	Name ? ↕	Logical space used ? ↕	Quota utilization ? ↕	Quota ? ↕	Object count ? ↕	Sign in/Copy URL ?	
☐	Tenant 01	2.00 GB	10%	20.00 GB	100	→ 📄	
☐	Tenant 02	85.00 GB	85%	100.00 GB	500	→ 📄	
☐	Tenant 03	500.00 TB	50%	1.00 PB	10,000	→ 📄	
☐	Tenant 04	475.00 TB	95%	500.00 TB	50,000	→ 📄	
☐	Tenant 05	5.00 GB	—	—	500	→ 📄	

2. Sélectionnez le compte locataire. Vous pouvez effectuer l'une des opérations suivantes :
 - Cochez la case correspondant au 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 locataire.
4. Sélectionnez **Enregistrer**.

Supprimer le compte locataire

Vous pouvez supprimer un compte locataire si vous souhaitez supprimer définitivement l'accès du locataire au système.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un ["navigateur Web pris en charge"](#) .
- Tu as ["autorisations d'accès spécifiques"](#) .
- Vous avez supprimé tous les compartiments et objets S3 associés au compte locataire.
- Si le locataire est autorisé à utiliser une connexion à une fédération de réseau, vous avez examiné les considérations relatives à ["suppression d'un locataire avec l'autorisation Utiliser la connexion à la fédération de grille"](#) .

Étapes

1. Sélectionnez **LOCATAIRES**.
2. Localisez le ou les comptes locataires que vous souhaitez supprimer.

Utilisez le champ de recherche pour rechercher un locataire par nom ou par ID de 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, puis sélectionnez **Actions > Supprimer**.
 - Sélectionnez le nom du locataire pour afficher la page de détails, puis sélectionnez **Actions > Supprimer**.
5. Sélectionnez **Oui**.

Gérer les services de la plateforme

Que sont les services de plateforme ?

Les services de la plateforme incluent la réplication CloudMirror, les notifications d'événements et le service d'intégration de recherche.

Si vous activez les services de plateforme pour les comptes de locataire S3, vous devez configurer votre grille afin que les locataires puissent accéder aux ressources externes nécessaires pour utiliser ces services.

Réplication CloudMirror

Le service de réplication StorageGRID CloudMirror est utilisé pour mettre en miroir des objets spécifiques d'un bucket StorageGRID vers une destination externe spécifiée.

Par exemple, vous pouvez utiliser la réplication CloudMirror pour mettre en miroir des enregistrements clients spécifiques dans Amazon S3, puis exploiter les services AWS pour effectuer des analyses sur vos données.



La réplication CloudMirror présente certaines similitudes et différences importantes avec la fonctionnalité de réplication inter-grille. Pour en savoir plus, voir ["Comparer la réplication inter-grille et la réplication CloudMirror"](#) .



La réplication CloudMirror n'est pas prise en charge si le verrouillage d'objet S3 est activé pour le compartiment source.

Notifications

Les notifications d'événements par compartiment sont utilisées pour envoyer des notifications sur des actions spécifiques effectuées sur des objets à un cluster Kafka externe spécifié ou à Amazon Simple Notification

Service.

Par exemple, vous pouvez configurer des alertes à envoyer aux administrateurs pour chaque objet ajouté à un bucket, où les objets représentent des fichiers journaux associés à un événement système critique.



Bien que la notification d'événement puisse être configurée sur un bucket avec le verrouillage d'objet S3 activé, les métadonnées du verrouillage d'objet S3 (y compris la date de conservation et le statut 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.

Par exemple, vous pouvez configurer vos buckets pour envoyer des métadonnées d'objet S3 à un service Elasticsearch distant. Vous pouvez ensuite utiliser Elasticsearch pour effectuer des recherches dans plusieurs compartiments et effectuer des analyses sophistiquées des modèles présents dans les métadonnées de votre objet.



Bien que l'intégration Elasticsearch puisse être configurée sur un bucket avec S3 Object Lock activé, les métadonnées S3 Object Lock (y compris la date de conservation et le statut de conservation légale) des objets ne seront pas incluses dans les messages de notification.

Les services de plateforme offrent aux locataires la possibilité 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 est généralement externe à votre déploiement StorageGRID, vous devez décider si vous souhaitez autoriser les locataires à utiliser ces services. Si vous le faites, vous devez activer l'utilisation des services de plateforme lorsque vous créez ou modifiez des comptes locataires. Vous devez également configurer votre réseau de manière à ce que les messages des services de plateforme générés par les locataires puissent atteindre leurs destinations.

Recommandations pour l'utilisation des services de la plateforme

Avant d'utiliser les services de la plateforme, tenez compte des recommandations suivantes :

- Si le contrôle de version et la réplication CloudMirror sont activés pour un compartiment S3 du système StorageGRID, vous devez également activer le contrôle de version du compartiment S3 pour le point de terminaison de destination. Cela permet à la réplication CloudMirror de générer des versions d'objet similaires sur le point de terminaison.
- Vous ne devez pas utiliser plus de 100 locataires actifs avec des requêtes S3 nécessitant une réplication CloudMirror, des notifications et une intégration de recherche. Avoir plus de 100 locataires actifs peut entraîner des performances client S3 plus lentes.
- Les demandes adressées à un point de terminaison qui ne peuvent pas être traitées seront mises en file d'attente jusqu'à un maximum de 500 000 demandes. Cette limite est partagée équitablement 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 injustement pénalisés.

Informations connexes

- ["Gérer les services de la plateforme"](#)
- ["Configurer les paramètres du proxy de stockage"](#)

- ["Surveiller StorageGRID"](#)

Réseau et ports pour les services de la plateforme

Si vous autorisez un locataire S3 à utiliser les services de plateforme, vous devez configurer la mise en réseau de la grille pour garantir que les messages des services de plateforme peuvent être livrés à leurs destinations.

Vous pouvez activer les services de plateforme pour un compte locataire S3 lorsque vous créez ou mettez à jour le compte locataire. Si les services de plateforme sont activés, le locataire peut créer des points de terminaison qui servent de destination pour la réplication CloudMirror, les notifications d'événements ou les 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 points de terminaison de destination.

Par exemple, les locataires peuvent configurer les types de points de terminaison de destination suivants :

- Un cluster Elasticsearch hébergé localement
- Une application locale qui prend en charge la réception de messages Amazon Simple Notification Service
- Un cluster Kafka hébergé localement
- Un bucket S3 hébergé localement sur la même instance ou sur une autre instance de StorageGRID
- Un point de terminaison externe, tel qu'un point de terminaison sur Amazon Web Services.

Pour garantir que les messages des services de plateforme peuvent être délivrés, vous devez configurer le 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 plateforme aux points de terminaison de destination.

Par défaut, les messages des services de la plateforme sont envoyés sur les ports suivants :

- **80** : pour les URI de point de terminaison commençant par http (la plupart des points de terminaison)
- **443** : pour les URI de point de terminaison commençant par https (la plupart des points de terminaison)
- **9092** : pour les URI de point de terminaison commençant par http ou https (points de terminaison Kafka uniquement)

Les locataires peuvent spécifier un port différent lorsqu'ils créent ou modifient un point de terminaison.



Si un déploiement StorageGRID est utilisé comme destination pour la réplication CloudMirror, les messages de réplication peuvent être reçus sur un port autre que 80 ou 443. Assurez-vous que le port utilisé pour S3 par le déploiement StorageGRID de destination est spécifié dans le point de terminaison.

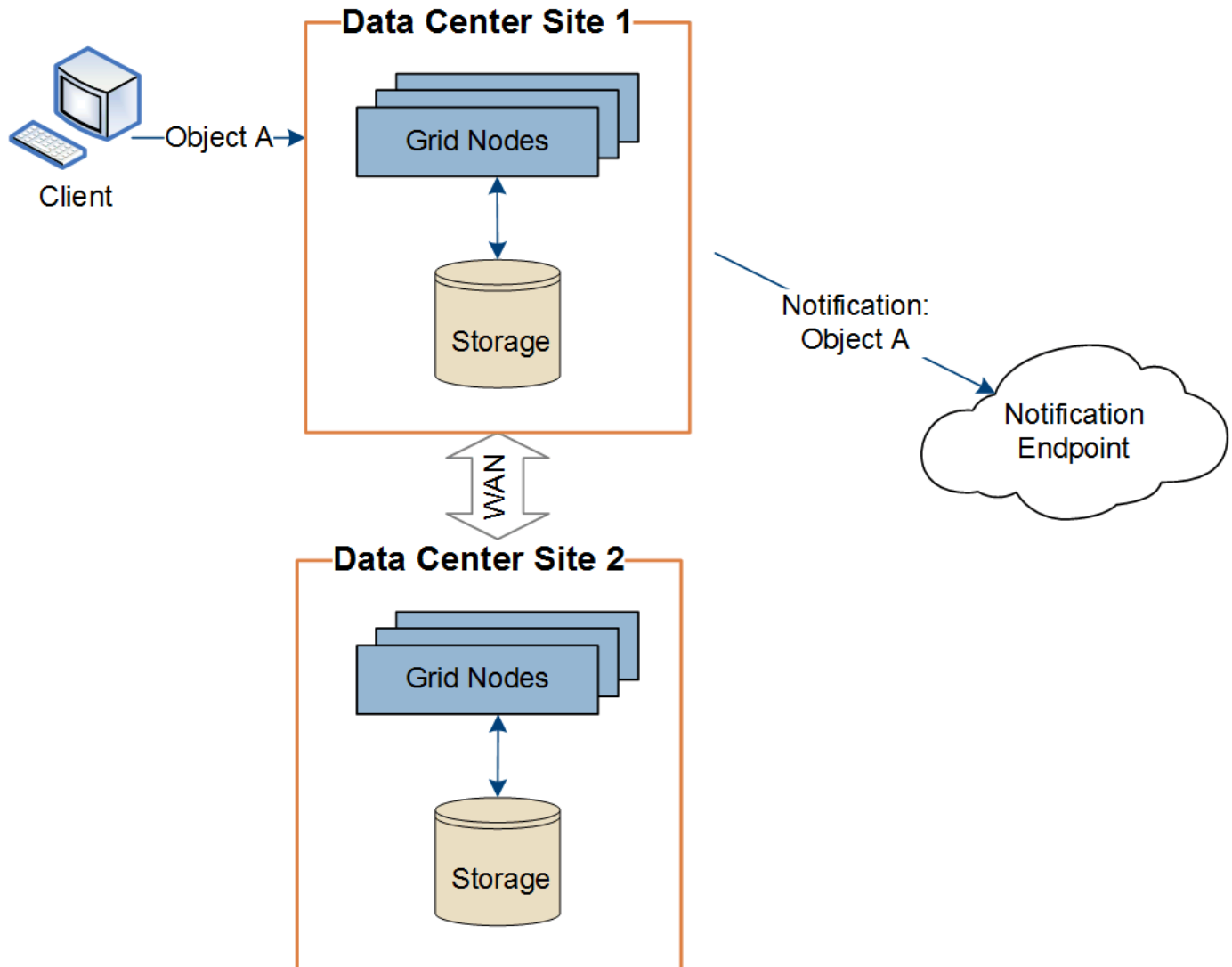
Si vous utilisez un serveur proxy non transparent, vous devez également ["configurer les paramètres du proxy de stockage"](#) pour permettre l'envoi de messages à des points de terminaison externes, tels qu'un point de terminaison sur Internet.

Informations connexes

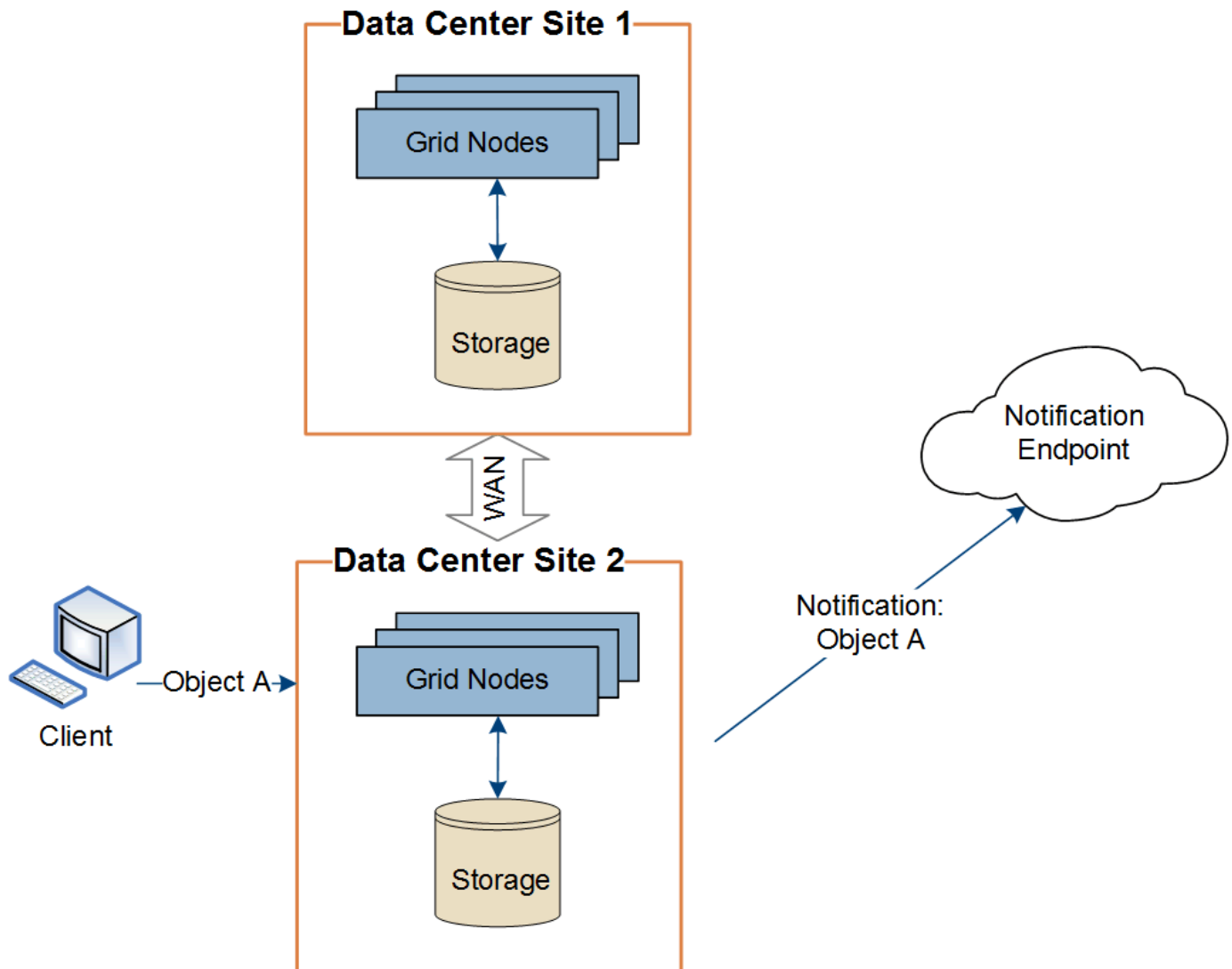
["Utiliser un compte locataire"](#)

Toutes les opérations de services de la plateforme sont effectuées site par site.

Autrement dit, 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 1 du centre de données, la notification concernant cette action est déclenchée et envoyée depuis le site 1 du centre de données.



Si le client effectue ensuite une opération de suppression d'API S3 sur ce même objet à partir du site de centre de données 2, la notification concernant l'action de suppression est déclenchée et envoyée à partir du site de centre de données 2.



Assurez-vous que le réseau de chaque site est configuré de manière à ce que les messages des services de la plateforme puissent être délivrés à leurs destinations.

Dépanner les services de la plateforme

Les points de terminaison utilisés dans les services de plateforme sont créés et gérés par les utilisateurs locataires dans le gestionnaire de locataires. Toutefois, si un locataire rencontre des problèmes lors de la configuration ou de l'utilisation des services de plateforme, vous pouvez peut-être utiliser le gestionnaire de grille pour vous aider à résoudre le problème.

Problèmes avec les nouveaux points de terminaison

Avant qu'un locataire puisse utiliser les services de la plateforme, il doit créer un ou plusieurs points de terminaison à l'aide du gestionnaire de locataires. Chaque point de terminaison représente une destination externe pour un service de plateforme, tel qu'un bucket StorageGRID S3, un bucket Amazon Web Services, une rubrique Amazon Simple Notification Service, une rubrique Kafka ou un cluster Elasticsearch hébergé localement ou sur AWS. Chaque point de terminaison inclut 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 point de terminaison, le système StorageGRID valide que le point de terminaison existe et qu'il peut être atteint à l'aide des informations d'identification spécifiées. La connexion au point de terminaison est validée à partir d'un nœud sur chaque site.

Si la validation du point de terminaison échoue, un message d'erreur explique pourquoi la validation du point de terminaison a échoué. L'utilisateur locataire doit résoudre le problème, puis essayer à nouveau de créer le point de terminaison.



La création du point de terminaison échouera si les services de plateforme ne sont pas activés pour le compte locataire.

Problèmes avec les points de terminaison existants

Si une erreur se produit lorsque StorageGRID tente d'atteindre un point de terminaison existant, un message s'affiche sur le tableau de bord dans le gestionnaire de locataires.

 One or more endpoints have experienced an error and might not be functioning properly. Go to the [Endpoints](#) page to view the error details. The last error occurred 2 hours ago.

Les utilisateurs locataires peuvent accéder à la page Points de terminaison pour consulter le message d'erreur le plus récent pour chaque point de terminaison et déterminer depuis combien de temps l'erreur s'est produite. La colonne **Dernière erreur** affiche le message d'erreur le plus récent pour chaque point de terminaison et indique depuis combien de temps l'erreur s'est produite. Les erreurs qui incluent le  l'icône s'est produite au cours des 7 derniers jours.

Platform services endpoints

A platform services endpoint stores the information StorageGRID needs to use an external resource as a target for a platform service (CloudMirror replication, notifications, or search integration). You must configure an endpoint for each platform service you plan to use.

 One or more endpoints have experienced an error. Select the endpoint for more details about the error. Meanwhile, the platform service request will be retried automatically.

5 endpoints Create endpoint

Delete endpoint

☐	Display name  	Last error  	Type  	URI  	URN  
☐	my-endpoint-2	 2 hours ago	Search	http://10.96.104.30:9200	urn:sgws:es::mydomain/sveloso/_doc
☐	my-endpoint-3	 3 days ago	Notifications	http://10.96.104.202:8080/	arn:aws:sns:us-west-2::example1
☐	my-endpoint-5	12 days ago	Notifications	http://10.96.104.202:8080/	arn:aws:sns:us-west-2::example3
☐	my-endpoint-4		Notifications	http://10.96.104.202:8080/	arn:aws:sns:us-west-2::example2
☐	my-endpoint-1		S3 Bucket	http://10.96.104.167:10443	urn:sgws:s3:::bucket1



Certains messages d'erreur dans la colonne **Dernière erreur** peuvent inclure un logID entre parenthèses. Un administrateur de grille ou un support technique peut utiliser cet ID pour localiser des informations plus détaillées sur l'erreur dans le fichier bycast.log.

Problèmes liés aux serveurs proxy

Si vous avez configuré un **"proxy de stockage"** entre les nœuds de stockage et les points de terminaison du service de la plateforme, des erreurs peuvent se produire si votre service proxy n'autorise pas les messages provenant de StorageGRID. Pour résoudre ces problèmes, vérifiez les paramètres de votre serveur proxy pour vous assurer que les messages liés au service de la plateforme ne sont pas bloqués.

Déterminer si une erreur s'est produite

Si des erreurs de point de terminaison 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 Points de terminaison pour voir plus de détails sur l'erreur.

Les opérations client échouent

Certains problèmes de services de plateforme peuvent entraîner l'échec des opérations client sur le bucket S3. Par exemple, les opérations du client S3 échoueront si le service interne de machine à états répliquée (RSM) s'arrête ou s'il y a trop de messages de services de plateforme en file d'attente pour livraison.

Pour vérifier l'état des services :

1. Sélectionnez **SUPPORT > Outils > Topologie de grille**.
2. Sélectionnez **site > Nœud de stockage > SSM > Services**.

Erreurs de point de terminaison récupérables et irrécupérables

Une fois les points de terminaison créés, des erreurs de demande de service de plateforme peuvent se produire pour diverses raisons. Certaines erreurs sont récupérables 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 bucket de destination n'existe pas.
- La notification ne peut pas être délivrée.

Si StorageGRID rencontre une erreur récupérable, la demande de service de plateforme sera relancée jusqu'à ce qu'elle réussisse.

D'autres erreurs sont irrécupérables. Par exemple, une erreur irrécupérable se produit si le point de terminaison est supprimé.

Si StorageGRID rencontre une erreur de point de terminaison irrécupérable :

- Dans le gestionnaire de grille, accédez à **Support > Outils > Métriques > Grafana > Présentation des services de la plateforme** pour afficher les détails de l'erreur.
- Dans le gestionnaire de locataires, accédez à **STOCKAGE (S3) > Points de terminaison des services de plateforme** pour afficher les détails de l'erreur.
- Vérifiez le `/var/local/log/bycast-err.log` pour les erreurs liées. Les nœuds de stockage dotés du service ADC contiennent ce fichier journal.

Les messages des services de la plateforme ne peuvent pas être livrés

Si la destination rencontre un problème qui l'empêche d'accepter les messages des services de plateforme, l'opération client sur le bucket réussit, mais le message des services de plateforme n'est pas remis. Par exemple, cette erreur peut se produire si les informations d'identification sont mises à jour sur la destination de telle sorte que StorageGRID ne peut plus s'authentifier auprès du service de destination.

Vérifiez les alertes associées.

Des performances plus lentes pour les demandes de service de la plateforme

Le logiciel StorageGRID peut limiter les requêtes S3 entrantes pour un bucket si la vitesse à laquelle les requêtes sont envoyées dépasse la vitesse à laquelle le point de terminaison de destination peut recevoir les requêtes. La limitation se produit uniquement lorsqu'il existe un arriéré de requêtes en attente d'être envoyées au point de terminaison de destination.

Le seul effet visible est que les requêtes S3 entrantes prendront plus de temps à s'exécuter. Si vous commencez à détecter des performances nettement plus lentes, vous devez réduire le taux d'ingestion ou utiliser un point de terminaison avec une capacité supérieure. Si l'arriéré des demandes continue de croître, les opérations S3 du client (telles que les demandes PUT) finiront par échouer.

Les requêtes CloudMirror sont plus susceptibles d'être affectées par les performances du point de terminaison de destination, car ces requêtes impliquent généralement plus de transfert de données que les requêtes d'intégration de recherche ou de notification d'événements.

Les demandes de service de la plateforme échouent

Pour afficher le taux d'échec des demandes pour les services de la plateforme :

1. Sélectionnez **NODES**.
2. Sélectionnez **site > Services de plateforme**.
3. Consultez le graphique des taux d'erreur des demandes.

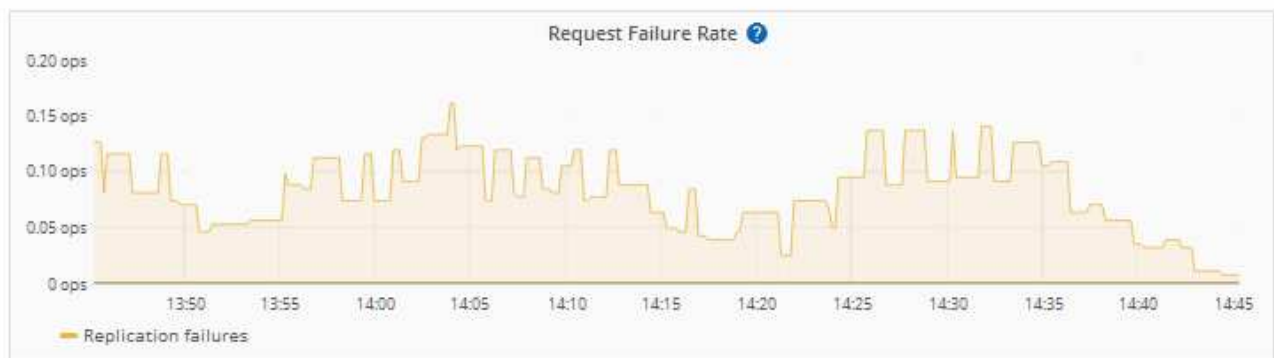
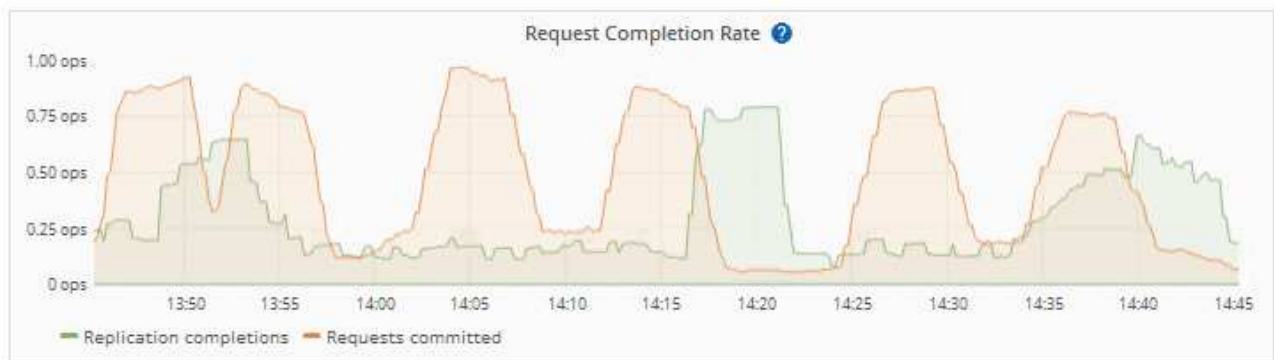
1 hour

1 day

1 week

1 month

Custom



Alerte d'indisponibilité des services de la plateforme

L'alerte **Services de plateforme indisponibles** indique qu'aucune opération de service de plateforme ne peut être effectuée sur un site car trop peu 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 la plateforme 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 qu'une simple majorité de ces nœuds de stockage sont en cours d'exécution et disponibles.



Si plusieurs nœuds de stockage contenant le service RSM échouent sur un site, vous perdez toutes les demandes de service de plateforme en attente pour ce site.

Conseils de dépannage supplémentaires pour les points de terminaison des services de plateforme

Pour plus d'informations, voir [Utiliser un compte locataire](#) > [Résoudre les problèmes des points de terminaison des services de la plateforme](#).

Informations connexes

["Dépannage du système StorageGRID"](#)

Gérer S3 Select pour les comptes locataires

Vous pouvez autoriser certains locataires S3 à utiliser S3 Select pour émettre des demandes SelectObjectContent sur des objets individuels.

S3 Select offre un moyen efficace de rechercher dans de grandes quantités de données sans avoir à déployer une base de données et les ressources associées pour permettre les recherches. Cela réduit également le coût et la latence de 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 un objet. L'implémentation StorageGRID de S3 Select inclut un sous-ensemble de commandes et de fonctionnalités S3 Select.

Considérations et exigences relatives à l'utilisation de S3 Select

Exigences en matière d'administration du réseau

L'administrateur du réseau doit accorder aux locataires la capacité S3 Select. Sélectionnez **Autoriser la sélection S3** lorsque ["créer un locataire"](#) ou ["modifier un locataire"](#).

Exigences relatives au format des objets

L'objet que vous souhaitez interroger doit être dans l'un des formats suivants :

- **CSV**. Peut être utilisé tel quel ou compressé dans des archives GZIP ou BZIP2.
- **Parquet**. Exigences supplémentaires pour les objets Parquet :
 - S3 Select prend uniquement en charge la compression en colonnes à l'aide de GZIP ou 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 compressé est de 512 Mo.
 - Vous devez utiliser les types de données spécifiés dans le schéma de l'objet.
 - Vous ne pouvez pas utiliser les types logiques INTERVAL, JSON, LIST, TIME ou UUID.

Exigences relatives aux points de terminaison

La requête SelectObjectContent doit être envoyée à un ["Point de terminaison de l'équilibreur de charge"](#)

[StorageGRID](#)" .

Les nœuds d'administration et de passerelle utilisés par le point de terminaison doivent être l'un des suivants :

- Un nœud d'appareil de services
- Un nœud logiciel basé sur VMware
- Un nœud bare metal exécutant un noyau avec cgroup v2 activé

Considérations générales

Les requêtes ne peuvent pas être envoyées directement aux nœuds de stockage.



Les demandes 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.

Voir le ["instructions d'utilisation de S3 Select"](#) .

Pour voir ["Cartes Grafana"](#) pour les opérations S3 Sélectionnez au fil du temps, sélectionnez **SUPPORT > Outils > Métriques** dans le Gestionnaire de grille.

Configurer les connexions client

Configurer les connexions client S3

En tant qu'administrateur de grille, vous gérez les options de configuration qui contrôlent la manière dont les applications clientes S3 se connectent à votre système StorageGRID pour stocker et récupérer des données.



Les détails Swift ont été supprimés de cette version du site de documentation. Voir ["StorageGRID 11.8 : Configurer les connexions client S3 et Swift"](#) .

Tâches de configuration

1. Exécutez les tâches prérequis dans StorageGRID, en fonction de la manière dont l'application cliente se connectera à StorageGRID.

Tâches requises

Vous devez obtenir :

- adresses IP
- noms de domaine
- Certificat SSL

Tâches facultatives

En option, configurez :

- Fédération d'identité
- SSO

1. Utilisez StorageGRID pour obtenir les valeurs dont l'application a besoin pour se connecter à la grille. Vous pouvez utiliser l'assistant de configuration S3 ou configurer chaque entité StorageGRID manuellement. +

Utiliser l'assistant de configuration S3

Suivez les étapes de l'assistant de configuration S3.

Configurer manuellement

1. Créer un groupe de haute disponibilité
2. Créer un point de terminaison d'équilibrage de charge
3. Créer un compte locataire
4. Créer un bucket et accéder aux clés
5. Configurer la règle et la politique ILM

1. 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.

Si nécessaire, effectuez une configuration d'application supplémentaire.

2. Exécutez des tâches continues dans l'application et dans StorageGRID pour gérer et surveiller le stockage d'objets au fil du temps.

Informations nécessaires pour attacher StorageGRID à une application cliente

Avant de pouvoir attacher StorageGRID à une application client S3, vous devez effectuer des étapes de configuration dans StorageGRID et obtenir une certaine valeur.

De quelles valeurs ai-je besoin ?

Le tableau suivant indique les valeurs que vous devez configurer dans StorageGRID et où ces valeurs sont utilisées par l'application S3 et le serveur DNS.

Valeur	Où la valeur est configurée	Où la valeur est utilisée
Adresses IP virtuelles (VIP)	StorageGRID > Groupe HA	Entrée DNS
Port	StorageGRID > Point de terminaison de l'équilibreur de charge	Application client
Certificat SSL	StorageGRID > Point de terminaison de l'équilibreur de charge	Application client
Nom du serveur (FQDN)	StorageGRID > Point de terminaison de l'équilibreur de charge	• Application client • Entrée DNS
ID de clé d'accès S3 et clé d'accès secrète	StorageGRID > Locataire et bucket	Application client
Nom du seau/conteneur	StorageGRID > Locataire et bucket	Application client

Comment puis-je obtenir ces valeurs ?

Selon vos besoins, vous pouvez procéder de l'une des manières suivantes pour obtenir les informations dont vous avez besoin :

- *Utilisez le "[Assistant de configuration S3](#)" *. L'assistant de configuration S3 vous aide à configurer rapidement les valeurs requises dans StorageGRID et génère un ou deux fichiers que vous pouvez utiliser lorsque vous configurez l'application S3. L'assistant vous guide à travers les étapes requises et vous aide à garantir que vos paramètres sont conformes aux meilleures pratiques de StorageGRID .



Si vous configurez une application S3, il est recommandé d'utiliser l'assistant de configuration S3, sauf si vous savez que vous avez des exigences particulières ou que votre implémentation nécessitera une personnalisation importante.

- *Utilisez le "[Assistant de configuration de FabricPool](#)" *. Semblable à l'assistant de configuration S3, l'assistant de configuration FabricPool vous aide à configurer rapidement les valeurs requises et génère un fichier que vous pouvez utiliser lorsque vous configurez un niveau de cloud FabricPool dans ONTAP.



Si vous prévoyez d'utiliser StorageGRID comme système de stockage d'objets pour un niveau cloud FabricPool , il est recommandé d'utiliser l'assistant de configuration FabricPool , sauf si vous savez que vous avez des exigences particulières ou que votre implémentation nécessitera une personnalisation importante.

- **Configurer les éléments manuellement.** Si vous vous connectez à une application S3 et préférez ne pas utiliser l'assistant de configuration S3, vous pouvez obtenir les valeurs requises en effectuant la configuration manuellement. Suivez ces étapes :
 - a. Configurez le groupe de haute disponibilité (HA) que vous souhaitez utiliser pour l'application S3. Voir "[Configurer des groupes de haute disponibilité](#)" .

- b. Créez le point de terminaison de l'équilibreur de charge que l'application S3 utilisera. Voir ["Configurer les points de terminaison de l'équilibreur de charge"](#) .
- c. Créez le compte locataire que l'application S3 utilisera. Voir ["Créer un compte locataire"](#) .
- d. Pour un locataire S3, connectez-vous au compte locataire et générez un ID de clé d'accès et une clé d'accès secrète pour chaque utilisateur qui accédera à l'application. Voir ["Créez vos propres clés d'accès"](#) .
- e. Créez un ou plusieurs compartiments S3 dans le compte locataire. Pour S3, voir ["Créer un bucket S3"](#) .
- f. Pour ajouter des instructions de placement spécifiques pour les objets appartenant au nouveau locataire ou bucket/conteneur, créez une nouvelle règle ILM et activez une nouvelle stratégie ILM pour utiliser cette règle. Voir ["Créer une règle ILM"](#) et ["Créer une politique ILM"](#) .

Sécurité pour les clients S3

Les comptes locataires StorageGRID utilisent des applications clientes S3 pour enregistrer les données d'objet dans StorageGRID. Vous devez examiner les mesures de sécurité mises en œuvre pour les applications clientes.

Résumé

La liste suivante résume la manière dont la sécurité est implémentée pour l'API REST S3 :

Sécurité de connexion

TLS

Authentification du serveur

Certificat de serveur X.509 signé par l'autorité de certification système ou certificat de serveur personnalisé fourni par l'administrateur

Authentification du client

ID de clé d'accès au compte S3 et clé d'accès secrète

Autorisation du client

Propriété du bucket et toutes les politiques de contrôle d'accès applicables

Comment StorageGRID assure la sécurité des applications clientes

Les applications clientes S3 peuvent se connecter au service Load Balancer sur les nœuds de passerelle ou les nœuds d'administration ou directement aux nœuds de stockage.

- Les clients qui se connectent au service Load Balancer peuvent utiliser HTTPS ou HTTP, selon la façon dont vous ["configurez le point de terminaison de l'équilibreur de charge"](#) .

HTTPS fournit une communication sécurisée et cryptée TLS et est recommandé. Vous devez joindre un certificat de sécurité au point de terminaison.

HTTP fournit une communication moins sécurisée et non chiffrée et ne doit être utilisé que pour les grilles de non-production ou de test.

- Les clients qui se connectent aux nœuds de stockage peuvent également utiliser HTTPS ou HTTP.

HTTPS est la valeur par défaut et est recommandé.

HTTP fournit une communication moins sécurisée et non chiffrée, mais peut être facultative "[activé](#)" pour les grilles hors production ou de test.

- Les communications entre StorageGRID et le client sont chiffrées à l'aide de TLS.
- Les communications entre le service d'équilibrage de charge et les nœuds de stockage au sein de la grille sont chiffrées, que le point de terminaison de l'équilibrage de charge soit configuré pour accepter les connexions HTTP ou HTTPS.
- Les clients doivent fournir "[En-têtes d'authentification HTTP](#)" à StorageGRID pour effectuer des opérations d'API REST.

Certificats de sécurité et applications clientes

Dans tous les cas, les applications clientes peuvent établir des connexions TLS à l'aide d'un certificat de serveur personnalisé téléchargé par l'administrateur de la grille ou d'un certificat généré par le système StorageGRID :

- Lorsque les applications clientes se connectent au service Load Balancer, elles utilisent le certificat qui a été configuré pour le point de terminaison de l'équilibreur de charge. Chaque point de terminaison d'équilibrage de charge possède son propre certificat : soit un certificat de serveur personnalisé téléchargé par l'administrateur de la grille, soit un certificat que l'administrateur de la grille a généré dans StorageGRID lors de la configuration du point de terminaison.

Voir "[Considérations relatives à l'équilibrage de charge](#)" .

- Lorsque les applications clientes se connectent directement à un nœud de stockage, elles utilisent soit les certificats de serveur générés par le système pour les nœuds de stockage lors de l'installation du système StorageGRID (qui sont signés par l'autorité de certification du système), soit un seul certificat de serveur personnalisé fourni pour la grille par un administrateur de grille. Voir "[ajouter un certificat API S3 personnalisé](#)" .

Les clients doivent être configurés pour faire confiance à l'autorité de certification qui a signé le certificat qu'ils utilisent pour établir des connexions TLS.

Algorithmes de hachage et de chiffrement pris en charge pour les bibliothèques TLS

Le système StorageGRID prend en charge un ensemble de suites de chiffrement que les applications clientes peuvent utiliser lors de l'établissement d'une session TLS. Pour configurer les chiffrements, accédez à **CONFIGURATION > Sécurité > Paramètres de sécurité** et sélectionnez **Politiques TLS et SSH**.

Versions prises en charge de TLS

StorageGRID prend en charge TLS 1.2 et TLS 1.3.



SSLv3 et TLS 1.1 (ou versions antérieures) ne sont plus pris en charge.

Utiliser l'assistant de configuration S3

Utiliser l'assistant de configuration S3 : considérations et exigences

Vous pouvez utiliser l'assistant de configuration S3 pour configurer StorageGRID comme système de stockage d'objets pour une application S3.

Quand utiliser l'assistant de configuration S3

L'assistant de configuration S3 vous guide à travers chaque étape de la configuration de StorageGRID pour une utilisation avec une application S3. Dans le cadre de l'exécution 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 vous assurer que vos paramètres sont conformes aux meilleures pratiques de StorageGRID .

Si vous avez le ["Autorisation d'accès root"](#) , vous pouvez terminer l'assistant de configuration S3 lorsque vous commencez à utiliser StorageGRID Grid Manager, ou vous pouvez accéder à l'assistant et le terminer à tout moment ultérieurement. Selon vos besoins, vous pouvez également configurer manuellement certains ou tous les éléments requis, 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 rempli ces conditions préalables.

Obtenir des adresses IP et configurer des interfaces VLAN

Si vous configurez un groupe haute disponibilité (HA), vous savez à quels nœuds l'application S3 se connectera et quel réseau StorageGRID sera utilisé. Vous savez également quelles valeurs saisir pour le sous-réseau CIDR, l'adresse IP de la passerelle et les adresses IP virtuelles (VIP).

Si vous prévoyez d'utiliser un réseau local virtuel pour séparer le trafic de l'application S3, vous avez déjà configuré l'interface VLAN. Voir ["Configurer les interfaces VLAN"](#) .

Configurer la fédération d'identité et l'authentification unique

Si vous prévoyez d'utiliser la fédération d'identité ou l'authentification unique (SSO) pour votre système StorageGRID , vous avez activé ces fonctionnalités. Vous savez également quel groupe fédéré doit avoir un accès root pour le compte locataire que l'application S3 utilisera. Voir ["Utiliser la fédération d'identité"](#) 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 du serveur de noms de domaine (DNS) mapperont ce nom de domaine complet aux adresses IP virtuelles (VIP) du groupe HA que vous créez à l'aide de l'assistant.

Si vous prévoyez d'utiliser des requêtes hébergées virtuellement de type S3, vous devez disposer ["noms de domaine de point de terminaison S3 configurés"](#) . Il est recommandé d'utiliser des requêtes de type hébergé virtuellement.

Examiner les exigences relatives à l'équilibreur de charge et aux certificats de sécurité

Si vous prévoyez d'utiliser l'équilibreur de charge StorageGRID , vous avez examiné les considérations générales 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 point de terminaison d'équilibrage de charge externe (tiers), vous disposez du nom de domaine complet (FQDN), du port et du certificat pour cet équilibreur de charge.

Configurer toutes les connexions de fédération de grille

Si vous souhaitez autoriser le locataire S3 à cloner les données de compte et à répliquer les objets de compartiment sur une autre grille à l'aide d'une connexion de fédération de grille, confirmez les éléments suivants avant de démarrer l'assistant :

- Tu as ["configuré la connexion à la fédération de grille"](#) .

- Le statut de la connexion est **Connecté**.
- Vous disposez de l'autorisation d'accès root.

Accéder et terminer l'assistant de configuration S3

Vous pouvez utiliser l'assistant de configuration S3 pour configurer StorageGRID pour une utilisation avec une application S3. L'assistant de configuration fournit les valeurs dont l'application a besoin pour accéder à un bucket StorageGRID et enregistrer des objets.

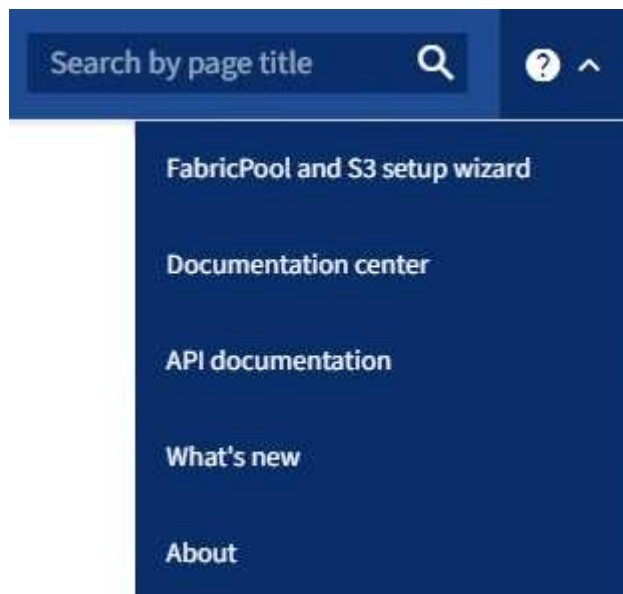
Avant de commencer

- Vous avez le ["Autorisation d'accès root"](#) .
- Vous avez examiné le ["considérations et exigences"](#) pour utiliser l'assistant.

Accéder à l'assistant

Étapes

1. Sign in au Grid Manager à l'aide d'un ["navigateur Web pris en charge"](#) .
2. Si la bannière * Assistant de configuration FabricPool et S3* apparaît sur le tableau de bord, sélectionnez le lien dans la bannière. Si la bannière n'apparaît plus, sélectionnez l'icône d'aide dans la barre d'en-tête du gestionnaire de grille et sélectionnez * Assistant de configuration FabricPool et S3*.



3. Dans la section Application S3 de la page de l'assistant de configuration de FabricPool et S3, sélectionnez **Configurer maintenant**.

Étape 1 sur 6 : Configurer le groupe HA

Un groupe HA est un ensemble de nœuds contenant chacun le service StorageGRID Load Balancer. Un groupe HA peut contenir des nœuds de passerelle, des nœuds d'administration ou les deux.

Vous pouvez utiliser un groupe HA pour aider à maintenir les connexions de données S3 disponibles. Si l'interface active du groupe HA échoue, une interface de sauvegarde peut gérer la charge de travail avec peu d'impact sur les opérations S3.

Pour plus de détails sur cette tâche, voir "[Gérer les groupes de haute disponibilité](#)".

Étapes

1. Si vous prévoyez d'utiliser un équilibreur de charge externe, vous n'avez pas besoin de créer un groupe HA. Sélectionnez **Ignorer cette étape** et accédez à [Étape 2 sur 6 : Configurer le point de terminaison de l'équilibreur de charge](#).
2. Pour utiliser l'équilibreur de charge StorageGRID, vous pouvez créer un nouveau groupe HA ou utiliser un groupe HA existant.

Créer un groupe HA

- Pour créer un nouveau groupe HA, sélectionnez **Créer un groupe HA**.
- Pour l'étape **Entrer les détails**, remplissez les champs suivants.

Champ	Description
Nom du groupe HA	Un nom d'affichage unique pour ce groupe HA.
Description (facultatif)	La description de ce groupe HA.

- Pour l'étape **Ajouter des interfaces**, sélectionnez les interfaces de nœud que vous souhaitez utiliser dans ce groupe HA.

Utilisez les en-têtes de colonnes pour trier les lignes ou saisissez 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.

- Pour l'étape **Prioriser les interfaces**, déterminez l'interface principale et toutes les interfaces de sauvegarde pour ce groupe HA.

Faites glisser les lignes pour modifier les valeurs dans 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 panne.

Si le groupe HA comprend plusieurs interfaces et que l'interface active échoue, les adresses IP virtuelles (VIP) se déplacent vers la première interface de secours dans l'ordre de priorité. Si cette interface échoue, les adresses VIP se déplacent vers l'interface de sauvegarde suivante, et ainsi de suite. Une fois les échecs résolus, les adresses VIP reviennent à l'interface la plus prioritaire disponible.

- Pour l'étape **Saisir les adresses IP**, remplissez les champs suivants.

Champ	Description
Sous-réseau CIDR	L'adresse du sous-réseau VIP en notation CIDR : une adresse IPv4 suivie d'une barre oblique et de la longueur du sous-réseau (0-32). L'adresse réseau ne doit avoir aucun bit d'hôte défini. Par exemple : 192.16.0.0/22 .
Adresse IP de la passerelle (facultatif)	Si les adresses IP S3 utilisées pour accéder à StorageGRID ne se trouvent pas sur le même sous-réseau que les adresses VIP StorageGRID , saisissez 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	Saisissez au moins une et pas plus de dix adresses VIP pour l'interface active dans le groupe HA. Toutes les adresses VIP doivent se trouver dans le sous-réseau VIP. Au moins une adresse doit être IPv4. En option, vous pouvez spécifier des adresses IPv4 et IPv6 supplémentaires.

f. Sélectionnez **Créer un groupe HA**, puis sélectionnez **Terminer** pour revenir à l'assistant de configuration S3.

g. Sélectionnez **Continuer** pour accéder à l'étape de l'équilibrage de charge.

Utiliser le groupe HA existant

a. Pour utiliser un groupe HA existant, sélectionnez le nom du groupe HA dans **Sélectionner un groupe HA**.

b. Sélectionnez **Continuer** pour accéder à l'étape de l'équilibrage de charge.

Étape 2 sur 6 : Configurer le point de terminaison de l'équilibreur de charge

StorageGRID utilise un équilibreur de charge pour gérer la charge de travail des applications clientes. L'équilibrage de charge maximise la vitesse et la capacité de connexion sur plusieurs nœuds de stockage.

Vous pouvez utiliser le service d'équilibrage de charge StorageGRID , qui existe sur tous les nœuds de passerelle et d'administration, ou vous connecter à un équilibreur de charge externe (tiers). L'utilisation de l'équilibreur de charge StorageGRID est recommandée.

Pour plus de détails sur cette tâche, voir "[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 point de terminaison 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 de terminaison

Étapes

1. Pour créer un point de terminaison d'équilibrage de charge, sélectionnez **Créer un point de terminaison**.
2. Pour l'étape **Saisir les détails du point de terminaison**, remplissez les champs suivants.

Champ	Description
Nom	Un nom descriptif pour le point de terminaison.
Port	Le port StorageGRID que vous souhaitez utiliser pour l'équilibrage de charge. Ce champ est défini par défaut sur 10433 pour le premier point de terminaison que vous créez, mais vous pouvez saisir n'importe quel port externe inutilisé. Si vous entrez 80 ou 443, le point de terminaison est configuré uniquement sur les nœuds de passerelle, car ces ports sont réservés sur les nœuds d'administration. Remarque : les ports utilisés par d'autres services de grille ne sont pas autorisés. Voir le "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 non recommandée.

3. Pour l'étape **Sélectionner le mode de liaison**, spécifiez le mode de liaison. Le mode de liaison contrôle la manière dont le point de terminaison est accessible à l'aide de n'importe quelle adresse IP ou à l'aide d'adresses IP et d'interfaces réseau spécifiques.

Mode	Description
Global (par défaut)	Les clients peuvent accéder au point de terminaison à l'aide de l'adresse IP de n'importe quel nœud de passerelle ou nœud d'administration, de l'adresse IP virtuelle (VIP) de n'importe quel groupe HA sur n'importe quel réseau ou d'un nom de domaine complet correspondant. Utilisez le paramètre Global (par défaut) sauf si vous devez restreindre l'accessibilité de ce point de terminaison.
IP virtuelles des groupes HA	Les clients doivent utiliser une adresse IP virtuelle (ou un nom de domaine complet correspondant) d'un groupe HA pour accéder à ce point de terminaison. Les points de terminaison avec ce mode de liaison peuvent tous utiliser le même numéro de port, à condition que les groupes HA que vous sélectionnez pour les points de terminaison ne se chevauchent pas.

Mode	Description
Interfaces de nœuds	Les clients doivent utiliser les adresses IP (ou les noms de domaine complets correspondants) des interfaces de nœuds sélectionnées pour accéder à ce point de terminaison.
Type de nœud	En fonction du type de nœud que vous sélectionnez, les clients doivent utiliser soit l'adresse IP (ou le nom de domaine complet correspondant) de n'importe quel nœud d'administration, soit l'adresse IP (ou le nom de domaine complet correspondant) de n'importe quel nœud de passerelle pour accéder à ce point de terminaison.

4. Pour l'étape **Accès locataire**, sélectionnez l'une des options suivantes :

Champ	Description
Autoriser tous les locataires (par défaut)	Tous les comptes locataires peuvent utiliser ce point de terminaison pour accéder à leurs buckets.
Autoriser les locataires sélectionnés	Seuls les comptes locataires sélectionnés peuvent utiliser ce point de terminaison pour accéder à leurs compartiments.
Bloquer les locataires sélectionnés	Les comptes locataires sélectionnés ne peuvent pas utiliser ce point de terminaison pour accéder à leurs compartiments. Tous les autres locataires peuvent utiliser ce point de terminaison.

5. Pour l'étape **Joindre le 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.
Générer un certificat	Utilisez cette option pour générer un certificat auto-signé. Voir " Configurer les points de terminaison de l'équilibreur de charge " pour plus de détails sur ce qu'il faut saisir.
Utiliser le certificat StorageGRID S3	Utilisez cette option uniquement si vous avez déjà téléchargé ou généré une version personnalisée du certificat global StorageGRID . Voir " Configurer les certificats API S3 " pour plus de détails.

6. Sélectionnez **Terminer** pour revenir à l'assistant de configuration S3.

7. Sélectionnez **Continuer** pour accéder à l'étape du locataire et du bucket.



Les modifications apportées à un certificat de point de terminaison peuvent prendre jusqu'à 15 minutes pour être appliquées à tous les nœuds.

Utiliser le point de terminaison de l'équilibreur de charge existant

Étapes

1. Pour utiliser un point de terminaison existant, sélectionnez son nom dans **Sélectionner un point de terminaison d'équilibrage de charge**.
2. Sélectionnez **Continuer** pour accéder à l'étape du locataire et du bucket.

Utiliser un équilibreur de charge externe

Étapes

1. Pour utiliser un équilibreur de charge externe, remplissez les champs suivants.

Champ	Description
Nom de domaine complet	Le nom de domaine complet (FQDN) de l'équilibreur de charge externe.
Port	Le 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 du locataire et du bucket.

Étape 3 sur 6 : Créer un locataire et un bucket

Un locataire est une entité qui peut utiliser des applications S3 pour stocker et récupérer des objets dans StorageGRID. Chaque locataire possède ses propres utilisateurs, clés d'accès, buckets, objets et un ensemble spécifique de fonctionnalités.

Un bucket est un conteneur utilisé pour stocker les objets et les métadonnées d'objet d'un locataire. Bien que les locataires puissent avoir de nombreux compartiments, l'assistant vous aide à créer un locataire et un compartiment de la manière la plus rapide et la plus simple. Si vous devez ajouter des buckets ou définir des options ultérieurement, vous pouvez utiliser le gestionnaire de locataires.

Pour plus de détails sur cette tâche, voir ["Créer un compte locataire"](#) et ["Créer un bucket S3"](#).

Étapes

1. Saisissez un nom pour le compte locataire.

Les noms des locataires n'ont pas besoin d'être uniques. Lorsque le compte locataire est créé, il reçoit un ID de compte numérique unique.

2. Définissez l'accès root pour le compte locataire, selon que votre système StorageGRID utilise ["fédération d'identité"](#), ["authentification unique \(SSO\)"](#), ou les deux.

Option	Fais ceci
Si la fédération d'identité n'est pas activée	Spécifiez le mot de passe à utiliser lors de la connexion au locataire en tant qu'utilisateur root local.

Option	Fais ceci
Si la fédération d'identité est activée	a. Sélectionnez un groupe fédéré existant pour avoir " Autorisation d'accès root " pour le locataire. b. Vous pouvez également spécifier le mot de passe à utiliser lors de la connexion au locataire en tant qu'utilisateur root local.
Si la fédération d'identité et l'authentification unique (SSO) sont activées	Sélectionnez un groupe fédéré existant pour avoir " Autorisation d'accès root " pour le locataire. Aucun utilisateur local ne peut se connecter.

3. 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 locataire sera l'utilisateur root. Si d'autres utilisateurs utilisent ce locataire, "[utiliser Tenant Manager](#)" pour configurer les clés et les autorisations.

4. Si vous souhaitez créer un bucket pour ce locataire maintenant, sélectionnez **Créer un bucket pour ce locataire**.



Si le verrouillage d'objet S3 est activé pour la grille, le compartiment créé à cette étape n'a pas le verrouillage d'objet S3 activé. Si vous devez utiliser un bucket S3 Object Lock pour cette application S3, ne choisissez pas de créer un bucket maintenant. Utilisez plutôt Tenant Manager pour "[créer le bucket](#)" plus tard.

- a. Saisissez le nom du bucket que l'application S3 utilisera. Par exemple : `s3-bucket` .

Vous ne pouvez pas modifier le nom du bucket après l'avoir créé.

- b. Sélectionnez la **Région** pour ce bucket.

Utiliser la région par défaut(`us-east-1`) sauf si vous prévoyez d'utiliser ILM à l'avenir pour filtrer les objets en fonction de la région du bucket.

5. Sélectionnez **Créer et continuer**.

Étape 4 sur 6 : Télécharger les données

À 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

- Si vous avez sélectionné **Créer automatiquement la clé d'accès S3 de l'utilisateur root**, 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.
- Sélectionnez **Télécharger les valeurs de configuration** pour télécharger un `.txt` fichier contenant les paramètres du point de terminaison de l'équilibreur de charge, du locataire, du bucket et de l'utilisateur root.

3. Enregistrez ces informations dans un endroit sûr.



Ne fermez pas cette page tant que vous n'avez pas copié les deux clés d'accès. Les clés ne seront plus disponibles après avoir fermé cette page. Assurez-vous de sauvegarder ces informations dans un endroit sûr, 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 l'étape de la règle et de la politique ILM.

Étape 5 sur 6 : Examiner la règle ILM et la politique 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 politique ILM incluse avec StorageGRID crée deux copies répliquées de tous les objets. Cette politique est en vigueur jusqu'à ce que vous activiez au moins une nouvelle politique.

Étapes

1. Consultez les informations fournies sur la page.
2. Si vous souhaitez ajouter des instructions spécifiques pour les objets appartenant au nouveau locataire ou au nouveau bucket, créez une nouvelle règle et une nouvelle politique. Voir "[Créer une règle ILM](#)" et "[Utiliser les politiques ILM](#)".
3. Sélectionnez **J'ai lu 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 au **Résumé**.

Étape 6 sur 6 : Révision du résumé

Étapes

1. Consultez le résumé.
2. Prenez note des détails dans les étapes suivantes, qui décrivent la configuration supplémentaire qui pourrait être nécessaire avant de vous connecter au client S3. Par exemple, la sélection de * Sign in en tant que root* vous amène au gestionnaire de locataires, où vous pouvez ajouter des utilisateurs locataires, créer des buckets supplémentaires et mettre à jour les paramètres des buckets.
3. Sélectionnez **Terminer**.
4. Configurez l'application à l'aide du fichier que vous avez téléchargé depuis StorageGRID ou des valeurs que vous avez obtenues manuellement.

Gérer les groupes HA

Que sont les groupes de haute disponibilité (HA) ?

Les groupes haute disponibilité (HA) fournissent des connexions de données hautement disponibles pour les clients S3 et des connexions hautement disponibles au Grid Manager et au Tenant Manager.

Vous pouvez regrouper les interfaces réseau de plusieurs nœuds d'administration et de passerelle dans un groupe haute disponibilité (HA). Si l'interface active du groupe HA échoue, une interface de sauvegarde peut gérer la charge de travail.

Chaque groupe HA fournit un accès aux services partagés sur les nœuds sélectionnés.

- Les groupes HA qui incluent des nœuds de passerelle, des nœuds d'administration ou les deux fournissent des connexions de données hautement disponibles pour les clients S3.
- Les groupes HA qui incluent uniquement des nœuds d'administration fournissent des connexions hautement disponibles au gestionnaire de grille et au gestionnaire de locataires.
- Un groupe HA qui comprend uniquement des appliances de services et des nœuds logiciels basés sur VMware peut fournir des connexions hautement disponibles pour ["Locataires S3 qui utilisent S3 Select"](#) . Les groupes HA sont recommandés lors de l'utilisation de S3 Select, mais pas obligatoires.

Comment créer un groupe HA ?

1. Vous sélectionnez une interface réseau pour un ou plusieurs nœuds d'administration ou nœuds de passerelle. Vous pouvez utiliser une interface Grid Network (eth0), une interface Client Network (eth2), une interface VLAN ou une interface d'accès que vous avez ajoutée au nœud.



Vous ne pouvez pas ajouter une interface à un groupe HA si elle dispose d'une adresse IP attribuée par DHCP.

2. Vous spécifiez une interface comme interface principale. L'interface principale est l'interface active sauf en cas de panne.
3. Vous déterminez l'ordre de priorité pour toutes les interfaces de sauvegarde.
4. Vous attribuez une à dix adresses IP virtuelles (VIP) au groupe. Les applications clientes peuvent utiliser n'importe laquelle de ces adresses VIP pour se connecter à StorageGRID.

Pour les instructions, voir ["Configurer des groupes de haute disponibilité"](#) .

Quelle est l'interface active ?

En fonctionnement normal, toutes les adresses VIP du groupe HA sont ajoutées à l'interface principale, qui est la première interface dans l'ordre de priorité. Tant que l'interface principale reste disponible, elle est utilisée lorsque les clients se connectent à n'importe quelle adresse VIP du groupe. Autrement dit, pendant le fonctionnement normal, l'interface principale est l'interface « active » du groupe.

De même, pendant le fonctionnement normal, toutes les interfaces de priorité inférieure pour le groupe HA agissent comme des interfaces de « secours ». Ces interfaces de sauvegarde ne sont pas utilisées à moins que l'interface principale (actuellement active) ne devienne indisponible.

Afficher l'état actuel du groupe HA d'un nœud

Pour voir si un nœud est affecté à un groupe HA et déterminer son état actuel, sélectionnez **NODES > node**.

Si l'onglet **Vue d'ensemble** inclut une entrée pour les **groupes HA**, le nœud est attribué aux groupes HA répertoriés. La valeur après le nom du groupe est l'état actuel du nœud dans le groupe HA :

- **Actif** : Le groupe HA est actuellement hébergé sur ce nœud.
- **Sauvegarde** : Le groupe HA n'utilise pas actuellement ce nœud ; il s'agit d'une interface de sauvegarde.
- **Arrêté** : le groupe HA ne peut pas être hébergé sur ce nœud car le service Haute disponibilité (maintenu en vie) a été arrêté manuellement.
- **Erreur** : Le groupe HA ne peut pas être hébergé sur ce nœud en raison d'une ou plusieurs des raisons suivantes :

- Le service Load Balancer (nginx-gw) n'est pas en cours d'exécution sur le nœud.
- L'interface eth0 ou VIP du nœud est en panne.
- Le nœud est en panne.

Dans cet exemple, le nœud d'administration principal a été ajouté à deux groupes HA. Ce nœud est actuellement l'interface active pour le groupe de clients Admin et une interface de sauvegarde pour le groupe de clients FabricPool .

DC1-ADM1 (Primary Admin Node) [🔗](#)

[Overview](#)
[Hardware](#)
[Network](#)
[Storage](#)
[Load balancer](#)
[Tasks](#)

Node information [?](#)

Name:	DC1-ADM1
Type:	Primary Admin Node
ID:	ce00d9c8-8a79-4742-bdef-c9c658db5315
Connection state:	🟢 Connected
Software version:	11.6.0 (build 20211207.1804.614bc17)
HA groups:	Admin clients (Active) FabricPool clients (Backup)
IP addresses:	172.16.1.225 - eth0 (Grid Network) 10.224.1.225 - eth1 (Admin Network) 47.47.0.2, 47.47.1.225 - eth2 (Client Network)

[Show additional IP addresses](#) ▼

Que se passe-t-il lorsque l'interface active échoue ?

L'interface qui héberge actuellement les adresses VIP est l'interface active. Si le groupe HA comprend plusieurs interfaces et que l'interface active échoue, les adresses VIP se déplacent vers la première interface de sauvegarde disponible dans l'ordre de priorité. Si cette interface échoue, les adresses VIP se déplacent vers la prochaine interface de sauvegarde disponible, et ainsi de suite.

Le basculement peut être déclenché pour l'une des raisons suivantes :

- Le nœud sur lequel l'interface est configurée tombe en panne.
- Le nœud sur lequel l'interface est configurée perd la connectivité avec tous les autres nœuds pendant au moins 2 minutes.
- L'interface active tombe en panne.
- Le service Load Balancer s'arrête.
- Le service de haute disponibilité s'arrête.



Le basculement peut ne pas être déclenché par des pannes de réseau externes au nœud qui héberge l'interface active. De même, le basculement n'est pas déclenché par les services du Grid Manager ou du Tenant Manager.

Le processus de basculement ne prend généralement que quelques secondes et est suffisamment rapide pour que les applications clientes subissent peu d'impact et puissent compter sur des comportements de nouvelle tentative normaux pour continuer à fonctionner.

Lorsque l'échec est résolu et qu'une interface de priorité supérieure redevient disponible, les adresses VIP sont automatiquement déplacées vers l'interface de priorité la plus élevée disponible.

Comment les groupes HA sont-ils utilisés ?

Vous pouvez utiliser des groupes haute disponibilité (HA) pour fournir des connexions hautement disponibles à StorageGRID pour les données d'objet et pour une utilisation administrative.

- Un groupe HA peut fournir des connexions administratives hautement disponibles au Grid Manager ou au Tenant Manager.
- Un groupe HA peut fournir des connexions de données hautement disponibles pour les clients S3.
- Un groupe HA qui contient une seule interface vous permet de fournir plusieurs adresses VIP et de définir explicitement des adresses IPv6.

Un groupe HA ne peut fournir une haute disponibilité que si tous les nœuds inclus dans le groupe fournissent les mêmes services. Lorsque vous créez un groupe HA, ajoutez des interfaces à partir des types de nœuds qui fournissent les services dont vous avez besoin.

- **Nœuds d'administration** : inclure le service d'équilibrage de charge et activer l'accès au gestionnaire de grille ou au gestionnaire de locataires.
- **Nœuds de passerelle** : inclure le service d'équilibrage de charge.

Objectif du groupe HA	Ajouter des nœuds de ce type au groupe HA
Accès au Grid Manager	• Nœud d'administration principal (Primaire) • Nœuds d'administration non principaux Remarque : le nœud d'administration principal doit être l'interface principale. Certaines procédures de maintenance ne peuvent être effectuées qu'à partir du nœud d'administration principal.
Accès au gestionnaire de locataires uniquement	• Nœuds d'administration principaux ou non principaux
Accès client S3 – Service d'équilibrage de charge	• Nœuds d'administration • Nœuds de passerelle

Objectif du groupe HA	Ajouter des nœuds de ce type au groupe HA
Accès client S3 pour "S3 Select"	• Appareils de service • Nœuds logiciels basés sur VMware Remarque : les groupes HA sont recommandés lors de l'utilisation de S3 Select, mais pas obligatoires.

Limitations de l'utilisation des groupes HA avec Grid Manager ou Tenant Manager

Si un service Grid Manager ou Tenant Manager échoue, le basculement du groupe HA n'est pas déclenché.

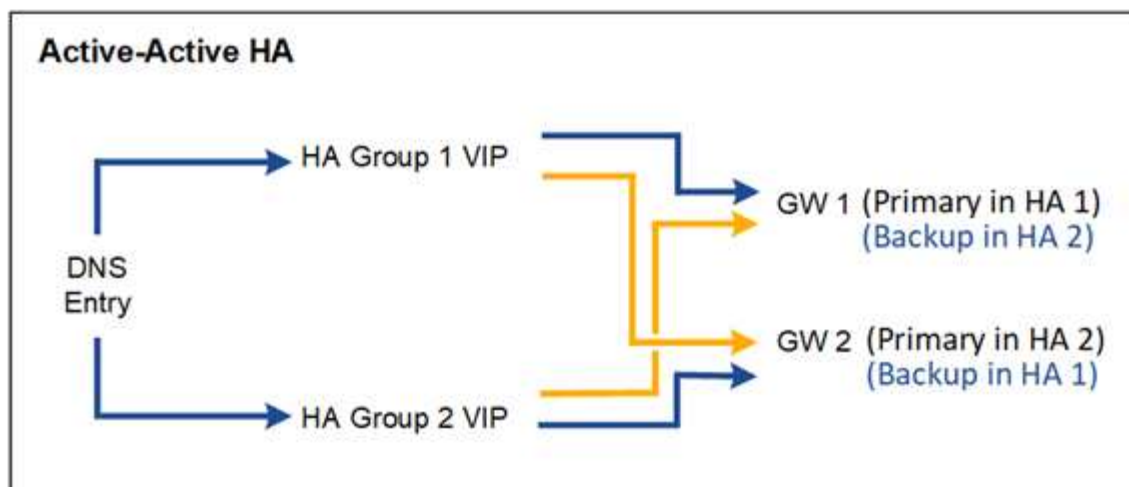
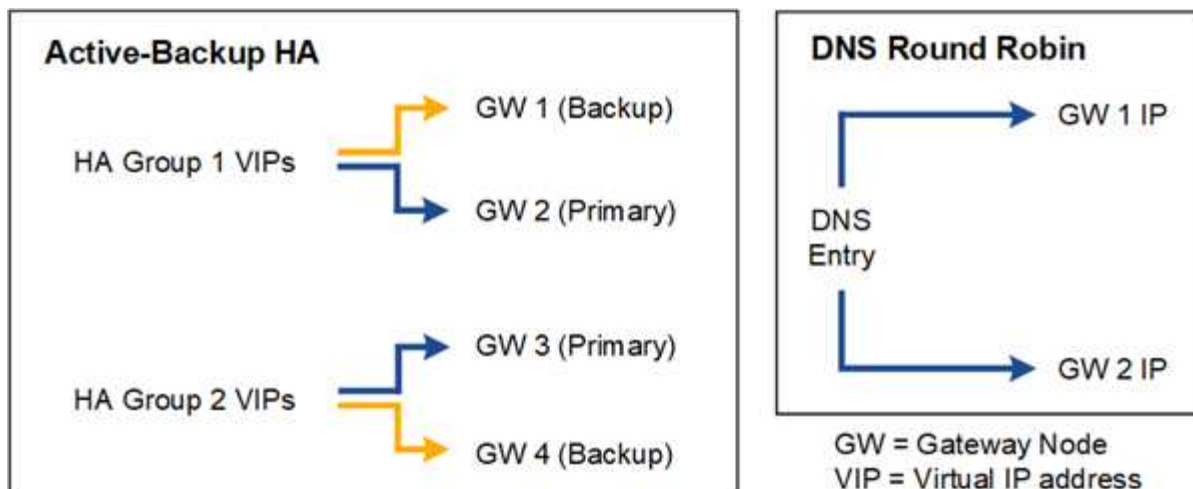
Si vous êtes connecté au Grid Manager ou au Tenant Manager lors du basculement, vous êtes déconnecté et devez vous reconnecter pour reprendre votre tâche.

Certaines procédures de maintenance ne peuvent pas être effectuées lorsque le nœud d'administration principal n'est pas disponible. Lors du basculement, vous pouvez utiliser Grid Manager pour surveiller votre système StorageGRID .

Options de configuration pour les groupes HA

Les diagrammes suivants fournissent des exemples de différentes manières de configurer des groupes HA. Chaque option présente des avantages et des inconvénients.

Dans les diagrammes, le bleu indique l'interface principale du groupe HA et le jaune indique l'interface de sauvegarde du groupe HA.



Le tableau résume les avantages de chaque configuration HA présentée dans le diagramme.

Configuration	Avantages	Inconvénients
HA de sauvegarde active	- Géré par StorageGRID sans dépendances externes. - Basculement rapide.	Un seul nœud dans un groupe HA est actif. Au moins un nœud par groupe HA sera inactif.
DNS Round Robin	- Augmentation du débit global. - Aucun hôte inactif.	- Basculement lent, qui peut dépendre du comportement du client. - Nécessite une configuration matérielle en dehors de StorageGRID. - Nécessite un contrôle de santé mis en œuvre par le client.

Configuration	Avantages	Inconvénients
HA actif-actif	• Le trafic est réparti sur plusieurs groupes HA. • Débit global élevé qui évolue avec le nombre de groupes HA. • Basculement rapide.	• Plus complexe à configurer. • Nécessite une configuration matérielle en dehors de StorageGRID. • Nécessite un contrôle de santé mis en œuvre par le client.

Configurer des groupes de haute disponibilité

Vous pouvez configurer des groupes de haute disponibilité (HA) pour fournir un accès hautement disponible aux services sur les nœuds d'administration ou les nœuds de passerelle.

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 root"](#) .
- Si vous prévoyez d'utiliser une interface VLAN dans un groupe HA, vous avez créé l'interface VLAN. Voir ["Configurer les interfaces VLAN"](#) .
- Si vous prévoyez d'utiliser une interface d'accès pour un nœud dans un groupe HA, vous avez créé l'interface :
 - **Red Hat Enterprise Linux (avant l'installation du nœud):** ["Créer des fichiers de configuration de nœud"](#)
 - **Ubuntu ou Debian (avant d'installer le nœud)** : ["Créer des fichiers de configuration de nœud"](#)
 - **Linux (après l'installation du nœud):** ["Linux : ajouter des interfaces trunk ou d'accès à un nœud"](#)
 - **VMware (après l'installation du nœud):** ["VMware : ajouter des interfaces de jonction ou d'accès à un nœud"](#)

Créer un groupe de haute disponibilité

Lorsque vous créez un groupe de haute disponibilité, vous sélectionnez une ou plusieurs interfaces et les organisez par ordre de priorité. Ensuite, vous attribuez une ou plusieurs adresses VIP au groupe.

Une interface doit être disponible pour qu'un nœud de passerelle ou un nœud d'administration soit inclus dans un groupe HA. Un groupe HA ne peut utiliser qu'une seule interface pour un nœud donné ; cependant, d'autres interfaces pour le même nœud peuvent être utilisées dans d'autres groupes HA.

Accéder à l'assistant

Étapes

1. Sélectionnez **CONFIGURATION > Réseau > Groupes de haute disponibilité**.
2. Sélectionnez **Créer**.

Entrez les détails du groupe HA

Étapes

1. Fournissez un nom unique pour le groupe HA.

2. Si vous le souhaitez, saisissez une description pour le groupe HA.
3. Sélectionnez **Continuer**.

Ajouter des interfaces au groupe HA

Étapes

1. Sélectionnez une ou plusieurs interfaces à ajouter à ce groupe HA.

Utilisez les en-têtes de colonnes pour trier les lignes ou saisissez un terme de recherche pour localiser les interfaces plus rapidement.

Add interfaces to the HA group

Select one or more interfaces for this HA group. You can select only one interface for each node.

?

Total interface count: 4

	Node	Interface	Site	IPv4 subnet	Node type
☐	DC1-ADM1-104-96	eth0	DC1	10.96.104.0/22	Primary Admin Node
☐	DC1-ADM1-104-96	eth2	DC1	—	Primary Admin Node
☐	DC2-ADM1-104-103	eth0	DC2	10.96.104.0/22	Admin Node
☐	DC2-ADM1-104-103	eth2	DC2	—	Admin Node

0 interfaces selected

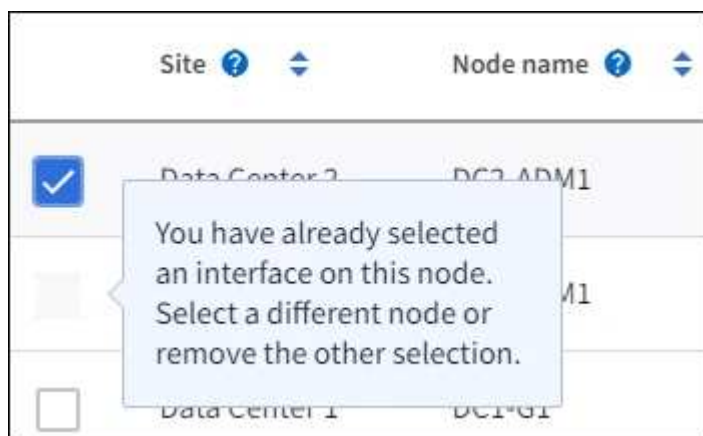


Après avoir créé une interface VLAN, attendez jusqu'à 5 minutes pour que la nouvelle interface apparaisse dans le tableau.

Lignes directrices pour la sélection des interfaces

- Vous devez sélectionner au moins une interface.
- Vous ne pouvez sélectionner qu'une seule interface pour un nœud.
- Si le groupe HA est destiné à la protection HA des services du nœud d'administration, qui incluent le gestionnaire de grille et le gestionnaire de locataires, sélectionnez les interfaces sur les nœuds d'administration uniquement.
- Si le groupe HA est destiné à la protection HA du trafic client S3, sélectionnez les interfaces sur 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 qu'en cas de basculement, les services fournis par le nœud précédemment actif peuvent ne pas être disponibles sur le nœud nouvellement actif. Par exemple, un nœud de passerelle de sauvegarde ne peut pas fournir une protection HA des services du nœud d'administration. De même, un nœud d'administration de sauvegarde 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 une interface si sa valeur de sous-réseau ou sa passerelle est 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**.

Déterminer l'ordre de priorité

Si le groupe HA comprend plusieurs interfaces, vous pouvez déterminer quelle est l'interface principale et quelles sont les interfaces de sauvegarde (basculement). Si l'interface principale échoue, les adresses VIP se déplacent vers l'interface de priorité la plus élevée disponible. Si cette interface échoue, les adresses VIP se déplacent vers l'interface de priorité la plus élevée disponible, et ainsi de suite.

Étapes

1. Faites glisser les lignes dans la colonne **Ordre de priorité** pour déterminer l'interface principale et toutes 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 panne.

Determine the priority order

Determine the primary interface and the backup (failover) interfaces for this HA group. Drag and drop rows or select the arrows.

Priority order ?	Node	Interface ?	Node type ?
1 (Primary interface)	⬆ DC1-ADM1-104-96	eth2	Primary Admin Node
2	⬆ DC2-ADM1-104-103	eth2	Admin Node



Si le groupe HA fournit un accès au gestionnaire de grille, vous devez sélectionner une interface sur le nœud d'administration principal pour être l'interface principale. Certaines procédures de maintenance ne peuvent être effectuées qu'à partir du nœud d'administration principal.

2. Sélectionnez **Continuer**.

Entrez les adresses IP

Étapes

1. Dans le champ **Sous-réseau 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).

L'adresse réseau ne doit avoir aucun bit d'hôte défini. 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.

Enter details for the HA group

Subnet CIDR ?

Specify the subnet in CIDR notation. The optional gateway IP and all VIPs must be in this subnet.

IPv4 address followed by a slash and the subnet length (0-32)

Gateway IP address (optional) ?

Optionally specify the IP address of the gateway, which must be in the subnet. If the subnet address length is 32, the gateway IP address is automatically set to the subnet IP.

Virtual IP address ?

Specify at least 1 and no more than 10 virtual IPs for the HA group. All virtual IPs must be in the same subnet. If the subnet length is 32, only one VIP is allowed, which is automatically set to the subnet/gateway IP.

[Add another IP address](#)

2. En option, si des clients administratifs ou locataires S3 accèdent à ces adresses VIP à partir d'un sous-réseau différent, saisissez l'**adresse IP de la passerelle**. L'adresse de la passerelle doit être dans le sous-réseau VIP.

Les utilisateurs clients et administrateurs utiliseront cette passerelle pour accéder aux adresses IP virtuelles.

3. Saisissez au moins une et pas plus de dix adresses VIP pour l'interface active dans le 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. En option, vous pouvez spécifier des adresses IPv4 et IPv6 supplémentaires.

4. Sélectionnez **Créer un groupe HA** et sélectionnez **Terminer**.

Le groupe HA est créé et vous pouvez désormais utiliser les adresses IP virtuelles configurées.

Prochaines étapes

Si vous utilisez ce groupe HA pour l'équilibrage de charge, créez un point de terminaison d'équilibrage de charge pour déterminer le port et le protocole réseau et pour joindre tous les certificats requis. Voir "[Configurer les points de terminaison de l'équilibreur de charge](#)".

Modifier un groupe de haute disponibilité

Vous pouvez modifier un groupe haute disponibilité (HA) pour changer 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 HA si vous souhaitez supprimer le nœud associé à une interface sélectionnée dans une procédure de mise hors service d'un site ou d'un nœud.

Étapes

1. Sélectionnez **CONFIGURATION > Réseau > Groupes de haute disponibilité**.

La page Groupes de haute disponibilité affiche tous les groupes HA existants.

2. Cochez la case correspondant au groupe HA que vous souhaitez 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 pour le groupe HA.
 - 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 fournit un accès au gestionnaire de grille, vous devez sélectionner une interface sur le nœud d'administration principal pour être l'interface principale. Certaines procédures de maintenance ne peuvent être effectuées qu'à partir du nœud d'administration principal

- c. Vous pouvez également faire glisser les lignes pour modifier l'ordre de priorité de l'interface principale et de toutes les interfaces de sauvegarde pour ce groupe HA.
- d. En option, mettez à jour les adresses IP virtuelles.

- e. Sélectionnez **Enregistrer** puis **Terminer**.

Supprimer un groupe de haute disponibilité

Vous pouvez supprimer un ou plusieurs groupes de haute disponibilité (HA) à la fois.



Vous ne pouvez pas supprimer un groupe HA s'il est lié à un point de terminaison d'équilibrage de charge. Pour supprimer un groupe HA, vous devez le supprimer de tous les points de terminaison d'équilibrage de charge qui l'utilisent.

Pour éviter toute interruption du client, mettez à jour toutes les applications clientes S3 concernées avant de supprimer un groupe HA. Mettez à jour chaque client pour se connecter à l'aide d'une autre adresse IP, par exemple, l'adresse IP virtuelle d'un groupe HA différent ou l'adresse IP configurée pour une interface lors de l'installation.

Étapes

1. Sélectionnez **CONFIGURATION > Réseau > Groupes de haute disponibilité**.
2. Consultez la colonne **Points de terminaison de l'équilibreur de charge** pour chaque groupe HA que vous souhaitez supprimer. Si des points de terminaison d'équilibrage de charge sont répertoriés :
 - a. Accédez à **CONFIGURATION > Réseau > Points de terminaison de l'équilibreur de charge**.
 - b. Cochez la case correspondant au point de terminaison.
 - c. Sélectionnez **Actions > Modifier le mode de liaison du point de terminaison**.
 - d. Mettez à jour le mode de liaison pour supprimer le groupe HA.
 - e. Sélectionnez **Enregistrer les modifications**.
3. Si aucun point de terminaison d'équilibrage de charge n'est répertorié, cochez la case correspondant à chaque groupe HA que vous souhaitez supprimer.
4. Sélectionnez **Actions > Supprimer le groupe HA**.
5. Consultez le message et sélectionnez **Supprimer le groupe HA** pour confirmer votre sélection.

Tous les groupes HA que vous avez sélectionnés sont supprimés. Une bannière de réussite verte apparaît sur la page Groupes de haute disponibilité.

Gérer l'équilibrage de charge

Considérations relatives à l'équilibrage de charge

Vous pouvez utiliser l'équilibrage de charge pour gérer les charges de travail d'ingestion et de récupération des clients S3.

Qu'est-ce que l'équilibrage de charge ?

Lorsqu'une application cliente enregistre ou récupère des données à partir d'un système StorageGRID, StorageGRID utilise un équilibreur de charge pour gérer la charge de travail d'ingestion et de récupération. L'équilibrage de charge maximise 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 tous les nœuds de passerelle et fournit un équilibrage de charge de couche 7. Il effectue la terminaison TLS (Transport Layer Security) des demandes client, inspecte les demandes et établit de nouvelles connexions sécurisées aux

nœuds de stockage.

Le service d'équilibrage de charge sur chaque nœud fonctionne indépendamment lors du transfert du trafic client vers les nœuds de stockage. Grâce à un processus de pondération, le service Load Balancer achemine davantage de requêtes vers les nœuds de stockage avec une disponibilité CPU plus élevée.



Bien que le service StorageGRID Load Balancer soit le mécanisme d'équilibrage de charge recommandé, vous souhaitez peut-être intégrer un équilibreur de charge tiers à la place. Pour plus d'informations, contactez votre représentant de compte NetApp ou reportez-vous à ["TR-4626 : Équilibreurs de charge tiers et globaux StorageGRID"](#).

De combien de nœuds d'équilibrage de charge ai-je besoin ?

En règle générale, chaque site de votre système StorageGRID doit inclure deux nœuds ou plus 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. Assurez-vous qu'il existe une infrastructure réseau, matérielle ou de virtualisation adéquate pour chaque nœud d'équilibrage de charge, que vous utilisiez des appliances de services, des nœuds bare metal ou des nœuds basés sur des machines virtuelles (VM).

Qu'est-ce qu'un point de terminaison d'équilibrage de charge ?

Un point de terminaison d'équilibrage de charge définit le port et le protocole réseau (HTTPS ou HTTP) que les demandes d'application client entrantes et sortantes utiliseront pour accéder aux nœuds contenant le service d'équilibrage de charge. Le point de terminaison définit également le type de client (S3), le mode de liaison et éventuellement une liste de locataires autorisés ou bloqués.

Pour créer un point de terminaison d'équilibrage de charge, sélectionnez **CONFIGURATION > Réseau > Points de terminaison d'équilibrage de charge** ou suivez l'assistant de configuration de FabricPool et S3. Pour les instructions :

- ["Configurer les points de terminaison de l'équilibreur de charge"](#)
- ["Utiliser l'assistant de configuration S3"](#)
- ["Utiliser l'assistant de configuration de FabricPool"](#)

Considérations pour le port

Le port d'un point de terminaison d'équilibrage de charge est par défaut 10433 pour le premier point de terminaison que vous créez, mais vous pouvez spécifier n'importe quel port externe inutilisé entre 1 et 65535. Si vous utilisez le port 80 ou 443, le point de terminaison utilisera le service Load Balancer sur les nœuds de passerelle uniquement. Ces ports sont réservés sur les nœuds d'administration. Si vous utilisez le même port pour plusieurs points de terminaison, vous devez spécifier un mode de liaison différent pour chaque point de terminaison.

Les ports utilisés par d'autres services de grille ne sont pas autorisés. Voir le ["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 cryptage TLS (Transport Layer Security). La connexion à StorageGRID sans cryptage TLS est prise en charge mais non recommandée, en particulier dans les environnements de production. Lorsque vous sélectionnez le protocole réseau pour le point de terminaison de l'équilibreur de charge StorageGRID, vous devez sélectionner **HTTPS**.

Considérations relatives aux certificats de point de terminaison d'équilibrage de charge

Si vous sélectionnez **HTTPS** comme protocole réseau pour le point de terminaison de l'équilibreur de charge, vous devez fournir un certificat de sécurité. Vous pouvez utiliser l'une de ces trois options lorsque vous créez le point de terminaison de l'équilibreur de charge :

- **Télécharger un certificat signé (recommandé).** Ce certificat peut être signé par une autorité de certification (CA) publique ou privée. L'utilisation d'un certificat de serveur CA publiquement approuvé pour sécuriser la connexion est la meilleure pratique. Contrairement aux certificats générés, les certificats signés par une autorité de certification peuvent être renouvelés sans interruption, ce qui peut aider à éviter les problèmes d'expiration.
- Vous devez obtenir les fichiers suivants avant de créer le point de terminaison de l'équilibreur de charge :
 - Le fichier de certificat du serveur personnalisé.
 - Le fichier de clé privée du certificat de serveur personnalisé.
 - En option, un ensemble de certificats CA provenant de chaque autorité de certification émettrice intermédiaire.
- **Générer un certificat auto-signé.**
- **Utilisez le certificat global StorageGRID S3.** Vous devez télécharger ou générer une version personnalisée de ce certificat avant de pouvoir le sélectionner pour le point de terminaison de l'équilibreur de charge. Voir "[Configurer les certificats API S3](#)".

De quelles valeurs ai-je besoin ?

Pour créer le certificat, vous devez connaître tous les noms de domaine et adresses IP que les applications clientes S3 utiliseront pour accéder au point de terminaison.

L'entrée **Subject DN** (Distinguished Name) du certificat doit inclure le nom de domaine complet que l'application cliente 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 d'équilibrage de charge. 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 requêtes de type hébergé virtuel S3, le certificat doit également inclure une entrée **Nom alternatif** pour chaque "[Nom de domaine du point de terminaison S3](#)" vous avez configuré, y compris tous 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 "[Directives de renforcement pour les certificats de serveur](#)".

Vous devez également définir une entrée DNS pour chaque nom dans le certificat de sécurité.

Comment gérer les certificats expirés ?



Si le certificat utilisé pour sécuriser la connexion entre l'application S3 et StorageGRID expire, l'application peut perdre temporairement l'accès à StorageGRID.

Pour éviter les problèmes d'expiration des certificats, suivez ces bonnes pratiques :

- Surveillez attentivement toutes les alertes qui avertissent de l'approche de la date d'expiration du certificat, telles que les alertes **Expiration du certificat du point de terminaison de l'équilibreur de charge** et **Expiration du certificat du serveur global pour l'API S3**.
- Gardez toujours les versions du certificat de l'application StorageGRID et S3 synchronisées. Si vous remplacez ou renouvelez le certificat utilisé pour un point de terminaison d'équilibrage de charge, vous devez remplacer ou renouveler le certificat équivalent utilisé par l'application S3.
- Utilisez un certificat CA signé publiquement. Si vous utilisez un certificat signé par une autorité de certification, vous pouvez remplacer les certificats sur le point d'expirer sans interruption.
- Si vous avez généré un certificat StorageGRID auto-signé et que ce certificat est sur le point d'expirer, vous devez remplacer manuellement le certificat dans StorageGRID et dans l'application S3 avant l'expiration du certificat existant.

Considérations sur le mode de liaison

Le mode de liaison vous permet de contrôler les adresses IP qui peuvent être utilisées pour accéder à un point de terminaison d'équilibrage de charge. Si un point de terminaison utilise un mode de liaison, les applications clientes ne peuvent accéder au point de terminaison que 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 nom de domaine complet ne peuvent pas accéder au point de terminaison.

Vous pouvez spécifier l'un des modes de liaison suivants :

- **Global** (par défaut) : les applications clientes peuvent accéder au point de terminaison à l'aide de l'adresse IP de n'importe quel nœud de passerelle ou nœud d'administration, de l'adresse IP virtuelle (VIP) de n'importe quel groupe HA sur n'importe quel réseau ou d'un nom de domaine complet correspondant. Utilisez ce paramètre sauf si vous devez restreindre l'accessibilité d'un point de terminaison.
- **IP virtuelles des groupes HA**. Les applications clientes doivent utiliser une adresse IP virtuelle (ou un nom de domaine complet correspondant) d'un groupe HA.
- **Interfaces de nœuds**. Les clients doivent utiliser les adresses IP (ou les noms de domaine complets correspondants) des interfaces de nœuds sélectionnées.
- **Type de nœud**. En fonction du type de nœud que vous sélectionnez, les clients doivent utiliser soit l'adresse IP (ou le nom de domaine complet correspondant) de n'importe quel nœud d'administration, soit l'adresse IP (ou le nom de domaine complet correspondant) de n'importe quel nœud de passerelle.

Considérations relatives à l'accès des locataires

L'accès des locataires est une fonctionnalité de sécurité facultative qui vous permet de contrôler les comptes de locataires StorageGRID qui peuvent utiliser un point de terminaison d'équilibrage de charge pour accéder à leurs buckets. Vous pouvez autoriser tous les locataires à accéder à un point de terminaison (par défaut), ou vous pouvez spécifier une liste des locataires autorisés ou bloqués pour chaque point de terminaison.

Vous pouvez utiliser cette fonctionnalité pour fournir une meilleure isolation de sécurité entre les locataires et leurs points de terminaison. Par exemple, vous pouvez utiliser cette fonctionnalité pour garantir que les documents top secret ou hautement classifiés appartenant à un locataire restent totalement 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 (comme dans le cas d'un accès anonyme), le propriétaire du bucket est utilisé pour déterminer le locataire.

Exemple d'accès des locataires

Pour comprendre comment fonctionne cette fonctionnalité de sécurité, considérez l'exemple suivant :

1. Vous avez créé deux points de terminaison d'équilibrage de charge, comme suit :
 - Point de terminaison **public** : utilise le port 10443 et autorise l'accès à tous les locataires.
 - Point de terminaison **Top secret** : utilise le port 10444 et autorise l'accès au locataire **Top secret** uniquement. Tous les autres locataires ne peuvent pas accéder à ce point de terminaison.
2. Le `top-secret.pdf` se trouve dans un bucket appartenant au locataire **Top secret**.

Pour accéder au `top-secret.pdf`, un utilisateur du locataire **Top secret** peut émettre une requête GET pour `https://w.x.y.z:10444/top-secret.pdf`. Étant donné que ce locataire est autorisé à utiliser le point de terminaison 10444, l'utilisateur peut accéder à l'objet. Cependant, si un utilisateur appartenant à un autre locataire émet la même demande à la même URL, il reçoit immédiatement un message d'accès refusé. L'accès est refusé même si les informations d'identification et la signature sont valides.

Disponibilité du processeur

Le service d'équilibrage de charge sur chaque nœud d'administration et nœud de passerelle fonctionne indépendamment lors du transfert du trafic S3 vers les nœuds de stockage. Grâce à un processus de pondération, le service Load Balancer achemine davantage de requêtes vers les nœuds de stockage avec une disponibilité CPU plus élevée. Les informations sur la charge du processeur du nœud sont mises à jour toutes les quelques minutes, mais la pondération peut être mise à jour plus fréquemment. Une valeur de pondération de base minimale est attribuée à tous les nœuds de stockage, même si un nœud signale une utilisation à 100 % ou ne parvient pas à signaler son utilisation.

Dans certains cas, les informations sur la disponibilité du processeur sont limitées au site sur lequel se trouve le service Load Balancer.

Configurer les points de terminaison de l'équilibreur de charge

Les points de terminaison de l'équilibreur de charge déterminent les ports et les protocoles réseau que les clients S3 peuvent utiliser lors de la connexion à l'équilibreur de charge StorageGRID sur les nœuds de passerelle et d'administration. Vous pouvez également utiliser des points de terminaison pour accéder au gestionnaire de grille, au gestionnaire de locataires ou aux deux.



Les détails Swift ont été supprimés de cette version du site de documentation. Voir "[Configurer les connexions client S3 et Swift](#)".

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 root](#)".
- Vous avez examiné le "[considérations pour l'équilibrage de charge](#)".

- Si vous avez précédemment remappé un port que vous avez l'intention d'utiliser pour le point de terminaison de l'équilibreur de charge, vous avez ["supprimé le remappage du port"](#) .
- Vous avez créé tous les groupes de haute disponibilité (HA) que vous prévoyez d'utiliser. Les groupes HA sont recommandés, mais pas obligatoires. Voir ["Gérer les groupes de haute disponibilité"](#) .
- Si le point de terminaison de l'équilibreur de charge doit être utilisé par ["Locataires S3 pour S3 Select"](#) , il ne doit pas utiliser les adresses IP ou les noms de domaine complets de nœuds bare-metal. Seuls les dispositifs de services et les nœuds logiciels basés sur VMware sont autorisés pour les points de terminaison d'équilibrage de charge utilisés pour S3 Select.
- Vous avez configuré toutes les interfaces VLAN que vous prévoyez d'utiliser. Voir ["Configurer les interfaces VLAN"](#) .
- Si vous créez un point de terminaison HTTPS (recommandé), vous disposez des informations relatives au certificat du serveur.



Les modifications apportées à un certificat de point de terminaison peuvent prendre jusqu'à 15 minutes pour être appliquées à tous les nœuds.

- Pour télécharger un certificat, vous avez besoin du certificat du serveur, de la clé privée du certificat et, éventuellement, d'un bundle CA.
- Pour générer un certificat, vous avez besoin de tous les noms de domaine et adresses IP que les clients S3 utiliseront pour accéder au point de terminaison. Vous devez également connaître le sujet (Nom distinctif).
- Si vous souhaitez utiliser le certificat API StorageGRID S3 (qui peut également être utilisé pour les connexions directes aux nœuds de stockage), vous avez déjà remplacé le certificat par défaut par un certificat personnalisé signé par une autorité de certification externe. Voir ["Configurer les certificats API S3"](#) .

Créer un point de terminaison d'équilibrage de charge

Chaque point de terminaison d'équilibrage de charge client S3 spécifie un port, un type de client (S3) et un protocole réseau (HTTP ou HTTPS). Les points de terminaison de l'équilibreur de charge de l'interface de gestion spécifient un port, un type d'interface et un réseau client non approuvé.

Accéder à l'assistant

Étapes

1. Sélectionnez **CONFIGURATION > Réseau > Points de terminaison de l'équilibreur de charge**.
2. Pour créer un point de terminaison pour un client S3 ou Swift, sélectionnez l'onglet **Client S3 ou Swift**.
3. Pour créer un point de terminaison pour l'accès au Grid Manager, au Tenant Manager ou aux deux, sélectionnez l'onglet **Interface de gestion**.
4. Sélectionnez **Créer**.

Entrez les détails du point de terminaison

Étapes

1. Sélectionnez les instructions appropriées pour saisir les détails du type de point de terminaison que vous souhaitez créer.

Client S3 ou Swift

Champ	Description
Nom	Un nom descriptif pour le point de terminaison, qui apparaîtra dans le tableau de la page Points de terminaison de l'équilibreur de charge.
Port	Le port StorageGRID que vous souhaitez utiliser pour l'équilibrage de charge. Ce champ est défini par défaut sur 10433 pour le premier point de terminaison que vous créez, mais vous pouvez saisir n'importe quel port externe inutilisé compris entre 1 et 65535. Si vous entrez 80 ou 8443, le point de terminaison est configuré uniquement sur les nœuds de passerelle, sauf si vous avez libéré le port 8443. Vous pouvez ensuite utiliser le port 8443 comme point de terminaison S3, et le port sera configuré sur les nœuds de passerelle et d'administration.
Type de client	Le type d'application cliente qui utilisera ce point de terminaison, soit S3 ou Swift .
Protocole réseau	Le protocole réseau que les clients utiliseront lors de la connexion à ce point de terminaison. • Sélectionnez HTTPS pour une communication sécurisée et cryptée TLS (recommandé). Vous devez joindre un certificat de sécurité avant de pouvoir enregistrer le point de terminaison. • Sélectionnez HTTP pour une communication moins sécurisée et non chiffrée. Utilisez HTTP uniquement pour une grille non destinée à la production.

Interface de gestion

Champ	Description
Nom	Un nom descriptif pour le point de terminaison, qui apparaîtra dans le tableau de la page Points de terminaison de l'équilibreur de charge.
Port	Le port StorageGRID que vous souhaitez utiliser pour accéder au Grid Manager, au Tenant Manager ou aux deux. • Gestionnaire de grille : 8443 • Gestionnaire locataire : 9443 • Gestionnaire de réseau et gestionnaire de locataire : 443 Remarque : Vous pouvez utiliser ces ports prédéfinis ou d'autres ports disponibles.
Type d'interface	Sélectionnez le bouton radio correspondant à l'interface StorageGRID à laquelle vous accéderez à l'aide de ce point de terminaison.

Champ	Description
Réseau de clients non fiables	Sélectionnez Oui si ce point de terminaison doit être accessible aux réseaux clients non approuvés. Sinon, sélectionnez Non. Lorsque vous sélectionnez Oui, le port est ouvert sur tous les réseaux clients non approuvés. Remarque : vous ne pouvez configurer un port pour qu'il soit ouvert ou fermé sur des réseaux clients non approuvés que lorsque vous créez le point de terminaison de l'équilibreur de charge.

1. Sélectionnez **Continuer**.

Sélectionnez un mode de reliure

Étapes

1. Sélectionnez un mode de liaison pour le point de terminaison afin de contrôler la manière dont le point de terminaison est accessible à l'aide de n'importe quelle adresse IP ou à l'aide d'adresses IP et d'interfaces réseau spécifiques.

Certains modes de liaison sont disponibles pour les points de terminaison client ou les points de terminaison d'interface de gestion. Tous les modes pour les deux types de points de terminaison sont répertoriés ici.

Mode	Description
Global (par défaut pour les points de terminaison client)	Les clients peuvent accéder au point de terminaison à l'aide de l'adresse IP de n'importe quel nœud de passerelle ou nœud d'administration, de l'adresse IP virtuelle (VIP) de n'importe quel groupe HA sur n'importe quel réseau ou d'un nom de domaine complet correspondant. Utilisez le paramètre Global sauf si vous devez restreindre l'accessibilité de ce point de terminaison.
IP virtuelles des groupes HA	Les clients doivent utiliser une adresse IP virtuelle (ou un nom de domaine complet correspondant) d'un groupe HA pour accéder à ce point de terminaison. Les points de terminaison avec ce mode de liaison peuvent tous utiliser le même numéro de port, à condition que les groupes HA que vous sélectionnez pour les points de terminaison ne se chevauchent pas.
Interfaces de nœuds	Les clients doivent utiliser les adresses IP (ou les noms de domaine complets correspondants) des interfaces de nœuds sélectionnées pour accéder à ce point de terminaison.

Mode	Description
Type de nœud (points de terminaison client uniquement)	En fonction du type de nœud que vous sélectionnez, les clients doivent utiliser soit l'adresse IP (ou le nom de domaine complet correspondant) de n'importe quel nœud d'administration, soit l'adresse IP (ou le nom de domaine complet correspondant) de n'importe quel nœud de passerelle pour accéder à ce point de terminaison.
Tous les nœuds d'administration (par défaut pour les points de terminaison de l'interface de gestion)	Les clients doivent utiliser l'adresse IP (ou le nom de domaine complet correspondant) de n'importe quel nœud d'administration pour accéder à ce point de terminaison.

Si plusieurs points de terminaison utilisent le même port, StorageGRID utilise cet ordre de priorité pour décider quel point de terminaison utiliser : **IP virtuelles des groupes HA > Interfaces de nœud > Type de nœud > Global**.

Si vous créez des points de terminaison d'interface de gestion, seuls les nœuds d'administration sont autorisés.

2. Si vous avez sélectionné **IP virtuelles des groupes HA**, sélectionnez un ou plusieurs groupes HA.

Si vous créez des points de terminaison d'interface de gestion, sélectionnez les VIP associés uniquement aux nœuds d'administration.

3. Si vous avez sélectionné **Interfaces de nœud**, sélectionnez une ou plusieurs interfaces de nœud pour chaque nœud d'administration ou nœud de passerelle que vous souhaitez associer à ce point de terminaison.
4. Si vous avez sélectionné **Type de nœud**, sélectionnez soit les nœuds d'administration, qui incluent à la fois le nœud d'administration principal et tous les nœuds d'administration non principaux, soit les nœuds de passerelle.

Contrôler l'accès des locataires



Un point de terminaison d'interface de gestion peut contrôler l'accès des locataires uniquement lorsque le point de terminaison dispose du [type d'interface de Tenant Manager](#).

Étapes

1. Pour l'étape **Accès locataire**, sélectionnez l'une des options suivantes :

Champ	Description
Autoriser tous les locataires (par défaut)	Tous les comptes locataires peuvent utiliser ce point de terminaison pour accéder à leurs buckets. Vous devez sélectionner cette option si vous n'avez pas encore créé de compte locataire. Après avoir ajouté des comptes locataires, vous pouvez modifier le point de terminaison de l'équilibreur de charge pour autoriser ou bloquer des comptes spécifiques.

Champ	Description
Autoriser les locataires sélectionnés	Seuls les comptes locataires sélectionnés peuvent utiliser ce point de terminaison pour accéder à leurs compartiments.
Bloquer les locataires sélectionnés	Les comptes locataires sélectionnés ne peuvent pas utiliser ce point de terminaison pour accéder à leurs compartiments. Tous les autres locataires peuvent utiliser ce point de terminaison.

- Si vous créez un point de terminaison **HTTP**, vous n'avez pas besoin de joindre un certificat. Sélectionnez **Créer** pour ajouter le nouveau point de terminaison de l'équilibreur de charge. Ensuite, allez à [Après avoir terminé](#). Sinon, sélectionnez **Continuer** pour joindre le certificat.

Joindre un certificat

Étapes

- Si vous créez un point de terminaison **HTTPS**, sélectionnez le type de certificat de sécurité que vous souhaitez attacher au point de terminaison.

Le certificat sécurise les connexions entre les clients S3 et le service Load Balancer sur le nœud d'administration ou les nœuds de passerelle.

- **Télécharger le certificat.** Sélectionnez cette option si vous avez des certificats personnalisés à télécharger.
- **Générer un certificat.** Sélectionnez cette option si vous disposez des valeurs nécessaires pour générer un certificat personnalisé.
- **Utilisez le certificat StorageGRID S3.** Sélectionnez cette option si vous souhaitez utiliser le certificat API S3 global, qui peut également être utilisé pour les connexions directes aux nœuds de stockage.

Vous ne pouvez pas sélectionner cette option à moins d'avoir remplacé le certificat API S3 par défaut, signé par l'autorité de certification de grille, par un certificat personnalisé signé par une autorité de certification externe. Voir ["Configurer les certificats API S3"](#).

- **Utiliser le certificat d'interface de gestion.** Sélectionnez cette option si vous souhaitez utiliser le certificat d'interface de gestion globale, qui peut également être utilisé pour les connexions directes aux nœuds d'administration.
- Si vous n'utilisez pas le certificat StorageGRID S3, 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** : Le fichier de certificat de serveur personnalisé au format PEM.
- **Clé privée du certificat** : Le fichier de clé privée du certificat du serveur personnalisé(.key).



Les clés privées EC doivent être de 224 bits ou plus. Les clés privées RSA doivent être de 2 048 bits ou plus.

- **CA bundle** : un fichier facultatif unique contenant les certificats de chaque autorité de certification émettrice intermédiaire (CA). Le fichier doit contenir chacun des fichiers de certificat CA codés en PEM, concaténés dans l'ordre de la chaîne de certificats.

c. Développez **Détails du certificat** pour voir 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 bundle CA** pour enregistrer le bundle 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 **Copier le certificat PEM** ou **Copier le bundle CA PEM** pour copier le contenu du certificat afin de le coller ailleurs.

d. Sélectionnez **Créer**. + Le point de terminaison de l'équilibreur de charge est créé. Le certificat personnalisé est utilisé pour toutes les nouvelles connexions ultérieures entre les clients S3 ou l'interface de gestion et le point de terminaison.

Générer un certificat

a. Sélectionnez **Générer un certificat**.

b. Spécifiez les informations du certificat :

Champ	Description
Nom de domaine	Un ou plusieurs noms de domaine entièrement qualifiés à inclure dans le certificat. Utilisez un * comme caractère générique pour représenter plusieurs noms de domaine.
propriété intellectuelle	Une ou plusieurs adresses IP à inclure dans le certificat.
Sujet (facultatif)	Sujet 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 adresse IP comme nom commun du sujet (CN).

Champ	Description
Jours de validité	Nombre de jours après la création pendant lesquels le certificat expire.
Ajouter des extensions d'utilisation de clés	Si cette option est sélectionnée (par défaut et recommandé), les extensions d'utilisation de clé et d'utilisation de clé étendue sont ajoutées au certificat généré. Ces extensions définissent l'objectif de la clé contenue dans le certificat. Remarque : laissez cette case à cocher sélectionnée, sauf si vous rencontrez des problèmes de connexion avec des clients plus anciens lorsque les certificats incluent ces extensions.

c. Sélectionnez **Générer**.

d. Sélectionnez **Détails du certificat** pour voir 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 afin de le coller ailleurs.

e. Sélectionnez **Créer**.

Le point de terminaison de l'équilibreur de charge est créé. Le certificat personnalisé est utilisé pour toutes les nouvelles connexions ultérieures entre les clients S3 ou l'interface de gestion et ce point de terminaison.

Après avoir 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 du fait que vous utilisez ou non un groupe HA de nœuds d'équilibrage de charge :

- Si vous avez configuré un groupe HA, les clients se connecteront aux adresses IP virtuelles de ce groupe HA.
- Si vous n'utilisez pas de groupe HA, les clients se connecteront 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 de terminaison requis, y compris tous les noms génériques.

2. Fournissez aux clients S3 les informations nécessaires pour se connecter au point de terminaison :

- Numéro de port
- Nom de domaine entièrement qualifié ou adresse IP
- Tous les détails du certificat requis

Afficher et modifier les points de terminaison de l'équilibreur de charge

Vous pouvez afficher les détails des points de terminaison d'équilibrage de charge existants, y compris les métadonnées du certificat pour un point de terminaison sécurisé. Vous pouvez modifier certains paramètres d'un point de terminaison.

- Pour afficher les informations de base de tous les points de terminaison de l'équilibreur de charge, consultez les tableaux sur la page Points de terminaison de l'équilibreur de charge.
- Pour afficher tous les détails sur un point de terminaison spécifique, y compris les métadonnées du certificat, sélectionnez le nom du point de terminaison dans le tableau. Les informations affichées varient en fonction du type de point de terminaison et de sa configuration.

S3 load balancer endpoint

Port:	10443
Client type:	S3
Network protocol:	HTTPS
Binding mode:	Global
Endpoint ID:	3d02c126-9437-478c-8b24-08384401d3cb

Remove

Binding mode

Certificate

Tenant access (2 allowed)

You can select a different binding mode or change IP addresses for the current binding mode.

Edit binding mode

Binding mode: Global

 This endpoint uses the Global binding mode. Unless there are one or more overriding endpoints for the same port, clients can access this endpoint using the IP address of any Gateway Node, any Admin Node, or the virtual IP of any HA group on any network.

- Pour modifier un point de terminaison, utilisez le menu **Actions** sur la page Points de terminaison de l'équilibreur de charge.



Si vous perdez l'accès à Grid Manager lors de la modification du port d'un point de terminaison d'interface de gestion, mettez à jour l'URL et le port pour retrouver l'accès.



Après avoir modifié un point de terminaison, vous devrez peut-être attendre jusqu'à 15 minutes pour que vos modifications soient appliquées à tous les nœuds.

Tâche	Menu Actions	Page de détails
Modifier le nom du point de terminaison	a. Cochez la case correspondant au point de terminaison. b. Sélectionnez Actions > Modifier le nom du point de terminaison. c. Entrez le nouveau nom. d. Sélectionnez Enregistrer.	a. Sélectionnez le nom du point de terminaison pour afficher les détails. b. Sélectionnez l'icône d'édition . c. Entrez le nouveau nom. d. Sélectionnez Enregistrer.
Modifier le port du point de terminaison	a. Cochez la case correspondant au point de terminaison. b. Sélectionnez Actions > Modifier le port du point de terminaison. c. Entrez un numéro de port valide. d. Sélectionnez Enregistrer.	<i>n / A</i>
Modifier le mode de liaison du point de terminaison	a. Cochez la case correspondant au point de terminaison. b. Sélectionnez Actions > Modifier le mode de liaison du point de terminaison. c. Mettez à jour le mode de liaison si nécessaire. d. Sélectionnez Enregistrer les modifications.	a. Sélectionnez le nom du point de terminaison 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 du point de terminaison	a. Cochez la case correspondant au point de terminaison. b. Sélectionnez Actions > Modifier le certificat du point de terminaison. c. Téléchargez ou générez un nouveau certificat personnalisé ou commencez à utiliser le certificat S3 global, selon vos besoins. d. Sélectionnez Enregistrer les modifications.	a. Sélectionnez le nom du point de terminaison pour afficher les détails. b. Sélectionnez l'onglet Certificat. c. Sélectionnez Modifier le certificat. d. Téléchargez ou générez un nouveau certificat personnalisé ou commencez à utiliser le certificat S3 global, selon vos besoins. e. Sélectionnez Enregistrer les modifications.

Tâche	Menu Actions	Page de détails
Modifier l'accès des locataires	a. Cochez la case correspondant au point de terminaison. b. Sélectionnez Actions > Modifier l'accès du locataire. c. Choisissez une option d'accès différente, sélectionnez ou supprimez des locataires de la liste, ou faites les deux. d. Sélectionnez Enregistrer les modifications.	a. Sélectionnez le nom du point de terminaison pour afficher les détails. b. Sélectionnez l'onglet Accès locataire. c. Sélectionnez Modifier l'accès du locataire. d. Choisissez une option d'accès différente, sélectionnez ou supprimez des locataires de la liste, ou faites les deux. e. Sélectionnez Enregistrer les modifications.

Supprimer les points de terminaison de l'équilibreur de charge

Vous pouvez supprimer un ou plusieurs points de terminaison à l'aide du menu **Actions**, ou vous pouvez supprimer un seul point de terminaison à partir de la page de détails.



Pour éviter toute interruption du client, mettez à jour toutes les applications clientes S3 affectées avant de supprimer un point de terminaison d'équilibrage de charge. Mettez à jour chaque client pour qu'il se connecte à l'aide d'un port attribué à un autre point de terminaison d'équilibrage de charge. Assurez-vous également de mettre à jour toutes les informations de certificat requises.



Si vous perdez l'accès à Grid Manager lors de la suppression d'un point de terminaison d'interface de gestion, mettez à jour l'URL.

- Pour supprimer un ou plusieurs points de terminaison :
 - a. Sur la page Équilibreur de charge, cochez la case correspondant à chaque point de terminaison que vous souhaitez supprimer.
 - b. Sélectionnez **Actions > Supprimer**.
 - c. Sélectionnez **OK**.
- Pour supprimer un point de terminaison de la page de détails :
 - a. Depuis la page Équilibreur de charge, sélectionnez le nom du point de terminaison.
 - b. Sélectionnez **Supprimer** sur la page de détails.
 - c. Sélectionnez **OK**.

Configurer les noms de domaine des points de terminaison S3

Pour prendre en charge les demandes de type S3 hébergées virtuellement, vous devez utiliser le gestionnaire de grille pour configurer la liste des noms de domaine de point de terminaison S3 auxquels les clients S3 se connectent.



L'utilisation d'une adresse IP pour un nom de domaine de point de terminaison n'est pas prise en charge. Les versions futures empêcheront cette configuration.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un ["navigateur Web pris en charge"](#).
- Tu as ["autorisations d'accès spécifiques"](#).
- Vous avez confirmé qu'une mise à niveau du réseau n'est pas en cours.



N'apportez aucune modification à la configuration du nom de domaine lorsqu'une mise à niveau de la grille est en cours.

À propos de cette tâche

Pour permettre aux clients d'utiliser les noms de domaine de point de terminaison S3, vous devez effectuer toutes les opérations suivantes :

- Utilisez le gestionnaire de grille pour ajouter les noms de domaine de point de terminaison S3 au système StorageGRID.
- Assurez-vous que le ["certificat que le client utilise pour les connexions HTTPS à StorageGRID"](#) est signé pour tous les noms de domaine dont le client a besoin.

Par exemple, si le point final est `s3.company.com`, vous devez vous assurer que le certificat utilisé pour les connexions HTTPS inclut le `s3.company.com` point de terminaison et le nom alternatif du sujet (SAN) générique du point de terminaison : `*.s3.company.com`.

- Configurer le serveur DNS utilisé par le client. Incluez les enregistrements DNS pour les adresses IP que les clients utilisent pour établir des connexions et assurez-vous que les enregistrements font référence à tous les noms de domaine de point de terminaison S3 requis, y compris tous 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 de haute disponibilité. Vous devez comprendre comment les applications clientes se connectent à la grille afin d'inclure les adresses IP correctes dans les enregistrements DNS.

Les clients qui utilisent des connexions HTTPS (recommandées) à la grille peuvent utiliser l'un de ces certificats :

- Les clients qui se connectent à un point de terminaison d'équilibrage de charge peuvent utiliser un certificat personnalisé pour ce point de terminaison. Chaque point de terminaison d'équilibrage de charge peut être configuré pour reconnaître différents noms de domaine de point de terminaison S3.
- Les clients qui se connectent à un point de terminaison d'équilibrage de charge ou directement à un nœud de stockage peuvent personnaliser le certificat API S3 global pour inclure tous les noms de domaine de point de terminaison S3 requis.



Si vous n'ajoutez pas de noms de domaine de point de terminaison S3 et que la liste est vide, la prise en charge des demandes de type S3 hébergées virtuellement est désactivée.

Ajouter un nom de domaine de point de terminaison S3

Étapes

1. Sélectionnez **CONFIGURATION > Réseau > Noms de domaine de point de terminaison S3**.
2. Saisissez 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 point de terminaison S3 requis.
 - Si les clients se connectent à un point de terminaison d'équilibrage de charge qui utilise son propre certificat, "[mettre à jour le certificat associé au point de terminaison](#)".
 - Si les clients se connectent à un point de terminaison d'équilibrage de charge qui utilise le certificat API S3 global ou directement aux nœuds de stockage, "[mettre à jour le certificat API S3 global](#)".
5. Ajoutez les enregistrements DNS requis pour garantir que les demandes de nom de domaine de point de terminaison peuvent être résolues.

Résultat

Désormais, lorsque les clients utilisent le point de terminaison `bucket.s3.company.com`, le serveur DNS résout le point de terminaison correct et le certificat authentifie le point de terminaison comme prévu.

Renommer un nom de domaine de point de terminaison S3

Si vous modifiez un nom utilisé par les applications S3, les demandes de type hébergé virtuellement échoueront.

Étapes

1. Sélectionnez **CONFIGURATION > Réseau > Noms de domaine de point de terminaison S3**.
2. Sélectionnez le champ du nom de domaine que vous souhaitez modifier et effectuez les modifications nécessaires.
3. Sélectionnez **Enregistrer**.
4. Sélectionnez **Oui** pour confirmer votre modification.

Supprimer un nom de domaine de point de terminaison S3

Si vous supprimez un nom utilisé par les applications S3, les demandes de type hébergé virtuellement échoueront.

Étapes

1. Sélectionnez **CONFIGURATION > Réseau > Noms de domaine de point de terminaison S3**.
2. Sélectionnez l'icône de suppression  à côté du nom de domaine.
3. Sélectionnez **Oui** pour confirmer la suppression.

Informations connexes

- "[Utiliser l'API REST S3](#)"
- "[Afficher les adresses IP](#)"
- "[Configurer des groupes de haute disponibilité](#)"

Résumé : Adresses IP et ports pour les connexions client

Pour stocker ou récupérer des objets, les applications clientes S3 se connectent au service Load Balancer, inclus sur tous les nœuds d'administration et les nœuds de passerelle, ou au service Local Distribution Router (LDR), inclus sur tous les nœuds de stockage.

Les applications clientes peuvent se connecter à StorageGRID à l'aide de l'adresse IP d'un nœud de grille et du numéro de port du service sur ce nœud. En option, vous pouvez créer des groupes haute disponibilité (HA) de nœuds d'équilibrage de charge pour fournir des connexions hautement disponibles qui utilisent 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 résume les différentes manières 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 points de terminaison d'équilibrage de charge et des groupes de haute disponibilité (HA), consultez [Où trouver les adresses IP](#) pour localiser ces valeurs dans le gestionnaire de grille.

Où la connexion est établie	Service auquel le client se connecte	adresse IP	Port
groupe HA	Équilibreur de charge	Adresse IP virtuelle d'un groupe HA	Port attribué au point de terminaison de l'équilibreur de charge
Nœud d'administration	Équilibreur de charge	Adresse IP du nœud d'administration	Port attribué au point de terminaison de l'équilibreur de charge
Nœud de passerelle	Équilibreur de charge	Adresse IP du nœud de passerelle	Port attribué au point de terminaison de l'équilibreur de charge
Nœud de stockage	LDR	Adresse IP du nœud de stockage	Ports S3 par défaut : • HTTPS : 18082 • HTTP : 18084

Exemples d'URL

Pour connecter une application cliente au point de terminaison de l'équilibreur de charge 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 192.0.2.5 et que le numéro de port du point de terminaison 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. Sign in 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 **NODES**.
 - 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 à partir d'applications clientes vers n'importe laquelle des adresses IP de la liste :

- **eth0**: Réseau de grille
- **eth1**: Réseau administrateur (facultatif)
- **eth2**: Réseau client (facultatif)



Si vous visualisez 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 HA est affichée sur eth2.

3. Pour trouver l'adresse IP virtuelle d'un groupe de haute disponibilité :
 - a. Sélectionnez **CONFIGURATION > Réseau > Groupes de haute disponibilité**.
 - b. Dans le tableau, notez l'adresse IP virtuelle du groupe HA.
4. Pour trouver le numéro de port d'un point de terminaison d'équilibreur de charge :
 - a. Sélectionnez **CONFIGURATION > Réseau > Points de terminaison de l'équilibreur de charge**.
 - b. Notez le numéro de port du point de terminaison que vous souhaitez utiliser.



Si le numéro de port est 80 ou 443, le point de terminaison est configuré uniquement sur les nœuds de passerelle, car ces ports sont réservés sur les nœuds d'administration. Tous les autres ports sont configurés sur les nœuds de passerelle et les nœuds d'administration.

- c. Sélectionnez le nom du point de terminaison dans le tableau.
- d. Confirmez que le **Type de client** (S3) correspond à l'application cliente qui utilisera le point de terminaison.

Gérer les réseaux et les connexions

Configurer les paramètres réseau

Vous pouvez configurer divers paramètres réseau à partir du Grid Manager pour affiner le fonctionnement de votre système StorageGRID .

Configurer les interfaces VLAN

Tu peux "[créer des interfaces LAN virtuelles \(VLAN\)](#)" pour isoler et partitionner le trafic pour la sécurité, la flexibilité et les performances. Chaque interface VLAN est associée à une ou plusieurs interfaces parentes sur les nœuds d'administration et les nœuds de passerelle. Vous pouvez utiliser des interfaces VLAN dans des groupes HA et dans des points de terminaison d'équilibrage de charge pour séparer le trafic client ou administrateur par application ou locataire.

Politiques de classification du trafic

Vous pouvez utiliser "[politiques de classification du trafic](#)" pour identifier et gérer différents types de trafic réseau, y compris le trafic lié à des compartiments spécifiques, des locataires, des sous-réseaux clients ou des points de terminaison d'équilibrage de charge. Ces politiques peuvent aider à limiter et à surveiller le trafic.

Lignes directrices pour les réseaux StorageGRID

Vous pouvez utiliser Grid Manager pour configurer et gérer les réseaux et connexions StorageGRID .

Voir "[Configurer les connexions client S3](#)" pour apprendre à connecter des clients S3.

Réseaux StorageGRID par défaut

Par défaut, StorageGRID prend en charge trois interfaces réseau par nœud de grille, ce qui vous permet de configurer la mise en réseau de chaque nœud de grille individuel afin de répondre à vos exigences de sécurité et d'accès.

Pour plus d'informations sur la topologie du réseau, voir "[Directives de mise en réseau](#)" .

Réseau de grille

Requis. Le réseau Grid est utilisé pour tout le trafic interne StorageGRID . Il fournit une connectivité entre tous les nœuds du réseau, 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 d'administration est généralement un réseau privé et n'a pas besoin d'être routable entre les sites.

Réseau de clients

Facultatif. Le réseau client est un réseau ouvert généralement utilisé pour fournir un accès aux applications client S3, de sorte que le réseau Grid peut être isolé et sécurisé. Le réseau client peut communiquer avec n'importe quel sous-réseau accessible via la passerelle locale.

Lignes directrices

- Chaque nœud 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 seule passerelle, par réseau, par nœud de grille est prise en charge et elle doit se trouver 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.

Réseau	Nom de l'interface
Grille	eth0
Administrateur (facultatif)	eth1
Client (facultatif)	eth2

- Si le nœud est connecté à un dispositif StorageGRID , des ports spécifiques sont utilisés pour chaque réseau. Pour plus de détails, consultez les instructions d'installation de votre appareil.
- L'itinéraire par défaut est généré automatiquement, par nœud. Si eth2 est activé, alors 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 ne devient opérationnel que lorsque le nœud de grille a rejoint le réseau
- Le réseau d'administration peut être configuré pendant le déploiement du nœud de grille pour permettre l'accès à l'interface utilisateur d'installation avant que la grille ne soit entièrement installée.

Interfaces optionnelles

En option, vous pouvez ajouter des interfaces supplémentaires à un nœud. Par exemple, vous souhaitez peut-être ajouter une interface de jonction à un nœud d'administration ou de passerelle, afin de pouvoir l'utiliser ["Interfaces VLAN"](#) pour séparer le trafic appartenant à différentes applications ou locataires. Ou, vous souhaitez peut-être ajouter une interface d'accès à utiliser dans un ["groupe de haute disponibilité \(HA\)"](#) .

Pour ajouter des interfaces de jonction ou d'accès, consultez les éléments suivants :

- **VMware (après l'installation du nœud):** ["VMware : ajouter des interfaces de jonction ou d'accès à un nœud"](#)
 - **Red Hat Enterprise Linux (avant l'installation du nœud):** ["Créer des fichiers de configuration de nœud"](#)
 - **Ubuntu ou Debian (avant d'installer le nœud) :** ["Créer des fichiers de configuration de nœud"](#)
 - **RHEL, Ubuntu ou Debian (après l'installation du nœud) :** ["Linux : ajouter des interfaces trunk ou d'accès à un nœud"](#)

Afficher les adresses IP

Vous pouvez afficher l'adresse IP de chaque nœud de grille 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"](#) .

À propos de cette tâche

Pour plus d'informations sur la modification des adresses IP, consultez ["Configurer les adresses IP"](#) .

Étapes

1. Sélectionnez **NODES** > *grid node* > **Aperçu**.
2. Sélectionnez **Afficher plus** à droite du titre Adresses IP.

Les adresses IP de ce nœud de grille sont répertoriées dans un tableau.

DC2-SGA-010-096-106-021 (Storage Node) [↗](#)



Overview Hardware Network Storage Objects ILM Tasks

Node information [?](#)

Name: DC2-SGA-010-096-106-021

Type: Storage Node

ID: f0890e03-4c72-401f-ae92-245511a38e51

Connection state: Connected

Storage used: Object data 7% [?](#)
Object metadata 5% [?](#)

Software version: 11.6.0 (build 20210915.1941.afce2d9)

IP addresses: 10.96.106.21 - eth0 (Grid Network)

[Hide additional IP addresses](#) [^](#)

Interface ⌵	IP address ⌵
eth0 (Grid Network)	10.96.106.21
eth0 (Grid Network)	fe80::2a0:98ff:fe64:6582
hic2	10.96.106.21
hic4	10.96.106.21
mtc2	169.254.0.1

Alerts

Alert name ⌵	Severity ? ⌵	Time triggered ⌵	Current values
ILM placement unachievable ↗	Major	2 hours ago ?	
A placement instruction in an ILM rule cannot be achieved for certain objects.			

Configurer les interfaces VLAN

Vous pouvez créer des interfaces LAN virtuelles (VLAN) sur des nœuds d'administration et des nœuds de passerelle et les utiliser dans des groupes HA et des points de terminaison d'équilibrage de charge pour isoler et partitionner le trafic pour la sécurité, la flexibilité et les performances.

Considérations relatives aux interfaces VLAN

- Vous créez une interface VLAN en saisissant un ID VLAN et en choisissant une interface parent sur un ou plusieurs nœuds.
- Une interface parent doit être configurée comme interface de jonction au niveau du commutateur.
- Une interface parent peut être le réseau Grid (eth0), le réseau client (eth2) ou une interface de jonction supplémentaire pour la machine virtuelle ou l'hôte bare-metal (par exemple, ens256).
- 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 de 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 gestionnaire de grille et au gestionnaire de locataires, sélectionnez les interfaces sur les nœuds d'administration uniquement.
- Si l'interface VLAN est destinée au trafic client S3, sélectionnez les interfaces sur les nœuds d'administration ou sur les nœuds de passerelle.
- Si vous devez ajouter des interfaces de jonction, consultez les éléments suivants pour plus de détails :
 - **VMware (après l'installation du nœud):** ["VMware : ajouter des interfaces de jonction ou d'accès à un nœud"](#)
 - **RHEL (avant l'installation du nœud):** ["Créer des fichiers de configuration de nœud"](#)
 - **Ubuntu ou Debian (avant d'installer le nœud) :** ["Créer des fichiers de configuration de nœud"](#)
 - **RHEL, Ubuntu ou Debian (après l'installation du nœud) :** ["Linux : ajouter des interfaces trunk ou d'accès à un nœud"](#)

Créer une interface VLAN

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 root"](#) .
- Une interface de jonction a été configurée dans le réseau et attachée au nœud VM ou Linux. Vous connaissez le nom de l'interface trunk.
- Vous connaissez l'ID du VLAN que vous configurez.

À propos de cette tâche

Votre administrateur réseau a peut-être configuré une ou plusieurs interfaces de jonction et un ou plusieurs VLAN pour séparer 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 les interfaces parentes (trunk) sur un ou plusieurs nœuds.

Accéder à l'assistant

Étapes

1. Sélectionnez **CONFIGURATION > Réseau > Interfaces VLAN**.
2. Sélectionnez **Créer**.

Saisissez les détails des interfaces VLAN

Étapes

1. Spécifiez l'ID du VLAN dans votre réseau. Vous pouvez saisir n'importe quelle valeur 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 administrateur 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 parentes 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 qui a déjà été utilisé, un message apparaît.

2. Vous pouvez également saisir une brève description de l'interface VLAN.
3. Sélectionnez **Continuer**.

Choisir les interfaces parentes

Le tableau répertorie les interfaces disponibles pour tous les nœuds d'administration et les nœuds de passerelle sur chaque site de votre grille. Les interfaces réseau d'administration (eth1) ne peuvent pas être utilisées comme interfaces parentes et ne sont pas affichées.

Étapes

1. Sélectionnez une ou plusieurs interfaces parentes auxquelles attacher ce VLAN.

Par exemple, vous souhaitez peut-être attacher un VLAN à l'interface réseau client (eth2) pour un nœud de passerelle et un nœud d'administration.

Parent interfaces

Select one or more parent interfaces for this VLAN interface. You can only select one parent interface on each node for each VLAN interface.

Search...

	Site ?	Node name ?	Interface ?	Description ?	Node type ?	Attached VLANs ?
☐	Data Center 2	DC2-ADM1	eth0	Grid Network	Non-primary Admin	—
☒	Data Center 2	DC2-ADM1	eth2	Client Network	Non-primary Admin	—
☐	Data Center 1	DC1-G1	eth0	Grid Network	Gateway	—
☒	Data Center 1	DC1-G1	eth2	Client Network	Gateway	—
☐	Data Center 1	DC1-ADM1	eth0	Grid Network	Primary Admin	—

2 interfaces are selected.

Previous

Continue

2. Sélectionnez **Continuer**.

Confirmer les paramètres

Étapes

1. Vérifiez 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 parente, sélectionnez **Choisir les interfaces parentes** 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 pour que la nouvelle interface apparaisse comme sélection sur la page Groupes de haute disponibilité et soit répertoriée dans la table **Interfaces réseau** pour le nœud (**NODES > parent interface node > Network**).

Modifier 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 parentes.

Par exemple, vous souhaitez peut-être supprimer une interface parent d'une interface VLAN si vous prévoyez de mettre hors service le nœud associé.

Notez ce qui suit :

- Vous ne pouvez pas modifier un ID VLAN si l'interface VLAN est utilisée dans un groupe HA.
- Vous ne pouvez pas supprimer une interface parente si cette interface parente est utilisée dans un groupe HA.

Par exemple, supposons que le VLAN 200 soit attaché aux interfaces parentes sur les 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 parente inutilisée pour le nœud B, mais vous ne pouvez pas supprimer l'interface parente utilisée pour le nœud A.

Étapes

1. Sélectionnez **CONFIGURATION > Réseau > Interfaces VLAN**.
2. Cochez la case correspondant à l'interface VLAN que vous souhaitez modifier. Ensuite, sélectionnez **Actions > Modifier**.
3. Vous pouvez également mettre à jour l'ID VLAN ou la description. Ensuite, sélectionnez **Continuer**.

Vous ne pouvez pas mettre à jour un ID VLAN si le VLAN est utilisé dans un groupe HA.

4. Vous pouvez également cocher ou décocher les cases pour ajouter des interfaces parentes ou pour supprimer les interfaces inutilisées. Ensuite, sélectionnez **Continuer**.
5. Vérifiez la configuration et apportez les modifications nécessaires.
6. Sélectionnez **Enregistrer**.

Supprimer 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 HA. Vous devez supprimer l'interface VLAN du groupe HA avant de pouvoir la supprimer.

Pour éviter toute interruption du trafic client, envisagez d'effectuer l'une des opérations suivantes :

- Ajoutez une nouvelle interface VLAN au groupe HA avant de supprimer cette interface VLAN.
- Créez un nouveau groupe HA 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 vers le bas de la liste des priorités. Attendez que la communication soit établie sur la nouvelle interface principale, puis supprimez l'ancienne interface du groupe HA. Enfin, supprimez l'interface VLAN sur ce nœud.

Étapes

1. Sélectionnez **CONFIGURATION > Réseau > Interfaces VLAN**.
2. Cochez la case correspondant à chaque interface VLAN que vous souhaitez supprimer. Ensuite, sélectionnez **Actions > Supprimer**.
3. Sélectionnez **Oui** pour confirmer votre sélection.

Toutes les interfaces VLAN que vous avez sélectionnées sont supprimées. Une bannière de réussite verte apparaît sur la page des interfaces VLAN.

Gérer les politiques de classification du trafic

Quelles sont les politiques de classification du trafic ?

Les politiques de classification du trafic vous permettent d'identifier et de surveiller différents types de trafic réseau. Ces politiques peuvent vous aider à limiter et à surveiller le trafic afin d'améliorer vos offres de qualité de service (QoS).

Les stratégies de classification du trafic sont appliquées aux points de terminaison sur le service StorageGRID Load Balancer pour les nœuds de passerelle et les nœuds d'administration. Pour créer des politiques de classification du trafic, vous devez déjà avoir créé des points de terminaison d'équilibrage de charge.

Règles de correspondance

Chaque politique de classification du trafic contient une ou plusieurs règles de correspondance pour identifier le trafic réseau lié à une ou plusieurs des entités suivantes :

- Seaux
- Sous-réseau
- Locataire
- Points de terminaison de l'équilibreur de charge

StorageGRID surveille le trafic qui correspond à n'importe quelle règle de la politique en fonction des objectifs de la règle. Tout trafic correspondant à une règle d'une politique est géré par cette politique. À l'inverse, vous pouvez définir des règles pour correspondre à tout le trafic, à l'exception d'une entité spécifiée.

Limitation du trafic

En option, vous pouvez ajouter les types de limites suivants à une politique :

- Bande passante globale
- Bande passante par requête
- Demandes simultanées
- Taux de demande

Les valeurs limites sont appliquées pour chaque équilibreur de charge. Si le trafic est réparti simultanément sur plusieurs équilibreurs de charge, les débits maximum totaux sont un multiple des limites de débit que vous spécifiez.



Vous pouvez créer des politiques pour limiter la bande passante globale ou pour limiter la bande passante par demande. Cependant, StorageGRID ne peut pas limiter les deux types de bande passante en même temps. Les limites de bande passante globales peuvent avoir un impact mineur supplémentaire sur les performances du trafic non limité.

Pour les limites de bande passante globales ou par demande, les demandes entrent ou sortent au débit que vous définissez. StorageGRID ne peut appliquer qu'une seule vitesse, donc la correspondance de politique la plus spécifique, par type de correspondance, est celle appliquée. La bande passante consommée par la demande n'est pas comptabilisée dans d'autres politiques de correspondance moins spécifiques contenant des politiques de limite de bande passante globale. Pour tous les autres types de limites, les demandes des clients sont retardées de 250 millisecondes et reçoivent une réponse 503 Slow Down pour les demandes qui dépassent toute limite de politique correspondante.

Dans le gestionnaire de grille, vous pouvez afficher les graphiques de trafic et vérifier que les politiques appliquent les limites de trafic que vous attendez.

Utiliser des politiques de classification du trafic avec des SLA

Vous pouvez utiliser des stratégies de classification du trafic conjointement avec des limites de capacité et la protection des données pour appliquer des accords de niveau de service (SLA) qui fournissent des détails sur la capacité, la protection des données et les performances.

L'exemple suivant montre trois niveaux d'un SLA. Vous pouvez créer des stratégies de classification du trafic pour atteindre les objectifs de performances de chaque niveau SLA.

Niveau de service	Capacité	Protection des données	Performances maximales autorisées	Coût
Or	1 Po de stockage autorisé	Règle ILM en 3 exemplaires	25 000 requêtes/sec Bande passante de 5 Go/s (40 Gbps)	\$\$\$ par mois
Argent	250 To de stockage autorisé	Règle ILM en 2 exemplaires	10 000 requêtes/sec Bande passante de 1,25 Go/s (10 Gbps)	\$\$ par mois

Niveau de service	Capacité	Protection des données	Performances maximales autorisées	Coût
Bronze	100 To de stockage autorisé	Règle ILM en 2 exemplaires	5 000 requêtes/s Bande passante de 1 Go/s (8 Gbps)	\$ par mois

Créer des politiques de classification du trafic

Vous pouvez créer des stratégies de classification du trafic si vous souhaitez surveiller et éventuellement limiter le trafic réseau par bucket, regex de bucket, CIDR, point de terminaison d'équilibrage de charge ou locataire. Vous pouvez également définir des limites pour une politique 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 avez le ["Autorisation d'accès root"](#) .
- Vous avez créé tous les points de terminaison d'équilibrage de charge que vous souhaitez faire correspondre.
- Vous avez créé tous les locataires que vous souhaitez faire correspondre.

Étapes

1. Sélectionnez **CONFIGURATION > Réseau > Classification du trafic**.
2. Sélectionnez **Créer**.
3. Saisissez un nom et une description (facultatif) pour la politique et sélectionnez **Continuer**.

Par exemple, décrivez à quoi s'applique cette politique de classification du trafic et ce qu'elle limitera.

4. Sélectionnez **Ajouter une règle** et spécifiez les détails suivants pour créer une ou plusieurs règles correspondantes pour la politique. Toute politique que vous créez doit avoir au moins une règle correspondante. Sélectionnez **Continuer**.

Champ	Description
Type	Sélectionnez les types de trafic auxquels la règle de correspondance s'applique. Les types de trafic sont les suivants : bucket, bucket regex, CIDR, point de terminaison de l'équilibreur de charge et locataire.

Champ	Description
Valeur de correspondance	Saisissez la valeur qui correspond au type sélectionné. • Bucket : saisissez un ou plusieurs noms de bucket. • Expression régulière de compartiment : saisissez une ou plusieurs expressions régulières utilisées pour faire correspondre un ensemble de noms de compartiment. L'expression régulière n'est pas ancrée. Utilisez l'ancre ^ pour faire correspondre le début du nom du bucket et utilisez l'ancre \$ pour faire correspondre la fin du nom. La correspondance d'expressions régulières 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. • Point de terminaison de l'équilibreur de charge : sélectionnez un nom de point de terminaison. Ce sont les points de terminaison de l'équilibreur de charge que vous avez définis sur le "Configurer les points de terminaison de l'équilibreur de charge" . • Locataire : la correspondance des locataires 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 bucket consulté est utilisée pour déterminer le locataire.
Correspondance inverse	Si vous souhaitez faire correspondre tout le trafic réseau <i>à l'exception</i> du trafic cohérent avec le type et la valeur de correspondance qui viennent d'être définis, cochez la case Correspondance inverse. Sinon, laissez la case à cocher décochée. Par exemple, si vous souhaitez que cette stratégie s'applique à tous les points de terminaison de l'équilibreur de charge sauf un, spécifiez le point de terminaison de l'équilibreur de charge à exclure et sélectionnez Correspondance inverse. Pour une politique contenant plusieurs correspondances où au moins l'une d'elles est une correspondance inverse, veillez à ne pas créer une politique qui correspond à toutes les demandes.

5. Vous pouvez également sélectionner **Ajouter une limite** et sélectionner les détails suivants pour ajouter une ou plusieurs limites afin de contrôler le trafic réseau correspondant à une règle.



StorageGRID collecte des métriques même si vous n'ajoutez aucune limite, afin que vous puissiez comprendre les tendances du trafic.

Champ	Description
Type	Le type de limite que vous souhaitez appliquer au trafic réseau correspondant à la règle. Par exemple, vous pouvez limiter la bande passante ou le débit de requête. Remarque : vous pouvez créer des politiques pour limiter la bande passante globale ou pour limiter la bande passante par requête. Cependant, StorageGRID ne peut pas limiter les deux types de bande passante en même temps. Lorsque la bande passante agrégée est utilisée, la bande passante par demande n'est pas disponible. À l'inverse, lorsque la bande passante par demande est utilisée, la bande passante globale n'est pas disponible. Les limites de bande passante globales peuvent avoir un impact mineur supplémentaire sur les performances du trafic non limité. Pour les limites de bande passante, StorageGRID applique la politique qui correspond le mieux au type de limite définie. Par exemple, si vous avez une politique qui limite le trafic dans une seule direction, le trafic dans la direction opposée sera illimité, même s'il existe du trafic correspondant à des politiques supplémentaires qui ont des limites de bande passante. StorageGRID implémente les « meilleures » correspondances pour les limites de bande passante dans l'ordre suivant : • Adresse IP exacte (masque /32) • Nom exact du bucket • Expression régulière de bucket • Locataire • Point final • Correspondances CIDR non exactes (pas /32) • Correspondances inverses
S'applique à	Si cette limite s'applique aux demandes de lecture client (GET ou HEAD) ou aux demandes d'écriture (PUT, POST ou DELETE).
Valeur	La valeur à laquelle le trafic réseau sera limité, en fonction de l'unité que vous sélectionnez. Par exemple, entrez 10 et sélectionnez Mio/s pour empêcher le trafic réseau correspondant à cette règle de dépasser 10 Mio/s. Remarque : Selon le paramètre des unités, les unités disponibles seront soit binaires (par exemple, Gio) soit décimales (par exemple, Go). Pour modifier le paramètre des unités, sélectionnez la liste déroulante utilisateur dans le coin supérieur droit du gestionnaire de grille, puis sélectionnez Préférences utilisateur.
Unité	L'unité qui décrit la valeur que vous avez saisie.

Par exemple, si vous souhaitez créer une limite de bande passante de 40 Go/s pour un niveau SLA, créez deux limites de bande passante agrégées : GET/HEAD à 40 Go/s et PUT/POST/DELETE à 40 Go/s.

6. Sélectionnez **Continuer**.

7. Lisez et révisez 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 politique, sélectionnez **Enregistrer et continuer**.

Le trafic client S3 est désormais géré conformément à la politique de classification du trafic.

Après avoir terminé

"[Afficher les mesures du trafic réseau](#)" pour vérifier que les policiers appliquent les limites de circulation que vous attendez.

Modifier la politique de classification du trafic

Vous pouvez modifier une politique de classification du trafic pour changer son nom ou sa description, ou pour créer, modifier ou supprimer des règles ou des limites pour la politique.

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 root](#)".

Étapes

1. Sélectionnez **CONFIGURATION > Réseau > Classification du trafic**.

La page Stratégies de classification du trafic s'affiche et les stratégies existantes sont répertoriées dans un tableau.

2. Modifiez la politique en utilisant le menu Actions ou la page de détails. Voir "[créer des politiques de classification du trafic](#)" pour quoi entrer.

Menu Actions

- a. Cochez la case correspondant à la politique.
- b. Sélectionnez **Actions > Modifier**.

Page de détails

- a. Sélectionnez le nom de la politique.
- b. Sélectionnez le bouton **Modifier** à côté du nom de la politique.

3. Pour l'étape Saisir le nom de la politique, modifiez éventuellement le nom ou la description de la politique et sélectionnez **Continuer**.
4. Pour l'étape Ajouter des règles de correspondance, ajoutez éventuellement une règle ou modifiez le **Type** et la **Valeur de correspondance** de la règle existante, puis sélectionnez **Continuer**.
5. Pour l'étape Définir les limites, ajoutez, modifiez ou supprimez éventuellement une limite et sélectionnez **Continuer**.
6. Consultez la politique mise à jour et sélectionnez **Enregistrer et continuer**.

Les modifications que vous avez apportées à la politique sont enregistrées et le trafic réseau est désormais géré conformément aux politiques de classification du trafic. Vous pouvez consulter les graphiques de circulation et vérifier que les politiques appliquent les limites de circulation que vous

attendez.

Supprimer une politique de classification du trafic

Vous pouvez supprimer une politique de classification du trafic si vous n'en avez plus besoin. Assurez-vous de supprimer la bonne politique, car une politique 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 avez le ["Autorisation d'accès root"](#).

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 politique en utilisant le menu Actions ou la page de détails.

Menu Actions

- a. Cochez la case correspondant à la politique.
- b. Sélectionnez **Actions > Supprimer**.

Page de détails de la politique

- a. Sélectionnez le nom de la politique.
- b. Sélectionnez le bouton **Supprimer** à côté du nom de la politique.

3. Sélectionnez **Oui** pour confirmer que vous souhaitez supprimer la politique.

La politique est supprimée.

Afficher les mesures du trafic réseau

Vous pouvez surveiller le trafic réseau en affichant les graphiques disponibles sur 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 avez le ["Accès root ou autorisation des comptes locataires"](#).

À propos de cette tâche

Pour toute stratégie de classification du trafic existante, vous pouvez afficher les métriques du service d'équilibrage de charge afin de déterminer si la stratégie limite avec succès le trafic sur le réseau. Les données des graphiques peuvent vous aider à déterminer si vous devez ajuster la politique.

Même si aucune limite n'est définie pour une politique de classification du trafic, des mesures sont collectées et les graphiques fournissent des informations utiles pour comprendre les tendances du trafic.

Étapes

1. Sélectionnez **CONFIGURATION > Réseau > Classification du trafic**.

La page Stratégies de classification du trafic s'affiche et les stratégies existantes sont répertoriées dans le tableau.

2. Sélectionnez le nom de la politique de classification du trafic pour laquelle vous souhaitez afficher les métriques.
3. Sélectionnez l'onglet **Métriques**.

Les graphiques de la politique de classification du trafic apparaissent. Les graphiques affichent les métriques uniquement pour le trafic correspondant à la politique sélectionnée.

Les graphiques suivants sont inclus sur la page.

- Taux de demande : ce graphique fournit la quantité de bande passante correspondant à cette politique gérée par tous les équilibres de charge. Les données reçues incluent les en-têtes de demande pour toutes les demandes et la taille des données du corps pour les réponses contenant des données du corps. Sent inclut les en-têtes de réponse pour toutes les demandes et la taille des données du corps de la réponse pour les demandes qui incluent des données de corps dans la réponse.



Lorsque les demandes sont terminées, ce graphique affiche uniquement l'utilisation de la bande passante. Pour les demandes d'objets lentes ou volumineuses, la bande passante instantanée réelle peut différer des valeurs indiquées dans ce graphique.

- Taux de réponse aux erreurs : ce graphique fournit un taux approximatif auquel les requêtes correspondant à cette politique renvoient des erreurs (code d'état HTTP ≥ 400) aux clients.
 - Durée moyenne des requêtes (sans erreur) : ce graphique fournit une durée moyenne des requêtes réussies correspondant à cette politique.
 - Utilisation de la bande passante de la politique : ce graphique fournit la quantité de bande passante correspondant à cette politique gérée par tous les équilibres de charge. Les données reçues incluent les en-têtes de demande pour toutes les demandes et la taille des données du corps pour les réponses contenant des données du corps. Sent inclut les en-têtes de réponse pour toutes les demandes et la taille des données du corps de la réponse pour les demandes qui incluent des données de corps dans la réponse.
4. Positionnez le curseur sur un graphique linéaire pour voir une fenêtre contextuelle de valeurs sur une partie spécifique du graphique.
 5. Sélectionnez **Tableau de bord Grafana** juste en dessous du titre Métriques pour afficher tous les graphiques d'une politique. 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 de demandes PUT/POST/DELETE correspondant à cette politique. Le positionnement sur une cellule individuelle affiche les taux par seconde. Les taux affichés dans la vue de survol sont tronqués en nombres entiers et peuvent indiquer 0 lorsqu'il y a des demandes différentes de zéro dans le bucket.
 - Taux de demande de lecture par taille d'objet : taux de demandes GET/HEAD correspondant à cette politique. Le positionnement sur une cellule individuelle affiche les taux par seconde. Les taux affichés dans la vue de survol sont tronqués en nombres entiers et peuvent indiquer 0 lorsqu'il y a des demandes différentes de zéro dans le bucket.
 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 politique dans le menu en haut à gauche de la page.
- d. Placez le curseur sur un graphique pour voir une fenêtre contextuelle indiquant la date et l'heure de l'échantillon, les tailles d'objets agrégées dans le décompte et le nombre de requêtes par seconde pendant cette période.

Les politiques de classification du trafic sont identifiées par leur ID. Les identifiants de stratégie sont répertoriés sur la page **Stratégies de classification du trafic**.

7. Analysez les graphiques pour déterminer à quelle fréquence la politique limite le trafic et si vous devez ajuster la politique.

Chiffres 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) aux systèmes externes utilisés pour la fédération d'identité et les pools de stockage cloud.

Versions prises en charge de TLS

StorageGRID prend en charge TLS 1.2 et TLS 1.3 pour les connexions aux systèmes externes utilisés pour la fédération d'identité et les pools de stockage cloud.

Les chiffrements TLS pris en charge pour une utilisation avec des systèmes externes ont été sélectionnés pour garantir la compatibilité avec une gamme de systèmes externes. La liste est plus longue que la liste des chiffrements pris en charge pour une utilisation avec les applications clientes S3. Pour configurer les chiffrements, accédez à **CONFIGURATION > Sécurité > Paramètres de sécurité** et sélectionnez **Politiques 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 représentant de compte NetApp si vous avez des demandes spécifiques concernant ces paramètres.

Avantages des connexions HTTP actives, inactives et simultanées

La façon dont vous configurez les connexions HTTP peut avoir un impact sur les performances du système StorageGRID. Les configurations diffèrent selon que la connexion HTTP est active ou inactive ou que vous avez plusieurs connexions simultanées.

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 garder les connexions HTTP inactives ouvertes

Vous devez garder les connexions HTTP ouvertes même lorsque les applications clientes sont inactives pour permettre aux applications clientes d'effectuer des transactions ultérieures sur la connexion ouverte. Sur la base des mesures du système et de l'expérience d'intégration, vous devez maintenir une connexion HTTP inactive ouverte pendant 10 minutes maximum. StorageGRID peut fermer automatiquement une connexion HTTP maintenue ouverte et inactive pendant plus de 10 minutes.

Les connexions HTTP ouvertes et inactives offrent les avantages suivants :

- Latence réduite 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 latence réduite est le principal avantage, en particulier compte tenu du temps nécessaire à l'établissement des connexions TCP/IP et TLS.

- Augmentation du taux de transfert de données en amorçant l'algorithme de démarrage lent TCP/IP avec les transferts précédemment effectués
- Notification instantanée de plusieurs classes de conditions de panne qui interrompent la connectivité entre l'application cliente et le système StorageGRID

Déterminer la durée pendant laquelle maintenir une connexion inactive ouverte est un compromis entre les avantages d'un démarrage lent associé à la connexion existante et l'allocation idéale de la connexion aux ressources internes du système.

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 en continu des transactions.

Déterminer la durée maximale pendant laquelle une connexion doit rester ouverte est un compromis entre les avantages de la persistance de la connexion et l'allocation idéale de la connexion aux ressources internes du système.

Pour les connexions client aux nœuds de stockage, la limitation des connexions HTTP actives offre les avantages suivants :

- Permet un équilibrage de charge optimal sur le système StorageGRID .

Au fil du temps, une connexion HTTP peut ne plus être optimale à mesure que les exigences d'équilibrage de charge changent. Le système réalise son meilleur équilibrage de charge lorsque les applications clientes établissent une connexion HTTP distincte pour chaque transaction, mais cela annule les gains bien plus précieux associés aux connexions persistantes.

- Permet aux applications clientes de diriger les transactions HTTP vers les services LDR disposant d'espace disponible.
- Permet de démarrer les procédures de maintenance.

Certaines procédures de maintenance démarrent uniquement 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 à certaines procédures de maintenance de démarrer rapidement. Si la durée des connexions client n'est pas limitée, la fin automatique des connexions actives peut prendre plusieurs minutes.

Avantages des connexions HTTP simultanées

Vous devez conserver plusieurs connexions TCP/IP au système StorageGRID ouvertes 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 démarrer immédiatement au lieu d'attendre que d'autres transactions soient terminées.

- Augmentation du débit

Le système StorageGRID peut effectuer des transactions parallèles et augmenter le débit global des transactions.

Les applications clientes doivent établir plusieurs connexions HTTP. Lorsqu'une application cliente doit effectuer une transaction, elle peut sélectionner et utiliser immédiatement toute connexion établie qui ne traite pas actuellement une transaction.

La topologie de chaque système StorageGRID présente un débit maximal différent pour les transactions et les connexions simultanées avant que les performances ne commencent à se dégrader. Le débit maximal dépend de facteurs tels que les ressources informatiques, les ressources réseau, les ressources de stockage et les liaisons WAN. Le nombre de serveurs et de services ainsi que le nombre d'applications prises en charge par le système StorageGRID sont également des facteurs.

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 cliente. Si l'application cliente se compose de plusieurs entités logicielles qui établissent chacune des connexions au système StorageGRID, vous devez additionner toutes les connexions entre les entités. Vous devrez peut-être ajuster 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 que le système peut prendre en charge.
- Les applications clientes qui interagissent avec le système StorageGRID sur un réseau à bande passante limitée peuvent devoir réduire le degré de concurrence pour garantir que les transactions individuelles sont terminées dans un délai raisonnable.
- Lorsque de nombreuses applications clientes partagent le système StorageGRID, vous devrez peut-être réduire le degré de concurrence pour éviter de dépasser les limites du système.

Séparation des pools de connexions HTTP pour les opérations de lecture et d'écriture

Vous pouvez utiliser des pools distincts de connexions HTTP pour les opérations de lecture et d'écriture et contrôler la quantité de pool à utiliser pour chacune. Des pools distincts de connexions HTTP vous permettent de mieux contrôler les transactions et d'équilibrer les charges.

Les applications clientes peuvent créer des charges à dominante de récupération (lecture) ou à dominante de stockage (écriture). Avec des pools distincts de connexions HTTP pour les transactions de lecture et d'écriture, vous pouvez ajuster la quantité de chaque pool à dédier aux transactions de lecture ou d'écriture.

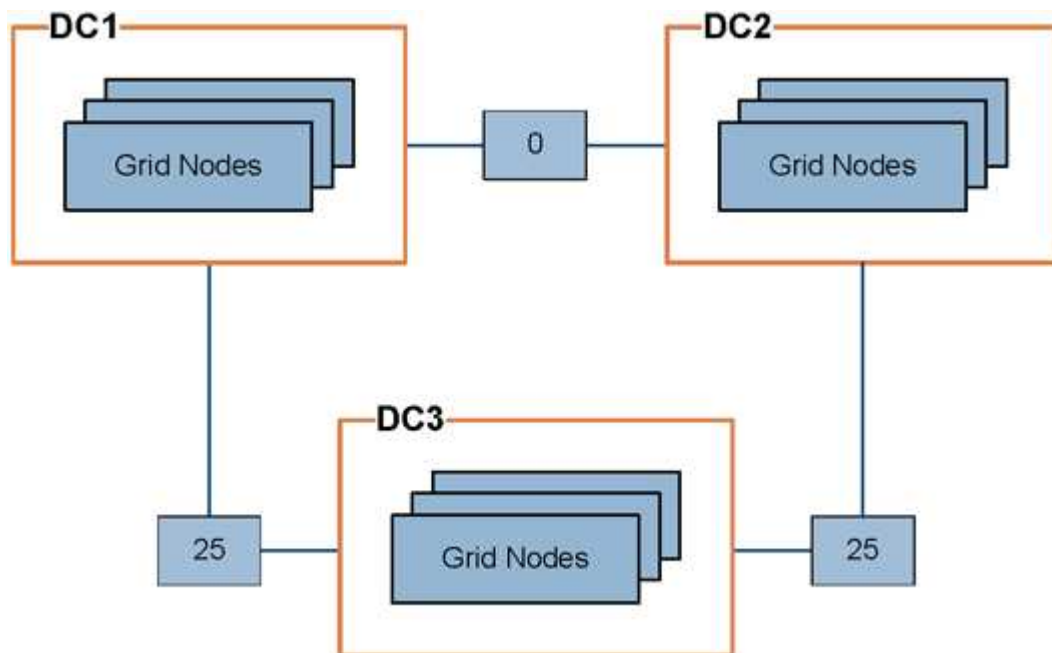
Gérer les coûts de liaison

Les coûts de liaison vous permettent de prioriser le site de centre de données qui fournit un service demandé lorsque deux sites de centre de données ou plus existent. Vous pouvez ajuster les coûts de liaison pour refléter la latence entre les sites.

Quels sont les coûts de liaison ?

- Les coûts de lien sont utilisés pour prioriser la copie d'objet utilisée pour effectuer les récupérations d'objet.
- Les coûts de liaison sont utilisés par l'API Grid Management et l'API Tenant Management pour déterminer les services StorageGRID internes à 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 diagramme montre une grille à trois sites avec des coûts de liaison configurés entre les sites :



- Le service d'équilibrage de charge sur les nœuds d'administration et les nœuds de passerelle distribue de manière égale les connexions client à tous les nœuds de stockage du même site de centre de données et à tous les sites de centre de données avec un coût de liaison de 0.

Dans l'exemple, un nœud de passerelle sur le site de centre de données 1 (DC1) distribue de manière égale les connexions client aux nœuds de stockage de DC1 et aux nœuds de stockage de DC2. Un nœud de passerelle sur DC3 envoie des connexions client uniquement aux nœuds de stockage sur DC3.

- Lors de la récupération d'un objet qui existe sous forme de plusieurs copies répliquées, StorageGRID récupère la copie dans le centre de données qui a le coût de liaison le plus bas.

Dans l'exemple, si une application cliente sur DC2 récupère un objet stocké à la fois sur DC1 et DC3, l'objet est récupéré à partir de DC1, car le coût de liaison de DC1 à DC2 est de 0, ce qui est inférieur au coût de 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 montre les

coûts des liens couramment utilisés.

Lien	Coût du lien	Remarques
Entre les sites de centres de données physiques	25 (par défaut)	Centres de données connectés par une liaison WAN.
Entre les sites de centres de données logiques au même emplacement physique	0	Centres de données logiques dans le même bâtiment physique ou campus connectés par un réseau local.

Coûts de mise à jour des liens

Vous pouvez mettre à jour les coûts de liaison entre les sites du centre de données pour 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**.



Link Cost

Updated: 2023-02-15 18:09:28 MST

Site Names (1 - 3 of 3) 

Site ID	Site Name	Actions
10	Data Center 1	
20	Data Center 2	
30	Data Center 3	

Show Records Per Page Previous 1 Next

Link Costs

Link Source	Link Destination			Actions
	10	20	30	
Data Center 1	0	25	25	



2. Sélectionnez un site sous **Source du lien** et entrez une valeur de coût comprise entre 0 et 100 sous **Destination du lien**.

Vous ne pouvez pas modifier le coût du lien si la source est la même que la destination.

Pour annuler les modifications, sélectionnez  **Revenir**.

3. Sélectionnez **Appliquer les modifications**.

Utiliser AutoSupport

Qu'est-ce AutoSupport?

La fonctionnalité AutoSupport permet à StorageGRID d'envoyer des packages d'état et de santé au support technique NetApp .

L'utilisation AutoSupport peut considérablement accélérer la détermination et la résolution des problèmes. Le support technique peut également surveiller les besoins de stockage de votre système et vous aider à déterminer si vous devez ajouter de nouveaux nœuds ou sites. En option, vous pouvez configurer les packages AutoSupport pour qu'ils soient envoyés vers une destination supplémentaire.

StorageGRID dispose de deux types d' AutoSupport:

- * StorageGRID AutoSupport* signale des problèmes logiciels StorageGRID . Activé par défaut lors de la première installation de StorageGRID. Tu peux ["modifier la configuration par défaut AutoSupport"](#) si nécessaire.



Si StorageGRID AutoSupport n'est pas activé, un message apparaît sur le tableau de bord du Grid Manager. Le message inclut un lien vers la page de configuration AutoSupport . Si vous fermez le message, il n'apparaîtra plus tant que le cache de votre navigateur n'aura pas été vidé, même si AutoSupport reste désactivé.

- **Appliance hardware AutoSupport** signale des problèmes liés à l'appliance StorageGRID . Vous devez ["configurer le matériel AutoSupport sur chaque appareil"](#) .

Qu'est-ce que Active IQ?

Active IQ est un conseiller numérique basé sur le cloud qui exploite l'analyse prédictive et la sagesse de la communauté de la base installée de NetApp. Ses évaluations continues des risques, ses alertes prédictives, ses conseils prescriptifs et ses actions automatisées vous aident à prévenir les problèmes avant qu'ils ne surviennent, ce qui améliore la santé du système et sa disponibilité.

Si vous souhaitez utiliser les tableaux de bord et les fonctionnalités Active IQ sur le site de support NetApp , vous devez activer AutoSupport.

["Documentation du Digital Advisor Active IQ"](#)

Informations incluses dans le package AutoSupport

Un package AutoSupport contient les fichiers et les détails suivants.

Nom des fichiers	Champs	Description
AUTOSUPPORT-HISTORY.XML	Numéro de séquence AutoSupport + Destination pour cet AutoSupport + Statut de livraison + Tentatives de livraison + Objet AutoSupport + URI de livraison + Dernière erreur + Nom de fichier PUT AutoSupport + Heure de génération + Taille compressée AutoSupport + Taille décompressée AutoSupport + Durée totale de collecte (ms)	Fichier historique AutoSupport .
AUTOSUPPORT.XML	Nœud + Protocole pour contacter le support + URL de support pour HTTP/HTTPS + Adresse de support + État AutoSupport OnDemand + URL du serveur AutoSupport OnDemand + Intervalle d'interrogation AutoSupport OnDemand	Fichier d'état AutoSupport . Fournit des détails sur le protocole utilisé, l'URL et l'adresse du support technique, l'intervalle d'interrogation et OnDemand AutoSupport s'il est activé ou désactivé.
BUCKETS.XML	ID de compartiment + ID de compte + Version de build + Configuration des contraintes d'emplacement + Conformité activée + Configuration de la conformité + Verrouillage d'objet S3 activé + Configuration du verrouillage d'objet S3 + Configuration de la cohérence + CORS activé + Configuration CORS + Heure du dernier accès activée + Politique activée + Configuration de la politique + Notifications activées + Configuration des notifications + Miroir Cloud activé + Configuration Miroir Cloud + Recherche activée + Configuration de la recherche + Balisage de compartiment activé + Configuration du balisage de compartiment + Configuration du contrôle de version	Fournit des détails de configuration et des statistiques au niveau du bucket. Les exemples de configurations de bucket incluent les services de plateforme, la conformité et la cohérence des buckets.

Nom des fichiers	Champs	Description
GRID-CONFIGURATIONS.XML	ID d'attribut + Nom d'attribut + Valeur + Index + ID de table + Nom de table	Fichier d'informations de configuration à l'échelle de la grille. Contient des informations sur les certificats de grille, l'espace réservé aux métadonnées, les paramètres de configuration à l'échelle de la grille (conformité, verrouillage d'objet S3, compression d'objet, alertes, syslog et configuration ILM), les détails du profil de codage d'effacement, le nom DNS et " Nom du NMS ".
GRID-SPEC.XML	Spécifications de la grille, XML brut	Utilisé pour configurer et déployer StorageGRID. Contient les spécifications de la grille, l'IP du serveur NTP, l'IP du serveur DNS, la topologie du réseau et les profils matériels des nœuds.
GRID-TASKS.XML	Nœud + Chemin de service + ID d'attribut + Nom d'attribut + Valeur + Index + ID de table + Nom de table	Fichier d'état des tâches de la grille (procédures de maintenance). Fournit des détails sur les tâches actives, terminées, terminées, échouées et en attente de la grille.
GRILLE.JSON	Grille + Révision + Version du logiciel + Description + Licence + Mots de passe + DNS + NTP + Sites + Nœuds	Informations sur la grille.
ILM-CONFIGURATION.XML	ID d'attribut + Nom d'attribut + Valeur + Index + ID de table + Nom de table	Liste des attributs pour les configurations ILM.
ILM-STATUT.XML	Nœud + Chemin de service + ID d'attribut + Nom d'attribut + Valeur + Index + ID de table + Nom de table	Fichier d'informations sur les métriques ILM. Contient les taux d'évaluation ILM pour chaque nœud et les mesures à l'échelle de la grille.
ILM.XML	XML brut ILM	Fichier de politique active ILM. Contient des détails sur les politiques ILM actives, telles que l'ID du pool de stockage, le comportement d'ingestion, les filtres, les règles et la description.
LOG.TGZ	<i>n / A</i>	Fichier journal téléchargeable. Contient <code>broadcast-err.log</code> et <code>servermanager.log</code> de chaque nœud.

Nom des fichiers	Champs	Description
MANIFEST.XML	Ordre de collecte + Nom du fichier de contenu AutoSupport pour ces données + Description de cet élément de données + Nombre d'octets collectés + Temps passé à collecter + Statut de cet élément de données + Description de l'erreur + Type de contenu AutoSupport pour ces données +	Contient les métadonnées AutoSupport et de brèves descriptions de tous les fichiers AutoSupport .
NMS-ENTITÉS.XML	Index d'attribut + OID d'entité + ID de nœud + ID de modèle d'appareil + Version du modèle d'appareil + Nom d'entité	Entités de groupe et de service dans le " arbre NMS ". Fournit des détails sur la topologie de la grille. Le nœud peut être déterminé en fonction des services exécutés sur le nœud.
OBJETS-STATUS.XML	Nœud + Chemin de service + ID d'attribut + Nom d'attribut + Valeur + Index + ID de table + Nom de table	État de l'objet, y compris l'état de l'analyse en arrière-plan, le transfert actif, le taux de transfert, le nombre total de transferts, le taux de suppression, les fragments corrompus, les objets perdus, les objets manquants, la tentative de réparation, le taux d'analyse, la période d'analyse estimée et l'état d'achèvement de la réparation.
SERVER-STATUS.XML	Nœud + Chemin de service + ID d'attribut + Nom d'attribut + Valeur + Index + ID de table + Nom de table	Configurations du serveur. Contient ces détails pour chaque nœud : type de plateforme, système d'exploitation, mémoire installée, mémoire disponible, connectivité de stockage, numéro de série du châssis du dispositif de stockage, nombre de disques défectueux du contrôleur de stockage, température du châssis du contrôleur de calcul, matériel de calcul, numéro de série du contrôleur de calcul, alimentation, taille du disque et type de disque.
SERVICE-STATUS.XML	Nœud + Chemin de service + ID d'attribut + Nom d'attribut + Valeur + Index + ID de table + Nom de table	Fichier d'informations sur le nœud de service. Contient des détails tels que l'espace table alloué, l'espace table libre, les métriques Reaper de la base de données, la durée de réparation du segment, la durée du travail de réparation, les redémarrages automatiques du travail et l'arrêt automatique du travail.

Nom des fichiers	Champs	Description
NIVEAUX DE STOCKAGE.XML	ID de niveau de stockage + Nom de niveau de stockage + ID de nœud de stockage + Chemin du nœud de stockage	Fichier de définitions de qualité de stockage pour chaque nœud de stockage.
RÉSUMÉ-ATTRIBUTS.XML	OID du groupe + Chemin du groupe + ID de l'attribut récapitulatif + Nom de l'attribut récapitulatif + Valeur + Index + ID de la table + Nom de la table	Données d'état du système de haut niveau qui résument les informations d'utilisation de StorageGRID . Fournit des détails tels que le nom de la grille, les noms des sites, le nombre de nœuds de stockage par grille et par site, le type de licence, la capacité et l'utilisation de la licence, les conditions de support logiciel et les détails des opérations S3.
ALERTES-SYSTEME.XML	Nom + Gravité + Nom du nœud + État de l'alerte + Nom du site + Heure de déclenchement de l'alerte + Heure de résolution de l'alerte + ID de règle + ID du nœud + ID du site + Silencieux + Autres annotations + Autres étiquettes	Alertes système actuelles indiquant des problèmes potentiels dans le système StorageGRID .
USERAGENTS.XML	Agent utilisateur + Nombre de jours + Nombre total de requêtes HTTP + Nombre total d'octets ingérés + Nombre total d'octets récupérés + Requêtes PUT + Requêtes GET + Requêtes DELETE + Requêtes HEAD + Requêtes POST + Requêtes OPTIONS + Temps moyen de requête (ms) + Temps moyen de requête PUT (ms) + Temps moyen de requête GET (ms) + Temps moyen de requête DELETE (ms) + Temps moyen de requête HEAD (ms) + Temps moyen de requête POST (ms) + Temps moyen de requête OPTIONS (ms)	Statistiques basées sur les agents utilisateurs de l'application. Par exemple, le nombre d'opérations PUT/GET/DELETE/HEAD par agent utilisateur et la taille totale en octets de chaque opération.

Nom des fichiers	Champs	Description
X-HEADER-DATA	X-Netapp-asup-generated-on + X-Netapp-asup-hostname + X-Netapp-asup-os-version + X-Netapp-asup-serial-num + X-Netapp-asup-subject + X-Netapp-asup-system-id + X-Netapp-asup-model-name +	Données d'en-tête AutoSupport .

Configurer AutoSupport

Par défaut, la fonctionnalité StorageGRID AutoSupport est activée lors de la première installation de StorageGRID. Cependant, vous devez configurer le matériel AutoSupport sur chaque appareil. Selon vos besoins, vous pouvez modifier la configuration AutoSupport .

Si vous souhaitez modifier la configuration de StorageGRID AutoSupport, effectuez vos modifications uniquement sur le nœud d'administration principal. Vous devez [configurer le matériel AutoSupport](#) sur chaque appareil.

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 root"](#) .
- Si vous utilisez HTTPS pour envoyer des packages AutoSupport , vous avez fourni un accès Internet sortant au nœud d'administration principal, soit directement, soit ["en utilisant 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 packages AutoSupport en HTTPS. Les serveurs AutoSupport de NetApp rejeteront les packages envoyés via HTTP.
- Si vous utilisez SMTP comme protocole pour les packages AutoSupport , vous avez configuré un serveur de messagerie SMTP.

À propos de cette tâche

Vous pouvez utiliser n'importe quelle combinaison des options suivantes pour envoyer des packages AutoSupport au support technique :

- **Hebdomadaire** : envoie automatiquement des packages AutoSupport une fois par semaine. Paramètre par défaut : Activé.
- **Déclenché par événement** : envoyez automatiquement des packages AutoSupport toutes les heures ou lorsque des événements système importants se produisent. Paramètre par défaut : Activé.
- **À la demande** : autorisez le support technique à demander à votre système StorageGRID d'envoyer automatiquement des packages AutoSupport , ce qui est utile lorsqu'ils travaillent activement sur un problème (nécessite le protocole de transmission HTTPS AutoSupport). Paramètre par défaut : désactivé.
- **Déclenché par l'utilisateur** : envoyez manuellement des packages AutoSupport à tout moment.

Spécifiez le protocole pour les packages AutoSupport

Vous pouvez utiliser l'un des protocoles suivants pour envoyer des packages AutoSupport :

- **HTTPS** : il s'agit du paramètre par défaut et recommandé pour les nouvelles installations. Ce protocole utilise le port 443. Si tu veux [activer la fonctionnalité AutoSupport à la demande](#) , vous devez utiliser HTTPS.
- **HTTP** : si vous sélectionnez HTTP, vous devez configurer un serveur proxy pour transférer les packages AutoSupport en HTTPS. Les serveurs AutoSupport de NetApp rejettent les packages envoyés via HTTP. Ce protocole utilise le port 80.
- **SMTP** : utilisez cette option si vous souhaitez que les packages AutoSupport soient envoyés par courrier électronique.

Le protocole que vous définissez est utilisé pour envoyer tous les types de packages AutoSupport .

Étapes

1. Sélectionnez **SUPPORT > Outils > * AutoSupport* > Paramètres**.
2. Sélectionnez le protocole que vous souhaitez utiliser pour envoyer des packages AutoSupport .
3. Si vous avez sélectionné **HTTPS**, indiquez si vous souhaitez utiliser un certificat de support NetApp (certificat TLS) pour sécuriser la connexion au serveur de support technique.
 - **Vérifier le certificat** (par défaut) : garantit que la transmission des packages AutoSupport est sécurisée. Le certificat de support NetApp est déjà installé avec le logiciel StorageGRID .
 - **Ne pas vérifier le certificat** : sélectionnez cette option uniquement lorsque vous avez une bonne raison de ne pas utiliser la validation de certificat, par exemple en cas de problème temporaire avec un certificat.
4. Sélectionnez **Enregistrer**. Tous les packages hebdomadaires, déclenchés par l'utilisateur et déclenchés par un événement sont envoyés à l'aide du protocole sélectionné.

Désactiver AutoSupport hebdomadaire

Par défaut, le système StorageGRID est configuré pour envoyer un package AutoSupport au support technique une fois par semaine.

Pour déterminer quand le package AutoSupport hebdomadaire sera envoyé, accédez à l'onglet *** AutoSupport* > Résultats**. Dans la section **Weekly AutoSupport**, regardez la valeur de **Next Scheduled Time**.

Vous pouvez désactiver l'envoi automatique des packages AutoSupport hebdomadaires à tout moment.

Étapes

1. Sélectionnez **SUPPORT > Outils > * AutoSupport* > Paramètres**.
2. Décochez la case **Activer AutoSupport hebdomadaire**.
3. Sélectionnez **Enregistrer**.

Désactiver AutoSupport déclenché par un événement

Par défaut, le système StorageGRID est configuré pour envoyer un package AutoSupport au support technique toutes les heures.

Vous pouvez désactiver AutoSupport déclenché par un événement à tout moment.

Étapes

1. Sélectionnez **SUPPORT > Outils > * AutoSupport* > Paramètres**.
2. Décochez la case **Activer AutoSupport déclenchée par événement**.

3. Sélectionnez **Enregistrer**.

Activer AutoSupport à la demande

AutoSupport on Demand peut vous aider à résoudre les problèmes sur lesquels le support technique travaille activement.

Par défaut, AutoSupport on Demand est désactivé. L'activation de cette fonctionnalité permet au support technique de demander à votre système StorageGRID d'envoyer automatiquement les packages AutoSupport. Le support technique peut également définir l'intervalle de temps d'interrogation pour les requêtes AutoSupport à la demande.

Le support technique ne peut pas activer ou désactiver AutoSupport à la demande.

Étapes

1. Sélectionnez **SUPPORT > Outils > * AutoSupport* > Paramètres**.
2. Sélectionnez **HTTPS** pour le protocole.
3. Cochez la case **Activer AutoSupport hebdomadaire**.
4. Cochez la case **Activer AutoSupport à la demande**.
5. Sélectionnez **Enregistrer**.

AutoSupport on Demand est activé et le support technique peut envoyer des demandes AutoSupport on Demand à StorageGRID.

Désactiver 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 ou une nouvelle version de StorageGRID est disponible, la nouvelle version est affichée sur la page de mise à niveau de StorageGRID.

Si nécessaire, vous pouvez éventuellement désactiver la vérification des mises à jour logicielles. Par exemple, si votre système ne dispose pas d'accès WAN, vous devez désactiver la vérification pour éviter les erreurs de téléchargement.

Étapes

1. Sélectionnez **SUPPORT > Outils > * AutoSupport* > Paramètres**.
2. Décochez la case **Vérifier les mises à jour logicielles**.
3. Sélectionnez **Enregistrer**.

Ajouter une destination AutoSupport supplémentaire

Lorsque vous activez AutoSupport, les packages de santé et d'état sont envoyés au support technique. Vous pouvez spécifier une destination supplémentaire pour tous les packages AutoSupport.

Pour vérifier ou modifier le protocole utilisé pour envoyer les packages AutoSupport, consultez les instructions pour [spécifier le protocole pour les packages AutoSupport](#).



Vous ne pouvez pas utiliser le protocole SMTP pour envoyer des packages AutoSupport vers une destination supplémentaire.

Étapes

1. Sélectionnez **SUPPORT > Outils > * AutoSupport* > Paramètres**.
2. Sélectionnez **Activer la destination AutoSupport supplémentaire**.
3. Précisez les éléments suivants :

Nom d'hôte

Le nom d'hôte du serveur ou l'adresse IP d'un serveur de destination AutoSupport supplémentaire.



Vous ne pouvez saisir qu'une seule destination supplémentaire.

Port

Le 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 du certificat

Si un certificat TLS est utilisé pour sécuriser la connexion à la destination supplémentaire.

- Sélectionnez **Vérifier le certificat** pour utiliser la validation du certificat.
- Sélectionnez **Ne pas vérifier le certificat** pour envoyer vos packages AutoSupport sans validation de certificat.

Sélectionnez cette option uniquement lorsque vous avez une bonne raison de ne pas utiliser la validation de certificat, par exemple en cas de problème temporaire avec un certificat.

4. Si vous avez sélectionné **Vérifier le certificat**, procédez comme suit :
 - a. Accédez à l'emplacement du certificat CA.
 - b. Téléchargez le fichier de certificat CA.

Les métadonnées du certificat CA s'affichent.

5. Sélectionnez **Enregistrer**.

Tous les futurs packages AutoSupport hebdomadaires, déclenchés par des événements et déclenchés par l'utilisateur seront envoyés vers la destination supplémentaire.

Configurer AutoSupport pour les appareils

AutoSupport pour les appliances signale les problèmes matériels StorageGRID et StorageGRID AutoSupport signale les problèmes logiciels StorageGRID, à une exception près : pour le SGF6112, StorageGRID AutoSupport signale les problèmes matériels et logiciels. Vous devez configurer AutoSupport sur chaque appareil, à l'exception du SGF6112, qui ne nécessite pas de configuration supplémentaire. AutoSupport est implémenté différemment pour les appliances de services et les appliances de stockage.

Vous utilisez SANtricity pour activer AutoSupport 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 appareils SG6000 et SG5700, "[configurer AutoSupport dans SANtricity System Manager](#)"

Les packages AutoSupport des appliances de la série E peuvent être inclus dans StorageGRID AutoSupport si vous configurez la livraison AutoSupport par proxy dans "[Gestionnaire de système SANtricity](#)".

StorageGRID AutoSupport ne signale pas les problèmes matériels, tels que les défauts de DIMM ou de carte

d'interface hôte (HIC). Cependant, certaines défaillances de composants peuvent déclencher "[alertes matérielles](#)". Pour les appliances StorageGRID avec un contrôleur de gestion de la carte mère (BMC), vous pouvez configurer des interruptions de messagerie et SNMP pour signaler les pannes matérielles :

- "[Configurer des notifications par e-mail pour les alertes BMC](#)"
- "[Configurer les paramètres SNMP pour BMC](#)"

Informations connexes

["Assistance NetApp"](#)

Déclencher manuellement un package AutoSupport

Pour aider le support technique à résoudre les problèmes liés à votre système StorageGRID, vous pouvez déclencher manuellement l'envoi d'un package AutoSupport

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 root ou de l'autorisation de configuration d'une autre grille.

Étapes

1. Sélectionnez **SUPPORT > Outils > * AutoSupport***.
2. Dans l'onglet **Actions**, sélectionnez **Envoyer AutoSupport déclenchée par l'utilisateur**.

StorageGRID tente d'envoyer un package AutoSupport au site de support NetApp. Si la tentative réussit, les valeurs **Résultat le plus récent** et **Dernière heure de réussite** dans l'onglet **Résultats** sont mises à jour. En cas de problème, la valeur **Résultat le plus récent** est mise à jour sur « Échec » et StorageGRID n'essaie pas d'envoyer à nouveau le package AutoSupport.



Après avoir envoyé un package AutoSupport déclenché par l'utilisateur, actualisez la page AutoSupport dans votre navigateur après 1 minute pour accéder aux résultats les plus récents.

Dépannage des packages AutoSupport

Si une tentative d'envoi d'un package AutoSupport échoue, le système StorageGRID entreprend différentes actions selon le type de package AutoSupport. Vous pouvez vérifier l'état des packages AutoSupport en sélectionnant **SUPPORT > Outils > * AutoSupport* > Résultats**.

Lorsque le package AutoSupport ne parvient pas à être envoyé, « Échec » s'affiche dans l'onglet **Résultats** de la page *** AutoSupport***.



Si vous avez configuré un serveur proxy pour transférer les packages AutoSupport vers NetApp, vous devez "[vérifier que les paramètres de configuration du serveur proxy sont corrects](#)".

Échec hebdomadaire du package AutoSupport

Si un package AutoSupport hebdomadaire ne parvient pas à être envoyé, le système StorageGRID prend les mesures suivantes :

1. Met à jour l'attribut Résultat le plus récent sur Nouvelle tentative.
2. Tente de renvoyer le package AutoSupport 15 fois toutes les quatre minutes pendant une heure.
3. Après une heure d'échecs d'envoi, met à jour l'attribut Résultat le plus récent sur Échec.
4. Tente d'envoyer à nouveau un package AutoSupport à la prochaine heure programmée.
5. Maintient le calendrier AutoSupport régulier si le package échoue parce que le service NMS n'est pas disponible et si un package est envoyé avant sept jours.
6. Lorsque le service NMS est à nouveau disponible, il envoie immédiatement un package AutoSupport si aucun package n'a été envoyé pendant sept jours ou plus.

Échec du package AutoSupport déclenché par l'utilisateur ou par un événement

Si un package AutoSupport déclenché par un utilisateur ou un événement ne parvient pas à être envoyé, le système StorageGRID exécute 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 de messagerie corrects, l'erreur suivante s'affiche :
`AutoSupport packages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`
2. N'essayez pas de renvoyer le colis.
3. Enregistre l'erreur dans `nms.log`.

Si une panne se produit et que 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 (héritées) > Configuration de la messagerie héritée**). Le message d'erreur suivant peut apparaître sur la page AutoSupport : `AutoSupport packages 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"](#).

Corriger une défaillance du package AutoSupport

Si une panne se produit et que 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 packages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`

Envoyer des packages AutoSupport de la série E via StorageGRID

Vous pouvez envoyer des packages E-Series SANtricity System Manager AutoSupport au support technique via un nœud d'administration StorageGRID plutôt que via le port de gestion du dispositif de stockage.

Voir ["AutoSupport du matériel de la série E"](#) pour plus d'informations sur l'utilisation AutoSupport avec les appareils de la série E.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous avez le ["Administrateur de l'appareil de stockage ou autorisation d'accès root"](#).

- Vous avez configuré SANtricity AutoSupport:
 - Pour les appareils SG6000 et SG5700, "[configurer AutoSupport dans SANtricity System Manager](#)"



Vous devez disposer du micrologiciel SANtricity 8.70 ou supérieur pour accéder à SANtricity System Manager à l'aide de Grid Manager.

À propos de cette tâche

Les packages AutoSupport de la série E contiennent des détails sur le matériel de stockage et sont plus spécifiques que les autres packages AutoSupport envoyés par le système StorageGRID .

Vous pouvez configurer une adresse de serveur proxy spéciale dans SANtricity System Manager pour transmettre des packages AutoSupport via un nœud d'administration StorageGRID sans utiliser le port de gestion de l'appliance. Les packages AutoSupport transmis de cette manière sont envoyés par le "[nœud d'administration de l'expéditeur préféré](#)" , et ils utilisent n'importe quel "[paramètres de proxy d'administration](#)" qui ont été configurés dans le Grid Manager.

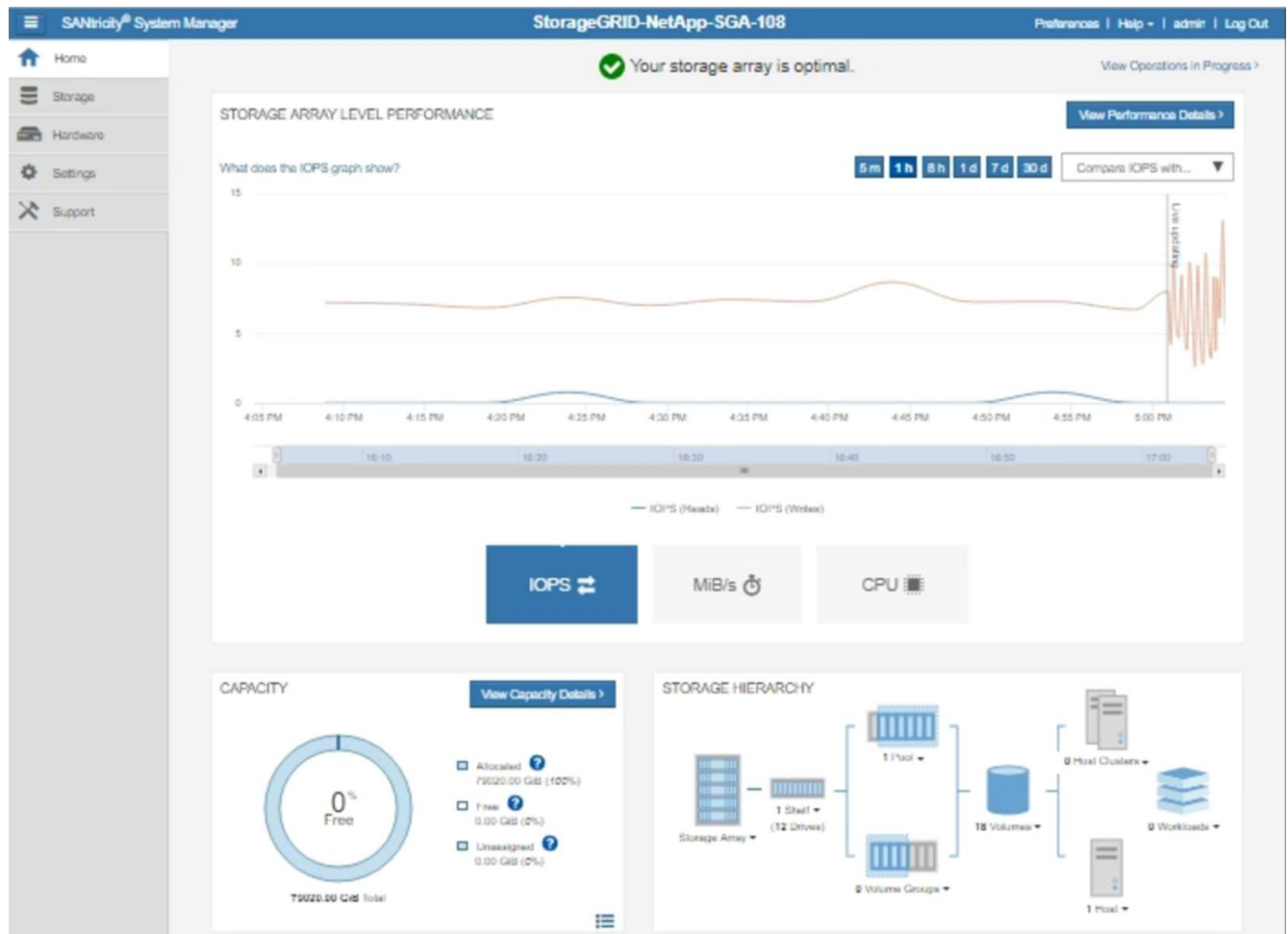


Cette procédure concerne uniquement la configuration d'un serveur proxy StorageGRID pour les packages AutoSupport de la série E. Pour plus de détails sur la configuration AutoSupport de la série E, consultez le "[Documentation NetApp E-Series et SANtricity](#)" .

Étapes

1. Dans le gestionnaire de grille, sélectionnez **NODES**.
2. Dans la liste des nœuds sur la gauche, sélectionnez le nœud du dispositif de stockage que vous souhaitez configurer.
3. Sélectionnez * SANtricity System Manager*.

La page d'accueil de SANtricity System Manager apparaît.



4. Sélectionnez **SUPPORT** > **Centre d'assistance** > * AutoSupport*.

La page des opérations AutoSupport s'affiche.

Technical Support

Chassis serial number: 031517000693

 [NetApp My Support](#)

US/Canada 888.463.8277

[Other Contacts](#)

Support Resources

Diagnostics

AutoSupport

AutoSupport operations

AutoSupport status: Enabled 

[Enable/Disable AutoSupport Features](#)
AutoSupport proactively monitors the health of your storage array and automatically sends support data ("dispatches") to the support team.

[Configure AutoSupport Delivery Method](#)
Connect to the support team via HTTPS, HTTP or Mail (SMTP) server delivery methods.

[Schedule AutoSupport Dispatches](#)
AutoSupport dispatches are sent daily at 03:06 PM UTC and weekly at 07:39 AM UTC on Thursday.

[Send AutoSupport Dispatch](#)
Automatically sends the support team a dispatch to troubleshoot system issues without waiting for periodic dispatches.

[View AutoSupport Log](#)
The AutoSupport log provides information about status, dispatch history, and errors encountered during delivery of AutoSupport dispatches.

[Enable AutoSupport Maintenance Window](#)
Enable AutoSupport Maintenance window to allow maintenance activities to be performed on the storage array without generating support cases.

[Disable AutoSupport Maintenance Window](#)
Disable AutoSupport Maintenance window to allow the storage array to generate support cases on component failures and other destructive actions.

5. Sélectionnez *Configurer la méthode de livraison AutoSupport*.

La page Configurer la méthode de livraison AutoSupport s'affiche.

6. Sélectionnez **HTTPS** comme méthode de livraison.



Le certificat qui active HTTPS est préinstallé.

7. Sélectionnez **via le serveur proxy**.

8. Entrer `tunnel-host` pour l'**adresse de l'hôte**.

`tunnel-host` est l'adresse spéciale à utiliser pour un nœud d'administration afin d'envoyer des packages AutoSupport de la série E.

9. Entrer `10225` pour le **Numéro de port**.

`10225` est le numéro de port sur le serveur proxy StorageGRID qui reçoit les packages 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 correct, un message dans une bannière verte apparaît : « Votre configuration AutoSupport a été

vérifiée. »

Si le test échoue, un message d'erreur apparaît dans une bannière rouge. Vérifiez vos paramètres DNS et votre réseau StorageGRID , assurez-vous que "[nœud d'administration de l'expéditeur préféré](#)" peut se connecter au site de support NetApp et réessayer le test.

11. Sélectionnez **Enregistrer**.

La configuration est enregistrée et un message de confirmation s'affiche : « La méthode de livraison AutoSupport a été configurée. »

Gérer les nœuds de stockage

Gérer les nœuds de stockage

Les nœuds de stockage fournissent une capacité de stockage sur disque et des services. La gestion des nœuds de stockage implique les opérations suivantes :

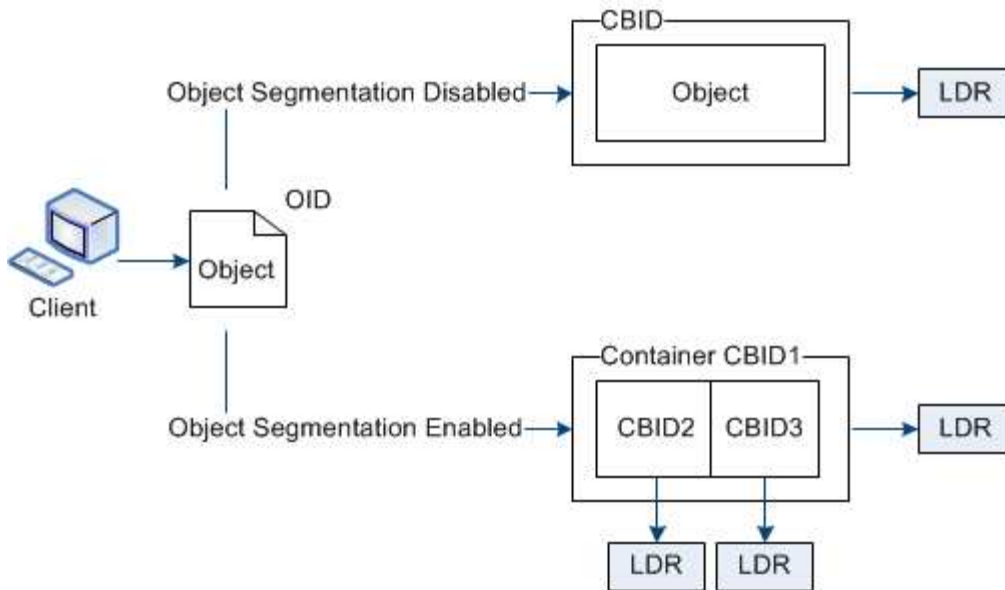
- Gestion des options de stockage
- Comprendre ce que sont les filigranes de volume de stockage et comment vous pouvez utiliser les remplacements de filigrane pour contrôler le moment où les nœuds de stockage deviennent en lecture seule
- Surveillance et gestion de l'espace utilisé pour les métadonnées des objets
- Configuration des paramètres globaux pour les objets stockés
- Application des paramètres de configuration du nœud de stockage
- Gestion des nœuds de stockage complets

Utiliser les options de stockage

Qu'est-ce que la segmentation d'objets ?

La segmentation d'objets est le processus de division d'un objet en une collection d'objets plus petits de taille fixe pour optimiser le stockage et l'utilisation des ressources pour les objets volumineux. Le téléchargement multi-parties S3 crée également des objets segmentés, avec un objet représentant chaque partie.

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 d'origine à partir de ses segments et renvoie l'objet au client.

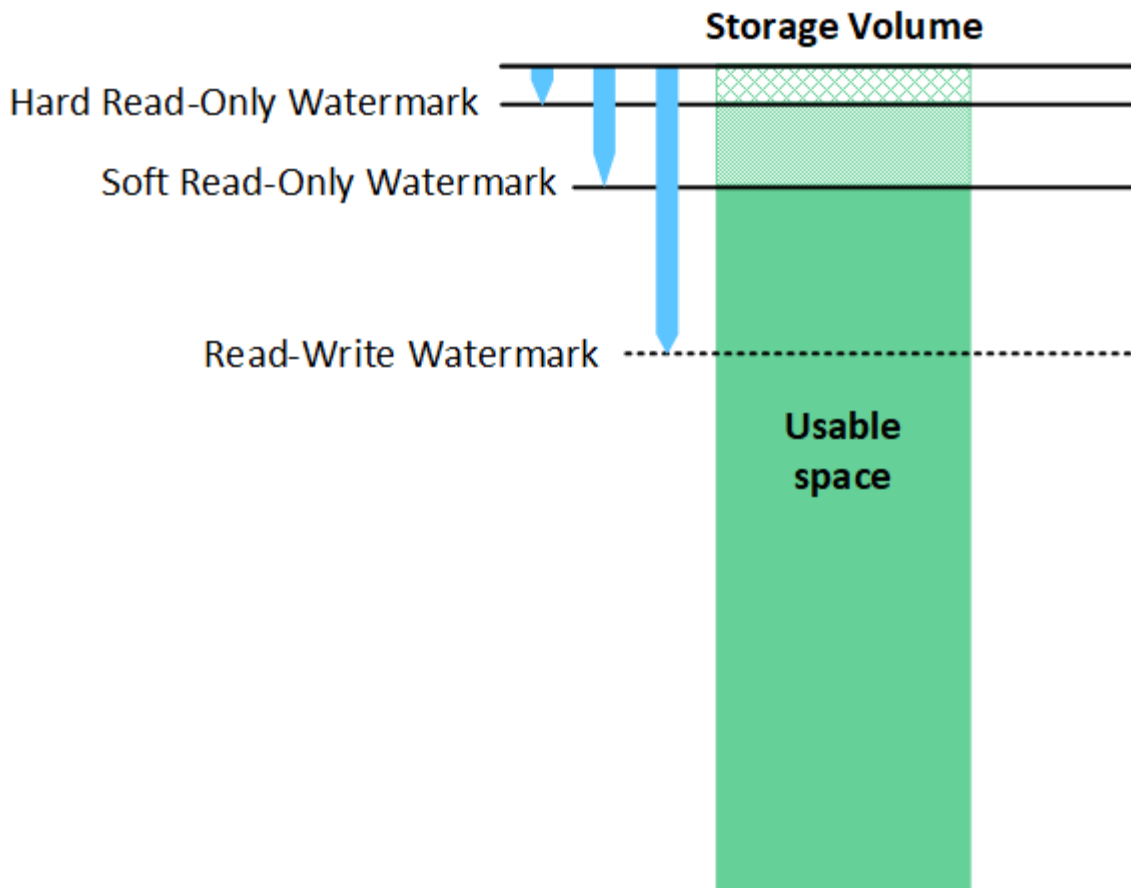
Le conteneur et les segments ne sont pas nécessairement stockés sur le même nœud de stockage. Le conteneur et les segments peuvent être stockés sur n'importe quel nœud de stockage au sein du pool de stockage spécifié dans la règle ILM.

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 une fois l'ingestion terminée, comme suit :

```
segment container + segment 1 + segment 2 = three stored objects
```

Que sont les filigranes de volume de stockage ?

StorageGRID utilise trois filigranes de volume de stockage pour garantir que les nœuds de stockage sont transférés en toute sécurité vers un état de lecture seule avant de manquer d'espace de manière critique et pour permettre aux nœuds de stockage qui sont passés à un état de lecture seule de redevenir en lecture-écriture.



Les filigranes de volume de stockage s'appliquent uniquement à l'espace utilisé pour les données d'objet répliquées et codées par effacement. Pour en savoir plus sur l'espace réservé aux métadonnées des objets sur le volume 0, rendez-vous sur ["Gérer le stockage des métadonnées des objets"](#).

Qu'est-ce que le filigrane souple en lecture seule ?

Le **filigrane en lecture seule du volume de stockage** est le premier filigrane à indiquer que l'espace utilisable d'un nœud de stockage pour les données d'objet est en train de devenir plein.

Si chaque volume d'un nœud de stockage dispose de moins d'espace libre que le filigrane en lecture seule de ce volume, le nœud de stockage passe en mode lecture seule. Le mode lecture seule signifie que le nœud de stockage annonce les services en lecture seule au reste du système StorageGRID, mais répond à toutes les demandes d'écriture en attente.

Par exemple, supposons que chaque volume d'un nœud de stockage possède un filigrane en lecture seule souple de 10 Go. Dès que chaque volume dispose de moins de 10 Go d'espace libre, le nœud de stockage passe en mode lecture seule logicielle.

Qu'est-ce que le filigrane en lecture seule ?

Le **filigrane de lecture seule du volume de stockage** est le prochain filigrane à indiquer que l'espace utilisable d'un nœud pour les données d'objet est en train de devenir plein.

Si l'espace libre sur un volume est inférieur au filigrane en lecture seule de ce volume, les écritures sur le volume échoueront. Toutefois, 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.

Par exemple, supposons que chaque volume d'un nœud de stockage possède 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 aucune demande d'écriture.

Le filigrane en lecture seule dur est toujours inférieur au filigrane en lecture seule souple.

Qu'est-ce que le filigrane en lecture-écriture ?

Le **filigrane de lecture-écriture du volume de stockage** s'applique uniquement aux nœuds de stockage qui sont passés en mode lecture seule. Il détermine quand le nœud peut redevenir en 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.

Par exemple, supposons que le nœud de stockage soit passé en mode lecture seule. Supposons également que chaque volume possède un filigrane de lecture-écriture de 30 Go. Dès que l'espace libre pour un volume augmente à 30 Go, le nœud redevient en lecture-écriture.

Le filigrane en lecture-écriture est toujours plus grand que le filigrane en lecture seule souple et que le filigrane en lecture seule rigide.

Afficher les filigranes du volume de stockage

Vous pouvez afficher les paramètres de filigrane actuels et les valeurs optimisées pour le système. Si des filigranes optimisés ne sont pas utilisés, vous pouvez déterminer si vous pouvez ou devez ajuster les paramètres.

Avant de commencer

- Vous avez terminé la mise à niveau vers StorageGRID 11.6 ou supérieur.
- Vous êtes connecté au Grid Manager à l'aide d'un ["navigateur Web pris en charge"](#) .
- Vous avez le ["Autorisation d'accès root"](#) .

Afficher les paramètres de filigrane actuels

Vous pouvez afficher les paramètres de filigrane de stockage actuels dans le gestionnaire de grille.

Étapes

1. Sélectionnez **SUPPORT > Autre > Filigranes de stockage**.
2. Sur la page Filigranes de stockage, cochez la case Utiliser des valeurs optimisées.
 - Si la case à cocher est sélectionnée, 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. Ne mettez pas à jour ces valeurs. En option, vous pouvez [Afficher les filigranes de stockage optimisés](#) .

- Si la case à cocher Utiliser les valeurs optimisées n'est pas sélectionnée, des filigranes personnalisés (non optimisés) sont utilisés. L'utilisation de paramètres de filigrane personnalisés n'est pas recommandée. Utilisez les instructions pour ["dépannage des alertes de remplacement du filigrane en lecture seule faible"](#) pour déterminer si vous pouvez ou devez ajuster les paramètres.

Lorsque vous spécifiez des paramètres de filigrane personnalisés, vous devez saisir des valeurs supérieures à 0.

Afficher les filigranes de stockage optimisés

StorageGRID utilise deux mesures Prometheus pour afficher les valeurs optimisées qu'il a calculées pour le filigrane en lecture seule du volume de stockage. Vous pouvez afficher les valeurs optimisées minimales et maximales pour chaque nœud de stockage de votre grille.

1. Sélectionnez **SUPPORT > Outils > Métriques**.
2. Dans la section Prometheus, sélectionnez le lien pour accéder à l'interface utilisateur de Prometheus.
3. Pour voir le filigrane en lecture seule minimal recommandé, entrez la métrique Prometheus suivante et sélectionnez **Exécuter** :

```
storagegrid_storage_volume_minimum_optimized_soft_readonly_watermark
```

La dernière colonne affiche la valeur optimisée minimale du filigrane en lecture seule souple pour tous les volumes de stockage sur chaque nœud de stockage. Si cette valeur est supérieure au paramètre personnalisé pour le filigrane en lecture seule logicielle du volume de stockage, l'alerte **Remplacement du filigrane en lecture seule faible** est déclenchée pour le nœud de stockage.

4. Pour voir le filigrane en lecture seule maximal recommandé, entrez la métrique Prometheus suivante et sélectionnez **Exécuter** :

```
storagegrid_storage_volume_maximum_optimized_soft_readonly_watermark
```

La dernière colonne affiche la valeur optimisée maximale du filigrane en lecture seule pour tous les volumes de stockage sur chaque nœud de stockage.

Gérer le stockage des métadonnées des objets

La capacité des métadonnées d'objet d'un système StorageGRID contrôle le nombre maximal d'objets pouvant être stockés sur ce système. Pour garantir que votre système StorageGRID dispose de suffisamment d'espace pour stocker de nouveaux objets, vous devez comprendre où et comment StorageGRID stocke les métadonnées des objets.

Que sont les métadonnées d'objet ?

Les métadonnées d'objet sont toutes les informations qui décrivent un objet. StorageGRID utilise les métadonnées des objets pour suivre les emplacements de tous les objets sur la grille et pour gérer le cycle de vie de chaque objet au fil du temps.

Pour un objet dans StorageGRID, les métadonnées de l'objet incluent les types d'informations suivants :

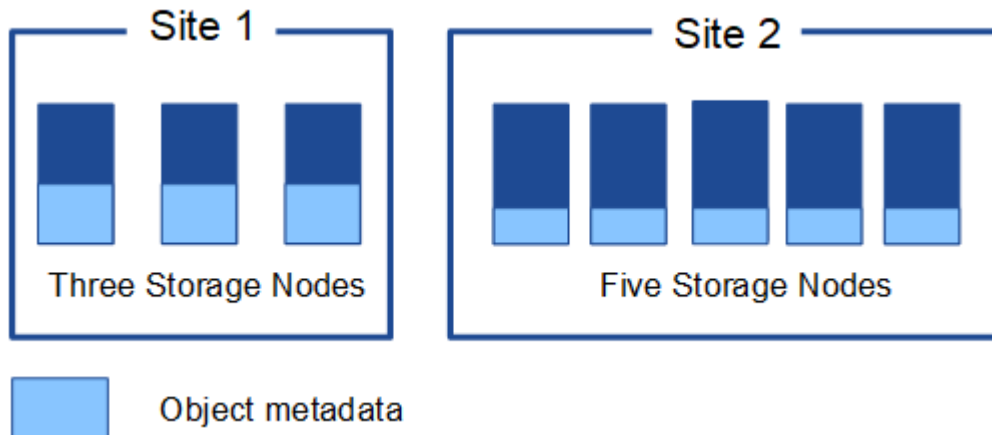
- Métadonnées système, y compris un ID unique pour chaque objet (UUID), le nom de l'objet, le nom du compartiment S3, le nom ou l'ID du compte locataire, la taille logique de l'objet, la date et l'heure de la première création de l'objet et la date et l'heure de la dernière modification de l'objet.
- Toutes les paires clé-valeur de métadonnées utilisateur personnalisées associées à l'objet.
- Pour les objets S3, toutes les paires clé-valeur de balise d'objet associées à l'objet.
- Pour les copies d'objets répliquées, l'emplacement de stockage actuel de chaque copie.
- Pour les copies d'objets codées par effacement, l'emplacement de stockage actuel de chaque fragment.
- Pour les copies d'objet dans un pool de stockage Cloud, l'emplacement de l'objet, y compris le nom du bucket externe et l'identifiant unique de l'objet.

- Pour les objets segmentés et les objets en plusieurs parties, identifiants de segment et tailles de données.

Comment les métadonnées des objets sont-elles stockées ?

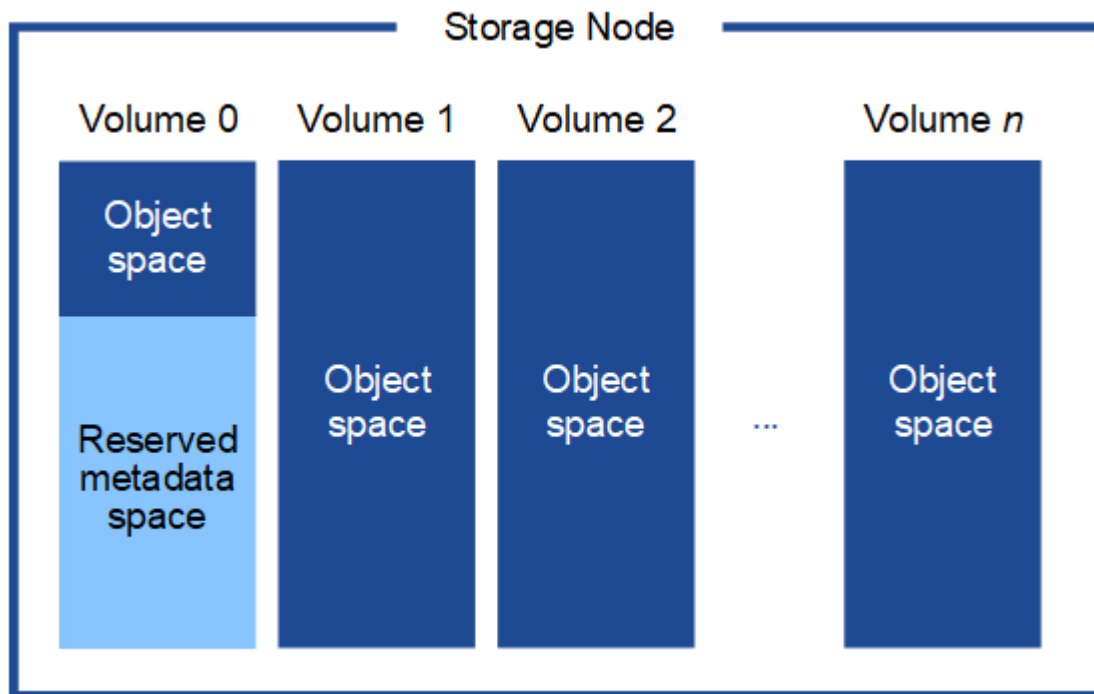
StorageGRID conserve les métadonnées des objets dans une base de données Cassandra, qui sont stockées indépendamment des données des objets. Pour assurer la redondance et protéger les métadonnées des objets contre la perte, StorageGRID stocke trois copies des métadonnées de tous les objets du système sur chaque site.

Cette figure représente les nœuds de stockage sur deux sites. Chaque site possède la même quantité de métadonnées d'objet, et les métadonnées de chaque site sont subdivisées entre tous les nœuds de stockage de ce site.



Où sont stockées les métadonnées des objets ?

Cette figure représente les volumes de stockage pour un seul nœud de stockage.



Comme indiqué dans la figure, StorageGRID réserve de l'espace pour les métadonnées d'objet sur le volume de stockage 0 de chaque nœud de stockage. Il utilise l'espace réservé pour stocker les métadonnées des

objets et effectuer les opérations essentielles de la base de données. Tout espace restant sur le volume de stockage 0 et tous les autres volumes de stockage du nœud de stockage sont utilisés exclusivement pour les données d'objet (copies répliquées et fragments codés par effacement).

La quantité d'espace réservée aux métadonnées d'objet sur un nœud de stockage particulier dépend de plusieurs facteurs, décrits ci-dessous.

Paramètre d'espace réservé aux métadonnées

L'espace réservé aux métadonnées 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 nœud 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.
- La 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 d'espace réservé aux métadonnées par défaut
11,5 à 11,9	128 Go ou plus 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 donné	4 To (4 000 Go)
	Moins de 128 Go sur n'importe quel nœud de stockage sur chaque site	3 To (3 000 Go)
11.0 ou version antérieure	N'importe quel montant	2 To (2 000 Go)

Afficher le paramètre d'espace réservé aux métadonnées

Suivez ces étapes pour afficher le paramètre d'espace réservé aux métadonnées pour votre système StorageGRID .

Étapes

1. Sélectionnez **CONFIGURATION > Système > Paramètres de stockage**.
2. Sur la page Paramètres de stockage, développez la section **Espace réservé aux métadonnées**.

Pour StorageGRID 11.8 ou supérieur, la valeur de l'espace réservé aux métadonnées doit être d'au moins 100 Go et d'au plus 1 Po.

Le paramètre par défaut pour une nouvelle installation de StorageGRID 11.6 ou supérieure dans laquelle chaque nœud de stockage dispose de 128 Go ou plus de RAM est de 8 000 Go (8 To).

Espace réservé réel pour les métadonnées

Contrairement au paramètre d'espace réservé aux métadonnées à l'échelle du système, l'espace réservé réel pour les métadonnées d'objet est déterminé pour chaque nœud de stockage. Pour tout nœud de stockage donné, l'espace réservé réel pour les métadonnées dépend de la taille du volume 0 pour le nœud et du paramètre d'espace réservé aux métadonnées à l'échelle du système.

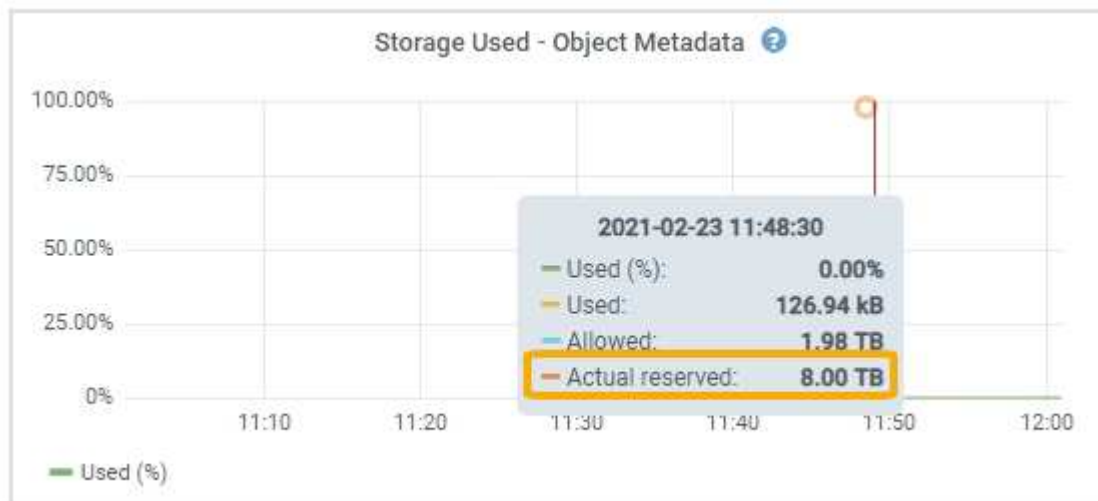
Taille du volume 0 pour le nœud	Espace réservé réel pour les métadonnées
Moins de 500 Go (utilisation hors production)	10% du volume 0
500 Go ou plus + ou + Nœuds de stockage de métadonnées uniquement	La plus petite de ces valeurs : • Volume 0 • Paramètre d'espace réservé aux métadonnées Remarque : un seul rangedb est requis pour les nœuds de stockage contenant uniquement des métadonnées.

Afficher l'espace réservé réel pour les métadonnées

Suivez ces étapes pour afficher l'espace réservé réel pour les métadonnées sur un nœud de stockage particulier.

Étapes

1. Dans le gestionnaire de grille, sélectionnez **NODES** > **Storage Node**.
2. Sélectionnez l'onglet **Stockage**.
3. Placez votre curseur sur le graphique Stockage utilisé - Métadonnées de l'objet et recherchez la valeur **Réservée réelle**.



Dans la capture d'écran, la valeur **Réservée réelle** est de 8 To. Cette capture d'écran concerne un grand nœud de stockage dans une nouvelle installation de StorageGRID 11.6. Étant donné que le paramètre d'espace réservé aux métadonnées à l'échelle du système est inférieur au volume 0 pour ce nœud de stockage, l'espace réservé réel pour ce nœud est égal au paramètre d'espace réservé aux métadonnées.

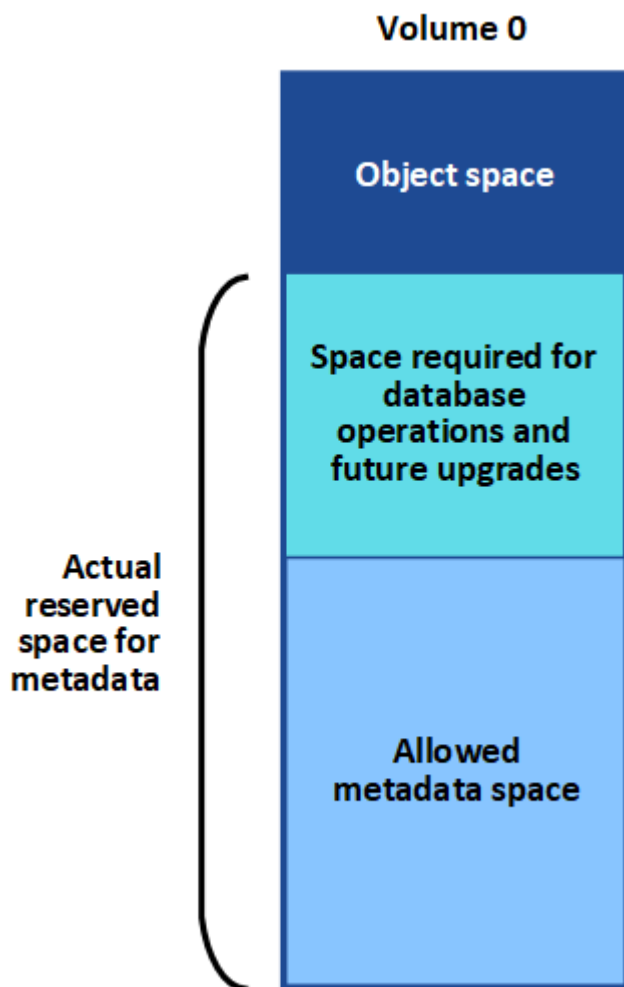
Exemple d'espace de métadonnées réservé réel

Supposons que vous installiez un nouveau système StorageGRID utilisant la version 11.7 ou ultérieure. Pour 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 aux métadonnées à l'échelle du système est défini sur 8 To. (Il s'agit de la valeur par défaut pour une nouvelle installation de StorageGRID 11.6 ou supérieure si 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 plus petit que le paramètre **Espace réservé aux métadonnées**.)

Espace de métadonnées autorisé

L'espace réservé réel de chaque nœud de stockage pour les métadonnées est subdivisé en espace disponible pour les métadonnées d'objet (l'espace de métadonnées autorisé) et l'espace requis pour les opérations de base de données essentielles (telles que le compactage et la réparation) et les futures mises à niveau matérielles et logicielles. L'espace de métadonnées autorisé régit la capacité globale de l'objet.



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.

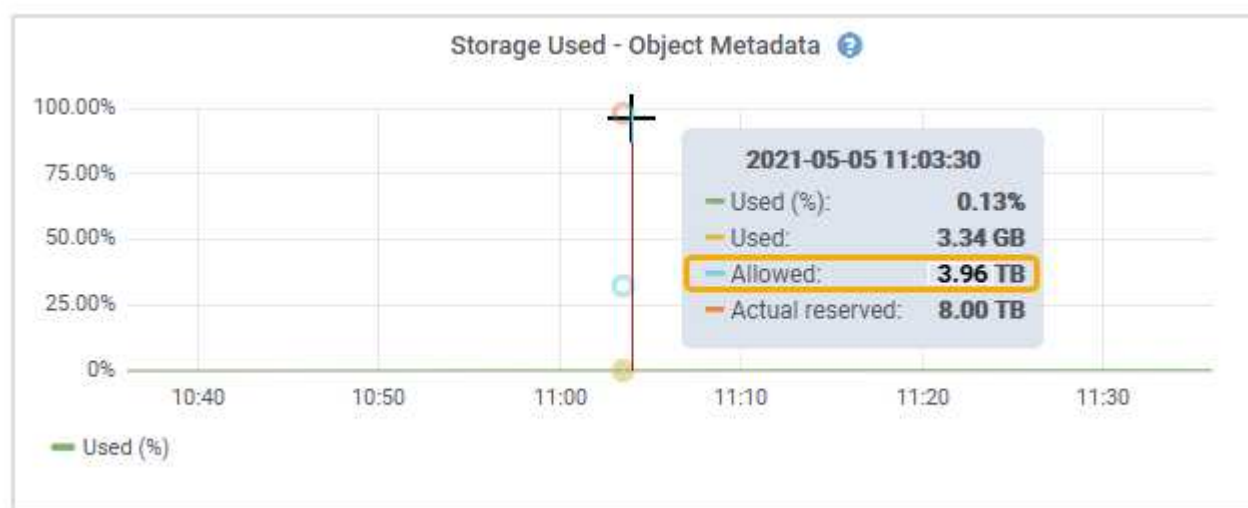
		Quantité de mémoire sur le nœud de stockage	
	< 128 Go	>= 128 Go	Espace réservé réel pour les métadonnées
≤ 4 To	60 % de l'espace réel réservé aux métadonnées, jusqu'à un maximum de 1,32 To	60 % de l'espace réel réservé aux métadonnées, jusqu'à un maximum de 1,98 To	4 To

Afficher l'espace de métadonnées autorisé

Suivez ces étapes pour afficher l'espace de métadonnées autorisé pour un nœud de stockage.

Étapes

1. Dans le gestionnaire de grille, sélectionnez **NODES**.
2. Sélectionnez le nœud de stockage.
3. Sélectionnez l'onglet **Stockage**.
4. Placez votre curseur sur le graphique Stockage utilisé - métadonnées de l'objet et recherchez la valeur **Autorisée**.



Dans la capture d'écran, la valeur **Autorisée** est de 3,96 To, ce qui correspond à la valeur maximale pour un nœud de stockage dont l'espace réservé réel pour les métadonnées est supérieur à 4 To.

La valeur **Autorisée** correspond à cette métrique Prometheus :

```
storagegrid_storage_utilization_metadata_allowed_bytes
```

Exemple d'espace de métadonnées autorisé

Supposons que vous installiez un système StorageGRID utilisant la version 11.6. Pour 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 aux métadonnées à l'échelle 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 plus petit que le paramètre **Espace réservé aux métadonnées**.)
- L'espace autorisé pour les métadonnées sur SN1 est de 3 To, sur la base du calcul indiqué dans le [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.

Comment les nœuds de stockage de différentes tailles affectent la capacité des objets

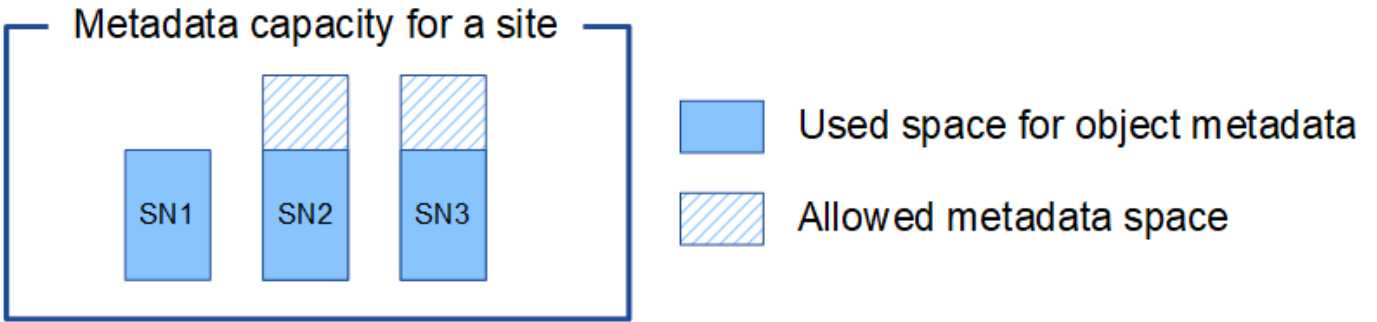
Comme décrit ci-dessus, StorageGRID répartit uniformément les métadonnées des objets sur les nœuds de stockage de chaque site. Pour cette raison, si un site contient des nœuds de stockage de différentes tailles, le plus petit nœud du site détermine la capacité de métadonnées du site.

Considérez l'exemple suivant :

- Vous disposez d'une grille à site unique contenant trois nœuds de stockage de tailles différentes.
- Le paramètre **Espace réservé aux métadonnées** est de 4 To.
- Les nœuds de stockage ont les valeurs suivantes pour l'espace de métadonnées réservé réel et l'espace de métadonnées autorisé.

Nœud de stockage	Taille du volume 0	Espace de métadonnées réservé réel	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

Étant donné que les métadonnées d'objet sont réparties uniformément sur les nœuds de stockage d'un site, chaque nœud de cet exemple ne peut contenir que 1,32 To de métadonnées. L'espace de métadonnées supplémentaire autorisé de 0,66 To pour SN2 et SN3 ne peut pas être utilisé.



De même, étant donné que StorageGRID conserve toutes les métadonnées d'objet pour 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.

Et comme la capacité des métadonnées d'objet contrôle le nombre maximal d'objets, lorsqu'un nœud n'a plus de capacité de métadonnées, la grille est effectivement pleine.

Informations connexes

- Pour savoir comment surveiller la capacité des métadonnées d'objet pour chaque nœud de stockage, consultez les instructions de ["Surveillance de StorageGRID"](#).
- Pour augmenter la capacité des métadonnées d'objets de votre système, ["étendre une 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 Grid Manager 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"](#).



La page Topologie de grille est obsolète et sera supprimée dans une prochaine version.

À propos de cette 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 la manière dont le paramètre Espace réservé aux métadonnées affecte l'espace autorisé pour le stockage des métadonnées d'objet sur un nœud de stockage particulier, voir ["Gérer le stockage des métadonnées des objets"](#).

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 **NODES**.
 - 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 **NODES**.
 - 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)

Storage Options

Overview

Configuration



Configure Storage Options

Updated: 2021-12-10 13:48:23 MST

Object Segmentation

Description	Settings
Segmentation	Enabled
Maximum Segment Size	1000000000

Storage Watermarks

Description	Settings
Storage Volume Read-Write Watermark Override	0
Storage Volume Soft Read-Only Watermark Override	0
Storage Volume Hard Read-Only Watermark Override	0
Metadata Reserved Space	800000000000

Apply Changes

a. Sélectionnez **Appliquer les modifications**.

Compresser les objets stockés

Vous pouvez activer la compression d'objets pour réduire la taille des objets stockés dans StorageGRID, afin que les objets consomment moins de stockage.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un [navigateur Web pris en charge](#).
- Tu as [autorisations d'accès spécifiques](#).

À propos de cette tâche

Par défaut, la compression d'objet est désactivée. Si vous activez la compression, StorageGRID tente de compresser chaque objet lors de son enregistrement, en utilisant une compression sans perte.



Si vous modifiez ce paramètre, l'application du nouveau paramètre prendra environ une minute. La valeur configurée est mise en cache pour les performances et la mise à l'échelle.

Avant d'activer la compression d'objet, tenez compte des points suivants :

- Vous ne devez pas sélectionner **Compresser les objets stockés** à moins que vous ne sachiez 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 cliente a déjà compressé un objet avant de l'enregistrer dans StorageGRID, la sélection de cette option ne réduira pas davantage la taille de l'objet.
- Ne sélectionnez pas **Compresser les objets stockés** si vous utilisez NetApp FabricPool avec StorageGRID.
- Si **Compresser les objets stockés** est sélectionné, les applications clientes S3 doivent éviter d'effectuer des opérations GetObject qui spécifient une plage d'octets à renvoyer. Ces opérations de « lecture de

plage » sont inefficaces car StorageGRID doit décompresser efficacement les objets pour accéder aux octets demandés. Les opérations GetObject qui demandent une petite plage d'octets à partir d'un très grand objet sont particulièrement inefficaces ; par exemple, il est 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 des clients peuvent expirer.



Si vous devez compresser des objets et que votre application cliente doit utiliser des lectures de plage, augmentez le délai d'expiration de lecture pour l'application.

Étapes

1. Sélectionnez **CONFIGURATION > Système > Paramètres de stockage > Compression d'objet**.
2. Cochez la case **Compresser les objets stockés**.
3. Sélectionnez **Enregistrer**.

Gérer des nœuds de stockage complets

À mesure que les nœuds de stockage atteignent leur capacité, vous devez étendre le système StorageGRID en ajoutant un nouveau stockage. Trois options sont disponibles : l'ajout de volumes de stockage, l'ajout d'étagères d'extension de stockage et l'ajout de nœuds de stockage.

Ajouter des volumes de stockage

Chaque nœud de stockage prend en charge un nombre maximal de volumes de stockage. Le maximum défini varie selon la plateforme. Si un nœud de stockage contient moins de volumes de stockage que le nombre maximal, vous pouvez ajouter des volumes pour augmenter sa capacité. Voir les instructions pour ["extension d'un système StorageGRID"](#).

Ajouter des étagères d'extension de stockage

Certains nœuds de stockage d'appliance StorageGRID, tels que le SG6060 ou le SG6160, peuvent prendre en charge des étagères de stockage supplémentaires. Si vous disposez d'appliances StorageGRID avec des capacités d'extension qui n'ont pas déjà été étendues à leur capacité maximale, vous pouvez ajouter des étagères de stockage pour augmenter la capacité. Voir les instructions pour ["extension d'un système StorageGRID"](#).

Ajouter des nœuds de stockage

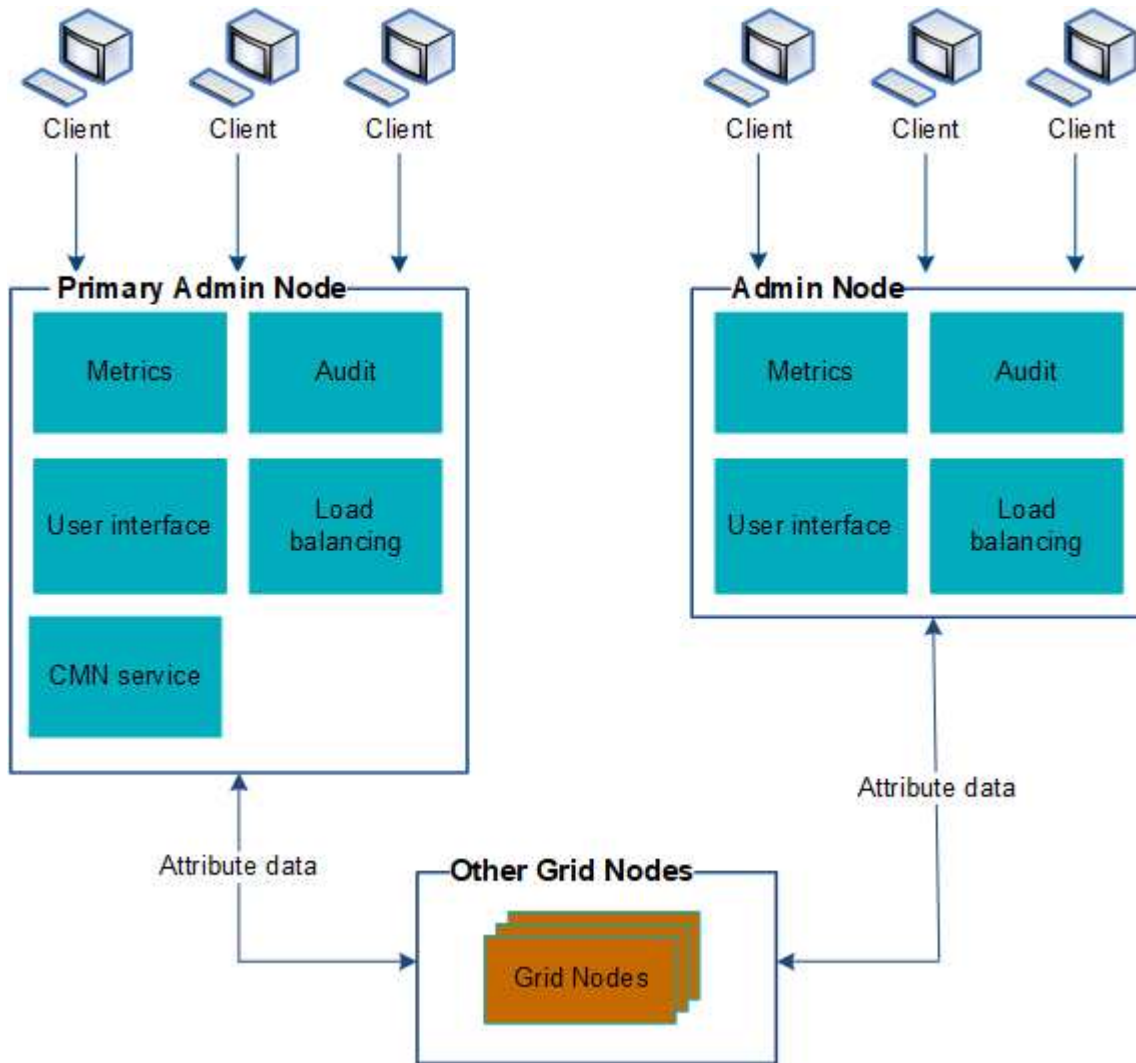
Vous pouvez augmenter la capacité de stockage en ajoutant des nœuds de stockage. Une attention particulière doit être portée aux règles ILM actuellement actives et aux exigences de capacité lors de l'ajout de stockage. Voir les instructions pour ["extension d'un système StorageGRID"](#).

Gérer les nœuds d'administration

Utiliser plusieurs nœuds d'administration

Un système StorageGRID peut inclure plusieurs nœuds d'administration pour vous permettre de surveiller et de configurer en continu votre système StorageGRID même si un nœud d'administration tombe en panne.

Si un nœud d'administration devient indisponible, le traitement des attributs continue, les alertes sont toujours déclenchées et les notifications par e-mail et les packages AutoSupport sont toujours envoyés. Cependant, le fait d'avoir plusieurs nœuds d'administration n'offre pas de protection de basculement, à l'exception des notifications et des packages AutoSupport .



Il existe deux options 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 n'importe quel autre nœud d'administration disponible.
- Si un administrateur système a configuré un groupe haute disponibilité de nœuds d'administration, les clients Web peuvent continuer à accéder au gestionnaire de grille ou au gestionnaire de locataires à l'aide de l'adresse IP virtuelle du groupe HA. Voir "[Gérer les groupes de haute disponibilité](#)".



Lors de l'utilisation d'un groupe HA, l'accès est interrompu si le nœud d'administration actif échoue. Les utilisateurs doivent se reconnecter après que l'adresse IP virtuelle du groupe HA bascule vers un autre nœud d'administration du groupe.

Certaines tâches de maintenance ne peuvent être effectuées qu'à l'aide du nœud d'administration principal. Si le nœud d'administration principal échoue, il doit être récupéré avant que le système StorageGRID soit à nouveau entièrement fonctionnel.

Identifier le nœud d'administration principal

Le nœud d'administration principal fournit plus de fonctionnalités que les nœuds d'administration non principaux. Par exemple, certaines procédures de maintenance doivent être effectuées à l'aide du nœud d'administration principal.

Pour plus d'informations sur les nœuds d'administration, voir "[Qu'est-ce qu'un nœud d'administration](#)".

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "[navigateur Web pris en charge](#)".
- Tu as "[autorisations d'accès spécifiques](#)".

Étapes

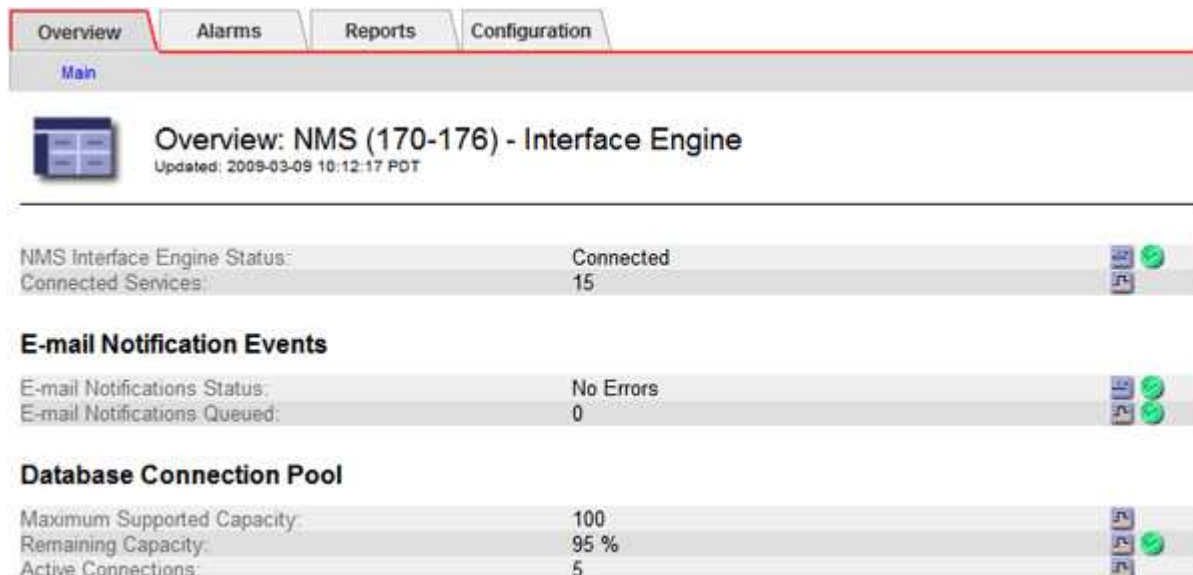
1. Sélectionnez **NODES**.
2. Saisissez **primaire** dans le champ de recherche.

Dans les résultats de la recherche, identifiez le nœud avec « Nœud d'administration principal » affiché dans la colonne Type. Un nœud d'administration principal doit être répertorié.

Afficher l'état des notifications et les files d'attente

Le service du système de gestion de réseau (NMS) sur les nœuds d'administration envoie des notifications au serveur de messagerie. Vous pouvez afficher l'état actuel du service NMS et 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**. Sélectionnez ensuite **site > Admin Node > NMS > Interface Engine**.



The screenshot displays the 'Overview: NMS (170-176) - Interface Engine' page. At the top, there are tabs for 'Overview', 'Alarms', 'Reports', and 'Configuration'. Below the tabs, the page title is 'Overview: NMS (170-176) - Interface Engine' with a timestamp 'Updated: 2009-03-09 10:12:17 PDT'. The main content area is divided into three sections:

- NMS Interface Engine Status:** Shows 'Connected' with a green status icon and 'Connected Services: 15'.
- E-mail Notification Events:** Shows 'E-mail Notifications Status: No Errors' and 'E-mail Notifications Queued: 0' with green status icons.
- Database Connection Pool:** Shows 'Maximum Supported Capacity: 100', 'Remaining Capacity: 95 %', and 'Active Connections: 5' with green status icons.

Les notifications sont traitées via la file d'attente des notifications par e-mail et sont envoyées au serveur de messagerie l'une après l'autre dans l'ordre dans lequel elles sont déclenchées. S'il y a un problème (par exemple, une erreur de connexion réseau) et que le serveur de messagerie n'est pas disponible lorsque la tentative d'envoi de la notification est effectuée, 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, la notification est supprimée de la file d'attente des notifications et une

tentative d'envoi de la notification suivante dans la file d'attente est effectuée.

Gérer les objets avec ILM

Gérer les objets avec ILM

Les règles de gestion du cycle de vie des informations (ILM) d'une politique ILM indiquent à StorageGRID comment créer et distribuer des copies des données d'objet et comment gérer ces copies au fil du temps.

À propos de ces instructions

La conception et la mise en œuvre des règles et politiques ILM nécessitent une planification minutieuse. Vous devez comprendre vos exigences opérationnelles, la topologie de votre système StorageGRID , vos besoins de protection des objets et les types de stockage disponibles. Ensuite, vous devez déterminer comment vous souhaitez que les différents types d'objets soient copiés, distribués et stockés.

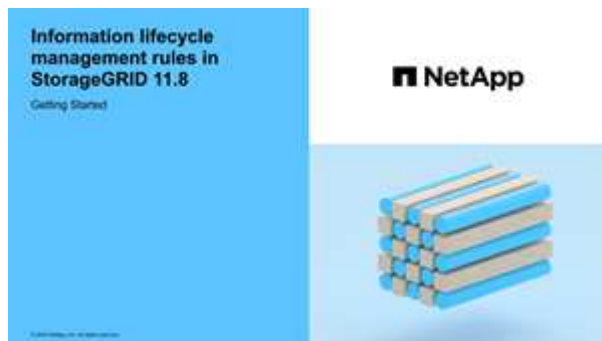
Utilisez ces instructions pour :

- En savoir plus sur StorageGRID ILM, notamment [comment ILM fonctionne tout au long de la vie d'un objet](#) .
- Apprenez à configurer ["piscines de stockage"](#) , ["Pools de stockage cloud"](#) , et ["Règles de l'ILM"](#) .
- Apprenez à ["créer, simuler et activer une politique ILM"](#) qui protégera les données des objets sur un ou plusieurs sites.
- Apprenez à ["gérer les objets avec S3 Object Lock"](#) , ce qui permet de garantir que les objets dans des compartiments S3 spécifiques ne sont pas supprimés ou écrasés pendant une durée spécifiée.

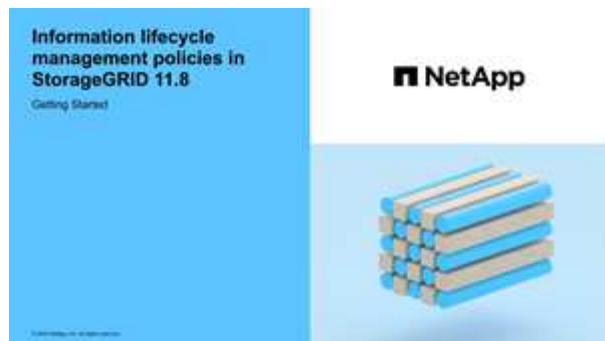
Apprendre encore plus

Pour en savoir plus, regardez ces vidéos :

- ["Vidéo : aperçu des règles de l'ILM"](#) .



- ["Vidéo : Présentation des politiques ILM"](#)



ILM et cycle de vie des objets

Comment ILM fonctionne tout au long de la vie d'un objet

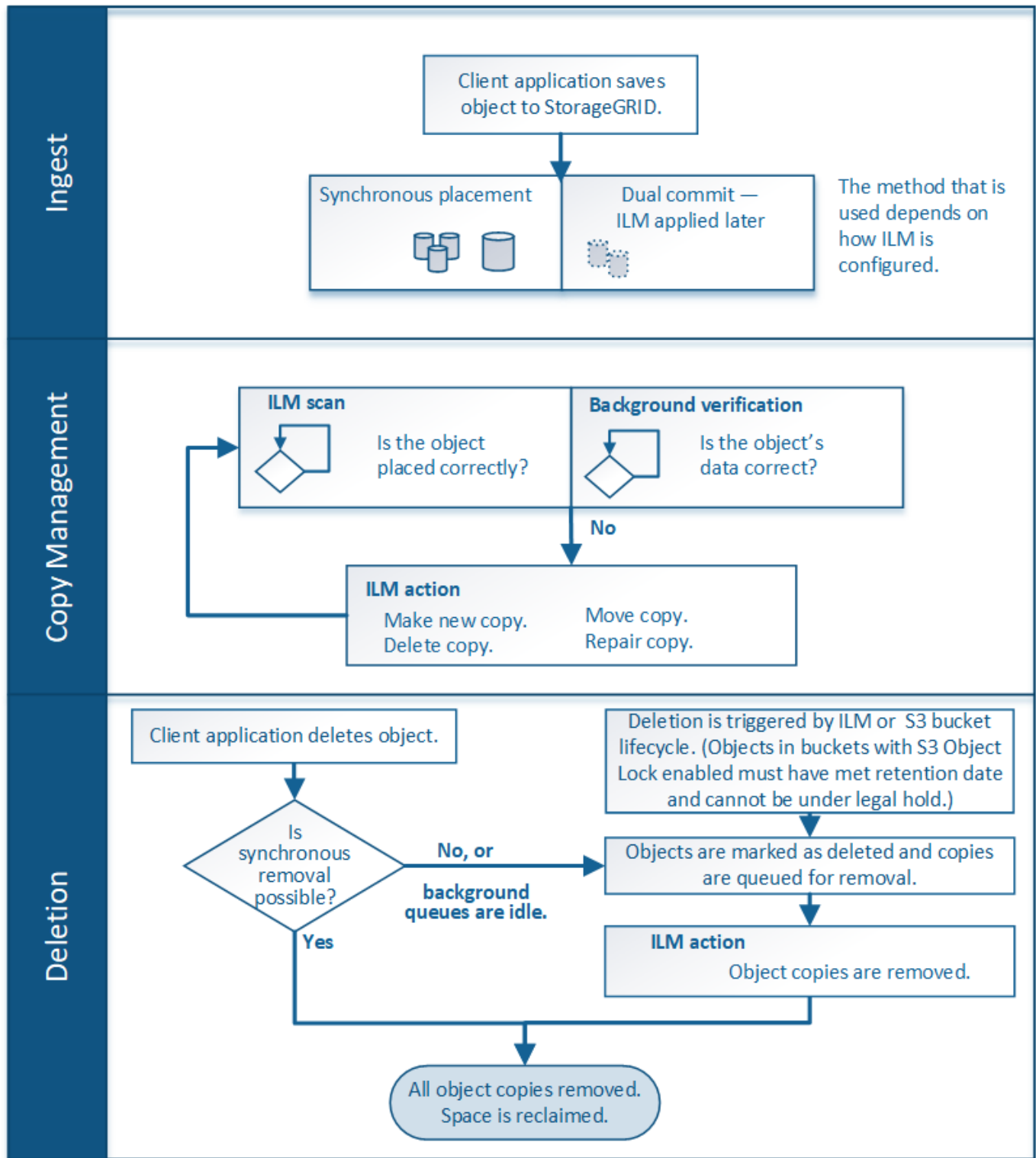
Comprendre comment StorageGRID utilise ILM pour gérer les objets à chaque étape de leur vie peut vous aider à concevoir une politique plus efficace.

- **Ingest** : l'ingestion commence lorsqu'une application cliente S3 établit une connexion pour enregistrer un objet sur le système StorageGRID et est terminée lorsque StorageGRID renvoie un message « ingestion réussie » au client. Les données d'objet sont protégées pendant l'ingestion soit en appliquant immédiatement les instructions ILM (placement synchrone), soit en créant des copies intermédiaires et en appliquant ILM ultérieurement (double validation), selon la manière dont les exigences ILM ont été spécifiées.
- **Gestion des copies** : après avoir créé le nombre et le 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 la perte.
 - **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 pour vérifier l'intégrité des données de l'objet. Si un problème est détecté, StorageGRID crée automatiquement une nouvelle copie d'objet ou un fragment d'objet codé par effacement de remplacement dans un emplacement qui répond aux exigences ILM actuelles. Voir "[Vérifier l'intégrité de l'objet](#)".
- **Suppression d'objet** : la gestion d'un objet se termine lorsque toutes les copies sont supprimées du système StorageGRID. Les objets peuvent être supprimés à la suite d'une demande de suppression par un client, ou à la suite d'une suppression par ILM ou d'une suppression causée par l'expiration d'un cycle de vie de compartiment S3.



Les objets d'un compartiment sur lequel le verrouillage d'objet S3 est activé ne peuvent pas être supprimés s'ils sont soumis à une conservation légale ou si une date de conservation a été spécifiée mais n'a pas encore été respectée.

Le diagramme résume le fonctionnement de l'ILM tout au long du cycle de vie d'un objet.



Comment les objets sont ingérés

Options d'ingestion

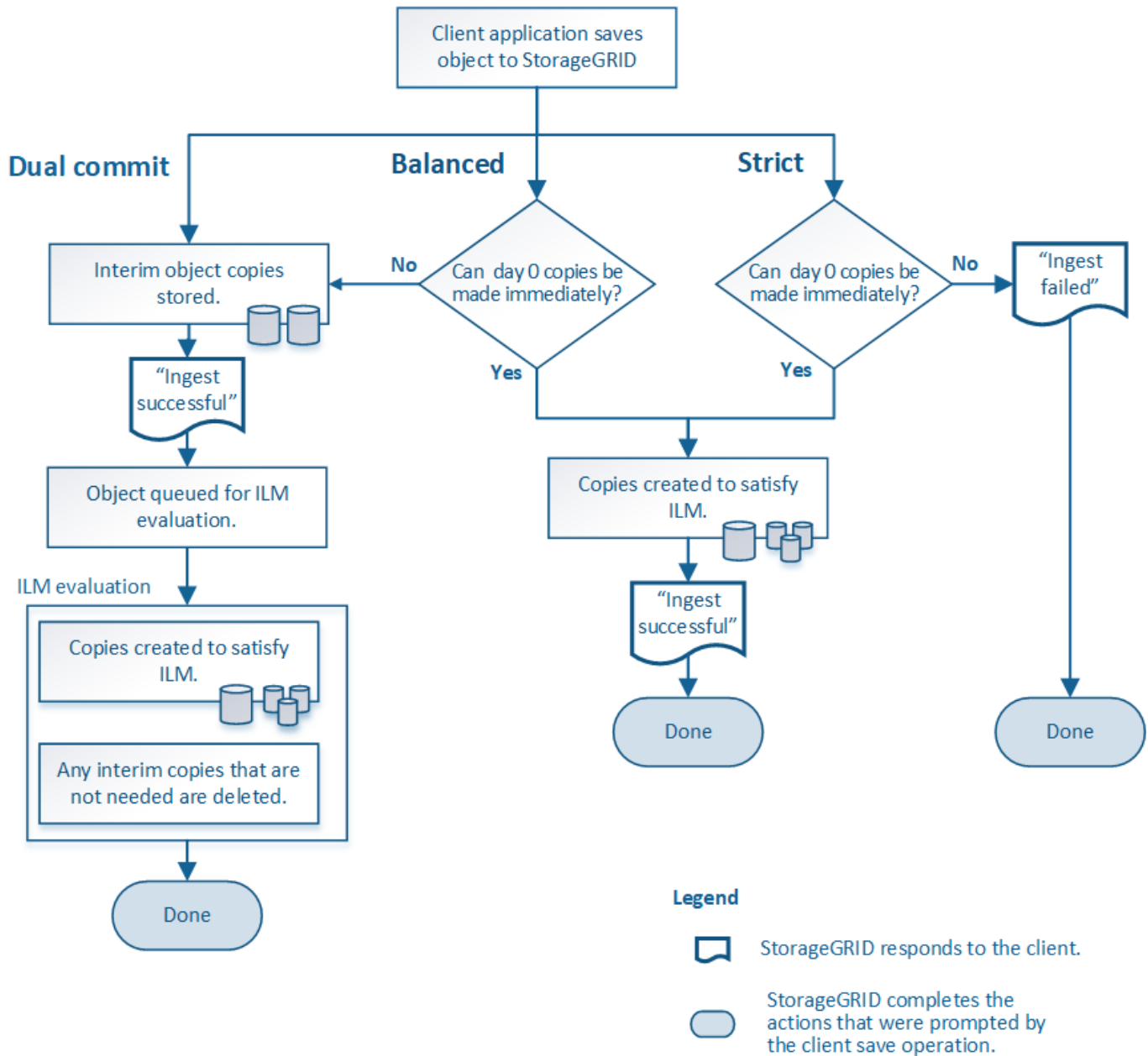
Lorsque vous créez une règle ILM, vous spécifiez l'une des trois options de protection des objets lors de l'ingestion : double validation, stricte ou équilibrée.

Selon votre choix, StorageGRID effectue des copies intermédiaires et met en file d'attente les objets pour une

évaluation ILM ultérieure, ou il utilise le placement synchrone et effectue immédiatement des copies pour répondre aux exigences ILM.

Organigramme des options d'ingestion

L'organigramme montre ce qui se passe lorsque des objets sont mis en correspondance par une règle ILM qui utilise chacune des trois options d'ingestion.



Double engagement

Lorsque vous sélectionnez l'option Double validation, StorageGRID effectue immédiatement des copies d'objets intermédiaires sur deux nœuds de stockage différents et renvoie un message « ingestion réussie » au client. L'objet est mis en file d'attente pour l'évaluation ILM, et les copies qui répondent aux instructions de placement de la règle sont effectuées ultérieurement. Si la politique ILM ne peut pas être traitée immédiatement après la double validation, la protection contre la perte de site peut prendre du temps à être mise en place.

Utilisez l'option Dual commit dans l'un ou l'autre de ces cas :

- Vous utilisez des règles ILM multisites et la latence d'ingestion du client est votre principale considération. Lorsque vous utilisez la double validation, vous devez vous assurer que votre grille peut effectuer le travail supplémentaire de création et de suppression des copies à double validation si elles ne satisfont pas ILM. Spécifiquement:
 - La charge sur le réseau doit être suffisamment faible pour éviter un retard ILM.
 - La grille doit disposer de ressources matérielles excédentaires (IOPS, CPU, 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 Dual commit peut aider à éviter les délais d'expiration du client. Avant de choisir l'option Double validation, vous devez tester l'application cliente avec des charges de travail réalistes.

Équilibré (par défaut)

Lorsque vous sélectionnez l'option Équilibré, StorageGRID utilise également le placement synchrone lors de l'ingestion et effectue immédiatement toutes les copies spécifiées dans les instructions de placement de la règle. Contrairement à l'option Strict, si StorageGRID ne peut pas effectuer immédiatement toutes les copies, il utilise à la place la validation double. Si la politique ILM utilise des placements sur plusieurs sites et qu'une protection immédiate contre la perte de site ne peut pas être obtenue, l'alerte **Placement ILM irréalisable** est déclenchée.

Utilisez l'option Équilibré pour obtenir la meilleure combinaison de protection des données, de performances de la grille et de réussite d'ingestion. Équilibré est l'option par défaut dans l'assistant de création de règle ILM.

Strict

Lorsque vous sélectionnez l'option Strict, StorageGRID utilise le placement synchrone lors de l'ingestion et effectue 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 parce qu'un emplacement de stockage requis est temporairement indisponible. Le client doit réessayer l'opération.

Utilisez l'option Strict si vous avez une exigence opérationnelle ou réglementaire de stocker immédiatement des objets uniquement dans les emplacements décrits dans la règle ILM. Par exemple, pour satisfaire à une exigence réglementaire, vous devrez peut-être utiliser l'option Strict et un filtre avancé Contrainte d'emplacement pour garantir que les objets ne sont jamais stockés dans certains centres de données.

Voir ["Exemple 5 : Règles et politique ILM pour un comportement d'ingestion strict"](#) .

Avantages, inconvénients et limites des options d'ingestion

Comprendre les avantages et les inconvénients de chacune des trois options de protection des données lors de l'ingestion (validation équilibrée, stricte ou double) peut vous aider à décider laquelle sélectionner pour une règle ILM.

Pour un aperçu des options d'ingestion, voir ["Options d'ingestion"](#) .

Avantages des options Équilibré et Strict

Par rapport à la validation double, qui crée des copies intermédiaires lors de l'ingestion, les deux options de placement synchrone peuvent offrir les avantages suivants :

- *** Meilleure sécurité des données *** : les données de l'objet sont immédiatement protégées comme spécifié dans les instructions de placement de la règle ILM, qui peuvent être configurées pour protéger contre une grande variété 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 seule copie locale.
- **Fonctionnement de grille plus efficace** : chaque objet est traité une seule fois, au fur et à mesure de son ingestion. Étant donné que le système StorageGRID n'a pas besoin de suivre ou de supprimer les copies intermédiaires, la charge de traitement est moindre et l'espace de base de données consommé est moindre.
- **(Équilibré) Recommandé** : L'option Équilibré offre une efficacité ILM optimale. L'utilisation de l'option Équilibré 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.
- **(Stricte) 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 Équilibré et Strict

Par rapport à la validation double, les options équilibrée et stricte présentent certains inconvénients :

- **Ingestions client plus longues** : les latences d'ingestion client peuvent être plus longues. Lorsque vous utilisez les options Équilibré ou Strict, un message « ingestion réussie » n'est pas renvoyé au client tant que tous les fragments codés par effacement ou les copies répliquées ne sont pas créés et stockés. Cependant, les données de l'objet atteindront probablement leur emplacement final beaucoup plus rapidement.
- **(Strict) Taux d'échec d'ingestion plus élevés** : avec l'option Strict, l'ingestion échoue lorsque StorageGRID ne peut pas effectuer immédiatement toutes les copies spécifiées dans la règle ILM. Vous pouvez constater des taux élevés d'échec d'ingestion si un emplacement de stockage requis est temporairement hors ligne ou si des problèmes de réseau entraînent des retards dans la copie d'objets entre les sites.
- **(Strict) Les placements de téléchargement multipartites S3 peuvent ne pas être comme prévu dans certaines circonstances** : Avec Strict, vous vous attendez à ce que les objets soient placés comme décrit par la règle ILM ou à ce que l'ingestion échoue. Cependant, avec un téléchargement multipartite S3, ILM est évalué pour chaque partie de l'objet au fur et à mesure de son ingestion, et pour l'objet dans son ensemble lorsque le téléchargement multipartite est terminé. Dans les circonstances suivantes, cela peut entraîner des placements différents de ceux que vous attendez :
 - **Si l'ILM change pendant qu'un téléchargement multipartite S3 est en cours** : Étant donné que chaque partie est placée selon la règle active lorsque la partie est ingérée, certaines parties de l'objet peuvent ne pas répondre aux exigences ILM actuelles une fois le téléchargement multipartite terminé. Dans ces cas, l'ingestion de l'objet n'échoue pas. Au lieu de cela, toute pièce qui n'est pas placée correctement est mise en file d'attente pour une réévaluation ILM et est déplacée vers l'emplacement correct ultérieurement.
 - **Lorsque les règles ILM filtrent sur la taille** : lors de l'évaluation de l'ILM pour une partie, StorageGRID filtre sur la taille de la partie, et non sur la taille de l'objet. Cela signifie que des parties d'un objet peuvent être stockées dans des emplacements qui ne répondent pas aux exigences ILM pour l'objet dans son ensemble. Par exemple, si une règle spécifie que tous les objets de 10 Go ou plus sont stockés sur DC1 tandis que tous les objets plus petits sont stockés sur DC2, lors de l'ingestion, chaque partie de 1 Go d'un téléchargement multipartite en 10 parties est stockée sur DC2. Lorsque l'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 que les nouveaux placements requis ne peuvent pas être effectués** : avec Strict, vous vous attendez à ce que les objets soient placés comme décrit par la règle ILM ou que l'ingestion échoue. Cependant, 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 toutes les modifications apportées au placement des objets déclenchées par la mise à jour ne sont pas effectuées immédiatement. Les modifications de placement sont effectuées lorsque l'ILM est réévalué par les processus ILM d'arrière-plan normaux. Si les modifications de placement 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 placement actuel jusqu'à ce que les modifications de placement soient possibles.

Limitations sur les placements d'objets avec les options Équilibré et Strict

Les options Équilibré ou Strict ne peuvent pas être utilisées pour les règles ILM qui ont l'une de ces instructions de placement :

- Placement dans un pool de stockage cloud au jour 0.
- Emplacements dans un pool de stockage cloud lorsque la règle a une heure de création définie par l'utilisateur comme heure de référence.

Ces restrictions existent parce que StorageGRID ne peut pas effectuer de copies de manière synchrone vers un pool de stockage cloud, et une heure de création définie par l'utilisateur peut être résolue au présent.

Comment les règles ILM et la cohérence interagissent pour affecter la protection des données

Votre règle ILM et votre choix de cohérence affectent la manière dont les objets sont protégés. Ces paramètres peuvent interagir.

Par exemple, le comportement d'ingestion sélectionné pour une règle ILM affecte le placement initial des copies d'objet, tandis que la cohérence utilisée lors du stockage d'un objet affecte le placement initial des métadonnées de l'objet. Étant donné que StorageGRID nécessite l'accès aux données et aux métadonnées d'un objet pour répondre aux demandes des clients, la sélection de niveaux de protection correspondants pour la cohérence et le comportement d'ingestion peut fournir une meilleure protection initiale des données et des réponses système plus prévisibles.

Voici un bref résumé des valeurs de cohérence disponibles dans StorageGRID:

- **Tous** : Tous les nœuds reçoivent immédiatement les métadonnées de l'objet, sinon la demande échouera.
- **Strong-global** : les métadonnées de l'objet sont immédiatement distribuées à tous les sites. Garantit la cohérence de lecture après écriture pour toutes les demandes client sur tous les sites.
- **Site fort** : les métadonnées de l'objet sont immédiatement distribuées aux autres nœuds du site. Garantit la cohérence de lecture après écriture pour toutes les demandes client au sein d'un site.
- **Lecture après nouvelle écriture** : assure la cohérence de lecture après écriture pour les nouveaux objets et la cohérence éventuelle pour les mises à jour d'objets. Offre des garanties de haute disponibilité et de protection des données. Recommandé dans la plupart des cas.
- **Disponible** : Fournit une cohérence éventuelle pour les nouveaux objets et les mises à jour d'objets. Pour les buckets S3, utilisez-les uniquement si nécessaire (par exemple, pour un bucket contenant des valeurs de journal rarement lues ou pour des opérations HEAD ou GET sur des clés qui n'existent pas). Non pris en charge pour les buckets S3 FabricPool .



Avant de sélectionner une valeur de cohérence, ["lire la description complète de la cohérence"](#) . Vous devez comprendre les avantages et les limites avant de modifier la valeur par défaut.

Exemple de la manière dont les règles de cohérence et les règles ILM peuvent interagir

Supposons que vous ayez une grille à deux sites avec la règle ILM suivante et la cohérence suivante :

- **Règle ILM** : Créez deux copies d'objet, une sur le site local et une sur un site distant. Adoptez un comportement d'ingestion strict.
- **cohérence** : Global fort (les métadonnées de l'objet sont immédiatement distribuées à tous les sites).

Lorsqu'un client stocke un objet dans la grille, StorageGRID effectue les deux copies de l'objet et distribue les métadonnées aux deux sites avant de renvoyer le succès au client.

L'objet est entièrement protégé contre la perte au moment de l'ingestion réussie du message. Par exemple, si le site local est perdu peu de temps après l'ingestion, des copies des données d'objet et des métadonnées d'objet existent toujours sur le site distant. L'objet est entièrement récupérable.

Si vous avez utilisé la même règle ILM et la cohérence de site forte, le client peut recevoir un message de réussite après la réplication des données d'objet sur le site distant, mais avant que les métadonnées d'objet y soient distribuées. Dans ce cas, le niveau de protection des métadonnées de l'objet ne correspond pas au niveau de protection des données de l'objet. Si le site local est perdu peu de temps après l'ingestion, les métadonnées de l'objet sont perdues. L'objet ne peut pas être récupéré.

L'interrelation entre la cohérence et les règles ILM peut être complexe. Contactez NetApp si vous avez besoin d'aide.

Informations connexes

["Exemple 5 : Règles et politique ILM pour un comportement d'ingestion strict"](#)

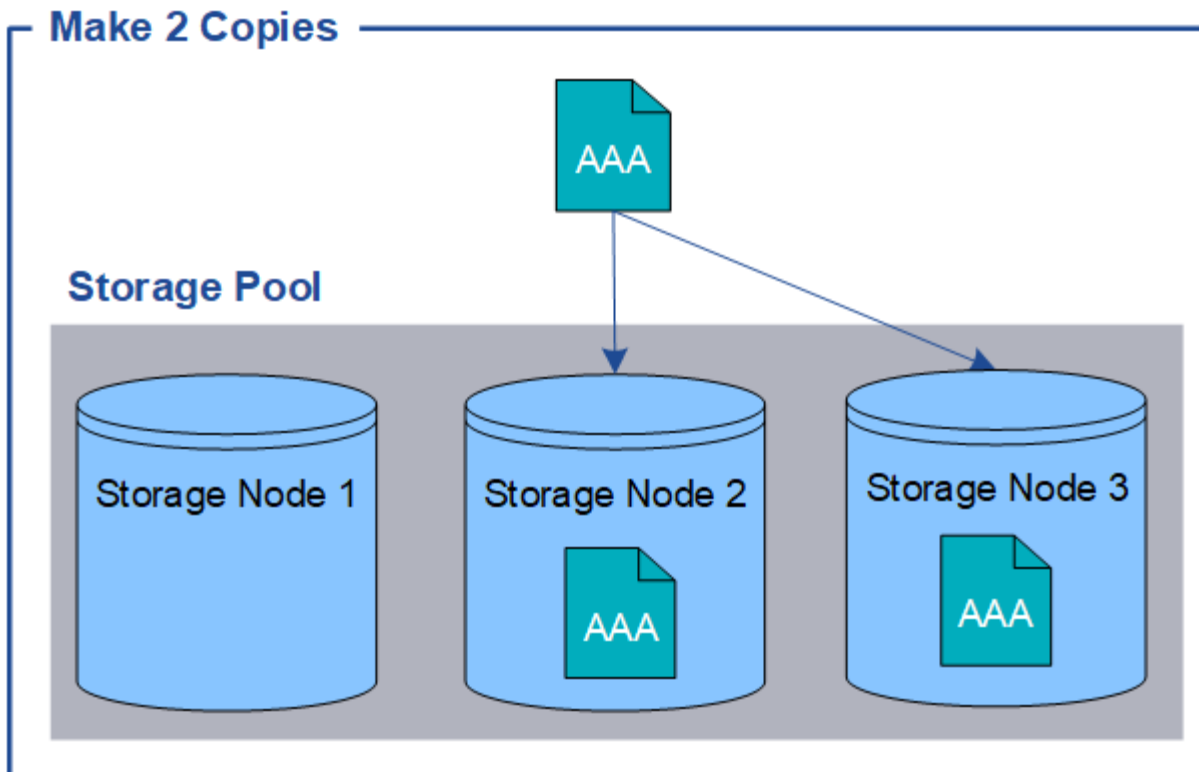
Comment les objets sont stockés (réplication ou codage d'effacement)

Qu'est-ce que la réplication ?

La réplication est l'une des deux méthodes utilisées par StorageGRID pour stocker les données d'objet (le codage d'effacement est l'autre méthode). Lorsque les objets correspondent à une règle ILM qui utilise la réplication, le système crée des copies exactes des données d'objet et stocke les copies sur des nœuds de stockage.

Lorsque vous configurez une règle ILM pour créer des copies répliquées, vous spécifiez le nombre de copies à créer, l'endroit où ces copies doivent être placées et la durée pendant laquelle les copies doivent être stockées à chaque emplacement.

Dans l'exemple suivant, la règle ILM spécifie que deux copies répliquées de chaque objet doivent être placées dans un pool de stockage contenant trois nœuds de stockage.



Lorsque StorageGRID fait correspondre des objets à cette règle, il crée deux copies de l'objet, en plaçant chaque copie sur un nœud de stockage différent dans le pool de stockage. 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 si l'un des nœuds du pool de stockage tombe en panne.



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 créez une règle ILM à 4 copies, seules trois copies seront effectuées : une copie pour chaque nœud de stockage. L'alerte **Placement ILM irréalisable** est déclenchée pour indiquer que la règle ILM n'a pas pu être complètement appliquée.

Informations connexes

- ["Qu'est-ce que le codage d'effacement"](#)
- ["Qu'est-ce qu'un pool de stockage"](#)
- ["Activer la protection contre la perte de site à l'aide du codage de répllication et d'effacement"](#)

Pourquoi vous ne devriez pas utiliser la répllication à copie unique

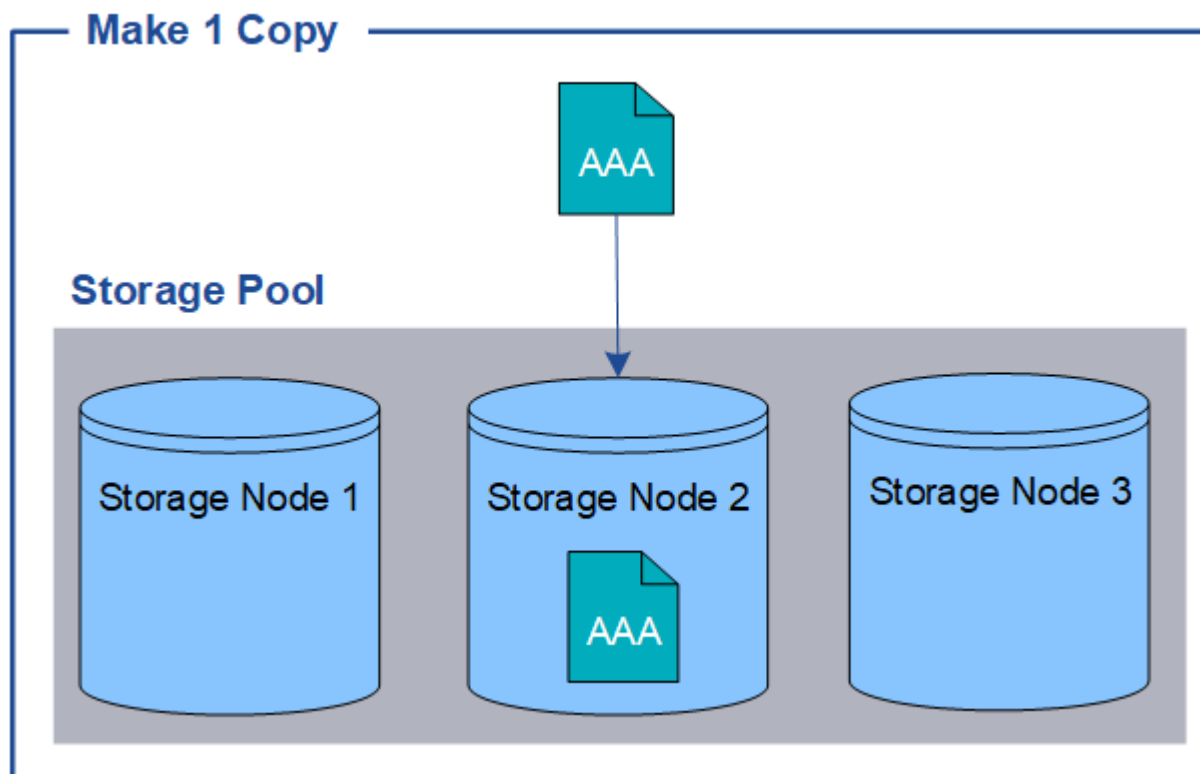
Lors de la création d'une règle ILM pour créer des copies répliquées, vous devez toujours spécifier au moins deux copies pour toute période dans les instructions de placement.



N'utilisez pas de règle ILM qui crée une seule copie répliquée pour une période donnée. Si une seule copie répliquée d'un objet existe, cet objet est perdu si un nœud de stockage échoue ou présente une erreur importante. Vous perdez également temporairement l'accès à l'objet pendant les procédures de maintenance telles que les mises à niveau.

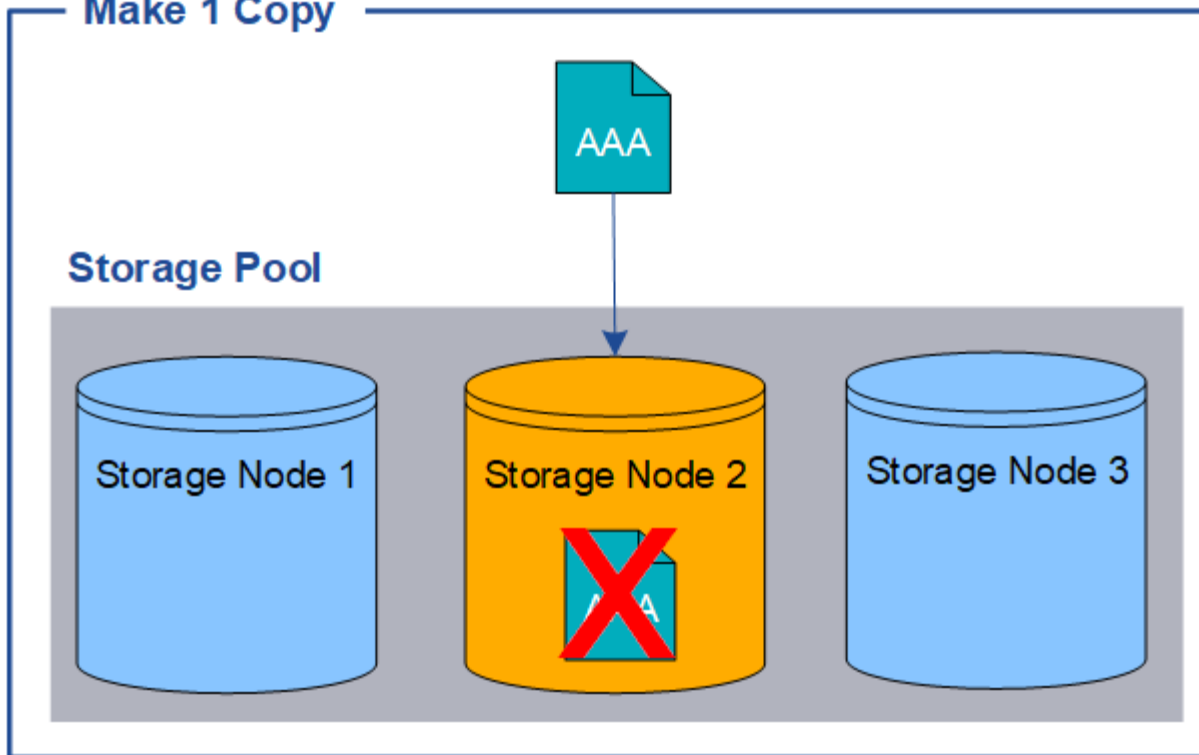
Dans l'exemple suivant, la règle ILM Make 1 Copy spécifie qu'une copie répliquée d'un objet doit être placée

dans un pool de stockage contenant trois nœuds de stockage. Lorsqu'un objet correspondant à cette règle est ingéré, StorageGRID place une seule copie sur un seul nœud de stockage.

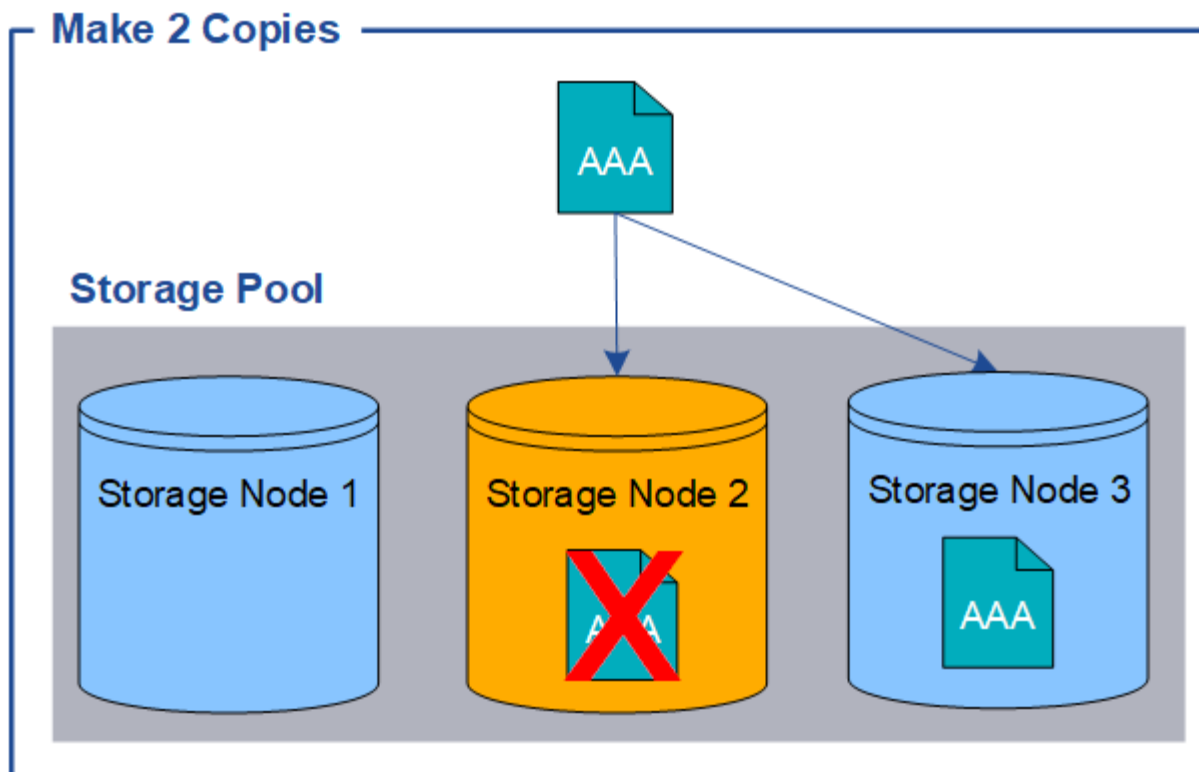


Lorsqu'une règle ILM crée une seule copie répliquée d'un objet, l'objet devient inaccessible lorsque le nœud de stockage n'est pas disponible. Dans cet exemple, vous perdrez temporairement l'accès à l'objet AAA chaque fois que le nœud de stockage 2 est hors ligne, par exemple lors d'une mise à niveau ou d'une autre procédure de maintenance. Vous perdrez entièrement l'objet AAA si le nœud de stockage 2 tombe en panne.

Make 1 Copy



Pour éviter de perdre des données d'objet, vous devez toujours faire au moins deux copies de tous les objets que vous souhaitez protéger par réplication. Si deux copies ou plus existent, vous pouvez toujours accéder à l'objet si un nœud de stockage tombe en panne ou est hors ligne.



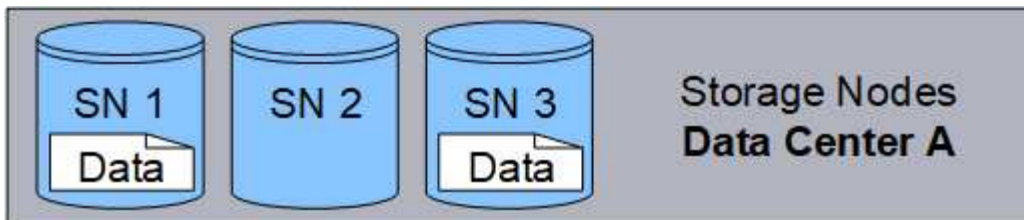
Qu'est-ce que le codage d'effacement ?

Le codage d'effacement est l'une des deux méthodes utilisées par StorageGRID pour stocker les données d'objet (la réplication est l'autre méthode). Lorsque des objets correspondent à une règle ILM qui utilise le codage d'effacement, ces objets sont découpés en fragments de données, des fragments de parité supplémentaires sont calculés et chaque fragment est stocké sur un nœud de stockage différent.

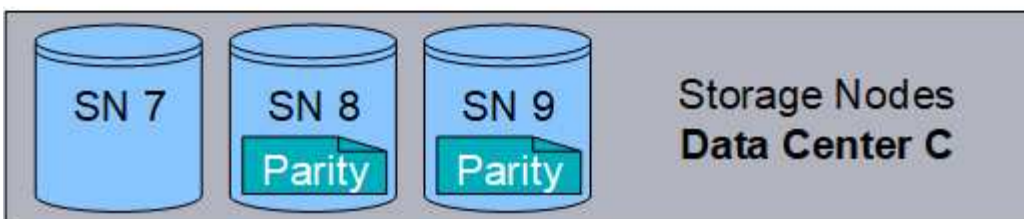
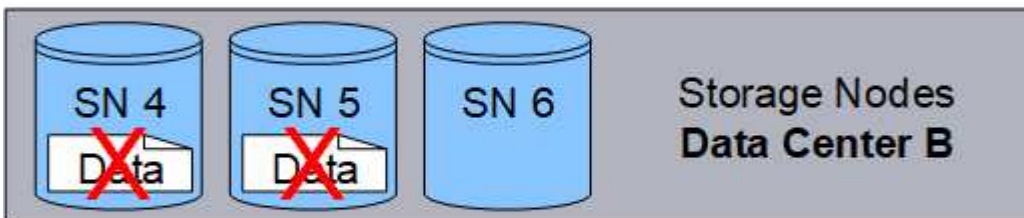
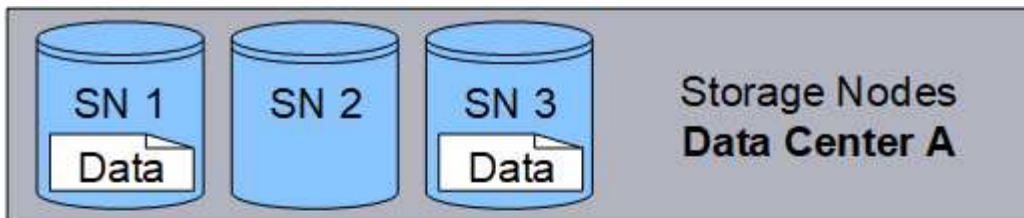
Lorsqu'un objet est accessible, il est réassemblé à l'aide des fragments stockés. Si des données ou un fragment de parité sont corrompus ou perdus, l'algorithme de codage d'effacement peut recréer ce fragment en utilisant un sous-ensemble des données et des fragments de parité restants.

Lorsque vous créez des règles ILM, StorageGRID crée des profils de codage d'effacement qui prennent en charge ces règles. Vous pouvez afficher une liste de profils de codage d'effacement, "[renommer un profil de codage d'effacement](#)", ou "[désactiver un profil de codage d'effacement s'il n'est actuellement utilisé dans aucune règle ILM](#)".

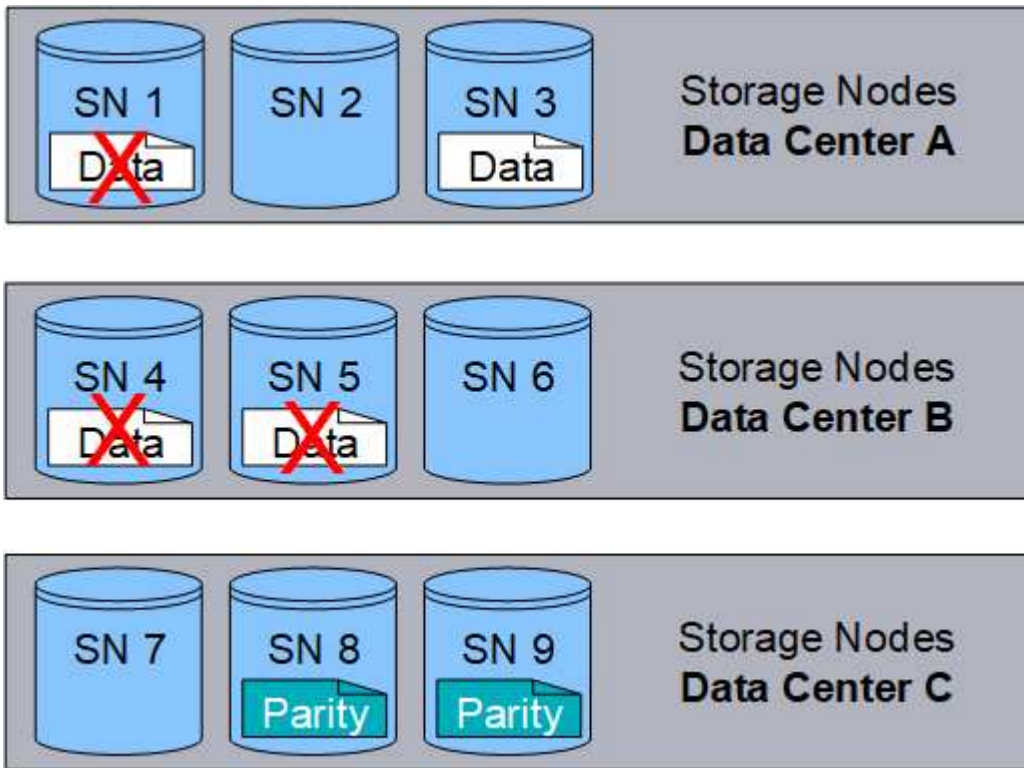
L'exemple suivant illustre l'utilisation d'un algorithme de codage d'effacement sur les données d'un objet. Dans cet exemple, la règle ILM utilise un schéma de codage d'effacement 4+2. Chaque objet est divisé en quatre fragments de données égaux et deux fragments de parité sont calculés à partir des données de l'objet. Chacun des six fragments est stocké sur un nœud différent sur trois sites de centres de données pour assurer la protection des données en cas de panne de nœud ou de perte de site.



Le schéma de codage d'effacement 4+2 peut être configuré de différentes manières. Par exemple, vous pouvez configurer un pool de stockage à site unique contenant 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, à condition que tous les autres fragments restent accessibles.



Si plus de deux nœuds de stockage sont perdus, l'objet n'est pas récupérable.



Informations connexes

- ["Qu'est-ce que la réplication"](#)
- ["Qu'est-ce qu'un pool de stockage"](#)
- ["Que sont les schémas de codage d'effacement"](#)
- ["Renommer un profil de codage d'effacement"](#)
- ["Désactiver un profil de codage d'effacement"](#)

Que sont les schémas de codage 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 créez ou modifiez une règle ILM, vous sélectionnez un schéma de codage d'effacement disponible. StorageGRID crée automatiquement des schémas de codage d'effacement en fonction du nombre de nœuds de stockage et de sites qui composent le pool de stockage que vous prévoyez d'utiliser.

Protection des données

Le système StorageGRID utilise l'algorithme de codage d'effacement Reed-Solomon. L'algorithme découpe un objet en k fragments de données et calcule m fragments de parité.

Le $k + m = n$ des fragments sont répartis sur n Nœuds de stockage pour assurer la protection des données comme suit :

- Pour récupérer ou réparer un objet, k des fragments sont nécessaires.
- Un objet peut supporter jusqu'à m fragments perdus ou corrompus. Plus la valeur de m , plus la tolérance

aux pannes est élevée.

La meilleure protection des données est assurée par le schéma de codage d'effacement avec la tolérance de panne de nœud ou de volume la plus élevée au sein d'un pool de stockage.

Frais de stockage

La surcharge de stockage d'un schéma de codage 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 surcharge de stockage pour calculer la quantité d'espace disque requise par chaque objet à code d'effacement :

$$\text{disk space} = \text{object size} + (\text{object size} * \text{storage overhead})$$

Par exemple, si vous stockez un objet de 10 Mo à l'aide du schéma 4+2 (qui présente une surcharge de stockage de 50 %), l'objet consomme 15 Mo de stockage en grille. Si vous stockez le même objet de 10 Mo en utilisant le schéma 6+2 (qui a une surcharge de stockage de 33 %), l'objet consomme environ 13,3 Mo.

Sélectionnez le schéma de codage d'effacement avec la valeur totale la plus basse de $k+m$ qui répond à vos besoins. Les schémas de codage d'effacement avec un nombre inférieur de fragments sont plus efficaces en termes de calcul car :

- Moins de fragments sont créés et distribués (ou récupérés) par objet
- Ils présentent de meilleures performances car la taille des fragments est plus grande
- Ils peuvent nécessiter l'ajout de moins de nœuds dans un ["extension lorsque davantage de stockage est nécessaire"](#)

Directives pour les pools de stockage

Lors de la sélection du pool de stockage à utiliser pour une règle qui créera une copie à code d'effacement, utilisez les instructions suivantes pour les pools de stockage :

- Le pool de stockage doit inclure trois sites ou plus, ou exactement un site.



Vous ne pouvez pas utiliser le codage d'effacement si le pool de stockage comprend deux sites.

- [Schémas de codage d'effacement pour les pools de stockage contenant trois sites ou plus](#)
- [Schémas de codage d'effacement pour les pools de stockage à site unique](#)

- N'utilisez pas de pool de stockage qui inclut le site Tous les sites.
- Le pool de stockage doit inclure au moins $k+m + 1$ Nœuds de stockage pouvant stocker des données d'objet.



Les nœuds de stockage peuvent être configurés lors de l'installation pour contenir uniquement des métadonnées d'objet et non des données d'objet. Pour plus d'informations, consultez la section ["Types de nœuds de stockage"](#).

Le nombre minimum de nœuds de stockage requis est $k+m$. Cependant, disposer d'au moins un nœud de stockage supplémentaire peut aider à prévenir les échecs d'ingestion ou les retards ILM si un nœud de stockage requis est temporairement indisponible.

Schémas de codage d'effacement pour les pools de stockage contenant trois sites ou plus

Le tableau suivant décrit les schémas de codage d'effacement actuellement pris en charge par StorageGRID pour les pools de stockage qui incluent trois sites ou plus. Tous ces systèmes offrent une protection contre la perte de site. Un site peut être perdu, et l'objet sera toujours accessible.

Pour les schémas de codage d'effacement qui offrent une protection contre la perte de site, le nombre recommandé de nœuds de stockage dans le pool de stockage dépasse $k+m + 1$ car chaque site nécessite un minimum de trois nœuds de stockage.

Schéma de codage d'effacement ($k+m$)	Nombre minimum 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 ?	Frais de 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%
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 nécessite un minimum de trois nœuds de stockage par site. Pour utiliser le schéma 7+5, chaque site nécessite un minimum de quatre nœuds de stockage. Il est recommandé d'utiliser cinq nœuds de stockage par site.

Lors de la sélection d'un système de codage d'effacement qui assure la protection du site, équilibrez l'importance relative des facteurs suivants :

- **Nombre de fragments** : les performances et la flexibilité d'extension sont généralement meilleures lorsque le nombre total de fragments est inférieur.
- **Tolérance aux pannes** : La tolérance aux pannes est augmentée en ayant plus de segments de parité (c'est-à-dire lorsque m a une valeur plus élevée.)
- **Trafic réseau** : Lors de la récupération après une panne, 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 avec une surcharge plus élevée nécessitent plus d'espace de stockage par objet.

Par exemple, lorsque vous choisissez entre un schéma 4+2 et un schéma 6+3 (qui ont tous deux une surcharge de stockage de 50 %), sélectionnez le schéma 6+3 si une tolérance aux pannes supplémentaire est requise. Sélectionnez le schéma 4+2 si les ressources réseau sont limitées. Si tous les autres facteurs sont égaux, sélectionnez 4+2 car il a un nombre total de fragments inférieur.



Si vous n’êtes pas sûr du schéma à utiliser, sélectionnez 4+2 ou 6+3, ou contactez le support technique.

Schémas de codage d’effacement pour les pools de stockage à site unique

Un pool de stockage à site unique 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 minimum de nœuds de stockage requis est $k+m$, mais un pool de stockage avec $k+m + 1$ Les nœuds de stockage sont recommandés. Par exemple, le schéma de codage d’effacement 2+1 nécessite un pool de stockage avec un minimum de trois nœuds de stockage, mais quatre nœuds de stockage sont recommandés.

Schéma de codage d’effacement ($k+m$)	Nombre minimum de nœuds de stockage	Nombre recommandé de nœuds de stockage	Frais de 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 codage d’effacement

Avant de décider d’utiliser la réplication ou le codage d’effacement pour protéger les données d’objet contre la perte, vous devez comprendre les avantages, les inconvénients et les exigences du codage d’effacement.

Avantages du codage d’effacement

Comparé à la réplication, le codage d’effacement offre une fiabilité, une disponibilité et une efficacité de stockage améliorées.

- **Fiabilité** : La fiabilité est mesurée en termes de tolérance aux pannes, c'est-à-dire le nombre de pannes simultanées pouvant être supportées sans perte de données. Avec la réplication, plusieurs copies identiques sont stockées sur différents nœuds et sur plusieurs sites. Avec le codage d'effacement, un objet est codé en fragments de données et de parité et distribué sur de nombreux nœuds et sites. Cette dispersion offre une protection contre les pannes de site et de nœud. Comparé à la réplication, le codage d'effacement offre une fiabilité améliorée à des coûts de stockage comparables.
- **Disponibilité** : La disponibilité peut être définie comme la capacité à récupérer des objets si les nœuds de stockage échouent ou deviennent inaccessibles. Comparé à la réplication, le codage d'effacement offre une disponibilité accrue à des coûts de stockage comparables.
- **Efficacité de stockage** : Pour des niveaux de disponibilité et de fiabilité similaires, les objets protégés par codage d'effacement consomment moins d'espace disque que les mêmes objets s'ils étaient protégés par réplication. Par exemple, un objet de 10 Mo répliqué sur deux sites consomme 20 Mo d'espace disque (deux copies), tandis qu'un objet codé par effacement sur trois sites avec un schéma de codage par effacement 6+3 ne consomme que 15 Mo d'espace disque.



L'espace disque pour les objets à code d'effacement est calculé comme la taille de l'objet plus la surcharge de stockage. Le pourcentage de surcharge de stockage est le nombre de fragments de parité divisé par le nombre de fragments de données.

Inconvénients du codage d'effacement

Comparé à la réplication, le codage d'effacement présente les inconvénients suivants :

- Un nombre accru de nœuds et de sites de stockage est recommandé, en fonction du schéma de codage d'effacement. En revanche, si vous répliquez des données d'objet, vous n'avez besoin que d'un seul nœud de stockage pour chaque copie. Voir "[Schémas de codage d'effacement pour les pools de stockage contenant trois sites ou plus](#)" et "[Schémas de codage d'effacement pour les pools de stockage à site unique](#)".
- Augmentation du coût et de la complexité des extensions de stockage. Pour étendre un déploiement qui utilise la réplication, vous ajoutez de la capacité de stockage à chaque emplacement où des copies d'objets sont effectuées. Pour étendre un déploiement qui utilise le codage d'effacement, vous devez prendre en compte à la fois le schéma de codage d'effacement utilisé et le niveau de remplissage des nœuds de stockage existants. Par exemple, si vous attendez que les nœuds existants soient remplis à 100 %, vous devez ajouter au moins $k+m$ Nœuds de stockage, mais si vous étendez lorsque les nœuds existants sont remplis à 70 %, vous pouvez ajouter deux nœuds par site tout en maximisant la capacité de stockage utilisable. Pour plus d'informations, consultez la section "[Ajouter une capacité de stockage pour les objets à code d'effacement](#)".
- Les temps de latence de récupération augmentent lorsque vous utilisez le codage d'effacement sur des sites géographiquement répartis. Les fragments d'objet d'un objet codé par effacement et distribué sur des sites distants prennent plus de temps à récupérer via des connexions WAN qu'un objet répliqué et disponible localement (le même site auquel le client se connecte).
- Lorsque vous utilisez le codage d'effacement sur des sites géographiquement répartis, l'utilisation du trafic réseau WAN est plus élevée pour les récupérations et les réparations, en particulier pour les objets fréquemment récupérés ou pour les réparations d'objets via des connexions réseau WAN.
- Lorsque vous utilisez le codage d'effacement sur plusieurs sites, le débit maximal des objets diminue fortement à mesure que la latence du réseau entre les sites augmente. Cette diminution est due à la diminution correspondante du débit du réseau TCP, qui affecte la rapidité avec laquelle le système StorageGRID peut stocker et récupérer des fragments d'objet.
- Utilisation accrue des ressources de calcul.

Quand utiliser le codage d'effacement

Le codage d'effacement est le mieux adapté aux exigences suivantes :

- Objets d'une taille supérieure à 1 Mo.



Le codage d'effacement est particulièrement adapté aux objets supérieurs à 1 Mo. N'utilisez pas le codage d'effacement pour les objets inférieurs à 200 Ko afin d'éviter la surcharge liée à la gestion de très petits fragments codés par effacement.

- Stockage à long terme ou à froid pour le contenu rarement récupéré.
- Haute disponibilité et fiabilité des données.
- Protection contre les pannes complètes du site et des nœuds.
- Efficacité du stockage.
- Déploiements sur un seul site nécessitant une protection efficace des données avec une seule copie à code d'effacement plutôt que plusieurs copies répliquées.
- Déploiements multisites où la latence inter-sites est inférieure à 100 ms.

Comment la rétention d'objet est déterminée

StorageGRID fournit des options permettant aux administrateurs de grille et aux utilisateurs locataires individuels de spécifier la durée de stockage des objets. En général, toutes les instructions de conservation fournies par un utilisateur locataire ont priorité sur les instructions de conservation fournies par l'administrateur de la grille.

Comment les utilisateurs locataires contrôlent la rétention des objets

Les utilisateurs locataires peuvent utiliser ces méthodes pour contrôler la durée de stockage de leurs objets dans StorageGRID:

- Si le paramètre global de verrouillage d'objet S3 est activé pour la grille, les utilisateurs du locataire S3 peuvent créer des compartiments avec le verrouillage d'objet S3 activé, puis sélectionner une **Période de conservation par défaut** pour chaque compartiment.
- Si le paramètre global de verrouillage d'objet S3 est activé pour la grille, les utilisateurs du locataire S3 peuvent créer des compartiments avec le verrouillage d'objet S3 activé, puis utiliser l'API REST S3 pour spécifier les paramètres de conservation jusqu'à la date et de conservation légale pour chaque version d'objet ajoutée à ce compartiment.
 - Une version d'objet soumise à une suspension légale ne peut être supprimée par aucune méthode.
 - Avant que la date de conservation d'une version d'objet ne soit atteinte, cette version ne peut être supprimée par aucune méthode.
 - Les objets dans les buckets avec le verrouillage d'objet S3 activé sont conservés par ILM « pour toujours ». Cependant, une fois sa date de conservation atteinte, une version d'objet peut être supprimée par une demande client ou par l'expiration du cycle de vie du bucket. Voir "[Gérer les objets avec S3 Object Lock](#)".
- Les utilisateurs locataires S3 peuvent ajouter une configuration de cycle de vie à leurs compartiments qui spécifie une action d'expiration. Si un cycle de vie de compartiment existe, StorageGRID stocke un objet jusqu'à ce que la date ou le nombre de jours spécifiés dans l'action Expiration soient atteints, sauf si le client supprime d'abord l'objet. Voir "[Créer une configuration du cycle de vie S3](#)".

- Un client S3 peut émettre une demande de suppression d'objet. StorageGRID donne toujours la priorité aux demandes de suppression des clients par rapport au cycle de vie du compartiment S3 ou à ILM pour déterminer s'il faut supprimer ou conserver un objet.

Comment les administrateurs de réseau contrôlent la conservation des objets

Les administrateurs de grille peuvent utiliser ces méthodes pour contrôler la conservation des objets :

- Définissez une période de conservation maximale du verrouillage d'objet S3 pour chaque locataire. Ensuite, les utilisateurs locataires peuvent définir une période de conservation par défaut pour chacun de leurs compartiments. La période de conservation maximale est également appliquée à tous les objets nouvellement ingérés pour ce bucket (date de conservation de l'objet).
- Créez des instructions de placement ILM pour contrôler la durée de stockage des objets. Lorsque des objets correspondent à une règle ILM, StorageGRID stocke ces objets jusqu'à ce que la dernière période de la règle ILM soit écoulée. Les objets sont conservés indéfiniment si « pour toujours » est spécifié pour les instructions de placement.
- Quelle que soit la personne qui contrôle la durée de conservation des objets, les paramètres ILM contrôlent les types de copies d'objets (répliquées ou codées par effacement) qui sont stockées et où se trouvent les copies (nœuds de stockage ou pools de stockage cloud).

Comment le cycle de vie du bucket S3 et l'ILM interagissent

Lorsqu'un cycle de vie de compartiment S3 est configuré, les actions d'expiration du cycle de vie remplacent la stratégie ILM pour les objets qui correspondent au filtre de cycle de vie. Par conséquent, un objet peut être conservé sur la grille même après l'expiration des instructions ILM de placement de l'objet.

Exemples de rétention d'objets

Pour mieux comprendre les interactions entre S3 Object Lock, les paramètres du cycle de vie du bucket, les demandes de suppression du client et ILM, considérez les exemples suivants.

Exemple 1 : le cycle de vie du bucket S3 conserve les objets plus longtemps que celui d'ILM

ILM

Conservez deux copies pendant 1 an (365 jours)

Cycle de vie du bucket

Expirer les objets dans 2 ans (730 jours)

Résultat

StorageGRID stocke l'objet pendant 730 jours. StorageGRID utilise les paramètres du cycle de vie du bucket pour déterminer s'il faut supprimer ou conserver un objet.



Si le cycle de vie du bucket spécifie que les objets doivent être conservés plus longtemps que spécifié par ILM, StorageGRID continue d'utiliser les instructions de placement ILM lors de la détermination du nombre et du type de copies à stocker. Dans cet exemple, deux copies de l'objet continueront d'être stockées dans StorageGRID du jour 366 au jour 730.

Exemple 2 : le cycle de vie du compartiment S3 expire les objets avant ILM

ILM

Conservez deux copies pendant 2 ans (730 jours)

Cycle de vie du bucket

Expirer les objets dans 1 an (365 jours)

Résultat

StorageGRID supprime les deux copies de l'objet après le jour 365.

Exemple 3 : la suppression du client remplace le cycle de vie du bucket et l'ILM

ILM

Stocker deux copies sur des nœuds de stockage « pour toujours »

Cycle de vie du bucket

Expirer les objets dans 2 ans (730 jours)

Demande de suppression du client

Publié le jour 400

Résultat

StorageGRID supprime les deux copies de l'objet le jour 400 en réponse à la demande de suppression du client.

Exemple 4 : Le verrouillage d'objet S3 remplace la demande de suppression du client

Verrouillage d'objet S3

La date de conservation pour une version d'objet est le 31/03/2026. Aucune mesure de conservation légale n'est en vigueur.

Règle ILM conforme

Stocker deux copies sur des nœuds de stockage « pour toujours »

Demande de suppression du client

Publié le 31/03/2024

Résultat

StorageGRID ne supprimera pas la version de l'objet car la date de conservation est encore dans 2 ans.

Comment les objets sont supprimés

StorageGRID peut supprimer des objets soit en réponse directe à une demande client, soit automatiquement suite à l'expiration du cycle de vie d'un bucket S3 ou aux exigences de la politique ILM. Comprendre les différentes manières dont les objets peuvent être supprimés et la manière dont StorageGRID gère les demandes de suppression peut vous aider à gérer les objets plus efficacement.

StorageGRID peut utiliser l'une des deux méthodes pour supprimer des objets :

- **Suppression synchrone** : lorsque StorageGRID reçoit une demande de suppression client, toutes les copies d'objet sont supprimées immédiatement. Le client est informé que la suppression a réussi après que les copies ont été supprimées.
- **Les objets sont mis en file d'attente pour suppression** : lorsque StorageGRID reçoit une demande de suppression, l'objet est mis en file d'attente pour suppression et le client est immédiatement informé que la

suppression a réussi. Les copies d'objets 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, minimise les retards de suppression potentiels et libère de l'espace le plus rapidement possible.

Le tableau résume quand StorageGRID utilise chaque méthode.

Méthode de suppression	Lorsqu'il est utilisé
Les objets sont mis en file d'attente pour suppression	Lorsque l'une des conditions suivantes est vraie : • La suppression automatique de l'objet a été déclenchée par l'un des événements suivants : ◦ La date d'expiration ou le nombre de jours dans la configuration du cycle de vie d'un bucket S3 est atteint. ◦ La dernière période spécifiée dans une règle ILM est écoulée. Remarque : les objets d'un compartiment pour lequel le verrouillage d'objet S3 est activé ne peuvent pas être supprimés s'ils sont soumis à une conservation légale ou si une date de conservation a été spécifiée mais n'a pas encore été respectée. • Un client S3 demande la suppression et une ou plusieurs de ces conditions sont vraies : ◦ Les copies ne peuvent pas être supprimées dans les 30 secondes car, par exemple, l'emplacement d'un objet est temporairement indisponible. ◦ Les files d'attente de suppression en arrière-plan sont inactives.
Les objets sont supprimés immédiatement (suppression synchrone)	Lorsqu'un client S3 effectue une demande de suppression et que toutes les conditions suivantes sont remplies : • Toutes les copies peuvent être supprimées dans les 30 secondes. • Les files d'attente de suppression en arrière-plan contiennent des objets à traiter.

Lorsque les clients S3 effectuent des demandes de suppression, StorageGRID commence par ajouter des objets à la file d'attente de suppression. Il passe ensuite à l'exécution de la suppression synchrone. S'assurer que la file d'attente de suppression en arrière-plan contient des objets à traiter permet à StorageGRID de traiter les suppressions plus efficacement, en particulier pour les clients à faible concurrence, tout en contribuant à éviter les retards de suppression des clients.

Temps nécessaire pour supprimer les objets

La façon dont StorageGRID supprime les objets peut affecter la façon dont le système semble fonctionner :

- Lorsque StorageGRID effectue une suppression synchrone, StorageGRID peut mettre jusqu'à 30 secondes pour renvoyer un résultat au client. Cela signifie que la suppression peut sembler se produire plus lentement, même si les copies sont en réalité supprimées plus rapidement que lorsque StorageGRID met les objets en file d'attente pour suppression.
- Si vous surveillez de près les performances de suppression lors d'une suppression en masse, vous

remarquerez peut-être que le taux de suppression semble lent après la suppression d'un certain nombre d'objets. Ce changement se produit lorsque StorageGRID passe de la mise en file d'attente des objets à supprimer à l'exécution d'une suppression synchrone. La réduction apparente du taux de suppression ne signifie pas que les copies d'objets sont supprimées plus lentement. Au contraire, cela indique qu'en moyenne, l'espace se libère désormais plus rapidement.

Si vous supprimez un grand nombre d'objets et que votre priorité est de libérer de l'espace rapidement, envisagez d'utiliser une demande client pour supprimer les objets plutôt que de les supprimer à l'aide d'ILM ou d'autres méthodes. En général, l'espace est libéré plus rapidement lorsque la suppression est effectuée 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 sont mises en file d'attente pour être supprimées ultérieurement (pour les demandes de suppression du 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'objets sont mises en file d'attente pour suppression (pour les suppressions client et d'autres méthodes).

Comment les objets versionnés S3 sont supprimés

Lorsque le contrôle de version est activé pour un compartiment S3, StorageGRID suit le comportement d'Amazon S3 lors de la réponse aux demandes de suppression, que ces demandes proviennent d'un client S3, de l'expiration d'un cycle de vie de compartiment S3 ou des exigences de la politique ILM.

Lorsque les objets sont versionnés, les demandes de suppression d'objet ne suppriment pas la version actuelle de l'objet et ne libèrent pas d'espace. Au lieu de cela, une demande de suppression d'objet crée un marqueur de suppression de zéro octet comme version actuelle de l'objet, ce qui rend la version précédente de l'objet « non actuelle ». Un marqueur de suppression d'objet devient un marqueur de suppression d'objet expiré lorsqu'il s'agit de la version actuelle et qu'il n'existe aucune version non actuelle.

Même si l'objet n'a pas été supprimé, StorageGRID se comporte comme si la version actuelle de l'objet n'était plus disponible. Les requêtes adressées à cet objet renvoient 404 Not Found. Cependant, étant donné que les données d'objet non actuelles n'ont pas été supprimées, les demandes spécifiant une version non actuelle de l'objet peuvent réussir.

Pour libérer de l'espace lors de la suppression d'objets versionnés ou pour supprimer les marqueurs de suppression, utilisez l'une des opérations suivantes :

- **Demande client S3** : Spécifiez l'ID de version de l'objet dans la demande d'objet S3 DELETE(`DELETE /object?versionId=ID`). Gardez à l'esprit que cette demande supprime uniquement les copies d'objets pour la version spécifiée (les autres versions occupent toujours de l'espace).
- **Cycle de vie du bucket** : utilisez le `NoncurrentVersionExpiration` action dans la configuration du cycle de vie du bucket. Lorsque le nombre de `NoncurrentDays` spécifié est atteint, StorageGRID supprime définitivement toutes les copies des versions d'objet non actuelles. Ces versions d'objet ne peuvent pas être récupérées.

Le `NewerNoncurrentVersions` L'action dans la configuration du cycle de vie du bucket spécifie le nombre de versions non actuelles conservées dans un bucket S3 versionné. S'il y a plus de versions non actuelles que `NewerNoncurrentVersions` spécifie que StorageGRID supprime les anciennes versions lorsque la valeur `NoncurrentDays` est 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 `NewerNoncurrentVersions` le seuil est conservé si ILM demande sa suppression.

Pour supprimer les marqueurs de suppression d'objets expirés, utilisez le `Expiration` action avec l'une des balises suivantes : `ExpiredObjectDeleteMarker` , `Days` , ou `Date` .

- **ILM:** "[Cloner une politique active](#)" et ajoutez deux règles ILM à la nouvelle politique :
 - Première règle : utilisez « Heure non actuelle » comme heure de référence pour faire correspondre les versions non actuelles de l'objet. Dans "[Étape 1 \(Saisir les détails\) de l'assistant Créer une règle ILM](#)" , sélectionnez **Oui** pour la question « Appliquer cette règle uniquement aux anciennes versions d'objet (dans les compartiments S3 avec le contrôle de version activé) ? »
 - Deuxième règle : utilisez **Heure d'ingestion** pour correspondre à la version actuelle. La règle « Heure non actuelle » doit apparaître dans la politique au-dessus de la règle **Heure d'ingestion**.

Pour supprimer les marqueurs de suppression d'objet expirés, utilisez une règle **Heure d'ingestion** pour faire correspondre les marqueurs de suppression actuels. Les marqueurs de suppression ne sont supprimés que lorsqu'une **période de jours** s'est écoulée et que le marqueur de suppression actuel a expiré (il n'existe aucune version non actuelle).

- **Supprimer les objets dans le bucket** : utilisez le gestionnaire de locataires pour "[supprimer toutes les versions d'objet](#)" , y compris les marqueurs de suppression, à partir d'un bucket.

Lorsqu'un objet versionné est supprimé, StorageGRID crée un marqueur de suppression de zéro octet comme version actuelle de l'objet. Tous les objets et marqueurs de suppression doivent être supprimés avant qu'un bucket versionné puisse être supprimé.

- Les marqueurs de suppression créés dans StorageGRID 11.7 ou une version antérieure ne peuvent être supprimés que via des demandes client S3. Ils ne sont pas supprimés par ILM, les règles de cycle de vie du bucket ou les objets de suppression dans les opérations de bucket.
- Les marqueurs de suppression d'un bucket créé dans StorageGRID 11.8 ou version ultérieure peuvent être supprimés par ILM, les règles de cycle de vie du bucket, les objets de suppression dans les opérations de bucket ou une suppression explicite du client S3.

Informations connexes

- "[Utiliser l'API REST S3](#)"
- "[Exemple 4 : Règles et politique ILM pour les objets versionnés S3](#)"

Créer et attribuer des niveaux de stockage

Les niveaux de stockage identifient le type de stockage utilisé par un nœud de stockage. Vous pouvez créer des niveaux 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](#)" .
- Tu as "[autorisations d'accès spécifiques](#)" .

À propos de cette 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 éventuellement 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 contiennent uniquement un type spécifique de nœud de stockage. Par exemple, vous souhaitez peut-être

que certains objets soient stockés sur vos nœuds de stockage les plus rapides, tels que les appliances de stockage entièrement flash StorageGRID .



Les nœuds de stockage peuvent être configurés lors de l'installation pour contenir uniquement des métadonnées d'objet et non des données d'objet. Les nœuds de stockage contenant uniquement des métadonnées ne peuvent pas se voir attribuer un niveau de stockage. Pour plus d'informations, consultez la section "[Types de nœuds de stockage](#)".

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 "[créer des pools de stockage](#)". L'utilisation de cette sélection garantit que le pool de stockage inclura chaque nœud de stockage du site, quelle que soit sa qualité 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. Au lieu de cela, attribuez chaque niveau de stockage à deux nœuds ou plus. Les niveaux de stockage attribués à un seul nœud peuvent entraîner des retards ILM si ce nœud devient indisponible.

Étapes

1. Sélectionnez **ILM > Niveaux de stockage**.
2. Définir des niveaux de stockage personnalisés :
 - a. Pour chaque niveau de stockage personnalisé que vous souhaitez ajouter, sélectionnez *Insérer*  pour ajouter une ligne.
 - b. Saisissez une étiquette descriptive.



Storage Grades

Updated: 2017-05-26 11:22:39 MDT

Storage Grade Definitions

Storage Grade	Label	Actions
0	Default	
1	disk	

Storage Grades

LDR	Storage Grade	Actions
Data Center 1/DC1-S1/LDR	Default	
Data Center 1/DC1-S2/LDR	Default	
Data Center 1/DC1-S3/LDR	Default	
Data Center 2/DC2-S1/LDR	Default	
Data Center 2/DC2-S2/LDR	Default	
Data Center 2/DC2-S3/LDR	Default	
Data Center 3/DC3-S1/LDR	Default	
Data Center 3/DC3-S2/LDR	Default	
Data Center 3/DC3-S3/LDR	Default	

Apply Changes

c. Sélectionnez **Appliquer les modifications**.

d. En option, si vous devez modifier une étiquette enregistrée, sélectionnez **Modifier*** et sélectionnez ***Appliquer les modifications**.



Vous ne pouvez pas supprimer les niveaux de stockage.

3. Attribuer de nouvelles catégories de stockage aux nœuds de stockage :

a. Localisez le nœud de stockage dans la liste LDR et sélectionnez son icône ***Modifier*** .

b. Sélectionnez le niveau de stockage approprié dans la liste.



LDR	Storage Grade	Actions
Data Center 1/DC1-S1/LDR	Default	
Data Center 1/DC1-S2/LDR	Default disk	
Data Center 1/DC1-S3/LDR	Default	
Data Center 2/DC2-S1/LDR	Default	
Data Center 2/DC2-S2/LDR	Default	
Data Center 2/DC2-S3/LDR	Default	
Data Center 3/DC3-S1/LDR	Default	
Data Center 3/DC3-S2/LDR	Default	
Data Center 3/DC3-S3/LDR	Default	

Apply Changes



Affectez une catégorie de stockage à un nœud de stockage donné une seule fois. Un nœud de stockage récupéré après une panne conserve le niveau de stockage précédemment attribué. Ne modifiez pas cette affectation une fois la stratégie ILM activée. Si l'affectation est modifiée, les données sont stockées en fonction du 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 regroupement logique de nœuds de stockage.

Lorsque vous installez StorageGRID, un pool de stockage par site est automatiquement créé. Vous pouvez configurer des pools de stockage supplémentaires selon vos besoins de stockage.



Les nœuds de stockage peuvent être configurés lors de l'installation pour contenir des données d'objet et des métadonnées d'objet, ou uniquement des métadonnées d'objet. Les nœuds de stockage contenant uniquement des métadonnées ne peuvent pas être utilisés dans les pools de stockage. Pour plus d'informations, consultez la section "[Types de nœuds de stockage](#)".

Les pools de stockage ont deux attributs :

- **Qualité de stockage** : pour les nœuds de stockage, les performances relatives du stockage de sauvegarde.
- **Site** : Le centre de données où les objets seront stockés.

Les pools de stockage sont utilisés dans les règles ILM pour déterminer où les données d'objet sont stockées et le type de stockage utilisé. Lorsque vous configurez des règles ILM pour la réplication, vous sélectionnez un ou plusieurs pools de stockage.

Directives pour la création de pools de stockage

Configurez et utilisez des pools de stockage pour vous protéger contre la perte de données en distribuant les données sur plusieurs sites. Les copies répliquées et les copies à code d'effacement nécessitent des configurations de pool de stockage différentes.

Voir ["Exemples d'activation de la protection contre la perte de site à l'aide de la réplication et du codage d'effacement"](#) .

Directives pour tous les pools de stockage

- Gardez les configurations de pool de stockage aussi simples que possible. 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 avec un nombre insuffisant de nœuds peut entraîner des retards ILM si un nœud devient indisponible.
- Évitez de créer ou d'utiliser des pools de stockage qui se chevauchent (contenant un ou plusieurs nœuds identiques). Si les pools de stockage se chevauchent, plusieurs copies des données d'objet peuvent être enregistrées sur le même nœud.
- En général, n'utilisez pas le pool de stockage Tous les nœuds de stockage (StorageGRID 11.6 et versions antérieures) ou le site Tous les sites. Ces éléments sont automatiquement mis à jour pour inclure tous les nouveaux sites que vous ajoutez dans une extension, ce qui peut ne pas correspondre au comportement souhaité.

Directives pour les pools de stockage utilisés pour les copies répliquées

- Pour la protection contre la perte de site à l'aide ["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 garantit que les copies d'objets répliquées sont placées exactement là où vous l'attendez (par exemple, une copie de chaque objet sur chaque site pour la protection contre la perte de site).

- Si vous ajoutez un site dans une extension, créez un nouveau pool de stockage contenant uniquement le nouveau site. Alors, ["mettre à jour les règles ILM"](#) pour contrôler quels objets sont 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 du disque 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.

Directives relatives aux pools de stockage utilisés pour les copies à code d'effacement

- Pour la protection contre la perte de site à l'aide ["codage d'effacement"](#) , créez des pools de stockage composés d'au moins trois sites. Si un pool de stockage comprend uniquement deux sites, vous ne pouvez pas utiliser ce pool de stockage pour le codage d'effacement. Aucun schéma de codage d'effacement n'est disponible pour un pool de stockage comportant deux sites.

- Le nombre de nœuds de stockage et de sites contenus dans le pool de stockage détermine lequel "[schémas de codage 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 codage d'effacement que vous sélectionnez. Par exemple, si vous utilisez un schéma de codage d'effacement 6+3, vous devez disposer d'au moins neuf nœuds de stockage. Cependant, il est recommandé de disposer d'au moins un nœud de stockage supplémentaire par site.
- Répartissez les nœuds de stockage sur les sites aussi uniformément que possible. Par exemple, pour prendre en charge un schéma de codage d'effacement 6+3, configurez un pool de stockage qui comprend au moins trois nœuds de stockage sur trois sites.
- Si vous avez des exigences de débit élevées, l'utilisation d'un pool de stockage comprenant plusieurs sites n'est pas recommandée si la latence du réseau entre les sites est supérieure à 100 ms. À mesure que la latence augmente, la vitesse à laquelle StorageGRID peut créer, placer et récupérer des fragments d'objet diminue fortement en raison de la diminution du débit du réseau TCP.

La diminution du débit affecte les taux maximum réalisables d'ingestion et de récupération d'objets (lorsque Équilibré ou Strict sont sélectionnés comme comportement d'ingestion) ou peut entraîner des retards dans la file d'attente ILM (lorsque la double validation est sélectionnée comme comportement d'ingestion). Voir "[Comportement d'ingestion de règle ILM](#)".



Si votre grille n'inclut qu'un seul site, vous ne pouvez pas utiliser le pool de stockage Tous les nœuds de stockage (StorageGRID 11.6 et versions antérieures) ou le site Tous les sites dans un profil de codage d'effacement. Ce comportement empêche le profil de devenir invalide si un deuxième site est ajouté.

Activer la protection contre la perte de site

Si votre déploiement StorageGRID inclut plusieurs sites, vous pouvez utiliser la réplication et le codage d'effacement avec des pools de stockage correctement configurés pour activer la protection contre la perte de site.

La réplication et le codage d'effacement nécessitent des configurations de pool de stockage différentes :

- Pour utiliser la réplication pour la protection contre la perte de site, utilisez les pools de stockage spécifiques au site qui sont automatiquement créés lors de l'installation de StorageGRID . Créez ensuite des règles ILM avec "[instructions de placement](#)" qui spécifient plusieurs pools de stockage afin qu'une copie de chaque objet soit placée sur chaque site.
- Pour utiliser le codage d'effacement pour la protection contre la perte de site, "[créer des pools de stockage composés de plusieurs sites](#)". Créez ensuite des règles ILM qui utilisent un pool de stockage composé de plusieurs sites et tout schéma de codage d'effacement disponible.



Lors de la configuration de votre déploiement StorageGRID pour la protection contre la perte de site, vous devez également prendre en compte les effets de "[options d'ingestion](#)" et "[cohérence](#)".

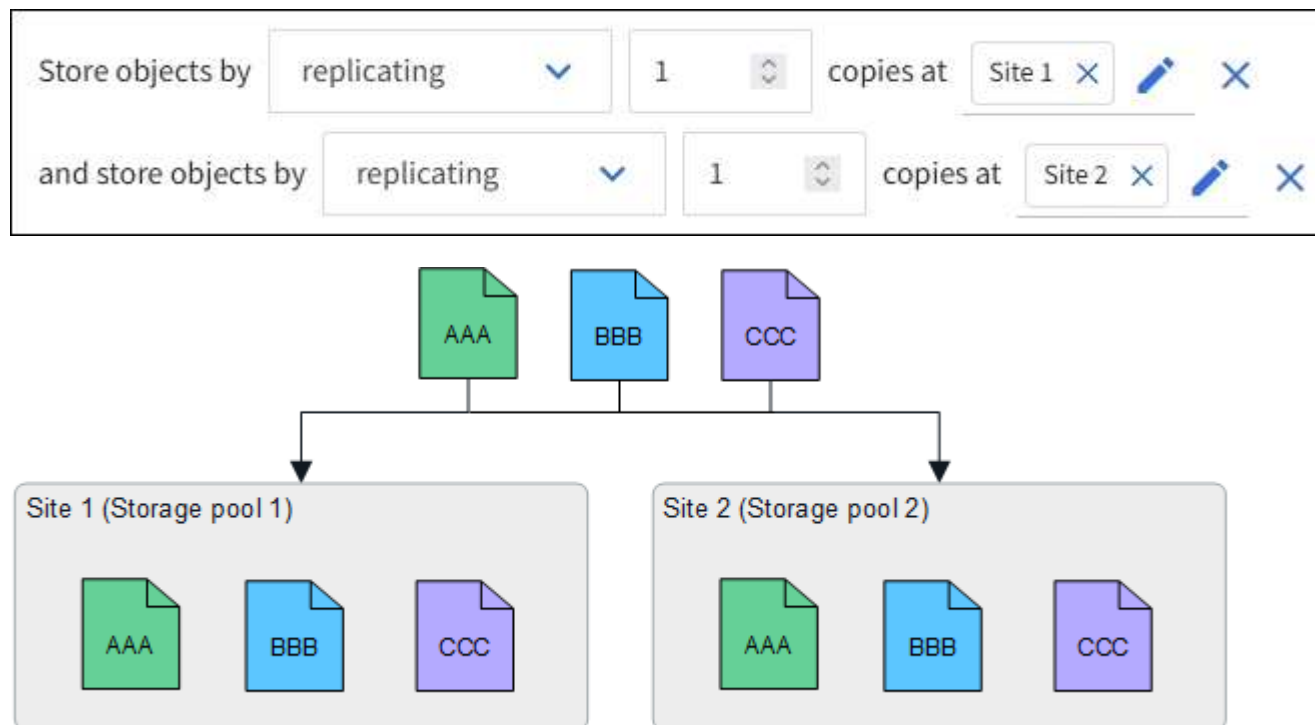
Exemple de réplication

Par défaut, un pool de stockage est créé pour chaque site lors de l'installation de StorageGRID . Le fait de disposer de pools de stockage constitués d'un seul site vous permet de 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 placements :
 - Stocker les objets en répliquant 1 copie sur le site 1
 - Stocker les objets en répliquant 1 copie sur le site 2

Placements des règles ILM :



Si un site est perdu, des copies des objets sont disponibles sur l'autre site.

Exemple de codage d'effacement

Disposer de pools de stockage composés de plusieurs sites par pool de stockage vous permet de configurer des règles ILM qui utilisent le codage 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 placement : stocker les objets par codage d'effacement à l'aide d'un schéma EC 4+2 dans le pool de stockage 1, qui contient trois sites

Placements des règles ILM :



Dans cet exemple :

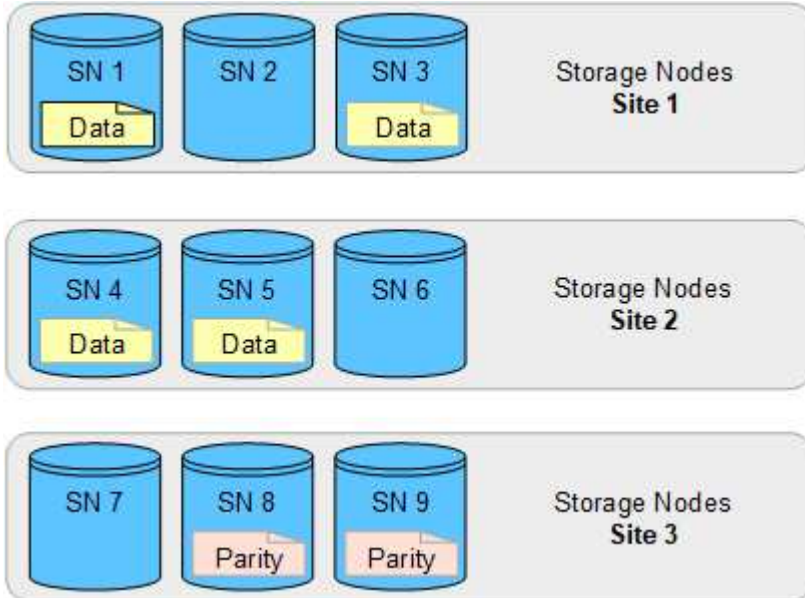
- La règle ILM utilise un schéma de codage d'effacement 4+2.
- Chaque objet est divisé en quatre fragments de données égaux et deux fragments de parité sont calculés à partir des données de l'objet.

- Chacun des six fragments est stocké sur un nœud différent sur trois sites de centres de données pour assurer la protection des données en cas de panne de nœud ou de perte de site.

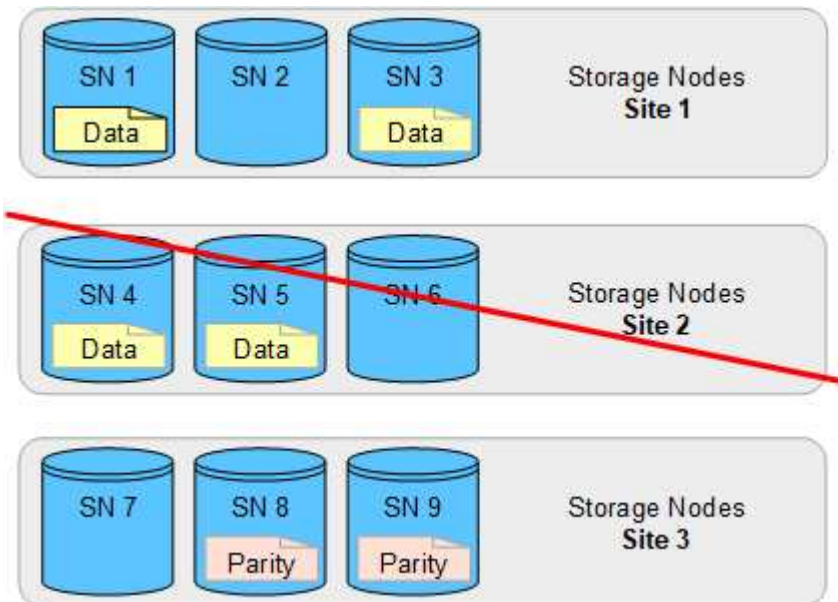


Le codage d'effacement est autorisé dans les pools de stockage contenant n'importe quel nombre de sites à l'exception de deux sites.

Règle ILM utilisant le schéma de codage d'effacement 4+2 :



Si un site est perdu, les données peuvent toujours être récupérées :



Créer un pool de stockage

Vous créez des pools de stockage pour 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 un ou plusieurs niveaux de stockage.



Lorsque vous installez StorageGRID 11.9 sur une nouvelle grille, des pools de stockage sont automatiquement créés pour chaque site. Cependant, si vous avez initialement installé StorageGRID 11.6 ou une version antérieure, les pools de stockage ne sont pas automatiquement créés pour chaque site.

Si vous souhaitez créer des pools de stockage cloud pour stocker des données d'objets en dehors de votre système StorageGRID, consultez le ["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"](#).
- Tu as ["autorisations d'accès spécifiques"](#).
- Vous avez examiné les instructions de création de pools de stockage.

À propos de cette tâche

Les pools de stockage déterminent où les données des objets sont stockées. Le nombre de pools de stockage dont vous avez besoin dépend du nombre de sites de votre grille et des types de copies que vous souhaitez : répliquées ou codées par effacement.

- Pour la réplication et le codage d'effacement sur un seul site, créez un pool de stockage pour chaque site. Par exemple, si vous souhaitez stocker des 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 qui inclut une entrée pour chaque site. Par exemple, si vous souhaitez effacer des objets de code sur trois sites, créez un pool de stockage.



N'incluez pas le site Tous les sites dans un pool de stockage qui sera utilisé dans un profil de codage d'effacement. Ajoutez plutôt une entrée distincte au pool de stockage pour chaque site qui stockera les données codées par effacement. Voir [cette étape](#) pour un exemple.

- Si vous disposez de plusieurs niveaux de stockage, ne créez pas de pool de stockage incluant différents niveaux de stockage sur un seul site. Voir le ["Directives pour la création de pools de stockage"](#).

Étapes

1. Sélectionnez **ILM > Pools de stockage**.

L'onglet Pools de stockage 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 de stockage est automatiquement mis à jour chaque fois que vous ajoutez de nouveaux sites de centre de données. N'utilisez pas ce pool dans les règles ILM.

2. Pour créer un nouveau pool de stockage, sélectionnez **Créer**.
3. Saisissez un nom unique pour le pool de stockage. Utilisez un nom qui sera facile à identifier lorsque vous configurerez des profils de codage d'effacement et des 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 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 qui utilisent un pool de stockage Tous les sites placent les objets sur n'importe quel site disponible, vous donnant ainsi moins de contrôle sur le placement des objets. De plus, un pool de stockage Tous les sites utilise immédiatement les nœuds de stockage d'un nouveau site, ce qui n'est peut-être pas le comportement auquel vous vous attendez.

5. Dans la liste déroulante **Qualité de stockage**, sélectionnez le type de stockage qui sera utilisé si une règle ILM utilise ce pool de stockage.

Le niveau de stockage, *inclut tous les niveaux de stockage*, inclut tous les nœuds de stockage sur le site sélectionné. Si vous avez créé des niveaux de stockage supplémentaires pour les nœuds de stockage de votre grille, ils sont répertoriés dans la liste déroulante.

6. Si vous souhaitez utiliser le pool de stockage dans un profil de codage d'effacement multisite, sélectionnez **Ajouter plus de nœuds** pour ajouter une entrée pour chaque site au pool de stockage.



Vous êtes averti si vous ajoutez plusieurs entrées avec des niveaux de stockage différents pour un site.

Pour supprimer une entrée, sélectionnez l'icône Supprimer .

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"](#).
- Tu as ["autorisations d'accès spécifiques"](#).

Étapes

1. Sélectionnez **ILM > Pools de stockage**.

Le tableau des pools de stockage inclut les informations suivantes pour chaque pool de stockage qui inclut des nœuds de stockage :

- **Nom** : le nom d'affichage unique du pool de stockage.
- **Nombre de nœuds** : le nombre de nœuds dans le pool de stockage.
- **Utilisation du stockage** : le pourcentage de l'espace utilisable total qui a été utilisé pour les données d'objet sur ce nœud. Cette valeur n'inclut pas les métadonnées de l'objet.
- **Capacité totale** : la 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 utilisé dans une ou plusieurs règles ILM, profils de codage d'effacement ou les deux.

2. Pour afficher les détails d'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 inclus dans le pool de stockage.

Le tableau comprend 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 qui a été utilisé pour le nœud de stockage.



La même valeur d'utilisation du stockage (%) est également affichée dans le graphique Stockage utilisé - Données d'objet pour chaque nœud de stockage (sélectionnez **NODES > Storage Node > Storage**).

4. Consultez l'onglet **Utilisation ILM** pour déterminer si le pool de stockage est actuellement utilisé dans des règles ILM ou des profils de codage d'effacement.
5. Vous pouvez également accéder à la page **Règles ILM** pour en savoir plus sur les règles qui utilisent le pool de stockage et les gérer.

Voir le ["instructions pour travailler avec les règles ILM"](#) .

Modifier le pool de stockage

Vous pouvez modifier un pool de stockage pour changer son nom ou pour mettre à jour les sites et les niveaux de stockage.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un ["navigateur Web pris en charge"](#) .
- Tu as ["autorisations d'accès spécifiques"](#) .
- Vous avez examiné le ["directives pour la création de pools de stockage"](#) .
- Si vous prévoyez de modifier un pool de stockage utilisé par une règle dans la stratégie ILM active, vous avez réfléchi à la manière dont vos modifications affecteront le placement des données d'objet.

À propos de cette tâche

Si vous ajoutez un nouveau site ou un nouveau niveau de stockage à un pool de stockage utilisé dans la stratégie ILM active, sachez que les nœuds de stockage du nouveau site ou du nouveau niveau de stockage ne seront pas utilisés automatiquement. Pour forcer StorageGRID à utiliser un nouveau site ou un nouveau niveau de stockage, vous devez activer une nouvelle stratégie ILM après avoir enregistré le pool de stockage modifié.

Étapes

1. Sélectionnez **ILM > Pools de stockage**.
2. Cochez la case correspondant au pool de stockage que vous souhaitez modifier.

Vous ne pouvez pas modifier le pool de stockage Tous les nœuds de stockage (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 codage d'effacement et que la modification rendrait le schéma de codage d'effacement invalide. Par exemple, si un pool de stockage utilisé dans un profil de codage d'effacement inclut actuellement un niveau de stockage avec un seul site, vous ne pouvez pas utiliser un niveau de stockage avec deux sites car la modification rendrait le schéma de codage d'effacement non valide.



L'ajout ou la suppression de sites d'un pool de stockage existant ne déplacera aucune donnée codée par effacement existante. Si vous souhaitez déplacer les données existantes du site, vous devez créer un nouveau pool de stockage et un profil EC pour réencoder les données.

6. Sélectionnez **Enregistrer**.

Après avoir terminé

Si vous avez ajouté un nouveau site ou un nouveau niveau de stockage à un pool de stockage utilisé dans la stratégie ILM active, activez une nouvelle stratégie ILM pour forcer StorageGRID à utiliser le nouveau site ou le nouveau niveau de stockage. Par exemple, clonez votre politique ILM existante, puis activez le clone. Voir ["Travailler avec les règles et les politiques ILM"](#) .

Supprimer 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 d'utilisation ILM dans le 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 codage d'effacement. Si nécessaire, sélectionnez **nom du pool de stockage > utilisation ILM** 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**.

Utiliser les pools de stockage cloud

Qu'est-ce qu'un pool de stockage cloud ?

Un pool de stockage cloud vous permet d'utiliser ILM pour déplacer des données d'objet en dehors de votre système StorageGRID . Par exemple, vous souhaitez peut-être

déplacer des objets rarement consultés vers un stockage cloud moins coûteux, tel qu'Amazon S3 Glacier, S3 Glacier Deep Archive, Google Cloud ou le niveau d'accès Archive dans le stockage Microsoft Azure Blob. Ou, vous souhaitez peut-être conserver une sauvegarde cloud des objets StorageGRID pour améliorer la reprise après sinistre.

Du point de vue ILM, un pool de stockage cloud est similaire à un pool de stockage. Pour stocker des objets dans l'un ou l'autre emplacement, vous sélectionnez le pool lors de la création des instructions de placement pour une règle ILM. Cependant, alors que les pools de stockage se composent de nœuds de stockage au sein du système StorageGRID, un pool de stockage cloud se compose d'un bucket externe (S3) ou d'un conteneur (stockage Azure Blob).

Le tableau compare les pools de stockage aux pools de stockage cloud et montre les similitudes et les différences de haut niveau.

	Piscine de stockage	Pool de stockage cloud
Comment est-il créé ?	Utilisation de l'option ILM > Pools de stockage dans Grid Manager.	Utilisation de l'option ILM > Pools de stockage > Pools de stockage cloud dans Grid Manager. Vous devez configurer le bucket ou le conteneur externe avant de pouvoir créer le pool de stockage cloud.
Combien de pools pouvez-vous créer ?	Illimité.	Jusqu'à 10.
Où sont stockés les objets ?	Sur un ou plusieurs nœuds de stockage 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 éventuellement configurer un cycle de vie de bucket pour transférer des objets vers un stockage à long terme et à faible coût, tel qu'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 RestoreObject. • 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 d'objets blob Azure, StorageGRID fait passer l'objet au niveau Archive. Remarque : En général, ne configurez pas la gestion du cycle de vie du stockage Blob Azure pour le conteneur utilisé pour un pool de stockage cloud. Les opérations RestoreObject sur les objets du pool de stockage cloud peuvent être affectées par le cycle de vie configuré.

	Piscine de stockage	Pool de stockage cloud
Qu'est-ce qui contrôle le placement des objets ?	Une règle ILM dans les politiques ILM actives.	Une règle ILM dans les politiques ILM actives.
Quelle méthode de protection des données est utilisée ?	Codage de réplication ou d'effacement.	Réplication.
Combien de copies de chaque objet sont autorisées ?	Multiple.	Une copie dans le Cloud Storage Pool et, éventuellement, une ou plusieurs copies dans StorageGRID. Remarque : vous ne pouvez pas stocker un objet dans plusieurs pools de stockage cloud à la fois.
Quels sont les avantages ?	Les objets sont rapidement accessibles à tout moment.	Stockage à faible coût. Remarque : les données FabricPool ne peuvent pas être hiérarchisées vers des pools de stockage cloud.

Cycle de vie d'un objet Cloud Storage Pool

Avant d'implémenter des pools de stockage cloud, examinez le cycle de vie des objets stockés dans chaque type de pool de stockage cloud.

S3 : Cycle de vie d'un objet Cloud Storage Pool

Les étapes décrivent les étapes du cycle de vie d'un objet stocké dans un pool de stockage cloud S3.



« Glacier » fait référence à la fois à la classe de stockage Glacier et à 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 accélérée. Seule la récupération en masse 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 d'opération de restauration POST.

1. Objet stocké dans StorageGRID

Pour démarrer le cycle de vie, une application cliente stocke un objet dans StorageGRID.

2. Objet déplacé vers le pool de stockage cloud S3

- Lorsque l'objet correspond à une règle ILM qui utilise un pool de stockage cloud S3 comme emplacement de placement, StorageGRID déplace l'objet vers le bucket S3 externe spécifié par le pool de stockage cloud.

- Lorsque l'objet a été déplacé vers le pool de stockage cloud S3, l'application cliente peut le récupérer à l'aide d'une requête S3 GetObject depuis StorageGRID, sauf si l'objet a été transféré vers le stockage Glacier.

3. Objet transféré vers Glacier (état non récupérable)

- En option, l'objet peut être transféré vers le stockage Glacier. Par exemple, le bucket S3 externe peut utiliser la configuration du cycle de vie pour transférer un objet vers le stockage Glacier immédiatement ou après un certain nombre de jours.



Si vous souhaitez effectuer la transition d'objets, vous devez créer une configuration de cycle de vie pour le bucket S3 externe et utiliser une solution de stockage qui implémente la classe de stockage Glacier et prend en charge l'API S3 RestoreObject.

- Pendant la transition, l'application cliente peut utiliser une requête S3 HeadObject pour surveiller l'état de l'objet.

4. Objet restauré à partir du stockage du glacier

Si un objet a été transféré vers le stockage Glacier, l'application cliente peut émettre une demande S3 RestoreObject 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 niveau d'accès aux données à utiliser pour l'opération de restauration (accélérée, standard ou en masse). 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 en émettant une demande RestoreObject. Au lieu de cela, la copie locale peut être récupérée directement, à l'aide d'une requête GetObject.

5. Objet récupéré

Une fois qu'un objet a été restauré, l'application cliente peut émettre une requête GetObject pour récupérer l'objet restauré.

Azure : cycle de vie d'un objet de pool de stockage cloud

Les étapes décrivent 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 cliente stocke un objet dans StorageGRID.

2. Objet déplacé vers le pool de stockage cloud Azure

Lorsque l'objet correspond à une règle ILM qui utilise un pool de stockage cloud Azure comme emplacement de placement, StorageGRID déplace l'objet vers le conteneur de stockage d'objets blob Azure externe spécifié par le pool de stockage cloud.

3. Objet transféré vers le niveau Archive (état non récupérable)

Immédiatement après avoir déplacé l'objet vers le pool de stockage cloud Azure, StorageGRID fait automatiquement passer l'objet vers le niveau d'archive de stockage d'objets blob Azure.

4. Objet restauré à partir du niveau Archive

Si un objet a été transféré vers le niveau Archive, l'application cliente peut émettre une demande S3 RestoreObject pour restaurer une copie récupérable dans le pool de stockage cloud Azure.

Lorsque StorageGRID reçoit le RestoreObject, il transfère temporairement l'objet vers le niveau Cool du stockage Azure Blob. Dès que la date d'expiration de la demande RestoreObject est atteinte, StorageGRID renvoie l'objet au niveau Archive.



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 niveau d'accès Archive en émettant une demande RestoreObject. Au lieu de cela, la copie locale peut être récupérée directement, à l'aide d'une requête GetObject.

5. Objet récupéré

Une fois qu'un objet a été restauré dans le pool de stockage cloud Azure, l'application cliente peut émettre une demande GetObject pour récupérer l'objet restauré.

Informations connexes

["Utiliser l'API REST S3"](#)

Quand utiliser les pools de stockage cloud

À l'aide des pools de stockage cloud, vous pouvez sauvegarder ou hiérarchiser des données vers un emplacement externe. De plus, vous pouvez sauvegarder ou hiérarchiser des données sur plusieurs clouds.

Sauvegarder les données StorageGRID vers un emplacement externe

Vous pouvez utiliser un pool de stockage cloud pour sauvegarder des objets StorageGRID vers un emplacement externe.

Si les copies dans StorageGRID sont inaccessibles, les données d'objet dans le pool de stockage cloud peuvent être utilisées pour répondre aux demandes des clients. Cependant, vous devrez peut-être émettre une demande S3 RestoreObject pour accéder à la copie de l'objet de sauvegarde dans le pool de stockage cloud.

Les données d'objet dans un pool de stockage cloud peuvent également être utilisées pour récupérer des données perdues de StorageGRID en raison d'une défaillance d'un volume de stockage ou d'un 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 récupéré.

Pour mettre en œuvre une solution de sauvegarde :

1. Créez un pool de stockage cloud unique.
2. Configurez une règle ILM qui stocke simultanément des copies d'objet sur des nœuds de stockage (en tant que copies répliquées ou codées par effacement) et une seule copie d'objet dans le pool de stockage cloud.
3. Ajoutez la règle à votre politique ILM. Ensuite, simulez et activez la politique.

Transférer 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 . Par exemple, supposons que vous disposez d'un grand nombre d'objets que vous devez conserver, mais que vous prévoyez d'y accéder rarement, voire jamais. Vous pouvez utiliser un pool de stockage cloud pour hiérarchiser les objets vers un stockage à moindre coût et pour libérer de l'espace dans StorageGRID.

Pour mettre en œuvre une solution de hiérarchisation :

1. Créez un pool de stockage cloud unique.
2. Configurez une règle ILM qui déplace les objets rarement utilisés des nœuds de stockage vers le pool de stockage cloud.
3. Ajoutez la règle à votre politique ILM. Ensuite, simulez et activez la politique.

Maintenir plusieurs points de terminaison cloud

Vous pouvez configurer plusieurs points de terminaison de pool de stockage cloud si vous souhaitez hiérarchiser ou sauvegarder des données d'objet sur plusieurs clouds. Les filtres de vos règles ILM vous permettent de spécifier quels objets sont stockés dans chaque pool de stockage cloud. Par exemple, vous souhaitez peut-être 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. Ou, vous souhaitez peut-être déplacer des données entre Amazon S3 Glacier et le stockage Azure Blob.



Lorsque vous utilisez plusieurs points de terminaison Cloud Storage Pool, gardez à l'esprit qu'un objet ne peut être stocké que dans un seul Cloud Storage Pool à la fois.

Pour implémenter plusieurs points de terminaison cloud :

1. Créez jusqu'à 10 pools de stockage cloud.
2. Configurez les règles ILM pour stocker les données d'objet appropriées au moment approprié dans chaque pool de stockage cloud. Par exemple, stockez les objets du compartiment A dans le pool de stockage Cloud A et stockez les objets du compartiment B dans le pool de stockage Cloud B. Ou stockez les objets dans le pool de stockage Cloud A pendant un certain temps, puis déplacez-les vers le pool de stockage Cloud B.
3. Ajoutez les règles à votre politique ILM. Ensuite, simulez et activez la politique.

Considérations relatives aux pools de stockage cloud

Si vous prévoyez d'utiliser un pool de stockage cloud pour déplacer des objets hors du système StorageGRID , vous devez consulter les considérations relatives à la configuration et à l'utilisation des pools de stockage cloud.

Considérations générales

- En général, le stockage d'archives cloud, tel qu'Amazon S3 Glacier ou le stockage Azure Blob, est un endroit peu coûteux pour stocker des données d'objet. Cependant, les coûts de récupération des données à partir du stockage d'archives dans le cloud sont relativement élevés. Pour obtenir le coût global le plus bas, vous devez tenir compte du moment et de la fréquence à laquelle vous accéderez aux objets du pool de stockage cloud. L'utilisation d'un pool de stockage cloud est recommandée uniquement pour le contenu auquel vous prévoyez d'accéder rarement.
- L'utilisation de pools de stockage Cloud avec FabricPool n'est pas prise en charge en raison de la latence supplémentaire nécessaire pour récupérer un objet à partir 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 le verrouillage d'objet S3 est activé sur le bucket S3 de destination d'un pool de stockage cloud, la tentative de configuration de la réplication du bucket (PutBucketReplication) échouera avec une erreur AccessDenied.
- Les combinaisons de plateforme, d'authentification et de protocole suivantes avec le verrouillage d'objet S3 ne sont pas prises en charge pour les pools de stockage cloud :
 - **Plateformes** : Google Cloud Platform et Azure
 - **Types d'authentification** : IAM Roles Anywhere et accès anonyme
 - **Protocole** : HTTP

Considérations relatives aux ports utilisés pour les pools de stockage cloud

Pour garantir que les règles ILM peuvent déplacer des objets vers et depuis le pool de stockage cloud spécifié, vous devez configurer le ou les réseaux qui contiennent les nœuds de stockage de votre 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 de terminaison commençant par http
- **443** : pour les URI de point de terminaison commençant par https

Vous pouvez spécifier un port différent lorsque vous créez ou modifiez un pool de stockage cloud.

Si vous utilisez un serveur proxy non transparent, vous devez également [configurer un proxy de stockage](#) pour permettre l'envoi de messages à 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 nécessite une connectivité réseau au cloud. Vous devez prendre en compte le coût de l'infrastructure réseau que vous utiliserez pour accéder au cloud et la provisionner de manière 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 point de terminaison du pool de stockage cloud externe, il émet diverses demandes pour surveiller la connectivité et garantir qu'il peut effectuer les opérations requises. Bien que certains coûts supplémentaires soient associés à ces demandes, le coût de la surveillance d'un pool de stockage cloud ne devrait représenter qu'une petite 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 d'un point de terminaison de pool de stockage cloud externe vers StorageGRID. Les objets peuvent être déplacés 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 stocker l'objet dans StorageGRID à la place. Dans ce cas, vous reconfigurez vos règles et votre politique ILM. Lorsque l'évaluation ILM se produit, StorageGRID émet plusieurs requêtes pour récupérer l'objet à partir du pool de stockage cloud. StorageGRID crée ensuite localement le nombre spécifié de copies répliquées ou codées par effacement. Une fois l'objet déplacé vers StorageGRID, la copie dans le pool de stockage cloud est supprimée.
- Les objets sont perdus en raison 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 récupéré.



Lorsque des objets sont déplacés vers StorageGRID à partir d'un pool de stockage cloud, StorageGRID émet plusieurs requêtes vers le point de terminaison du pool de stockage cloud pour chaque objet. Avant de déplacer un grand nombre d'objets, contactez le support technique pour obtenir de l'aide afin d'estimer le délai et les coûts associés.

S3 : autorisations requises pour le compartiment Cloud Storage Pool

Les politiques du bucket S3 externe utilisé pour un pool de stockage cloud doivent accorder à StorageGRID l'autorisation de déplacer un objet vers le bucket, d'obtenir l'état d'un objet, de restaurer un objet à partir du stockage Glacier lorsque cela est nécessaire, etc. Idéalement, StorageGRID devrait avoir un accès de contrôle total au bucket(`s3:*`); cependant, si cela n'est pas possible, la politique de bucket 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 relatives au cycle de vie du bucket externe

Le mouvement des objets entre StorageGRID et le bucket S3 externe spécifié dans le pool de stockage cloud est contrôlé par les règles ILM et les stratégies ILM actives dans StorageGRID. En revanche, la transition des objets 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 qui implémente la classe de stockage Glacier) est contrôlée par la configuration du cycle de vie de ce compartiment.

Si vous souhaitez transférer des objets du pool de stockage Cloud, vous devez créer la configuration de cycle de vie appropriée sur le bucket S3 externe et utiliser une solution de stockage qui implémente la classe de stockage Glacier et prend en charge l'API S3 `RestoreObject`.

Par exemple, supposons que vous souhaitiez que tous les objets déplacés de StorageGRID vers le pool de stockage cloud soient immédiatement transférés vers le stockage Amazon S3 Glacier. Vous devez créer une configuration de cycle de vie sur le bucket S3 externe qui spécifie une action unique (**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 transférerait tous les objets de compartiment vers Amazon S3 Glacier le jour de leur création (c'est-à-dire le jour où ils ont été déplacés de StorageGRID vers le pool de stockage cloud).



Lors de la configuration du cycle de vie du bucket externe, n'utilisez jamais d'actions **Expiration** pour définir le moment où les objets expirent. Les actions d'expiration amènent le système de stockage externe à supprimer les objets expirés. Si vous tentez ultérieurement d'accéder à un objet expiré à partir de StorageGRID, l'objet supprimé ne sera pas trouvé.

Si vous souhaitez transférer des objets du pool de stockage cloud vers S3 Glacier Deep Archive (au lieu d'Amazon S3 Glacier), spécifiez `<StorageClass>DEEP_ARCHIVE</StorageClass>` dans le cycle de vie du bucket. Cependant, sachez que vous ne pouvez pas utiliser le Expedited niveau pour restaurer les objets de S3 Glacier Deep Archive.

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. Lors de la création d'un compte de stockage à utiliser avec un pool de stockage cloud, vous devez utiliser le niveau Hot comme niveau par défaut. Même si StorageGRID définit immédiatement le niveau sur Archive lorsqu'il déplace des objets vers le pool de stockage cloud, l'utilisation d'un paramètre par défaut sur Chaud garantit qu'aucun frais de suppression anticipée ne vous sera facturé pour les objets supprimés du niveau Froid avant le minimum de 30 jours.

Azure : la gestion du cycle de vie n'est pas 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. Les opérations du cycle de vie peuvent interférer avec les opérations du pool de stockage Cloud.

Informations connexes

["Créer un pool de stockage cloud"](#)

Comparer les pools de stockage cloud et la réplication CloudMirror

Lorsque vous commencez à utiliser les pools de stockage Cloud, il peut être utile de comprendre les similitudes et les différences entre les pools de stockage Cloud et le

	Pool de stockage cloud	Service de réplication CloudMirror
Quel est le but principal ?	Agit comme une cible d'archivage. La copie de l'objet dans le pool de stockage Cloud peut être la seule copie de l'objet ou une copie supplémentaire. Autrement dit, au lieu de conserver deux copies sur site, vous pouvez conserver une copie dans StorageGRID et envoyer une copie au pool de stockage cloud.	Permet à un locataire de répliquer automatiquement des objets d'un bucket dans StorageGRID (source) vers un bucket 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 Grid Manager ou de l'API Grid Management. Peut être sélectionné comme emplacement de placement dans une règle ILM. Alors qu'un pool de stockage se compose d'un groupe de nœuds de stockage, un pool de stockage cloud est défini à l'aide d'un point de terminaison S3 ou Azure distant (adresse IP, informations d'identification, etc.).	Un utilisateur locataire configure la réplication CloudMirror en définissant un point de terminaison CloudMirror (adresse IP, informations d'identification, etc.) à l'aide du Tenant Manager ou de l'API S3. Une fois le point de terminaison CloudMirror configuré, tout bucket appartenant à ce compte locataire peut être configuré pour pointer vers le point de terminaison CloudMirror.
Qui est responsable de sa mise en place ?	En règle générale, un administrateur de réseau	En règle générale, un utilisateur locataire
Quelle est la destination ?	• Toute infrastructure S3 compatible (y compris Amazon S3) • Niveau d'archive d'objets blob Azure • Plateforme Google Cloud (GCP)	• Toute infrastructure S3 compatible (y compris Amazon S3) • Plateforme Google Cloud (GCP)
Qu'est-ce qui provoque le déplacement des objets vers la destination ?	Une ou plusieurs règles ILM dans les politiques ILM actives. Les règles ILM définissent les objets que StorageGRID déplace vers le pool de stockage cloud et quand les objets sont déplacés.	L'acte d'ingérer un nouvel objet dans un bucket source qui a été configuré avec un point de terminaison CloudMirror. Les objets qui existaient dans le bucket source avant que le bucket ne soit configuré avec le point de terminaison CloudMirror ne sont pas répliqués, sauf s'ils sont modifiés.

	Pool de stockage cloud	Service de réplication CloudMirror
Comment les objets sont-ils récupérés ?	Les applications doivent effectuer des demandes auprès de StorageGRID pour récupérer les objets qui ont été déplacés vers un pool de stockage cloud. Si la seule copie d'un objet a été transférée vers un stockage d'archivage, StorageGRID gère le processus de restauration de l'objet afin qu'il puisse être récupéré.	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 soit à StorageGRID , soit à la destination S3. Par exemple, supposons que vous utilisiez la réplication CloudMirror pour mettre en miroir des objets vers une organisation partenaire. Le partenaire peut utiliser ses propres applications pour lire ou mettre à jour des objets directement depuis la destination S3. L'utilisation de StorageGRID n'est pas requise.
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 Cloud Storage Pool).	Oui, car la copie 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 bucket StorageGRID , mais il continue d'exister dans le bucket de destination. De même, les objets du bucket de destination peuvent être supprimés sans affecter la source.
Comment accéder aux objets après un sinistre (système StorageGRID non opérationnel) ?	Les nœuds StorageGRID défaillants doivent être récupérés. Au cours de ce processus, des copies d'objets répliqués peuvent être restaurées à l'aide des copies du pool de stockage cloud.	Les copies d'objet dans la destination CloudMirror sont indépendantes de StorageGRID, elles sont donc accessibles directement avant la récupération des nœuds StorageGRID .

Créer un pool de stockage cloud

Un pool de stockage cloud spécifie un seul compartiment Amazon S3 externe ou un autre fournisseur compatible 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 du conteneur externe que StorageGRID utilisera pour stocker les objets, le type de fournisseur de cloud (stockage Amazon S3/GCP ou Azure Blob) et les informations dont StorageGRID a besoin pour accéder au compartiment ou au conteneur externe.

StorageGRID valide le pool de stockage cloud dès que vous l'enregistrez. Vous devez donc vous assurer que

le bucket ou le conteneur spécifié dans le pool de stockage cloud existe et est accessible.

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 examiné le [Considérations relatives aux pools de stockage cloud](#) .
- Le bucket ou conteneur externe référencé par le Cloud Storage Pool existe déjà et vous disposez de [l'informations sur le point de terminaison du service](#) .
- Pour accéder au seau ou au conteneur, vous avez le [informations de compte pour le type d'authentification](#) tu choisiras.

Étapes

1. Sélectionnez **ILM > Pools de stockage > Pools de stockage cloud**.
2. Sélectionnez **Créer**, puis saisissez les informations suivantes :

Champ	Description
Nom du pool de stockage cloud	Un nom qui décrit brièvement le pool de stockage cloud et son objectif. Utilisez un nom qui sera facile à identifier lorsque vous configurerez les règles ILM.
Type de fournisseur	Quel fournisseur de cloud utiliserez-vous pour ce pool de stockage cloud : • Amazon S3/GCP : sélectionnez cette option pour un fournisseur Amazon S3, Commercial Cloud Services (C2S) S3, Google Cloud Platform (GCP) ou autre fournisseur compatible S3. • Stockage d'objets blob Azure
Seau ou récipient	Le nom du bucket S3 externe ou du conteneur Azure. 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, saisissez les informations du 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 de l'URL :

Option	Description
Détection automatique	Tentez de détecter automatiquement le style d'URL à utiliser, en fonction des informations fournies. Par exemple, si vous spécifiez une adresse IP, StorageGRID utilisera une URL de type chemin. Sélectionnez cette option uniquement si vous ne savez pas quel style spécifique utiliser.
Style d'hébergement virtuel	Utilisez une URL de type hébergement virtuel pour accéder au bucket. Les URL de type hébergé virtuellement incluent le nom du bucket dans le nom de domaine. Exemple: <code>https://bucket-name.s3.company.com/key-name</code>
Chemin de style	Utilisez une URL de type chemin pour accéder au bucket. Les URL de style chemin incluent le nom du bucket à la fin. Exemple: <code>https://s3.company.com/bucket-name/key-name</code> Remarque : l'option d'URL de style chemin 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 d'objets blob Azure

- a. À l'aide de l'un des formats suivants, saisissez l'URI du point de terminaison du service.

- `https://host:port`
- `http://host:port`

Exemple: `https://myaccount.blob.core.windows.net:443`

Si vous ne spécifiez pas de port, par défaut le port 443 est utilisé pour HTTPS et le port 80 est utilisé pour HTTP.

4. Sélectionnez **Continuer**. Sélectionnez ensuite le type d'authentification et saisissez les informations requises pour le point de terminaison du pool de stockage cloud :

Clé d'accès

Pour Amazon S3/GCP ou autre fournisseur compatible S3

- a. **ID de clé d'accès** : saisissez l'ID de clé d'accès du compte propriétaire du compartiment externe.
- b. **Clé d'accès secrète** : Saisissez la clé d'accès secrète.

Rôles IAM partout

Pour le service AWS IAM Roles Anywhere

StorageGRID utilise AWS Security Token Service (STS) pour générer dynamiquement un jeton de courte durée pour accéder aux ressources AWS.

- a. **Région AWS IAM Roles Anywhere** : sélectionnez la région pour le pool de stockage cloud. Par exemple : `us-east-1`.
- b. **URN d'ancre de confiance** : saisissez l'URN de l'ancre de confiance qui valide les demandes d'informations d'identification STS de courte durée. Peut être une autorité de certification racine ou intermédiaire.
- c. **URN du profil** : saisissez l'URN du profil IAM Roles Anywhere qui répertorie les rôles pouvant être assumés par toute personne de confiance.
- d. **URN du rôle** : saisissez l'URN du rôle IAM qui peut être assumé par toute personne de confiance.
- e. **Durée de la session** : saisissez la durée des informations d'identification de sécurité temporaires et de la session de rôle. Entrez au moins 15 minutes et pas plus de 12 heures.
- f. **Certificat d'autorité de certification du serveur** (facultatif) : un ou plusieurs certificats d'autorité de certification approuvés, au format PEM, pour vérifier le serveur IAM Roles Anywhere. Si omis, le serveur ne sera pas vérifié.
- g. **Certificat d'entité finale** : La clé publique, au format PEM, du certificat X509 signé par l'ancre de confiance. AWS IAM Roles Anywhere utilise cette clé pour émettre un jeton STS.
- h. **Clé privée de l'entité finale** : la clé privée du certificat de l'entité finale.

CAP (portail d'accès C2S)

Pour le service S3 des services cloud commerciaux (C2S)

- a. **URL des informations d'identification temporaires** : saisissez l'URL complète que StorageGRID utilisera pour obtenir des informations d'identification temporaires auprès du serveur CAP, y compris tous les paramètres API obligatoires et facultatifs attribués à votre compte C2S.
- b. **Certificat CA du serveur** : sélectionnez **Parcourir** et téléchargez le certificat CA que StorageGRID utilisera pour vérifier le serveur CAP. Le certificat doit être codé en PEM et émis par une autorité de certification gouvernementale (CA) appropriée.
- c. **Certificat client** : sélectionnez **Parcourir** et téléchargez le certificat que StorageGRID utilisera pour s'identifier auprès du serveur CAP. Le certificat client doit être codé en PEM, émis par une autorité de certification gouvernementale (CA) appropriée et donner accès à votre compte C2S.
- d. **Clé privée client** : sélectionnez **Parcourir** et téléchargez la clé privée codée PEM pour le certificat client.
- e. Si la clé privée du client est chiffrée, saisissez la phrase secrète permettant de déchiffrer la clé privée du client. Sinon, laissez le champ **Phrase de passe de la clé privée du client** vide.



Si le certificat client doit être chiffré, utilisez le format traditionnel pour le chiffrement. Le format crypté PKCS #8 n'est pas pris en charge.

Stockage d'objets blob Azure

Pour Azure Blob Storage, clé partagée uniquement

- a. **Nom du compte** : saisissez le nom du compte de stockage propriétaire du conteneur externe
- b. **Clé du compte** : Saisissez la clé secrète du compte de stockage

Vous pouvez utiliser le portail Azure pour trouver ces valeurs.

Anonyme

Aucune information supplémentaire n'est requise.

5. Sélectionnez **Continuer**. Choisissez ensuite le type de vérification du serveur que vous souhaitez utiliser :

Option	Description
Utiliser les certificats d'autorité de certification racine dans le système d'exploitation Storage Node	Utilisez les certificats Grid CA installés sur le système d'exploitation pour sécuriser les connexions.
Utiliser un certificat CA personnalisé	Utilisez un certificat CA personnalisé. Sélectionnez Parcourir et téléchargez le certificat codé PEM.
Ne pas vérifier le certificat	La sélection de cette option signifie que les connexions TLS au pool de stockage cloud ne sont pas sécurisées.

6. Sélectionnez **Enregistrer**.

Lorsque vous enregistrez un pool de stockage cloud, StorageGRID effectue les opérations suivantes :

- Valide que le bucket ou le conteneur et le point de terminaison de service existent et qu'ils peuvent être atteints à l'aide des informations d'identification que vous avez spécifiées.
- Écrit un fichier marqueur dans le bucket ou le conteneur pour l'identifier comme un pool de stockage cloud. Ne supprimez jamais ce fichier, qui est nommé `x-ntap-sgws-cloud-pool-uuid`.

Si la validation du pool de stockage Cloud échoue, vous recevez un message d'erreur expliquant pourquoi la validation a échoué. Par exemple, une erreur peut être signalée s'il y a une erreur de certificat ou si le bucket 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.

Afficher les détails du pool de stockage cloud

Vous pouvez afficher les détails d'un pool de stockage cloud pour déterminer où il est utilisé et 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](#) .
- Tu as ["autorisations d'accès spécifiques"](#) .

Étapes

1. Sélectionnez **ILM > Pools de stockage > Pools de stockage cloud**.

Le tableau des pools de stockage cloud inclut les informations suivantes pour chaque pool de stockage cloud qui inclut des nœuds de stockage :

- **Nom** : Le nom d'affichage unique du pool.
- **URI** : l'identifiant de ressource uniforme du pool de stockage cloud.
- **Type de fournisseur** : quel fournisseur de cloud est utilisé pour ce pool de stockage cloud.
- **Conteneur** : le nom du bucket utilisé pour le pool de stockage cloud.
- **Utilisation ILM** : Comment la piscine est actuellement utilisée. Un pool de stockage cloud peut être inutilisé ou utilisé dans une ou plusieurs règles ILM, profils de codage d'effacement ou les deux.
- **Dernière erreur** : la dernière erreur détectée lors d'un contrôle d'état de ce pool de stockage cloud.

2. Pour afficher les détails d'un pool de stockage cloud spécifique, sélectionnez son nom.

La page de détails de la piscine apparaît.

3. Consultez l'onglet **Authentification** pour en savoir plus sur le type d'authentification de ce pool de stockage cloud et pour modifier les détails d'authentification.
4. Consultez l'onglet **Vérification du serveur** pour en savoir plus sur les détails de la vérification, modifier la vérification, télécharger un nouveau certificat ou copier le PEM du certificat.
5. Consultez l'onglet **Utilisation ILM** pour déterminer si le pool de stockage cloud est actuellement utilisé dans des règles ILM ou des profils de codage d'effacement.
6. En option, accédez à la page **Règles ILM** pour ["connaître et gérer toutes les règles"](#) qui utilisent le pool de stockage cloud.

Modifier un pool de stockage cloud

Vous pouvez modifier un pool de stockage cloud pour changer son nom, son point de terminaison de service ou d'autres détails ; cependant, vous ne pouvez pas modifier le bucket S3 ou le conteneur Azure d'un pool de stockage cloud.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un [navigateur Web pris en charge](#) .
- Tu as ["autorisations d'accès spécifiques"](#) .
- Vous avez examiné le ["Considérations relatives aux pools de stockage cloud"](#) .

Étapes

1. Sélectionnez **ILM > Pools de stockage > Pools de stockage cloud**.

Le tableau Pools de stockage cloud répertorie les pools de stockage cloud existants.

2. Cochez la case correspondant au pool de stockage cloud que vous souhaitez modifier, puis sélectionnez **Actions > Modifier**.

Vous pouvez également sélectionner le nom du pool de stockage cloud, puis sélectionner **Modifier**.

3. Si nécessaire, modifiez le nom du pool de stockage cloud, le point de terminaison du service, les informations d'authentification ou la méthode de vérification du certificat.



Vous ne pouvez pas modifier le type de fournisseur, le bucket 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 développer l'accordéon **Détails du certificat** pour consulter le certificat actuellement utilisé.

4. Sélectionnez **Enregistrer**.

Lorsque vous enregistrez un pool de stockage cloud, StorageGRID valide que le bucket ou le conteneur et le point de terminaison de service existent et qu'ils sont accessibles à l'aide des informations d'identification que vous avez spécifiées.

Si la validation du pool de stockage Cloud échoue, un message d'erreur s'affiche. Par exemple, une erreur peut être signalée s'il y a une erreur de certificat.

Voir les instructions pour "[dépannage des pools de stockage cloud](#)", résolvez le problème, puis essayez à nouveau d'enregistrer le pool de stockage cloud.

Supprimer 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 ILM pour déplacer les données de l'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 > Pools de stockage > Pools de stockage cloud**.
2. Consultez la colonne d'utilisation d'ILM dans le 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 codage d'effacement.

3. Si le pool de stockage cloud est utilisé, sélectionnez **nom du pool de stockage cloud > utilisation ILM**.
4. "[Cloner chaque règle ILM](#)" qui place actuellement les objets dans le pool de stockage cloud que vous souhaitez supprimer.
5. Déterminez où vous souhaitez déplacer les objets existants gérés par chaque règle que vous avez clonée.

Vous pouvez utiliser un ou plusieurs pools de stockage ou un pool de stockage Cloud différent.

6. Modifiez chacune des règles que vous avez clonées.

Pour l'étape 2 de l'assistant de création de règle ILM, sélectionnez le nouvel emplacement dans le champ **copies à**.

7. "[Créer une nouvelle politique ILM](#)" et remplacez chacune des anciennes règles par une règle clonée.

8. Activer la nouvelle politique.

9. Attendez qu'ILM supprime les objets du pool de stockage cloud et les place dans le nouvel emplacement.

Supprimer le pool de stockage cloud

Lorsque le pool de stockage cloud est vide et 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 bucket 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 "[Dépannage des pools de stockage cloud](#)".



Lorsque vous créez un pool de stockage cloud, StorageGRID écrit un fichier marqueur dans le bucket ou le conteneur pour l'identifier comme pool de stockage cloud. Ne supprimez pas ce fichier, qui est nommé `x-ntap-sgws-cloud-pool-uuid`.

Étapes

1. Sélectionnez **ILM > Pools de stockage > Pools de stockage cloud**.
2. Si la colonne d'utilisation d'ILM indique que le pool de stockage cloud n'est pas utilisé, cochez la case.
3. Sélectionnez **Actions > Supprimer**.
4. Sélectionnez **OK**.

Dépannage des pools de stockage cloud

Utilisez ces étapes de dépannage pour vous aider à résoudre les erreurs que vous pourriez rencontrer lors de la création, de la modification ou de la suppression d'un pool de stockage cloud.

Déterminer si une erreur s'est produite

StorageGRID effectue un simple contrôle de santé sur chaque pool de stockage cloud en lisant l'objet connu `x-ntap-sgws-cloud-pool-uuid` pour garantir que le pool de stockage cloud est accessible et fonctionne correctement. Lorsque StorageGRID rencontre une erreur sur le point de terminaison, il effectue une vérification de l'état toutes les minutes à partir de chaque nœud de stockage. Une fois l'erreur résolue, les contrôles de santé s'arrêtent. Si un contrôle d'intégrité détecte un problème, un message s'affiche dans la colonne Dernière erreur du tableau Pools de stockage cloud sur la page Pools de stockage.

Le tableau affiche l'erreur la plus récente détectée pour chaque pool de stockage cloud et indique depuis combien de temps l'erreur s'est produite.

De plus, une alerte **Erreur de connectivité du pool de stockage cloud** est déclenchée si le contrôle d'intégrité détecte qu'une ou plusieurs nouvelles erreurs du 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 Pools de stockage (sélectionnez **ILM > Pools de stockage**), examinez les messages d'erreur dans la colonne 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. Depuis la page Cloud Storage Pool, sélectionnez le point de terminaison, puis sélectionnez **Effacer l'erreur**. Un message de confirmation indique que StorageGRID a corrigé l'erreur pour le pool de stockage cloud.

Si le problème sous-jacent a été résolu, le message d'erreur n'est plus affiché. Cependant, si le problème sous-jacent n'a pas été résolu (ou si une erreur différente est rencontrée), le message d'erreur s'affichera dans la colonne Dernière erreur dans quelques minutes.

Erreur : le contrôle de santé a échoué. Erreur du point de terminaison

Vous pouvez rencontrer cette erreur lorsque vous activez le verrouillage d'objet S3 avec la rétention par défaut pour votre compartiment Amazon S3 après avoir commencé à utiliser ce compartiment pour un pool de stockage cloud. Cette erreur se produit lorsque l'opération PUT n'a pas d'en-tête HTTP avec une valeur de somme de contrôle de charge utile telle que `Content-MD5`. Cette valeur d'en-tête est requise par AWS pour les opérations PUT dans les buckets avec S3 Object Lock activé.

Pour corriger ce problème, suivez les étapes décrites dans "[Modifier un pool de stockage cloud](#)" sans apporter aucune modification. Cette action déclenche la validation de la configuration du pool de stockage Cloud qui détecte et met à jour automatiquement l'indicateur de verrouillage d'objet S3 sur une configuration de point de terminaison du pool de stockage Cloud.

Erreur : ce pool de stockage cloud contient du contenu inattendu

Vous pouvez rencontrer cette erreur lorsque vous essayez de créer, de modifier ou de supprimer un pool de stockage cloud. Cette erreur se produit si le bucket ou le conteneur inclut le `x-ntap-sgws-cloud-pool-uuid` fichier marqueur, mais ce fichier ne possède pas le champ de métadonnées avec l'UUID attendu.

En règle générale, vous ne verrez cette erreur que si vous créez un nouveau pool de stockage cloud et qu'une autre instance de StorageGRID utilise déjà le même pool de stockage cloud.

Essayez l'une de ces étapes pour corriger le problème :

- Si vous configurez un nouveau pool de stockage cloud et que le bucket contient le `x-ntap-sgws-cloud-pool-uuid` fichier et clés d'objet supplémentaires similaires à l'exemple suivant, créez un nouveau bucket et utilisez ce nouveau bucket à la place.

Exemple d'une clé d'objet supplémentaire : `my-bucket.3E64CF2C-B74D-4B7D-AFE7-AD28BC18B2F6.1727326606730410`

- Si le `x-ntap-sgws-cloud-pool-uuid` le fichier est le seul objet dans le bucket, supprimez ce fichier.

Si ces étapes ne s'appliquent pas à votre scénario, contactez le support.

Erreur : impossible de créer ou de mettre à jour le pool de stockage cloud. Erreur du point de terminaison

Vous pouvez rencontrer cette erreur dans les circonstances suivantes :

- Lorsque vous essayez de créer ou de modifier un pool de stockage cloud.
- Lorsque vous sélectionnez une combinaison de plateforme, d'authentification ou de protocole non prise en charge avec S3 Object Lock lors de la configuration d'un nouveau pool de stockage cloud. Voir ["Considérations relatives aux pools 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, examinez le message d'erreur du point de terminaison.

- Si le message d'erreur contient `Get url: EOF` , vérifiez que le point de terminaison de service utilisé pour le pool de stockage cloud n'utilise pas HTTP pour un conteneur ou un bucket nécessitant HTTPS.
- Si le message d'erreur contient `Get url: net/http: request canceled while waiting for connection` , vérifiez que la configuration réseau permet aux nœuds de stockage d'accéder au point de terminaison de service utilisé pour le pool de stockage cloud.
- Si l'erreur est due à une plate-forme, une authentification ou un protocole non pris en charge, passez à une configuration prise en charge avec S3 Object Lock et essayez à nouveau d'enregistrer le nouveau pool de stockage cloud.
- Pour tous les autres messages d'erreur de point de terminaison, essayez une ou plusieurs des solutions suivantes :
 - Créez un conteneur ou un bucket externe portant le même nom que celui que vous avez saisi pour le pool de stockage cloud et essayez à nouveau d'enregistrer le nouveau pool de stockage cloud.
 - Corrigez le nom du conteneur ou du bucket que vous avez spécifié pour le pool de stockage cloud et essayez à nouveau d'enregistrer le nouveau pool de stockage cloud.

Erreur : échec de l'analyse du certificat CA

Vous pouvez rencontrer cette erreur lorsque vous essayez 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 entré lors de la configuration du pool de stockage cloud.

Pour corriger le problème, vérifiez le certificat CA que vous avez fourni pour les problèmes.

Erreur : aucun pool de stockage cloud avec cet ID n'a été trouvé

Vous pouvez rencontrer cette erreur lorsque vous essayez de modifier ou de supprimer un pool de stockage cloud. Cette erreur se produit si le point de terminaison renvoie une réponse 404, ce qui peut signifier l'une des choses suivantes :

- Les informations d'identification utilisées pour le pool de stockage cloud ne disposent pas d'autorisation de lecture pour le bucket.
- Le bucket utilisé pour le pool de stockage cloud n'inclut pas le `x-ntap-sgws-cloud-pool-uuid` fichier marqueur.

Essayez une ou plusieurs de ces étapes pour corriger le problème :

- Vérifiez que l'utilisateur associé à la clé d'accès configurée dispose des autorisations requises.
- Modifiez le pool de stockage cloud avec les informations d'identification disposant des autorisations requises.
- Si les autorisations sont correctes, contactez le support.

Erreur : impossible de vérifier le contenu du pool de stockage cloud. Erreur du point de terminaison

Vous pouvez rencontrer cette erreur lorsque vous essayez 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 bucket Cloud Storage Pool.

Pour corriger le problème, examinez le message d'erreur du point de terminaison.

Erreur : des objets ont déjà été placés dans ce bucket

Vous pouvez rencontrer cette erreur lorsque vous essayez 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 trouvaient dans le bucket avant la configuration du pool de stockage cloud ou des données qui ont été placées dans le bucket par une autre source après la création du pool de stockage cloud.

Essayez une ou plusieurs de ces étapes pour corriger le problème :

- Suivez les instructions pour déplacer des objets vers StorageGRID dans « Cycle de vie d'un objet Cloud Storage Pool ».
- 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 bucket.



Ne supprimez jamais manuellement des objets d'un pool de stockage cloud qui auraient pu y être placés par ILM. Si vous tentez ultérieurement d'accéder à un objet supprimé manuellement à partir de StorageGRID, l'objet supprimé ne sera pas trouvé.

Erreur : le proxy a rencontré une erreur externe lors de la tentative d'accès au pool de stockage cloud

Vous pouvez rencontrer cette erreur si vous avez configuré un proxy de stockage non transparent entre les nœuds de stockage et le point de terminaison S3 externe utilisé pour le pool de stockage cloud. Cette erreur se produit si le serveur proxy externe ne peut pas atteindre le point de terminaison du pool de stockage cloud. Par exemple, le serveur DNS peut ne pas être en mesure de résoudre le nom d'hôte ou il peut y avoir un problème de réseau externe.

Essayez une ou plusieurs de ces étapes pour corriger le problème :

- Vérifiez les paramètres du pool de stockage cloud (**ILM > Pools de stockage**).
- Vérifiez la configuration réseau du serveur proxy de stockage.

Erreur : le certificat X.509 n'a plus de validité

Vous pouvez rencontrer cette erreur lorsque vous essayez de supprimer un pool de stockage cloud. Cette erreur se produit lorsque l'authentification nécessite un certificat X.509 pour garantir que le pool de stockage cloud externe correct est validé et que le pool externe est vide avant la suppression de la configuration du pool de stockage cloud.

Essayez ces étapes pour corriger le problème :

- Mettez à jour le certificat configuré pour l'authentification auprès du pool de stockage cloud.
- Assurez-vous que toute alerte d'expiration de certificat sur ce pool de stockage cloud est résolue.

Informations connexes

["Cycle de vie d'un objet Cloud Storage Pool"](#)

Gérer les profils de codage d'effacement

Vous pouvez afficher les détails d'un profil de codage d'effacement et renommer un profil si nécessaire. Vous pouvez désactiver un profil de codage d'effacement s'il n'est actuellement utilisé dans aucune règle 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"](#).

Afficher les détails du profil de codage d'effacement

Vous pouvez afficher les détails d'un profil de codage d'effacement pour déterminer son état, le schéma de codage d'effacement utilisé et d'autres informations.

Étapes

1. Sélectionnez **CONFIGURATION > Système > Codage d'effacement**.
2. Sélectionnez le profil. La page de détails du profil apparaît.
3. Vous pouvez également consulter l'onglet Règles ILM pour obtenir la liste des règles ILM qui utilisent le profil et les stratégies ILM qui utilisent ces règles.
4. Vous pouvez également consulter l'onglet Nœuds de stockage pour obtenir des détails sur chaque nœud de stockage dans le pool de stockage du profil, comme le site où il se trouve et l'utilisation du stockage.

Renommer un profil de codage d'effacement

Vous souhaitez peut-être renommer un profil de codage d'effacement pour rendre plus évident ce que fait le profil.

Étapes

1. Sélectionnez **CONFIGURATION > Système > Codage d'effacement**.
2. Sélectionnez le profil que vous souhaitez renommer.
3. Sélectionnez **Renommer**.
4. Saisissez un nom unique pour le profil de codage d'effacement.

Le nom du profil de codage d'effacement est ajouté au nom du pool de stockage dans l'instruction de placement d'une règle ILM.



Les noms de profil de codage 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 codage d'effacement

Vous pouvez désactiver un profil de codage d'effacement si vous ne prévoyez plus de l'utiliser et si le profil n'est actuellement utilisé dans aucune règle ILM.



Confirmez qu'aucune opération de réparation de données codées par effacement ou procédure de mise hors service n'est en cours. Un message d'erreur est renvoyé si vous tentez de désactiver un profil de codage d'effacement pendant que l'une de ces opérations est en cours.

À propos de cette tâche

StorageGRID vous empêche de désactiver un profil de codage d'effacement si l'une des conditions suivantes est vraie :

- Le profil de codage d'effacement est actuellement utilisé dans une règle ILM.
- Le profil de codage d'effacement n'est plus utilisé dans aucune règle ILM, mais les données d'objet et les fragments de parité du profil existent toujours.

Étapes

1. Sélectionnez **CONFIGURATION > Système > Codage d'effacement**.
2. Dans l'onglet Actif, vérifiez la colonne **Statut** pour confirmer que le profil de codage d'effacement que vous souhaitez désactiver n'est utilisé dans aucune règle ILM.

Vous ne pouvez pas désactiver un profil de codage d'effacement s'il est utilisé dans une règle ILM. Dans l'exemple, le profil 2+1 Data Center 1 est utilisé dans au moins une règle ILM.

☐	Profile name ?	Status ?	Storage pool ?	Erasure-coding scheme ?
☐	2+1 Data Center 1	Used in 5 rules	Data Center 1	2+1
☐	New profile	Deactivated	Data Center 1	2+1

3. Si le profil est utilisé dans une règle ILM, suivez ces étapes :
 - a. Sélectionnez **ILM > Règles**.
 - b. Sélectionnez chaque règle et examinez le diagramme de conservation pour déterminer si la règle utilise le profil de codage d'effacement que vous souhaitez désactiver.
 - c. Si la règle ILM utilise le profil de codage d'effacement que vous souhaitez désactiver, déterminez si la règle est utilisée dans une stratégie ILM.
 - d. Effectuez les étapes supplémentaires du tableau, en fonction de l'endroit où le profil de codage d'effacement est utilisé.

Où le profil a-t-il été utilisé ?	Étapes supplémentaires à effectuer avant de désactiver le profil	Reportez-vous à ces instructions supplémentaires
Jamais utilisé dans aucune règle ILM	Aucune étape supplémentaire n'est requise. Continuez avec cette procédure.	Aucun

Où le profil a-t-il été utilisé ?	Étapes supplémentaires à effectuer avant de désactiver le profil	Reportez-vous à ces instructions supplémentaires
Dans une règle ILM qui n'a jamais été utilisée dans aucune politique ILM	i. Modifiez ou supprimez toutes les règles ILM affectées. Si vous modifiez la règle, supprimez tous les emplacements qui utilisent le profil de codage d'effacement. ii. Continuez avec cette procédure.	"Travailler avec les règles et les politiques ILM"
Dans une règle ILM qui se trouve actuellement dans une politique ILM active	i. Cloner la politique. ii. Supprimez la règle ILM qui utilise le profil de codage d'effacement. iii. Ajoutez une ou plusieurs nouvelles règles ILM pour garantir la protection des objets. iv. Enregistrez, simulez et activez la nouvelle politique. v. Attendez que la nouvelle politique soit appliquée et que les objets existants soient déplacés vers de nouveaux emplacements en fonction des nouvelles règles que vous avez ajoutées. Remarque : selon le nombre d'objets et la taille de votre système StorageGRID , les opérations ILM peuvent prendre des semaines, voire des mois, pour déplacer les objets vers de nouveaux emplacements, en fonction des nouvelles règles ILM. Bien que vous puissiez tenter en toute sécurité de désactiver un profil de codage d'effacement alors qu'il est toujours associé à des données, l'opération de désactivation échouera. Un message d'erreur vous informera si le profil n'est pas encore prêt à être désactivé. vi. Modifiez ou supprimez la règle que vous avez supprimée de la politique. Si vous modifiez la règle, supprimez tous les emplacements qui utilisent le profil de codage d'effacement. vii. Continuez avec cette procédure.	"Créer une politique ILM" "Travailler avec les règles et les politiques ILM"

Où le profil a-t-il été utilisé ?	Étapes supplémentaires à effectuer avant de désactiver le profil	Reportez-vous à ces instructions supplémentaires
Dans une règle ILM qui se trouve actuellement dans une politique ILM	i. Modifier la politique. ii. Supprimez la règle ILM qui utilise le profil de codage d'effacement. iii. Ajoutez une ou plusieurs nouvelles règles ILM pour garantir que tous les objets sont protégés. iv. Sauvegarder la politique. v. Modifiez ou supprimez la règle que vous avez supprimée de la politique. Si vous modifiez la règle, supprimez tous les emplacements qui utilisent le profil de codage d'effacement. vi. Continuez avec cette procédure.	"Créer une politique ILM" "Travailler avec les règles et les politiques ILM"

e. Actualisez la page Profils de codage 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 de codage d'effacement s'affiche.



Vous pouvez sélectionner plusieurs profils à désactiver en même temps, à condition que chaque profil ne soit utilisé dans aucune règle.

5. Si vous êtes sûr de vouloir désactiver le profil, sélectionnez **Désactiver**.

Résultats

- Si StorageGRID est en mesure de désactiver le profil de codage d'effacement, son statut est Désactivé. Vous ne pouvez plus sélectionner ce profil pour aucune règle ILM. Vous ne pouvez pas réactiver un profil désactivé.
- Si StorageGRID ne parvient pas à 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 de réessayer le processus de désactivation.

Configurer les régions (facultatif et S3 uniquement)

Les règles ILM peuvent filtrer les objets en fonction des régions dans lesquelles les compartiments S3 sont créés, vous permettant de stocker des objets 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 qui peuvent être utilisées par les compartiments de votre système.



Vous ne pouvez pas modifier la région d'un bucket une fois celui-ci créé.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "[navigateur Web pris en charge](#)".
- Tu as "[autorisations d'accès spécifiques](#)".

À propos de cette tâche

Lors de la création d'un bucket S3, vous pouvez spécifier que le bucket soit créé dans une région spécifique. La spécification d'une région permet au bucket d'être géographiquement proche de ses utilisateurs, ce qui peut aider à optimiser la latence, à minimiser les coûts et à répondre aux exigences réglementaires.

Lorsque vous créez une règle ILM, vous souhaitez peut-être 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 le `us-west-2` région. Vous pouvez ensuite spécifier que des copies de ces objets soient placées sur des nœuds de stockage sur un site de centre de données dans cette région pour optimiser la latence.

Lors de la configuration des régions, suivez ces instructions :

- Par défaut, tous les buckets sont considérés comme appartenant au `us-east-1` région.
- Vous devez créer les régions à l'aide du gestionnaire de grille avant de pouvoir spécifier une région non par défaut lors de la création de compartiments à l'aide de l'API Tenant Manager ou Tenant Management ou avec l'élément de demande `LocationConstraint` pour les demandes d'API S3 PUT Bucket. Une erreur se produit si une demande PUT Bucket utilise une région qui n'a pas été définie dans StorageGRID.
- Vous devez utiliser le nom exact de la région lorsque vous créez le bucket S3. Les noms de région sont sensibles à la casse. Les caractères valides sont les chiffres, les lettres et les traits d'union.



EU n'est pas considéré comme un alias pour eu-west-1. Si vous souhaitez utiliser la région UE ou eu-ouest-1, vous devez utiliser le nom exact.

- Vous ne pouvez pas supprimer ou modifier une région si elle est utilisée dans une règle attribuée à une politique (active ou inactive).
- Si vous utilisez une région non valide comme filtre avancé dans une règle ILM, vous ne pouvez pas ajouter cette règle à une stratégie.

Une région non valide peut se produire si vous utilisez une région comme filtre avancé dans une règle ILM, mais que vous supprimez ultérieurement cette région, ou si vous utilisez l'API Grid Management 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 devrez rajouter la région si vous souhaitez utiliser le filtre avancé Contrainte d'emplacement pour rechercher des objets dans ce compartiment.

Étapes

1. Sélectionnez **ILM > Régions**.

La page Régions apparaît, avec les régions actuellement définies répertoriées. **Région 1** indique la région par défaut, `us-east-1`, qui ne peut être ni modifié ni supprimé.

2. Pour ajouter une région :

- Sélectionnez **Ajouter une autre région**.
- Saisissez le nom d'une région que vous souhaitez utiliser lors de la création de buckets S3.

Vous devez utiliser ce nom de région exact comme élément de demande `LocationConstraint` lorsque

vous créez le bucket 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 une politique (active ou inactive).

4. Lorsque vous avez terminé vos modifications, sélectionnez **Enregistrer**.

Vous pouvez désormais sélectionner ces régions dans la section Filtres avancés à l'étape 1 de l'assistant Créer une règle ILM. Voir ["Utiliser des filtres avancés dans les règles ILM"](#) .

Créer une règle ILM

Utiliser les règles ILM pour gérer les objets

Pour gérer les objets, vous créez un ensemble de règles de gestion du cycle de vie des informations (ILM) et les organisez dans une politique ILM.

Chaque objet ingéré dans le système est évalué par rapport à la politique active. Lorsqu'une règle de la politique correspond aux métadonnées d'un objet, les instructions de la règle déterminent les actions que StorageGRID entreprend pour copier et stocker cet objet.



Les métadonnées des objets ne sont pas gérées par les règles ILM. Au lieu de cela, les métadonnées des objets sont stockées dans une base de données Cassandra dans ce que l'on appelle un magasin de métadonnées. Trois copies des métadonnées de l'objet sont automatiquement conservées sur chaque site pour protéger les données contre toute perte.

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'objets au fil du temps. Lorsque la période d'un placement expire, les instructions du placement suivant sont automatiquement appliquées par la prochaine évaluation ILM.
- **Comportement d'ingestion** : Le comportement d'ingestion d'une règle vous permet de choisir comment les objets filtrés par la règle sont protégés lorsqu'ils sont ingérés (lorsqu'un client S3 enregistre un objet dans la grille).

Filtrage des 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 peut n'utiliser aucun filtre. Toute règle qui n'utilise pas de filtres s'applique à tous les objets, elle doit donc être la dernière règle (par défaut) d'une stratégie 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 spécifiques ou aux deux.

Les filtres de base vous offrent un moyen simple d'appliquer différentes règles à un grand nombre d'objets. Par exemple, les dossiers financiers de votre entreprise peuvent devoir être stockés pour répondre aux exigences réglementaires, tandis que les données du service marketing peuvent devoir être stockées pour faciliter les opérations quotidiennes. Après avoir créé des comptes locataires 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 marketing.

- Les filtres avancés vous offrent un contrôle précis. 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 de localisation (S3 uniquement)
 - Taille de l'objet
 - Métadonnées de l'utilisateur
 - Balise d'objet (S3 uniquement)

Vous pouvez filtrer les objets selon des critères très spécifiques. Par exemple, les objets stockés par le service d'imagerie d'un hôpital peuvent être utilisés fréquemment lorsqu'ils ont moins de 30 jours et rarement par la suite, tandis que les objets contenant des informations sur les visites des patients peuvent devoir être copiés vers le service de facturation du siège du réseau de santé. Vous pouvez créer des filtres qui identifient chaque type d'objet en fonction du nom de l'objet, de la taille, des balises d'objet S3 ou de tout autre critère pertinent, puis créer des règles distinctes pour stocker chaque ensemble d'objets de manière appropriée.

Vous pouvez combiner des filtres selon vos besoins dans une seule règle. Par exemple, le service marketing peut souhaiter stocker des fichiers image volumineux différemment de ses enregistrements de fournisseurs, tandis que le service des ressources humaines peut avoir besoin de stocker les enregistrements du personnel dans une zone géographique spécifique et les informations de politique 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 où, quand et comment les données d'objet sont stockées. 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 placement :

- Vous commencez par spécifier l'heure de référence, qui détermine quand les instructions de placement commencent. L'heure de référence peut être celle à laquelle un objet est ingéré, celle à laquelle un objet est accédé, celle à laquelle un objet versionné devient non actuel ou une heure définie par l'utilisateur.
- Ensuite, vous spécifiez quand 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 au moment où l'objet a été ingéré.

- Enfin, vous spécifiez le type de copies (réplication ou codage d'effacement) et l'emplacement où les copies sont stockées. Par exemple, vous souhaitez peut-être stocker deux copies répliquées sur deux sites différents.

Chaque règle peut définir plusieurs emplacements pour une même période et des emplacements différents pour différentes périodes.

- Pour placer des objets à plusieurs emplacements au cours d'une même période, sélectionnez **Ajouter un autre type ou emplacement** pour ajouter plusieurs lignes pour cette période.
- Pour placer des objets à différents endroits et à différentes périodes, sélectionnez **Ajouter une autre période** pour ajouter la période suivante. Ensuite, spécifiez une ou plusieurs lignes dans la période.

L'exemple montre deux instructions de placement sur la page Définir les placements de l'assistant Créer une règle ILM.

Time period and placements Sort by start date

If you want a rule to apply only to specific objects, select **Previous** and add advanced filters. When objects are evaluated, the rule is applied if the object's metadata matches the criteria in the filter.

Time period 1
From Day store for days

Store objects by copies at ,

and store objects by using

[Add other type or location](#)
1

Time period 2
From Day store forever

Store objects by copies at

[Add other type or location](#)
2

La première instruction de placement 1 comporte deux lignes pour la première année :

- La première ligne crée deux copies d'objets répliquées sur deux sites de centres de données.
- La deuxième ligne crée une copie codée par effacement 6+3 utilisant tous les sites du centre de données.

La deuxième instruction de placement 2 crée deux copies après un an et conserve ces copies pour toujours.

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'intervalle entre les périodes que vous avez définies et que l'instruction de placement finale continue soit indéfiniment, soit jusqu'à ce que vous n'ayez plus besoin de copies d'objet.

À l'expiration de chaque période de la règle, les instructions de placement de contenu pour la période suivante sont appliquées. De nouvelles copies d'objets sont créées et toutes les copies inutiles sont supprimées.

Comportement d'ingestion de règle ILM

Le comportement d'ingestion contrôle si les copies d'objet sont immédiatement placées conformément aux instructions de la règle, ou si des copies intermédiaires sont effectuées et les instructions de placement sont appliquées ultérieurement. Les comportements d'ingestion suivants sont disponibles pour les règles ILM :

- **Équilibré** : StorageGRID tente de réaliser toutes les copies spécifiées dans la règle ILM lors de l'ingestion ; si cela n'est pas possible, des copies intermédiaires sont réalisées et le succès est renvoyé au client. Les copies spécifiées dans la règle ILM sont réalisées 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.
- **Double validation** : StorageGRID effectue immédiatement des copies intermédiaires de l'objet et renvoie la réussite au client. Les copies spécifiées dans la règle ILM sont réalisées lorsque cela est possible.

Informations connexes

- ["Options d'ingestion"](#)
- ["Avantages, inconvénients et limites des options d'ingestion"](#)
- ["Comment les règles de cohérence et de gestion des informations interagissent pour affecter la protection des données"](#)

Exemple de règle ILM

À titre d'exemple, une règle ILM pourrait spécifier ce qui suit :

- S'applique uniquement aux objets appartenant au locataire A.
- Créez deux copies répliquées de ces objets et stockez chaque copie dans un site différent.
- Conservez les deux copies « pour toujours », ce qui signifie que StorageGRID ne les supprimera pas automatiquement. Au lieu de cela, StorageGRID conservera ces objets jusqu'à ce qu'ils soient supprimés par une demande de suppression du client ou par l'expiration d'un cycle de vie de bucket.
- Utilisez l'option Équilibré pour le comportement d'ingestion : l'instruction de placement sur deux sites est appliquée dès que le locataire A enregistre un objet dans StorageGRID, sauf s'il n'est pas possible de créer immédiatement les deux copies requises.

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

Informations connexes

- ["Qu'est-ce qu'un pool de stockage"](#)
- ["Qu'est-ce qu'un pool de stockage cloud"](#)

Accéder à l'assistant Créer une règle ILM

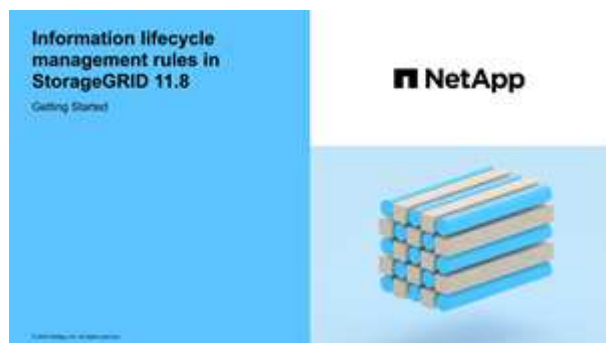
Les règles ILM vous permettent de gérer le placement des données d'objet au fil du temps. Pour créer une règle ILM, utilisez l'assistant Créer une règle ILM.



Si vous souhaitez créer la règle ILM par défaut pour une stratégie, suivez les instructions ["instructions pour créer une règle ILM par défaut"](#) plutôt.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un ["navigateur Web pris en charge"](#) .
- Tu as ["autorisations d'accès spécifiques"](#) .
- Si vous souhaitez spécifier à quels comptes locataires cette règle s'applique, vous disposez de la ["Autorisation des comptes locataires"](#) ou vous connaissez l'ID de compte pour chaque compte.
- Si vous souhaitez que la règle filtre les objets en fonction des métadonnées de l'heure du dernier accès, les mises à jour de l'heure du dernier accès doivent être activées par le compartiment S3.
- Vous avez configuré tous les pools de stockage cloud que vous prévoyez d'utiliser. Voir ["Créer un pool de stockage cloud"](#) .
- Vous connaissez le ["options d'ingestion"](#) .
- Si vous devez créer une règle conforme à utiliser avec S3 Object Lock, vous connaissez le ["exigences pour S3 Object Lock"](#) .
- En option, vous avez regardé la vidéo : ["Vidéo : aperçu des règles de l'ILM"](#) .



À propos de cette tâche

Lors de la création de règles ILM :

- Tenez compte de la topologie et des configurations de stockage du système StorageGRID .
- Tenez compte des types de copies d'objets que vous souhaitez créer (répliquées ou codées par effacement) et du nombre de copies de chaque objet requises.
- Déterminez quels types de métadonnées d'objet sont utilisés dans les applications qui se connectent au système StorageGRID . Les règles ILM filtrent les objets en fonction de leurs métadonnées.
- Réfléchissez à l'endroit où vous souhaitez que les copies d'objets soient placées au fil du temps.
- Décidez quelle option d'ingestion utiliser (validation équilibrée, stricte ou double).

Étapes

1. Sélectionnez **ILM > Règles**.
2. Sélectionnez **Créer**. ["Étape 1 \(Entrez les détails\)"](#) de l'assistant Créer une règle ILM apparaît.

Étape 1 sur 3 : Saisir les détails

L'étape **Saisir les détails** de l'assistant Créer une règle ILM vous permet de saisir 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.

À propos de cette 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 de l'objet 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 ou noms de bucket, ou des filtres avancés, tels que la taille de l'objet ou les métadonnées de l'utilisateur.

Étapes

1. Saisissez 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 la reconnaître ultérieurement.

3. Vous pouvez également sélectionner un ou plusieurs comptes de locataire S3 auxquels cette règle s'applique. 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 l'autorisation de comptes locataires, vous ne pouvez pas sélectionner de locataires dans la liste. Saisissez plutôt l'ID du locataire ou saisissez plusieurs ID sous forme de chaîne délimitée par des virgules.

4. Vous pouvez également spécifier les compartiments S3 auxquels cette règle s'applique.

Si **s'applique à tous les buckets** est sélectionné (par défaut), la règle s'applique à tous les buckets S3.

5. Pour les locataires S3, sélectionnez éventuellement **Oui** pour appliquer la règle uniquement aux anciennes versions d'objet dans les compartiments S3 pour lesquels le contrôle de version est activé.

Si vous sélectionnez **Oui**, « Heure non actuelle » sera automatiquement sélectionné pour l'heure de référence dans "[Étape 2 de l'assistant Créer une règle ILM](#)".



L'heure non actuelle s'applique uniquement aux objets S3 dans les compartiments où la gestion des versions est activée. Voir "[Opérations sur les buckets, PutBucketVersioning](#)" et "[Gérer les objets avec S3 Object Lock](#)".

Vous pouvez utiliser cette option pour réduire l'impact du stockage des objets versionnés en filtrant les versions d'objets non actuelles. Voir "[Exemple 4 : Règles et politique ILM pour les objets versionnés S3](#)".

6. Vous pouvez également sélectionner **Ajouter un filtre avancé** pour spécifier des filtres supplémentaires.

Si vous ne configurez pas de filtrage avancé, la règle s'applique à tous les objets qui correspondent aux filtres de base. Pour plus d'informations sur le filtrage avancé, voir [Utiliser des filtres avancés dans les règles ILM](#) et [Spécifier plusieurs types et valeurs de métadonnées](#).

7. Sélectionnez **Continuer**. "[Étape 2 \(Définir les emplacements\)](#)" de l'assistant Créer une règle ILM apparaît.

Utiliser des 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 un filtrage avancé pour une règle, vous sélectionnez le type de métadonnées que vous souhaitez faire correspondre, sélectionnez un opérateur et spécifiez une valeur de métadonnées. Lorsque les objets sont évalués, la règle ILM est appliquée 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 sur ou avant • est après • est sur 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 n'importe quelle règle susceptible de modifier l'emplacement d'un grand nombre d'objets existants. Définissez le temps d'ingestion comme étant supérieur ou égal à l'heure approximative à laquelle la nouvelle politique entrera en vigueur pour garantir que les objets existants ne sont pas déplacés inutilement.
Clé	• égal à • n'est pas égal à • contient • ne contient pas • commence par • ne commence pas par • se termine par • ne se termine pas avec	Tout ou partie d'une clé d'objet S3 unique. Par exemple, vous souhaitez peut-être faire correspondre des objets qui se terminent par <code>.txt</code> ou commencer par <code>test-object/</code>.
Heure du dernier accès	• est • n'est pas • est avant • est sur ou avant • est après • est sur ou après	Heure et date de la dernière récupération de l'objet (lu ou visualisé). Remarque : si vous prévoyez de "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.
Contrainte de localisation (S3 uniquement)	• égal à • n'est pas égal à	La région dans laquelle un bucket S3 a été créé. Utilisez ILM > Régions pour définir les régions affichées. Remarque : une valeur <code>us-east-1</code> correspondra aux objets dans les buckets créés dans la région <code>us-east-1</code> ainsi qu'aux objets dans les buckets qui n'ont aucune région spécifiée. Voir "Configurer les 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 à - moins que - inférieur ou égal à - supérieur à - supérieur ou égal à	La taille de l'objet. Le codage d'effacement est particulièrement adapté aux objets supérieurs à 1 Mo. N'utilisez pas le codage d'effacement pour les objets inférieurs à 200 Ko afin d'éviter la surcharge liée à la gestion de très petits fragments codés par effacement.
Métadonnées de l'utilisateur	- contient - se termine par - égal à - existe - commence par - ne contient pas - ne se termine pas avec - n'est pas égal à - n'existe pas - ne commence pas par	Paire clé-valeur, où Nom des métadonnées de l'utilisateur est la clé et Valeur des métadonnées est la valeur. Par exemple, pour filtrer les objets qui ont des métadonnées utilisateur de <code>color=blue</code>, préciser <code>color</code> pour Nom des métadonnées de l'utilisateur, <code>equals</code> pour l'opérateur, et <code>blue</code> pour Valeur de métadonnées. Remarque : les noms des métadonnées utilisateur ne sont pas sensibles à la casse ; les valeurs des métadonnées utilisateur sont sensibles à la casse.
Balise d'objet (S3 uniquement)	- contient - se termine par - égal à - existe - commence par - ne contient pas - ne se termine pas avec - n'est pas égal à - n'existe pas - ne commence pas par	Paire clé-valeur, où Nom de balise d'objet est la clé et Valeur de balise d'objet est la valeur. Par exemple, pour filtrer sur les objets qui ont une balise d'objet de <code>Image=True</code>, préciser <code>Image</code> pour Nom de balise d'objet, <code>equals</code> pour l'opérateur, et <code>True</code> pour valeur de balise d'objet. Remarque : les noms et les valeurs des balises d'objet sont sensibles à la casse. Vous devez saisir ces éléments exactement tels qu'ils ont été définis pour l'objet.

Spécifier plusieurs types et valeurs de métadonnées

Lorsque vous définissez un 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 **Taille de l'objet** et spécifier deux valeurs de métadonnées.

- La première valeur de métadonnées spécifie les objets supérieurs ou égaux à 10 Mo.

- La deuxième valeur de métadonnées spécifie les objets inférieurs ou égaux à 100 Mo.

Filter group 1 Objects with all of following metadata will be evaluated by this rule:

Object size greater than or equal to 10 MB

and Object size less than or equal to 100 MB

L'utilisation de plusieurs entrées vous permet d'avoir un contrôle précis sur les objets correspondants. Dans l'exemple suivant, la règle s'applique aux objets dont la valeur des métadonnées utilisateur camera_type est Marque A ou Marque B. Toutefois, la règle s'applique uniquement aux objets de marque B dont la taille est inférieure à 10 Mo.

Filter group 1 Objects with all of following metadata will be evaluated by this rule:

User metadata camera_type equals Brand A

[Add another advanced filter](#)

or **Filter group 2** Objects with all of following metadata will be evaluated by this rule:

User metadata camera_type equals Brand B

and Object size less than or equal to 10 MB

[Add another advanced filter](#)

Étape 2 sur 3 : Définir les emplacements

L'étape **Définir les emplacements** de l'assistant Créer une règle ILM vous permet de définir les instructions de placement qui déterminent la durée de stockage des objets, le type de copies (répliquées ou codées par effacement), l'emplacement de stockage et le nombre de copies.



Les captures d'écran présentées sont des exemples. Vos résultats peuvent varier en fonction de votre version de StorageGRID .

À propos de cette 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 démarrer le jour 0. Les instructions peuvent continuer indéfiniment ou jusqu'à ce que vous n'ayez plus besoin de copies d'objets.

Chaque instruction de placement peut comporter plusieurs lignes si vous souhaitez créer différents types de copies ou utiliser différents emplacements pendant 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 codée à effacement 2+1 est réalisée et sauvegardée sur un seul site.

Time period 1
From Day
0
store
for
365
days

Store objects by
replicating
1
copies at
Site 1

and store objects by
replicating
1
copies at
Site 2

Add other type or location

Time period 2
From Day
365
store
forever

Store objects by
erasure coding
using
2+1 EC scheme at Site 3

Add other type or location

Étapes

1. Pour **Heure de référence**, sélectionnez le type d'heure à utiliser lors du calcul de l'heure de début d'une instruction de placement.

Option	Description
Temps d'ingestion	Le moment où l'objet a été ingéré.
Heure du dernier accès	L'heure à laquelle l'objet a été récupéré pour la dernière fois (lu ou visualisé). Pour utiliser cette option, les mises à jour de l'heure du dernier accès doivent être activées pour le compartiment S3. "Utiliser l'heure du dernier accès dans les règles ILM" .
Heure de création définie par l'utilisateur	Une heure spécifiée dans les métadonnées définies par l'utilisateur.
Temps non actuel	« Heure non actuelle » est automatiquement sélectionné si vous avez sélectionné Oui pour la question « Appliquer cette règle uniquement aux anciennes versions d'objet (dans les compartiments S3 avec le contrôle de version activé) ? » dans "Étape 1 de l'assistant Créer une règle ILM" .

Si vous souhaitez créer une règle *conforme*, vous devez sélectionner **Heure d'ingestion**. ["Gérer les objets avec S3 Object Lock"](#) .

2. Dans la section **Période et emplacements**, saisissez une heure de début et une durée pour la première période.

Par exemple, vous souhaitez peut-être spécifier où stocker les objets pendant la première année (À partir du jour 0, stocker pendant 365 jours). Au moins une instruction doit commencer au jour 0.

3. Si vous souhaitez créer des copies répliquées :

- a. Dans la liste déroulante **Stocker les objets par**, sélectionnez **réplication**.
- b. Sélectionnez le nombre de copies que vous souhaitez réaliser.

Un avertissement apparaît si vous modifiez le nombre de copies à 1. Une règle ILM qui crée une seule copie répliquée pour une période donnée expose les données à un risque de perte permanente.

["Pourquoi vous ne devriez pas utiliser la réplication à copie unique"](#) .

Pour éviter le risque, effectuez une ou plusieurs des actions suivantes :

- Augmenter le nombre de copies pour la période.
- Ajoutez des copies à d'autres pools de stockage ou à un pool de stockage cloud.
- Sélectionnez **codage d'effacement** au lieu de **réplication**.

Vous pouvez ignorer cet avertissement en toute sécurité si cette règle crée déjà plusieurs copies pour toutes les périodes.

- c. Dans le champ **copies à**, sélectionnez les pools de stockage que vous souhaitez 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 effectuées : une copie pour chaque nœud de stockage.

L'alerte **Placement ILM irréalisable** est déclenchée pour indiquer que la règle ILM n'a pas pu être complètement appliquée.

Si vous spécifiez plusieurs pools 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 est égal 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 pour maintenir l'utilisation du disque équilibrée entre les pools, tout en garantissant qu'aucun site n'obtienne 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. Pour cette raison, ne spécifiez pas le pool de stockage Tous les nœuds de stockage (StorageGRID 11.6 et versions antérieures) et un autre pool de stockage.

4. Si vous souhaitez créer une copie à code d'effacement :

- a. Dans la liste déroulante **Stocker les objets par**, sélectionnez **codage d'effacement**.



Le codage d'effacement est particulièrement adapté aux objets supérieurs à 1 Mo. N'utilisez pas le codage d'effacement pour les objets inférieurs à 200 Ko afin d'éviter la surcharge liée à la gestion de très petits fragments codés par effacement.

- b. Si vous n'avez pas ajouté de filtre de taille d'objet pour une valeur supérieure à 200 Ko, 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 200 Ko.

- c. Sélectionnez le pool de stockage que vous souhaitez ajouter et le schéma de codage d'effacement que vous souhaitez utiliser.

L'emplacement de stockage d'une copie codée par effacement comprend le nom du schéma de codage par effacement, suivi du nom du pool de stockage.

Les schémas de codage d'effacement disponibles sont limités par le nombre de nœuds de stockage dans le pool de stockage que vous sélectionnez. **UN Recommended** Le badge apparaît à côté des schémas qui fournissent soit le ["meilleure protection ou la surcharge de stockage la plus faible"](#).

5. En option :

- a. Sélectionnez **Ajouter un autre type ou emplacement** pour créer des copies supplémentaires à différents emplacements.
- b. Sélectionnez **Ajouter une autre période** pour ajouter des périodes différentes.



Les suppressions d'objets se produisent en fonction des paramètres suivants :

- Les objets sont automatiquement supprimés à la fin de la période finale, à moins qu'une autre période ne se termine **pour toujours**.
- Selon ["paramètres de période de rétention du compartiment et du locataire"](#), les objets peuvent ne pas être supprimés même si la période de conservation ILM se termine.

6. Si vous souhaitez stocker des objets dans un pool de stockage cloud :

- a. Dans la liste déroulante **Stocker les objets par**, sélectionnez **réplication**.
- b. Sélectionnez le champ **copies à**, 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 seule instruction de placement. 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 dans un pool de stockage cloud en même temps. Un message d'erreur s'affiche si plusieurs emplacements qui utilisent un pool de stockage cloud ont des dates qui se chevauchent ou si plusieurs lignes du même emplacement utilisent un pool de stockage cloud.
- Vous pouvez stocker un objet dans un pool de stockage cloud en même temps que cet objet est stocké sous forme de copies répliquées ou codées par effacement dans StorageGRID. Cependant, vous devez inclure plus d'une ligne dans les instructions de placement pour la période, afin de pouvoir spécifier le nombre et les types de copies pour chaque emplacement.

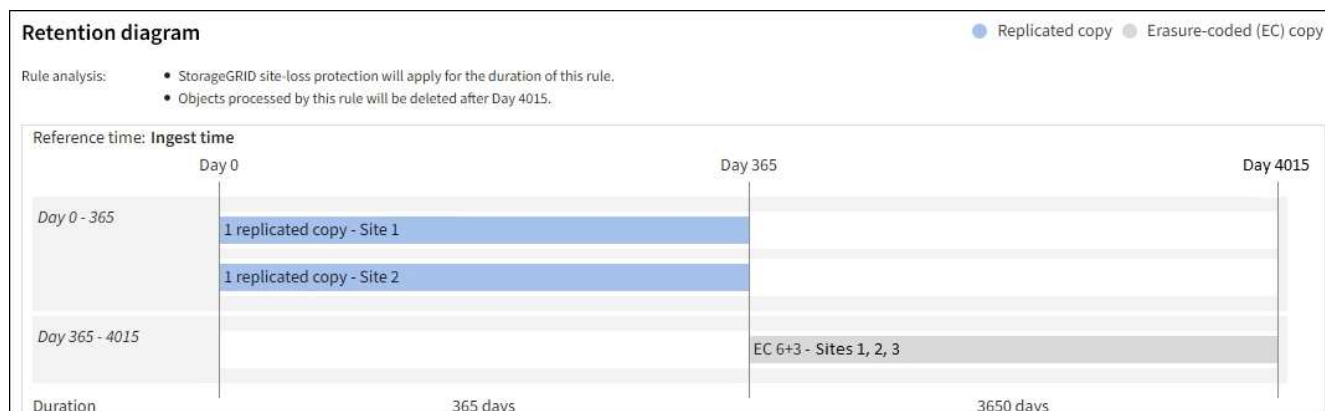
7. Dans le diagramme de rétention, confirmez vos instructions de placement.

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 et pendant 10 ans supplémentaires, une copie à code d'effacement 6+3 sera sauvegardée sur trois sites. Après 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.

Consultez ["Activer la protection contre la perte de site."](#)



- Sélectionnez **Continuer**. "[Étape 3 \(Sélectionner le comportement d'ingestion\)](#)" de l'assistant Créer une règle ILM apparaît.

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. Par exemple, vous souhaitez peut-être laisser les objets qui ont été consultés au cours des trois derniers mois sur les nœuds de stockage locaux, tout en déplaçant les objets qui n'ont pas été consultés récemment vers un emplacement hors site. Vous pouvez également utiliser l'heure du dernier accès comme filtre avancé si vous souhaitez qu'une règle ILM s'applique uniquement aux objets qui ont été consultés pour la dernière fois à une date spécifique.

À propos de cette tâche

Avant d'utiliser l'heure du dernier accès dans une règle ILM, passez en revue 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 à un objet ne déclenche pas d'évaluation ILM immédiate. Au lieu de cela, les emplacements de l'objet sont évalués et l'objet est déplacé selon les besoins lorsque l'ILM d'arrière-plan évalue l'objet. Cela peut prendre deux semaines ou plus après l'accès à l'objet.

Tenez compte de cette latence lors de la création de règles ILM basées sur l'heure du dernier accès et évitez les placements qui utilisent des périodes de temps 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 de l'heure du dernier accès sont désactivées par défaut pour les compartiments S3.



Gardez à l'esprit que l'activation des mises à jour de l'heure du dernier accès peut réduire les performances, en particulier dans les systèmes avec de petits objets. L'impact sur les performances se produit car StorageGRID doit mettre à jour les objets avec de nouveaux horodatages chaque fois que les objets sont récupérés.

Le tableau suivant résume si l'heure du dernier accès est mise à jour pour tous les objets du bucket pour différents types de demandes.

Type de demande	Si l'heure du dernier accès est mise à jour lorsque les mises à jour de l'heure du dernier accès sont désactivées	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
Demande de copie d'un objet d'un bucket 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
Demande de finalisation d'un téléchargement en plusieurs parties	Oui, pour l'objet assemblé	Oui, pour l'objet assemblé

Étape 3 sur 3 : Sélectionner le comportement d'ingestion

L'étape **Sélectionner le comportement d'ingestion** de l'assistant Créer une règle ILM vous permet de choisir comment les objets filtrés par cette règle sont protégés lorsqu'ils sont ingérés.

À propos de cette tâche

StorageGRID peut effectuer des copies intermédiaires et mettre en file d'attente les objets pour une évaluation ILM ultérieure, ou il peut effectuer des copies pour répondre immédiatement aux instructions de placement de la règle.

Étapes

1. Sélectionnez le ["comportement d'ingestion"](#) à utiliser.

Pour plus d'informations, consultez la section ["Avantages, inconvénients et limites des options d'ingestion"](#).

Vous ne pouvez pas utiliser l'option Équilibré ou Strict si la règle utilise l'un de ces placements :



- Un pool de stockage cloud au jour 0
- Un pool de stockage cloud lorsque la règle utilise une heure de création définie par l'utilisateur comme heure de référence

Voir ["Exemple 5 : Règles et politique 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 politique est activée.

Pour afficher les détails de la règle, sélectionnez le nom de la règle sur la page des règles ILM.

Créer une règle ILM par défaut

Avant de créer une stratégie ILM, vous devez créer une règle par défaut pour placer tous les objets ne correspondant pas à une autre règle dans la stratégie. La règle par défaut ne peut utiliser aucun filtre. Cela doit s'appliquer à tous les locataires, à tous les buckets 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"](#) .
- Tu as ["autorisations d'accès spécifiques"](#) .

À propos de cette tâche

La règle par défaut est la dernière règle à être évaluée dans une politique ILM, elle ne peut donc utiliser aucun filtre. Les instructions de placement pour la règle par défaut sont appliquées à tous les objets qui ne correspondent pas à une autre règle de la politique.

Dans cet exemple de politique, 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 locataires.

Proposed policy name

Example ILM policy

Reason for change

Example

Manage rules

1. Select the rules you want to add to the policy.
2. Determine the order in which the rules will be evaluated by dragging and dropping the rows. The default rule will be automatically placed at the end of the policy and cannot be moved.

Select rules

Rule order	Rule name	Filters
1	EC for test-tenant-1	Tenant is test-tenant-1
Default	Default rule	—

Lorsque vous créez la règle par défaut, gardez ces exigences à l'esprit :

- La règle par défaut sera automatiquement placée comme dernière règle lorsque vous l'ajouterez à une politique.
- La règle par défaut ne peut utiliser aucun filtre de base ou avancé.
- 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 à code d'effacement comme règle par défaut pour une stratégie. Les règles de codage d'effacement doivent utiliser un filtre avancé pour empêcher le codage d'effacement des objets plus petits.

- En général, la règle par défaut doit conserver les objets pour toujours.
- Si vous utilisez (ou prévoyez d'activer) le paramètre global de verrouillage d'objet S3, la règle par défaut doit être conforme.

Étapes

1. Sélectionnez **ILM > Règles**.
2. Sélectionnez **Créer**.

L'étape 1 (Saisir les détails) de l'assistant Créer une règle ILM s'affiche.

3. Saisissez 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 **Comptes locataires** vide.

La règle par défaut doit s'appliquer à tous les comptes locataires.

6. Laissez la sélection du menu déroulant Nom du bucket comme **s'applique à tous les buckets**.

La règle par défaut doit s'appliquer à tous les compartiments S3.

7. Conservez la réponse par défaut, **Non**, pour la question « Appliquer cette règle uniquement aux anciennes versions d'objet (dans les compartiments S3 avec le contrôle de version activé) ? »

8. N'ajoutez pas de filtres avancés.

La règle par défaut ne peut spécifier aucun filtre.

9. Sélectionnez **Suivant**.

L'étape 2 (Définir les emplacements) apparaît.

10. Pour l'heure de référence, sélectionnez n'importe quelle option.

Si vous avez conservé la réponse par défaut, **Non**, pour la question « Appliquer cette règle uniquement aux anciennes versions d'objet ? » L'heure non actuelle ne sera pas incluse dans la liste déroulante. La règle par défaut doit s'appliquer à toutes les versions d'objet.

11. Spécifiez les instructions de placement pour la règle par défaut.

- La règle par défaut doit conserver les objets pour toujours. Un avertissement s'affiche lorsque vous activez une nouvelle politique si la règle par défaut ne conserve pas les objets pour toujours. Vous devez confirmer qu'il s'agit du comportement que vous attendez.
- La règle par défaut doit créer des copies répliquées.



N'utilisez pas de règle qui crée des copies à code d'effacement comme règle par défaut pour une stratégie. Les règles de codage d'effacement doivent inclure le filtre avancé **Taille de l'objet (Mo) supérieure à 200 Ko** pour empêcher le codage d'effacement des objets plus petits.

- Si vous utilisez (ou prévoyez d'activer) le paramètre global de verrouillage d'objet S3, la règle par défaut doit être conforme :
 - Il doit créer au moins deux copies d'objet répliquées ou une copie à 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'objets ne peuvent pas être enregistrées dans un pool de stockage cloud.
 - 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 « pour toujours ».

12. Consultez le diagramme de rétention pour confirmer vos instructions de placement.

13. Sélectionnez **Continuer**.

L'étape 3 (Sélectionner le comportement d'ingestion) apparaît.

14. Sélectionnez l'option d'ingestion à utiliser et sélectionnez **Créer**.

Gérer les politiques ILM

Utiliser les politiques ILM

Une politique de gestion du cycle de vie des informations (ILM) est un ensemble ordonné de règles ILM qui détermine la manière dont le système StorageGRID gère les données des objets au fil du temps.



Une stratégie ILM mal configurée peut entraîner une perte de données irrécupérable. Avant d'activer une stratégie ILM, examinez attentivement la stratégie ILM et ses règles ILM, puis simulez la stratégie ILM. Confirmez toujours que la politique ILM fonctionnera comme prévu.

Politique ILM par défaut

Lorsque vous installez StorageGRID et ajoutez des sites, une stratégie ILM par défaut est automatiquement créée, comme suit :

- Si votre grille contient un site, la politique 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.

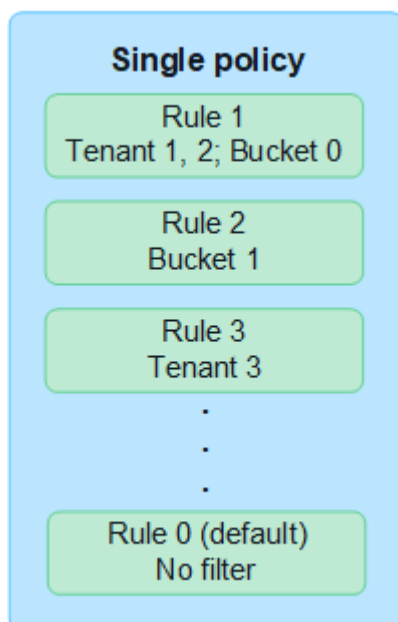
Si la politique par défaut ne répond pas à vos besoins de stockage, vous pouvez créer vos propres règles et politiques. Voir "[Créer une règle ILM](#)" et "[Créer une politique ILM](#)".

Une ou plusieurs politiques ILM actives ?

Vous pouvez avoir une ou plusieurs politiques ILM actives à la fois.

Une politique

Si votre grille utilise un schéma de protection des données simple avec quelques règles spécifiques au locataire et au bucket, utilisez une seule politique ILM active. Les règles ILM peuvent contenir des filtres pour gérer différents buckets ou locataires.



Lorsque vous n'avez qu'une seule politique et que les exigences d'un locataire changent, vous devez créer une nouvelle politique ILM ou cloner la politique existante pour appliquer les modifications, simuler, puis activer la nouvelle politique ILM. Les modifications apportées à la politique ILM peuvent entraîner des déplacements d'objets qui peuvent prendre plusieurs jours et provoquer une latence du système.

Politiques multiples

Pour offrir différentes options de qualité de service aux locataires, vous pouvez avoir plusieurs politiques actives à la fois. Chaque politique peut gérer des locataires, des compartiments S3 et des objets spécifiques. Lorsque vous appliquez ou modifiez une stratégie pour un ensemble spécifique de locataires ou d'objets, les stratégies appliquées aux autres locataires et objets ne sont pas affectées.

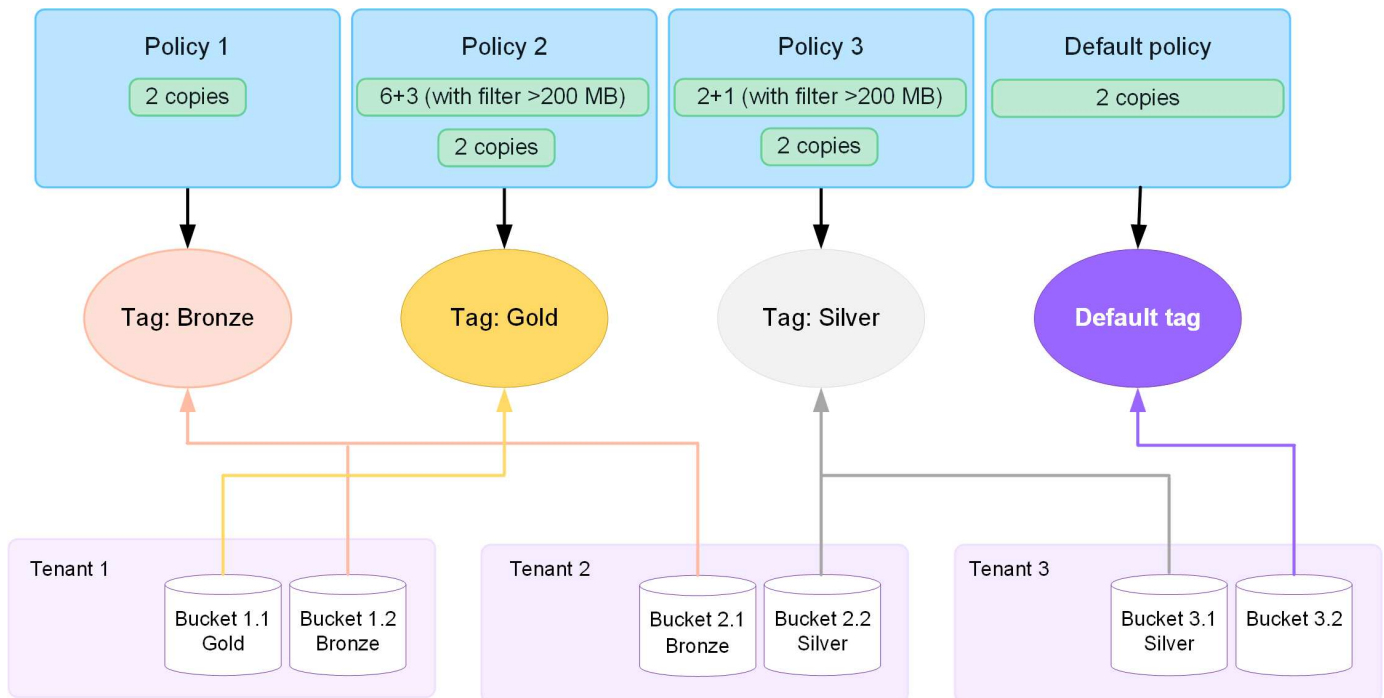
Balises de politique ILM

Si vous souhaitez permettre aux locataires de basculer facilement entre plusieurs politiques de protection des données pour chaque compartiment, utilisez plusieurs politiques ILM avec des *balises de politique ILM*. Vous attribuez chaque stratégie ILM à une balise, puis les locataires balisent un bucket pour appliquer la stratégie à ce bucket. Vous pouvez définir des balises de stratégie ILM uniquement sur les compartiments S3.

Par exemple, vous pouvez avoir trois balises nommées Or, Argent et Bronze. Vous pouvez attribuer une politique ILM à chaque balise, en fonction de la durée et de l'endroit où cette politique stocke les objets. Les locataires peuvent choisir la politique à utiliser en étiquetant leurs seaux. Un bucket étiqueté Gold est géré par la politique Gold et reçoit le niveau Gold de protection des données et de performance.

Balise de politique ILM par défaut

Une balise de stratégie ILM par défaut est automatiquement créée lorsque vous installez StorageGRID. Chaque grille doit avoir une politique active attribuée à la balise par défaut. La politique par défaut s'applique à tous les buckets S3 non balisés.



Comment une politique ILM évalue-t-elle les objets ?

Une politique ILM active contrôle le placement, la durée et la protection des données des objets.

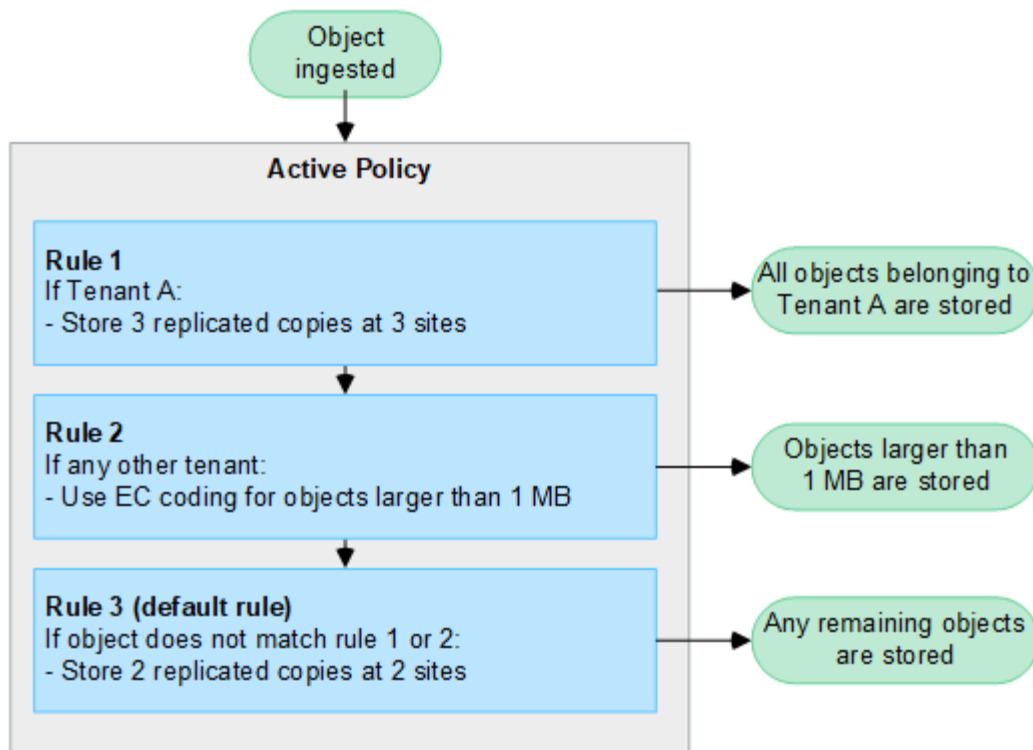
Lorsque les clients enregistrent des objets dans StorageGRID, les objets sont évalués par rapport à l'ensemble ordonné de règles ILM dans la politique, comme suit :

1. Si les filtres de la première règle de la politique correspondent à un objet, l'objet est ingéré selon le comportement d'ingestion de cette règle et stocké selon les 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 suivante de la politique jusqu'à ce qu'une correspondance soit établie.
3. Si aucune règle ne correspond à un objet, le comportement d'ingestion et les instructions de placement de la règle par défaut dans la politique sont appliqués. La règle par défaut est la dernière règle d'une politique. La règle par défaut doit s'appliquer à tous les locataires, à tous les buckets S3 et à toutes les versions d'objet, et ne peut utiliser aucun filtre avancé.

Exemple de politique ILM

À titre d'exemple, une politique ILM pourrait contenir trois règles ILM qui spécifient les éléments suivants :

- **Règle 1 : Copies dupliquées 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 : Codage d'effacement pour les objets supérieurs à 1 Mo**
 - Faites correspondre tous les objets des autres locataires, mais uniquement s'ils sont supérieurs à 1 Mo. Ces objets plus grands sont stockés à l'aide du codage d'effacement 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)**
 - Il s'agit de la dernière règle par défaut de la politique. N'utilise pas de filtres.
 - Créez deux copies répliquées de tous les objets ne correspondant pas à la règle 1 ou à la règle 2 (objets n'appartenant pas au locataire A et dont la taille est de 1 Mo ou moins).



Quelles sont les politiques actives et inactives ?

Chaque système StorageGRID doit avoir au moins une politique ILM active. Si vous souhaitez avoir plusieurs stratégies ILM actives, créez des balises de stratégie ILM et attribuez une stratégie à chaque balise. Les locataires appliquent ensuite des balises aux compartiments S3. La politique par défaut est appliquée à tous les objets des compartiments auxquels aucune balise de politique n'est attribuée.

Lorsque vous créez une stratégie ILM pour la première fois, vous sélectionnez une ou plusieurs règles ILM et les organisez dans un ordre spécifique. Après avoir simulé la politique pour confirmer son comportement, vous l'activez.

Lorsque vous activez une stratégie ILM, StorageGRID utilise cette stratégie pour gérer tous les objets, y compris les objets existants et les objets nouvellement ingérés. Les objets existants peuvent être déplacés vers de nouveaux emplacements lorsque les règles ILM de la nouvelle politique sont implémentées.

Si vous activez plusieurs stratégies ILM à la fois et que les locataires appliquent des balises de stratégie aux compartiments S3, les objets de chaque compartiment sont gérés en fonction de la stratégie attribuée à la balise.

Un système StorageGRID suit l'historique des politiques qui ont été activées ou désactivées.

Considérations pour la création d'une politique ILM

- Utilisez uniquement la politique fournie par le système, la politique de base 2 copies, dans les systèmes de test. Pour StorageGRID 11.6 et les versions antérieures, la règle Créer 2 copies de cette stratégie utilise le pool de stockage Tous les nœuds de stockage, qui contient tous les sites. Si votre système StorageGRID possède plusieurs sites, deux copies d'un objet peuvent être placées 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 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 susceptibles d'être ingérés dans votre grille. Assurez-vous que la politique inclut des règles pour faire correspondre et placer ces objets comme requis.
- Gardez la politique ILM aussi simple que possible. Cela évite les situations potentiellement 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 politique sont dans le bon ordre. Lorsque la politique est activée, les objets nouveaux et existants sont évalués par les règles dans l'ordre répertorié, en commençant par le haut. Par exemple, si la première règle d'une politique 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 avec une autre règle, la règle par défaut contrôle où cet objet est placé et pendant combien de temps il est conservé.
- Avant d'activer une nouvelle politique, examinez toutes les modifications que la politique apporte au placement des objets existants. La modification de l'emplacement d'un objet existant peut entraîner des problèmes de ressources temporaires lorsque les nouveaux emplacements sont évalués et mis en œuvre.

Créer des politiques ILM

Créez une ou plusieurs politiques ILM pour répondre à vos exigences de qualité de service.

Disposer d'une seule politique ILM active vous permet d'appliquer les mêmes règles ILM à tous les locataires et compartiments.

Le fait de disposer de plusieurs stratégies ILM actives vous permet d'appliquer les règles ILM appropriées à des locataires et des compartiments spécifiques pour répondre à plusieurs exigences de qualité de service.

Créer une politique ILM

À propos de cette tâche

Avant de créer votre propre politique, vérifiez que le "[politique ILM par défaut](#)" ne répond pas à vos besoins de stockage.



Utilisez uniquement les politiques fournies par le système, 2 copies de politique (pour les grilles à un seul site) ou 1 copie par site (pour les grilles multi-sites), dans les systèmes de test. Pour StorageGRID 11.6 et les versions antérieures, la règle par défaut de cette stratégie utilise le pool de stockage Tous les nœuds de stockage, qui contient tous les sites. Si votre système StorageGRID possède plusieurs sites, deux copies d'un objet peuvent être placées sur le même site.



Si le ["le paramètre global de verrouillage des objets S3 a été activé"](#) , vous devez vous assurer que la politique ILM est conforme aux exigences des buckets pour lesquels le verrouillage d'objet S3 est activé. Dans cette section, suivez les instructions qui mentionnent l'activation du verrouillage d'objet S3.

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"](#) .
- Tu as ["règles ILM créées"](#) selon que le verrouillage d'objet S3 est activé.

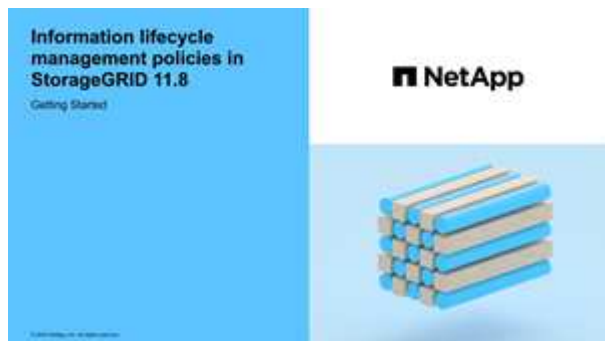
Le verrouillage des objets S3 n'est pas activé

- Tu as ["créé les règles ILM"](#) vous souhaitez ajouter à la politique. Si nécessaire, vous pouvez enregistrer une politique, créer des règles supplémentaires, puis modifier la politique pour ajouter les nouvelles règles.
- Tu as ["créé une règle ILM par défaut"](#) qui ne contient aucun filtre.

Verrouillage d'objet S3 activé

- Le ["le paramètre global de verrouillage des objets S3 est déjà activé"](#) pour le système StorageGRID .
- Tu as ["créé les règles ILM conformes et non conformes"](#) vous souhaitez ajouter à la politique. Si nécessaire, vous pouvez enregistrer une politique, créer des règles supplémentaires, puis modifier la politique pour ajouter les nouvelles règles.
- Tu as ["créé une règle ILM par défaut"](#) pour la politique qui est conforme.

- En option, vous avez regardé la vidéo : ["Vidéo : Présentation des politiques ILM"](#)



Voir aussi ["Utiliser les politiques ILM"](#) .

Étapes

1. Sélectionnez **ILM > Politiques**.

Si le paramètre global de verrouillage d'objet S3 est activé, la page des stratégies ILM indique quelles règles ILM sont conformes.

2. Déterminez comment vous souhaitez créer la politique ILM.

Créer une nouvelle politique

- a. Sélectionnez **Créer une politique**.

Cloner la politique existante

- a. Cochez la case correspondant à la politique avec laquelle vous souhaitez commencer, puis sélectionnez **Cloner**.

Modifier la politique existante

- a. Si une politique est inactive, vous pouvez la modifier. Cochez la case correspondant à la politique inactive avec laquelle vous souhaitez commencer, puis sélectionnez **Modifier**.

3. Dans le champ **Nom de la politique**, saisissez un nom unique pour la politique.
4. Si vous le souhaitez, dans le champ **Raison du changement**, saisissez la raison pour laquelle vous créez une nouvelle politique.
5. Pour ajouter des règles à la politique, sélectionnez **Sélectionner les règles**. Sélectionnez un nom de règle pour afficher les paramètres de cette règle.

Si vous clonez une politique :

- Les règles utilisées par la politique que vous clonez sont sélectionnées.
- Si la politique que vous clonez utilisait des règles sans filtres qui n'étaient 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 règle, vous pouvez déplacer la règle à la fin de la nouvelle politique.

Le verrouillage des objets S3 n'est pas activé

- a. Sélectionnez une règle par défaut pour la politique. Pour créer une nouvelle règle par défaut, sélectionnez **Page de règles ILM**.

La règle par défaut s'applique à tous les objets qui ne correspondent pas à une autre règle de la politique. La règle par défaut ne peut utiliser aucun filtre et est toujours évaluée en dernier.



N'utilisez pas la règle « Créer 2 copies » comme règle par défaut pour une stratégie. La règle Créer 2 copies utilise un pool de stockage unique, Tous les nœuds de stockage, qui contient tous les sites. Si votre système StorageGRID possède plusieurs sites, deux copies d'un objet peuvent être placées sur le même site.

Verrouillage d'objet S3 activé

- a. Sélectionnez une règle par défaut pour la politique. Pour créer une nouvelle règle par défaut, sélectionnez **Page de règles ILM**.

La liste des règles contient uniquement les règles conformes et n'utilise aucun filtre.



N'utilisez pas la règle « Créer 2 copies » comme règle par défaut pour une stratégie. La règle Créer 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.

- b. Si vous avez besoin d'une règle « par défaut » différente pour les objets dans les 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 souhaitez peut-être utiliser un pool de stockage cloud pour stocker des objets dans des buckets pour lesquels le verrouillage d'objet S3 n'est pas activé.



Vous ne pouvez sélectionner qu'une seule règle non conforme qui n'utilise pas de filtre.

Voir aussi ["Exemple 7 : Politique ILM conforme pour le verrouillage d'objet S3"](#) .

6. Lorsque vous avez terminé de sélectionner la règle par défaut, sélectionnez **Continuer**.
7. Pour l'étape Autres règles, sélectionnez toutes les autres règles que vous souhaitez ajouter à la politique. Ces règles utilisent au moins un filtre (compte locataire, nom de bucket, filtre avancé ou heure de référence non actuelle). Sélectionnez ensuite **Sélectionner**.

La fenêtre Créer une politique répertorie désormais les règles que vous avez sélectionnées. La règle par défaut se trouve 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 comme avant-dernière règle de la politique.



Un avertissement apparaît si une règle ne conserve pas les objets pour toujours. Lorsque vous activez cette stratégie, vous devez confirmer que vous souhaitez que StorageGRID supprime les objets lorsque les instructions de placement de la règle par défaut expirent (à moins qu'un cycle de vie de compartiment ne conserve les objets pendant une période plus longue).

8. 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 non plus déplacer la règle « par défaut » non conforme si elle a été sélectionnée.



Vous devez confirmer que les règles ILM sont dans le bon ordre. Lorsque la politique est activée, les objets nouveaux et existants sont évalués par les règles dans l'ordre répertorié, en commençant par le haut.

9. Si nécessaire, sélectionnez **Sélectionner des règles** pour ajouter ou supprimer des règles.
10. Lorsque vous avez terminé, sélectionnez **Enregistrer**.
11. Répétez ces étapes pour créer des stratégies ILM supplémentaires.
12. [Simuler une politique ILM](#) . Vous devez toujours simuler une politique avant de l'activer pour vous assurer qu'elle fonctionne comme prévu.

Simuler une politique

Simulez une politique sur des objets de test avant d'activer la politique et de l'appliquer à vos données de production.

Avant de commencer

- Vous connaissez le bucket/la clé d'objet S3 pour chaque objet que vous souhaitez tester.

Étapes

1. En utilisant un client S3 ou le "[Console S3](#)" , ingérer les objets nécessaires pour tester chaque règle.
2. Sur la page des politiques ILM, cochez la case correspondant à la politique, puis sélectionnez **Simuler**.
3. Dans le champ **Objet**, saisissez le S3 bucket/object-key pour un objet de test. Par exemple :
bucket-01/filename.png .
4. Si le contrôle de version S3 est activé, saisissez éventuellement un ID de version pour l'objet dans le champ **ID de version**.
5. Sélectionnez **Simuler**.
6. Dans la section Résultats de la simulation, confirmez que chaque objet correspond à la règle correcte.
7. Pour déterminer quel pool de stockage ou quel profil de codage d'effacement est en vigueur, sélectionnez le nom de la règle correspondante pour accéder à la page des détails de la règle.



Examinez toutes les modifications apportées au placement des objets répliqués et codés par effacement existants. La modification de l'emplacement d'un objet existant peut entraîner des problèmes de ressources temporaires lorsque les nouveaux emplacements sont évalués et mis en œuvre.

Résultats

Toutes les modifications apportées aux règles de la politique seront reflétées dans les résultats de la simulation et afficheront la nouvelle correspondance et la correspondance précédente. La fenêtre de stratégie Simuler conserve les objets que vous avez testés jusqu'à ce que vous sélectionniez **Effacer tout** ou l'icône de suppression  pour chaque objet dans la liste des résultats de simulation.

Informations connexes

["Exemples de simulations de politiques ILM"](#)

Activer une politique

Lorsque vous activez une nouvelle stratégie ILM unique, les objets existants et les objets nouvellement ingérés sont gérés par cette stratégie. Lorsque vous activez plusieurs stratégies, les balises de stratégie ILM attribuées aux compartiments déterminent les objets à gérer.

Avant d'activer une nouvelle politique :

1. Simulez la politique pour confirmer qu'elle se comporte comme prévu.
2. Examinez toutes les modifications apportées au placement des objets répliqués et codés par effacement existants. La modification de l'emplacement d'un objet existant peut entraîner des problèmes de ressources temporaires lorsque les nouveaux emplacements sont évalués et mis en œuvre.



Des erreurs dans une politique ILM peuvent entraîner une perte de données irrécupérable.

À propos de cette tâche

Lorsque vous activez une politique ILM, le système distribue la nouvelle politique à tous les nœuds. Toutefois, la nouvelle politique active pourrait ne pas prendre effet tant que tous les nœuds de la grille ne seront pas disponibles pour recevoir la nouvelle politique. Dans certains cas, le système attend d'implémenter une nouvelle politique active pour garantir que les objets de la grille ne sont pas supprimés accidentellement. Spécifiquement:

- Si vous apportez des modifications de politique qui **augmentent la redondance ou la durabilité des données**, ces modifications sont mises en œuvre immédiatement. Par exemple, si vous activez une nouvelle politique qui inclut une règle à trois copies au lieu d'une règle à deux copies, cette politique sera mise en œuvre immédiatement car elle augmente la redondance des données.
- Si vous apportez des modifications de politique qui **pourraient réduire la redondance ou la durabilité des données**, ces modifications ne seront pas mises en œuvre tant que tous les nœuds de la grille ne seront pas disponibles. Par exemple, si vous activez une nouvelle politique qui utilise une règle à deux copies au lieu d'une règle à trois copies, la nouvelle politique apparaîtra dans l'onglet Politique active, mais elle ne prendra effet que lorsque tous les nœuds seront en ligne et disponibles.

Étapes

Suivez les étapes pour activer une ou plusieurs politiques :

Activer une politique

Suivez ces étapes si vous n'avez qu'une seule politique active. Si vous disposez déjà d'une ou plusieurs politiques actives et que vous activez des politiques supplémentaires, suivez les étapes pour activer plusieurs politiques.

1. Lorsque vous êtes prêt à activer une politique, sélectionnez **ILM > Politiques**.

Vous pouvez également activer une seule politique à partir de la page **ILM > Balises de politique**.

2. Dans l'onglet Politiques, cochez la case correspondant à la politique que vous souhaitez activer, puis sélectionnez **Activer**.
3. Suivez l'étape appropriée :
 - Si un message d'avertissement vous invite à confirmer que vous souhaitez activer la politique, sélectionnez **OK**.
 - Si un message d'avertissement contenant des détails sur la politique s'affiche :
 - i. Passez en revue les détails pour vous assurer que la politique gérera les données comme prévu.
 - ii. Si la règle par défaut stocke les objets pendant un nombre limité de jours, examinez le diagramme de rétention, puis saisissez ce nombre de jours dans la zone de texte.
 - iii. Si la règle par défaut stocke les objets pour toujours, mais qu'une ou plusieurs autres règles ont une conservation limitée, saisissez **oui** dans la zone de texte.
 - iv. Sélectionnez **Activer la politique**.

Activer plusieurs politiques

Pour activer plusieurs politiques, vous devez créer des balises et attribuer une politique à chaque balise.



Lorsque plusieurs balises sont utilisées, si les locataires réaffectent fréquemment les balises de stratégie aux compartiments, les performances de la grille peuvent être affectées. Si vous avez des locataires non approuvés, envisagez d'utiliser uniquement la balise par défaut.

1. Sélectionnez **ILM > Balises de politique**.
2. Sélectionnez **Créer**.
3. Dans la boîte de dialogue Créer une balise de stratégie, saisissez un nom de balise et, éventuellement, une description pour la balise.



Les noms et descriptions des balises sont visibles par les locataires. Choisissez des valeurs qui aideront les locataires à prendre une décision éclairée lors de la sélection des balises de stratégie à attribuer à leurs compartiments. Par exemple, si la politique attribuée supprime des objets après une période donnée, vous pouvez le communiquer dans la description. N'incluez pas d'informations sensibles dans ces champs.

4. Sélectionnez **Créer une balise**.
5. Dans le tableau des balises de stratégie ILM, utilisez le menu déroulant pour sélectionner une stratégie à attribuer à la balise.
6. Si des avertissements apparaissent dans la colonne Limitations de la politique, sélectionnez **Afficher les détails de la politique** pour consulter la politique.

7. Assurez-vous que chaque politique gère les données comme prévu.
8. Sélectionnez **Activer les politiques attribuées**. Ou sélectionnez **Effacer les modifications** pour supprimer l'attribution de stratégie.
9. Dans la boîte de dialogue Activer les stratégies avec de nouvelles balises, examinez les descriptions de la manière dont chaque balise, stratégie et règle gèrera les objets. Apportez les modifications nécessaires pour garantir que les politiques géreront les objets comme prévu.
10. Lorsque vous êtes sûr de vouloir activer les politiques, saisissez **oui** dans la zone de texte, puis sélectionnez **Activer les politiques**.

Informations connexes

"Exemple 6 : Modification d'une politique ILM"

Exemples de simulations de politiques ILM

Les exemples de simulations de politiques ILM fournissent des lignes directrices pour structurer et modifier les simulations pour votre environnement.

Exemple 1 : Vérifier les règles lors de la simulation d'une politique ILM

Cet exemple décrit comment vérifier les règles lors de la simulation d'une politique.

Dans cet exemple, la **politique ILM d'exemple** est simulée sur les objets ingérés dans deux buckets. La politique comprend trois règles, comme suit :

- La première règle, **Deux copies, deux ans pour le bucket-a**, s'applique uniquement aux objets du bucket-a.
- La deuxième règle, **objets EC > 1 Mo**, s'applique à tous les buckets mais filtre sur les 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 courante.

Après avoir simulé la politique, confirmez que chaque objet correspond à la règle correcte.

Simulation results				
Use this table to confirm the results of applying this policy to the selected objects.				
Clear all				
Object	Version ID	Rule matched	Previous match	Actions
bucket-a/bucket-a object.pdf	—	Two copies, two years for bucket-a	—	
bucket-b/test object greater than 1 MB.pdf	—	EC objects > 1 MB	—	
bucket-b/test object less than 1 MB.pdf	—	Two copies, two data centers	—	

Dans cet exemple :

- bucket-a/bucket-a object.pdf`correspondait correctement à la première règle, qui filtre sur les objets dans `bucket-a`.
- bucket-b/test object greater than 1 MB.pdf`est dans `bucket-b`, donc cela ne correspondait pas à la première règle. Au lieu de cela, il a été correctement mis en correspondance par la deuxième règle, qui filtre les objets supérieurs à 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 n'inclut aucun filtre.

Exemple 2 : Réorganiser les règles lors de la simulation d'une stratégie ILM

Cet exemple montre comment vous pouvez réorganiser les règles pour modifier les résultats lors de la simulation d'une politique.

Dans cet exemple, la politique **Démo** est simulée. Cette politique, qui vise à rechercher les objets possédant des métadonnées utilisateur series=x-men, comprend trois règles, comme suit :

- La première règle, **PNGs**, filtre les noms de clés qui se terminent par .png .
- La deuxième règle, **X-men**, s'applique uniquement aux objets du locataire A et filtre pour series=x-men métadonnées utilisateur.
- La dernière règle, **Deux copies de 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 politique, sélectionnez **Simuler**.
2. Dans le champ **Objet**, saisissez le bucket/la clé d'objet S3 pour un objet de test et sélectionnez **Simuler**.

Les résultats de la simulation apparaissent, montrant que le Havok.png l'objet correspondait à la règle **PNGs**.

Simulation results				
Use this table to confirm the results of applying this policy to the selected objects.				
Clear all ?				
Object	Version ID	Rule matched	Previous match	Actions
photos/Havok.png	—	PNGs	—	X

Cependant, Havok.png était censé tester la règle des **X-men**.

3. Pour résoudre le problème, réorganisez les règles.
 - a. Sélectionnez **Terminer** pour fermer la fenêtre Simuler la politique ILM.
 - b. Sélectionnez **Modifier** pour modifier la politique.
 - c. Faites glisser la règle **X-men** vers le haut de la liste.
 - d. Sélectionnez **Enregistrer**.
4. Sélectionnez **Simuler**.

Les objets que vous avez précédemment testés sont réévalués par rapport à la politique mise à jour et les

nouveaux résultats de simulation sont affichés. Dans l'exemple, la colonne Règle correspondante montre que la `Havok.png` l'objet correspond désormais à la règle de métadonnées X-men, comme prévu. La colonne Correspondance précédente indique que la règle PNG correspond à l'objet dans la simulation précédente.

Simulation results				
Use this table to confirm the results of applying this policy to the selected objects.				
Clear all ?				
Object	Version ID	Rule matched ?	Previous match ?	Actions
photos/Havok.png	—	X-men	PNGs	X

Exemple 3 : Corriger une règle lors de la simulation d'une politique ILM

Cet exemple montre comment simuler une politique, corriger une règle dans la politique et continuer la simulation.

Dans cet exemple, la politique **Démo** est simulée. Cette politique vise à trouver des objets qui ont `series=x-men` métadonnées utilisateur. Cependant, des résultats inattendus se sont produits lors de la simulation de cette politique par rapport à la `Beast.jpg` objet. Au lieu de correspondre à la règle de métadonnées X-men, l'objet correspond à la règle par défaut, Deux copies de deux centres de données.

Simulation results				
Use this table to confirm the results of applying this policy to the selected objects.				
Clear all ?				
Object	Version ID	Rule matched ?	Previous match ?	Actions
photos/Beast.jpg	—	Two copies two data centers	—	X

Lorsqu'un objet de test ne correspond pas à la règle attendue dans la politique, vous devez examiner chaque règle de la politique et corriger les erreurs.

Étapes

1. Sélectionnez **Terminer** pour fermer la boîte de dialogue Simuler la politique. Sur la page des détails de la politique, sélectionnez **Diagramme de rétention**. Sélectionnez ensuite **Développer tout** ou **Afficher les détails** pour chaque règle selon vos besoins.
2. Consultez le compte locataire de la règle, l'heure de référence et les critères de filtrage.

À titre d'exemple, supposons 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 politique, vous pouvez soit cloner la règle, soit supprimer la règle de la politique, puis la modifier.
 - Si la règle fait partie de la politique active, vous devez cloner la règle. Vous ne pouvez pas modifier ou supprimer une règle de la politique active.

4. Effectuez à nouveau la simulation.

Dans cet exemple, la règle corrigée des X-men correspond désormais à la `Beast.jpg` objet basé sur le `series=x-men` métadonnées utilisateur, comme prévu.

Simulation results				
Use this table to confirm the results of applying this policy to the selected objects.				
Clear all 				
Object 	Version ID 	Rule matched  	Previous match  	Actions
photos/Beast.jpg	—	X-men	—	

Gérer les balises de politique ILM

Vous pouvez afficher les détails des balises de stratégie ILM, modifier une balise ou supprimer une balise.

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"](#).

Afficher les détails de la balise de politique ILM

Pour afficher les détails d'une balise :

1. Sélectionnez **ILM > Balises de politique**.
2. Sélectionnez le nom de la politique dans le tableau. La page de détails de la balise apparaît.
3. Sur la page des détails, consultez l'historique précédent des politiques attribuées.
4. Consultez une politique en la sélectionnant.

Modifier la balise de politique ILM



Les noms et descriptions des balises sont visibles par les locataires. Choisissez des valeurs qui aideront les locataires à prendre une décision éclairée lors de la sélection des balises de stratégie à attribuer à leurs compartiments. Par exemple, si la politique attribuée supprime des objets après une période donnée, vous pouvez le communiquer dans la description. N'incluez pas d'informations sensibles dans ces champs.

Pour modifier la description d'une balise existante :

1. Sélectionnez **ILM > Balises de politique**.
2. Cochez la case correspondant à la balise, puis sélectionnez **Modifier**.

Vous pouvez également sélectionner le nom de la balise. La page de détails de la balise apparaît et vous pouvez sélectionner **Modifier** sur cette page.

3. Modifiez la description de la balise selon vos besoins

4. Sélectionnez **Enregistrer**.

Supprimer la balise de politique ILM

Lorsque vous supprimez une balise de stratégie, la stratégie par défaut sera appliquée à tous les compartiments auxquels cette balise est attribuée.

Pour supprimer une balise :

1. Sélectionnez **ILM > Balises de politique**.
2. Cochez la case correspondant à la balise, puis sélectionnez **Supprimer**. Une boîte de dialogue de confirmation apparaît.

Vous pouvez également sélectionner le nom de la balise. La page de détails de la balise apparaît et vous pouvez sélectionner **Supprimer** sur cette page.

3. Sélectionnez **Oui** pour supprimer la balise.

Vérifier une politique ILM avec la recherche de métadonnées d'objet

Après avoir activé une stratégie ILM, ingérez des objets de test représentatifs dans le système StorageGRID , puis effectuez une recherche de métadonnées d'objet pour confirmer que les copies sont effectuées comme prévu et placées aux emplacements corrects.

Avant de commencer

Vous disposez d'un identifiant d'objet, qui peut être l'un des suivants : * **UUID** : l'identifiant unique universel de l'objet. * **CBID** : l'identifiant unique de l'objet dans StorageGRID. Vous pouvez obtenir le CBID d'un objet à partir du journal d'audit. Entrez le CBID en majuscules. * **Seau S3 et clé d'objet** : lorsqu'un objet est ingéré via l'interface S3, l'application cliente utilise une combinaison de compartiment et de clé d'objet pour stocker et identifier l'objet. Si le bucket S3 est versionné et que vous souhaitez rechercher une version spécifique d'un objet S3 à l'aide du bucket et de la clé d'objet, vous disposez de l'**ID de version**.

Étapes

1. Ingérer l'objet.
2. Sélectionnez **ILM > Recherche de métadonnées d'objet**.
3. Tapez l'identifiant de l'objet dans le champ **Identifiant**. Vous pouvez saisir un UUID, un CBID ou une clé de bucket/objet S3.
4. Si vous le souhaitez, saisissez 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 :

- Métadonnées système, telles que l'ID d'objet (UUID), le type de résultat (objet, marqueur de suppression, compartiment S3) et la taille logique de l'objet. Reportez-vous à l'exemple de capture d'écran ci-dessous pour plus de détails.
- Toutes les paires clé-valeur de métadonnées utilisateur personnalisées associées à l'objet.
- Pour les objets S3, toutes les paires clé-valeur de balise d'objet associées à l'objet.
- Pour les copies d'objets répliquées, l'emplacement de stockage actuel de chaque copie.

- Pour les copies d'objets codées par effacement, l'emplacement de stockage actuel de chaque fragment.
 - Pour les copies d'objet dans un pool de stockage Cloud, l'emplacement de l'objet, y compris le nom du bucket externe et l'identifiant unique de l'objet.
 - Pour les objets segmentés et les objets en plusieurs parties, une liste de segments d'objet comprenant les identifiants de segment et les tailles de données. Pour les objets comportant plus de 100 segments, seuls les 100 premiers segments sont affichés.
 - Toutes les métadonnées d'objet au format de stockage interne non traité. Ces métadonnées brutes incluent des métadonnées système internes dont la persistance d'une version à l'autre n'est pas garantie.
6. Confirmez que l'objet est stocké au bon emplacement ou aux bons emplacements et qu'il s'agit du bon type de copie.

Si l'option Audit est activée, vous pouvez également surveiller le journal d'audit pour le message Règles d'objet ORLM respectées. Le message d'audit ORLM peut vous fournir plus d'informations sur l'état du processus d'évaluation ILM, mais il ne peut pas vous donner 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, consultez la section "[Examiner les journaux d'audit](#)".

L'exemple suivant montre les résultats de la recherche de métadonnées d'objet pour un objet de test S3 stocké sous forme de deux copies répliquées.



La capture d'écran suivante est un exemple. Vos résultats varieront en fonction de votre version de StorageGRID .

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": {
      "PAIIS": "2",

```

Informations connexes

["Utiliser l'API REST S3"](#)

Travailler avec les politiques et les règles ILM

À mesure que vos besoins de stockage évoluent, vous devrez peut-être mettre en place des stratégies supplémentaires ou modifier les règles ILM associées à une stratégie. Vous pouvez afficher les mesures 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"](#).
- Tu as ["autorisations d'accès spécifiques"](#).

Voir les politiques ILM

Pour afficher les politiques ILM actives et inactives et l'historique d'activation des politiques :

1. Sélectionnez **ILM > Politiques**.
2. Sélectionnez **Politiques** pour afficher une liste des politiques actives et inactives. Le tableau répertorie le nom de chaque politique, les balises auxquelles la politique est attribuée et si la politique est active ou inactive.
3. Sélectionnez **Historique d'activation** pour afficher une liste des dates de début et de fin d'activation des politiques.
4. Sélectionnez un nom de politique pour afficher les détails de la politique.



Si vous affichez les détails d'une politique dont le statut est Modifié ou Supprimé, un message s'affiche expliquant que vous consultez la version de la politique qui était active pendant la période spécifiée et qui a depuis été modifiée ou supprimée.

Modifier une politique ILM

Vous ne pouvez modifier qu'une politique inactive. Si vous souhaitez modifier une politique active, désactivez-la ou créez un clone et modifiez le clone.

Pour modifier une politique :

1. Sélectionnez **ILM > Politiques**.
2. Cochez la case correspondant à la politique que vous souhaitez modifier, puis sélectionnez **Modifier**.
3. Modifiez la politique en suivant les instructions dans "[Créer des politiques ILM](#)".
4. Simulez la politique avant de la réactiver.



Une stratégie ILM mal configurée peut entraîner une perte de données irrécupérable. Avant d'activer une stratégie ILM, examinez attentivement la stratégie ILM et ses règles ILM, puis simulez la stratégie ILM. Confirmez toujours que la politique ILM fonctionnera comme prévu.

Cloner une politique ILM

Pour cloner une stratégie ILM :

1. Sélectionnez **ILM > Politiques**.
2. Cochez la case correspondant à la politique que vous souhaitez cloner, puis sélectionnez **Cloner**.
3. Créez une nouvelle politique en commençant par la politique que vous avez clonée en suivant les instructions de "[Créer des politiques ILM](#)".



Une stratégie ILM mal configurée peut entraîner une perte de données irrécupérable. Avant d'activer une stratégie ILM, examinez attentivement la stratégie ILM et ses règles ILM, puis simulez la stratégie ILM. Confirmez toujours que la politique ILM fonctionnera comme prévu.

Supprimer une politique ILM

Vous ne pouvez supprimer une politique ILM que si elle est inactive. Pour supprimer une politique :

1. Sélectionnez **ILM > Politiques**.
2. Cochez la case correspondant à la politique inactive que vous souhaitez supprimer.
3. Sélectionnez **Supprimer**.

Afficher les détails des règles ILM

Pour afficher les détails d'une règle ILM, y compris le diagramme de rétention et les instructions de placement de la règle :

1. Sélectionnez **ILM > Règles**.
2. Sélectionnez le nom de la règle dont vous souhaitez afficher les détails. Exemple:

De plus, vous pouvez utiliser la page de détails pour cloner, modifier ou supprimer une règle. Vous ne pouvez pas modifier ou supprimer une règle si elle est utilisée dans une politique.

Cloner une règle ILM

Vous pouvez cloner une règle existante si vous souhaitez créer une nouvelle règle qui utilise certains des paramètres de la règle existante. Si vous devez modifier une règle utilisée dans une politique, clonez la règle et apportez des modifications au clone. Après avoir apporté des modifications au clone, vous pouvez supprimer la règle d'origine de la stratégie et la remplacer par la version modifiée selon vos besoins.



Vous ne pouvez pas cloner une règle ILM si elle a été créée à l'aide de StorageGRID version 10.2 ou antérieure.

Étapes

1. Sélectionnez **ILM > Règles**.
2. Cochez la case correspondant à la règle que vous souhaitez cloner, puis sélectionnez **Cloner**. Vous pouvez également sélectionner le nom de la règle, puis sélectionner **Cloner** dans la page des détails de la règle.

3. Mettez à jour la règle clonée en suivant les étapes pour [modification d'une règle ILM](#) et [utiliser des filtres avancés dans les règles ILM](#) .

Lors du clonage d'une règle ILM, vous devez saisir un nouveau nom.

Modifier une règle ILM

Vous devrez peut-être modifier une règle ILM pour modifier un filtre ou une instruction de placement.

Vous ne pouvez pas modifier une règle si elle est utilisée dans une politique ILM. Au lieu de cela, vous pouvez [cloner la règle](#) et apportez les modifications nécessaires à la copie clonée.



Une stratégie ILM mal configurée peut entraîner une perte de données irrécupérable. Avant d'activer une stratégie ILM, examinez attentivement la stratégie ILM et ses règles ILM, puis simulez la stratégie ILM. Confirmez toujours que la politique ILM fonctionnera comme prévu.

Étapes

1. Sélectionnez **ILM > Règles**.
2. Confirmez que la règle que vous souhaitez modifier n'est utilisée dans aucune politique ILM.
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 des détails de la règle.
4. Suivez les étapes de l'assistant Modifier la règle ILM. Si nécessaire, suivez les étapes pour [créer une règle ILM](#) et [utiliser des filtres avancés dans les règles ILM](#) .

Lors de la modification d'une règle ILM, vous ne pouvez pas modifier son nom.

Supprimer une règle ILM

Pour que la liste des règles ILM actuelles reste gérable, supprimez toutes les règles ILM que vous n'êtes pas susceptible d'utiliser.

Étapes

Pour supprimer une règle ILM actuellement utilisée dans une stratégie active :

1. Cloner la politique.
2. Supprimez la règle ILM du clone de stratégie.
3. Enregistrez, simulez et activez la nouvelle politique pour vous assurer que les objets sont protégés comme prévu.
4. Accédez aux étapes permettant de supprimer une règle ILM actuellement utilisée dans une stratégie inactive.

Pour supprimer une règle ILM actuellement utilisée dans une stratégie inactive :

1. Sélectionnez la politique inactive.
2. Supprimez la règle ILM de la politique ou [supprimer la politique](#) .
3. Accédez aux étapes permettant de supprimer une règle ILM qui n'est pas actuellement utilisée.

Pour supprimer une règle ILM qui n'est pas actuellement utilisée :

1. Sélectionnez **ILM > Règles**.
2. Confirmez que la règle que vous souhaitez supprimer n'est utilisée dans aucune politique.
3. Si la règle que vous souhaitez supprimer n'est pas utilisée, sélectionnez la règle et sélectionnez **Actions > 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.

Afficher les métriques ILM

Vous pouvez afficher les métriques d'ILM, telles que le nombre d'objets dans la file d'attente et le taux d'évaluation. Vous pouvez surveiller ces mesures pour déterminer les performances du système. Une file d'attente ou un taux d'évaluation important peut indiquer que le système n'est pas en mesure de suivre le taux d'ingestion, que la charge des applications clientes est excessive ou qu'une condition anormale existe.

Étapes

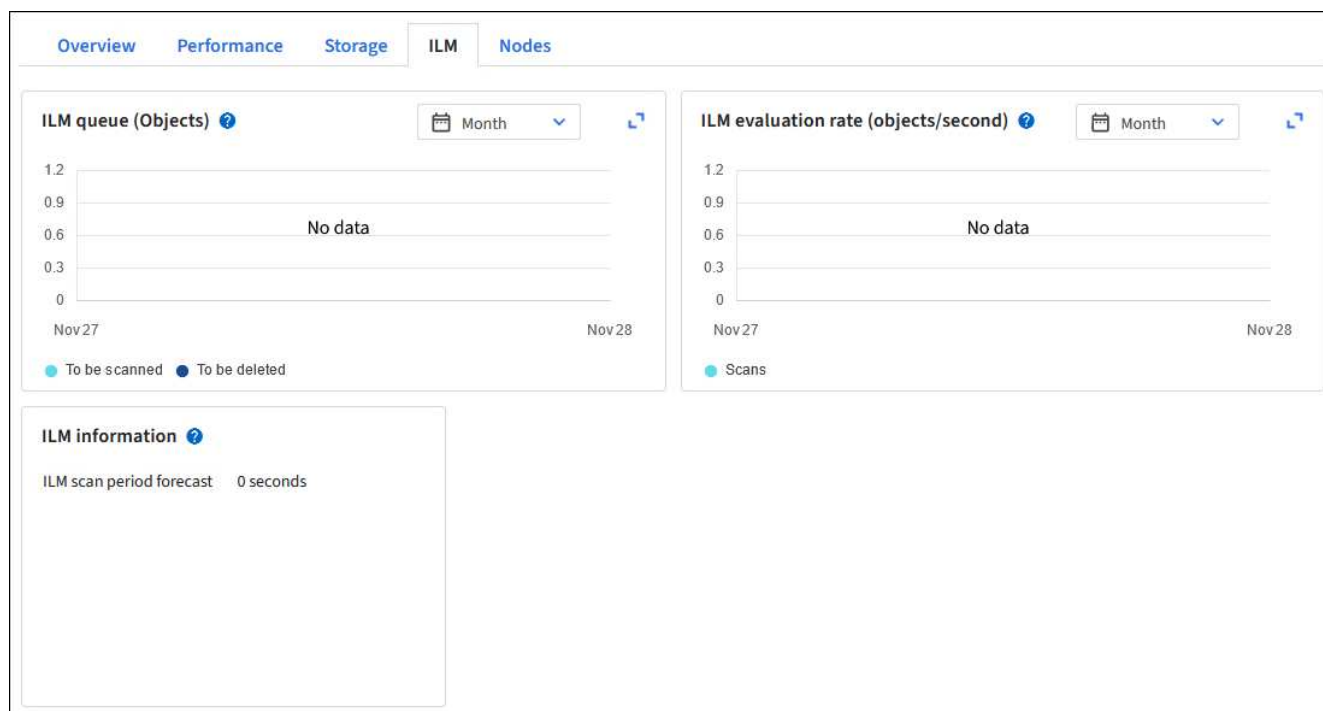
1. Sélectionnez **Tableau de bord > ILM**.



Étant donné que le tableau de bord peut être personnalisé, l'onglet ILM peut ne pas être disponible.

2. Surveillez les métriques sur l'onglet ILM.

Vous pouvez sélectionner le point d'interrogation (?) pour voir une description des éléments sur l'onglet ILM.



Utiliser le verrouillage d'objet S3

Gérer les objets avec S3 Object Lock

En tant qu'administrateur de grille, vous pouvez activer le verrouillage d'objet S3 pour votre système StorageGRID et implémenter une stratégie ILM conforme pour garantir

que les objets dans des compartiments S3 spécifiques ne sont pas supprimés ou écrasés pendant une durée spécifiée.

Qu'est-ce que S3 Object Lock ?

La fonctionnalité StorageGRID S3 Object Lock est une solution de protection d'objets équivalente à S3 Object Lock dans Amazon Simple Storage Service (Amazon S3).

Lorsque le paramètre global de verrouillage d'objet S3 est activé pour un système StorageGRID , un compte de locataire S3 peut créer des buckets avec ou sans verrouillage d'objet S3 activé. Si le verrouillage d'objet S3 est activé pour un bucket, le contrôle de version du bucket est requis et est activé automatiquement.

Un bucket sans verrouillage d'objet S3 ne peut contenir que des objets sans paramètres de conservation spécifiés. Aucun objet ingéré n'aura de paramètres de rétention.

Un bucket avec verrouillage d'objet S3 peut contenir des objets avec et sans paramètres de rétention spécifiés par les applications clientes S3. Certains objets ingérés auront des paramètres de rétention.

Un bucket avec verrouillage d'objet S3 et rétention par défaut configuré peut contenir des objets téléchargés avec des paramètres de rétention spécifiés et de nouveaux objets sans paramètres de rétention. Les nouveaux objets utilisent le paramètre par défaut, car le paramètre de rétention n'a pas été configuré au niveau de l'objet.

En effet, tous les objets nouvellement ingérés ont des paramètres de rétention lorsque la rétention par défaut est configurée. Les objets existants sans paramètres de conservation d'objets restent inchangés.

Modes de rétention

La fonctionnalité 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 rétention d'Amazon S3.

- En mode conformité :
 - L'objet ne peut pas être supprimé tant que sa date de conservation n'est pas atteinte.
 - La date de conservation de l'objet peut être augmentée, mais elle ne peut pas être diminuée.
 - La date de conservation de l'objet 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 que sa date de conservation ne soit atteinte.
 - 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 d'objet S3 activé, les utilisateurs peuvent utiliser l'application cliente S3 pour spécifier éventuellement les paramètres de conservation suivants pour chaque objet ajouté au compartiment :

- **Mode de conservation** : Soit la conformité, soit la gouvernance.
- **Date de conservation jusqu'à** : si la date de conservation jusqu'à d'une version d'objet est dans le futur,

l'objet peut être récupéré, mais il ne peut pas être supprimé.

- **Conservation légale** : L'application d'une conservation légale à une version d'objet verrouille immédiatement cet objet. Par exemple, vous pourriez avoir besoin de suspendre légalement un objet lié à une enquête ou à un litige juridique. Une conservation légale n'a pas de date d'expiration, mais reste en place jusqu'à ce qu'elle soit explicitement supprimée. Les conservations légales sont indépendantes de la date de conservation.



Si un objet est sous conservation légale, personne ne peut supprimer l'objet, quel que soit son mode de conservation.

Pour plus de détails sur les paramètres de l'objet, voir ["Utiliser l'API REST S3 pour configurer le verrouillage d'objet S3"](#).

Paramètre de rétention par défaut pour les buckets

Si un bucket est créé avec le verrouillage d'objet S3 activé, les utilisateurs peuvent éventuellement spécifier les paramètres par défaut suivants pour le bucket :

- **Mode de conservation par défaut** : Conformité ou gouvernance.
- **Période de conservation par défaut** : durée pendant laquelle les nouvelles versions d'objet ajoutées à ce bucket doivent être conservées, à compter du jour de leur ajout.

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 bucket S3"](#) et ["Mettre à jour la conservation par défaut du verrouillage des objets S3"](#).

Comparaison de S3 Object Lock avec la conformité héritée

Le verrouillage d'objet S3 remplace la fonctionnalité de conformité qui était disponible dans les versions antérieures de StorageGRID. Étant donné que la fonctionnalité de verrouillage d'objet S3 est conforme aux exigences d'Amazon S3, elle rend obsolète la fonctionnalité propriétaire de conformité StorageGRID, désormais appelée « conformité héritée ».



Le paramètre de conformité global est obsolète. Si vous avez activé ce paramètre à l'aide d'une version précédente de StorageGRID, le paramètre de verrouillage d'objet S3 est activé automatiquement. Vous pouvez continuer à utiliser StorageGRID pour gérer les paramètres des buckets conformes existants ; toutefois, vous ne pouvez pas créer de nouveaux buckets conformes. Pour plus de détails, voir ["Base de connaissances NetApp : Gestion des buckets compatibles hérités 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 elle se compare à la fonctionnalité de verrouillage d'objet S3 dans StorageGRID.

	Verrouillage d'objet S3	Conformité (héritage)
Comment la fonctionnalité est-elle activée à l'échelle mondiale ?	Depuis le Gestionnaire de grille, sélectionnez CONFIGURATION > Système > Verrouillage d'objet S3 .	N'est plus pris en charge.

	Verrouillage d'objet S3	Conformité (héritage)
Comment la fonctionnalité est-elle activée pour un bucket ?	Les utilisateurs doivent activer le verrouillage d'objet S3 lors de la création d'un nouveau bucket 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 buckets est-il pris en charge ?	Oui. Le contrôle de version du bucket est requis et est activé automatiquement lorsque le verrouillage d'objet S3 est activé pour le bucket.	Non.
Comment la rétention d'objet est-elle définie ?	Les utilisateurs peuvent définir une date de conservation pour chaque version d'objet ou une période de conservation par défaut pour chaque compartiment.	Les utilisateurs doivent définir une période de conservation pour l'ensemble du bucket. La période de conservation s'applique à tous les objets du bucket.
La durée de conservation peut-elle être modifiée ?	• En mode de conformité, la date de conservation d'une version d'objet peut être augmentée mais jamais diminuée. • En mode gouvernance, les utilisateurs disposant d'autorisations spéciales peuvent diminuer ou même supprimer les paramètres de conservation d'un objet.	La période de rétention d'un bucket peut être augmentée mais jamais diminuée.
Où la conservation légale est-elle contrôlée ?	Les utilisateurs peuvent placer une suspension légale ou lever une suspension légale pour n'importe quelle version d'objet dans le bucket.	Une suspension légale est placée sur le seau et affecte tous les objets qu'il contient.

	Verrouillage d'objet S3	Conformité (héritage)
Quand les objets peuvent-ils être supprimés ?	- En mode de conformité, une version d'objet peut être supprimée une fois la date de conservation atteinte, en supposant que l'objet ne soit pas sous conservation légale. - En mode gouvernance, les utilisateurs disposant d'autorisations spéciales peuvent supprimer un objet avant que sa date de conservation ne soit atteinte, en supposant que l'objet ne soit pas sous conservation légale.	Un objet peut être supprimé après l'expiration de la période de conservation, à condition que le bucket ne soit pas sous conservation légale. Les objets peuvent être supprimés automatiquement ou manuellement.
La configuration du cycle de vie du bucket est-elle prise en charge ?	Oui	Non

Tâches de verrouillage d'objet S3

En tant qu'administrateur de grille, vous devez collaborer étroitement avec les utilisateurs locataires pour garantir que les objets sont protégés d'une manière qui répond à leurs exigences de conservation.



L'application des paramètres du locataire sur la grille peut prendre 15 minutes ou plus en fonction de la connectivité réseau, de l'état du nœud et des opérations Cassandra.

Les listes suivantes destinées aux administrateurs de grille et aux utilisateurs locataires contiennent les tâches de haut niveau pour l'utilisation de la fonctionnalité de verrouillage d'objet S3.

Administrateur de réseau

- Activez le paramètre de verrouillage d'objet S3 global pour l'ensemble du système StorageGRID .
- Assurez-vous que les politiques de gestion du cycle de vie de l'information (ILM) sont *conformes* ; c'est-à-dire qu'elles répondent aux ["exigences des buckets avec S3 Object Lock activé"](#) .
- Si nécessaire, autorisez un locataire à utiliser la conformité comme mode de conservation. Sinon, seul le mode Gouvernance est autorisé.
- Si nécessaire, définissez une période de conservation maximale pour un locataire.

Utilisateur locataire

- Passez en revue les considérations relatives aux buckets et aux objets avec S3 Object Lock.
- Si nécessaire, contactez l'administrateur de la grille pour activer le paramètre de verrouillage d'objet S3 global et définir les autorisations.
- Créez des buckets avec le verrouillage d'objet S3 activé.
- Vous pouvez également configurer les paramètres de conservation par défaut pour un bucket :
 - Mode de conservation par défaut : Gouvernance ou Conformité, si autorisé par l'administrateur du réseau.

- Période de conservation par défaut : doit être inférieure ou égale à la période de conservation maximale définie par l'administrateur du réseau.
- Utilisez l'application client S3 pour ajouter des objets et éventuellement définir une conservation spécifique à l'objet :
 - Mode de rétention. Gouvernance ou conformité, si autorisée par l'administrateur du réseau.
 - Date de conservation : doit être inférieure ou égale à ce qui est autorisé par la période de conservation maximale définie par l'administrateur de la grille.

Conditions requises pour le verrouillage d'objet S3

Vous devez examiner les exigences d'activation du paramètre global de verrouillage d'objet S3, les exigences de création de règles ILM et de stratégies ILM conformes, ainsi que les restrictions que StorageGRID impose aux buckets et aux 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 du gestionnaire de grille ou de l'API de gestion de grille avant qu'un locataire S3 puisse créer un bucket avec le verrouillage d'objet S3 activé.
- L'activation du paramètre global de verrouillage d'objet S3 permet à tous les comptes de locataire S3 de créer des buckets avec le verrouillage d'objet S3 activé.
- Une fois que vous avez activé le paramètre global de verrouillage d'objet S3, vous ne pouvez pas désactiver le paramètre.
- Vous ne pouvez pas activer le verrouillage d'objet S3 global à moins que la règle par défaut de toutes les stratégies ILM actives soit *conforme* (c'est-à-dire que la règle par défaut doit être conforme aux exigences des compartiments avec le verrouillage d'objet S3 activé).
- Lorsque le paramètre global de verrouillage d'objet S3 est activé, vous ne pouvez pas créer une nouvelle stratégie ILM ni activer une stratégie ILM existante, sauf si la règle par défaut de la stratégie est conforme. Une fois le paramètre de verrouillage d'objet S3 global activé, les pages de règles ILM et de politiques ILM indiquent quelles règles ILM sont conformes.

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 dans toutes les stratégies ILM actives est conforme. Une règle conforme satisfait aux exigences des deux compartiments avec le verrouillage d'objet S3 activé et de tous les compartiments existants pour lesquels la conformité héritée est activée :

- Il doit créer au moins deux copies d'objet répliquées ou une copie à 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'objets ne peuvent pas être enregistrées dans un pool de stockage cloud.
- 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 « pour toujours ».

Exigences relatives aux politiques ILM

Lorsque le paramètre global de verrouillage d'objet S3 est activé, les stratégies ILM actives et inactives peuvent inclure des règles conformes et non conformes.

- La règle par défaut dans une politique ILM active ou inactive doit être conforme.
- Les règles non conformes s'appliquent uniquement aux objets dans les compartiments pour lesquels le verrouillage d'objet S3 n'est pas activé ou pour lesquels la fonctionnalité de conformité héritée n'est pas activée.
- Les règles de conformité peuvent s'appliquer aux objets de n'importe quel compartiment ; le verrouillage d'objet S3 ou la conformité héritée n'ont pas besoin d'être activés pour le compartiment.

"Exemple de politique ILM conforme pour le verrouillage des objets S3"

Exigences pour les buckets avec S3 Object Lock activé

- Si le paramètre global de verrouillage d'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 buckets avec le verrouillage d'objets S3 activé.
- Si vous prévoyez d'utiliser S3 Object Lock, vous devez activer S3 Object Lock lorsque vous créez le bucket. Vous ne pouvez pas activer le verrouillage d'objet S3 pour un bucket existant.
- Lorsque le verrouillage d'objet S3 est activé pour un bucket, StorageGRID active automatiquement le contrôle de version pour ce bucket. Vous ne pouvez pas désactiver le verrouillage d'objet S3 ou suspendre le contrôle de version du bucket.
- Vous pouvez également spécifier un mode de conservation par défaut et une période de conservation pour chaque compartiment à l'aide du gestionnaire de locataires, de l'API de gestion des locataires ou de l'API REST S3. Les paramètres de conservation par défaut du bucket s'appliquent uniquement aux nouveaux objets ajoutés au bucket 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 pour chaque version d'objet lors de son téléchargement.
- La configuration du cycle de vie du bucket est prise en charge pour les buckets avec S3 Object Lock activé.
- La réplication CloudMirror n'est pas prise en charge pour les buckets avec S3 Object Lock activé.

Exigences relatives aux objets dans les compartiments avec le verrouillage d'objet S3 activé

- Pour protéger une version d'objet, vous pouvez spécifier des paramètres de rétention par défaut pour le compartiment ou spécifier des paramètres de rétention pour chaque version d'objet. Les paramètres de conservation au niveau de l'objet peuvent être spécifiés à l'aide de l'application cliente 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 une date de conservation et un paramètre de conservation légale, l'un mais pas l'autre, ou aucun des deux. La spécification d'une date de conservation ou d'un paramètre de conservation légale 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 les buckets avec S3 Object Lock activé

Chaque objet enregistré dans un bucket avec S3 Object Lock activé passe par ces étapes :

1. Objet ingéré

Lorsqu'une version d'objet est ajoutée à un bucket sur lequel le verrouillage d'objet S3 est activé, les paramètres de rétention sont appliqués comme suit :

- Si des paramètres de conservation sont spécifiés pour l'objet, les paramètres au niveau de l'objet sont appliqués. Tous les paramètres de bucket 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 S3 Object Lock.

Si les paramètres de conservation sont appliqués, l'objet et toutes les métadonnées définies par l'utilisateur S3 sont protégés.

2. Conservation et suppression d'objets

Plusieurs copies de chaque objet protégé sont stockées par StorageGRID pendant la période de conservation spécifiée. Le nombre et le type exacts de copies d'objets ainsi que les emplacements de stockage sont déterminés par les règles de conformité des politiques ILM actives. La possibilité de supprimer un objet protégé avant que sa date de conservation ne soit atteinte dépend de son mode de conservation.

- Si un objet est sous conservation légale, personne ne peut supprimer l'objet, quel que soit son mode de conservation.

Informations connexes

- ["Créer un bucket S3"](#)
- ["Mettre à jour la conservation par défaut du verrouillage des objets S3"](#)
- ["Utiliser l'API REST S3 pour configurer le verrouillage d'objet S3"](#)
- ["Exemple 7 : Politique ILM conforme pour le verrouillage d'objet S3"](#)

Activer le verrouillage des objets S3 globalement

Si un compte de locataire S3 doit se conformer aux exigences réglementaires lors de l'enregistrement des données d'objet, vous devez activer le verrouillage d'objet S3 pour l'ensemble de votre système StorageGRID . L'activation du paramètre global de verrouillage d'objet S3 permet à tout utilisateur de locataire S3 de créer et de gérer des buckets et des objets avec le verrouillage d'objet S3.

Avant de commencer

- Vous avez le ["Autorisation d'accès root"](#) .
- Vous êtes connecté au Grid Manager à l'aide d'un ["navigateur Web pris en charge"](#) .
- Vous avez examiné le flux de travail S3 Object Lock et vous comprenez les considérations.
- Vous avez confirmé que la règle par défaut de la politique ILM active est conforme. Voir ["Créer une règle ILM par défaut"](#) pour plus de détails.

À propos de cette tâche

Un administrateur de grille 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 plus être désactivé.

Vérifiez les paramètres de conformité des locataires existants après avoir activé le paramètre global de verrouillage d'objet S3. Lorsque vous activez ce paramètre, les paramètres de verrouillage d'objet S3 par locataire dépendent de la version de StorageGRID au moment de la création du locataire.



Le paramètre de conformité global est obsolète. Si vous avez activé ce paramètre à l'aide d'une version précédente de StorageGRID, le paramètre de verrouillage d'objet S3 est activé automatiquement. Vous pouvez continuer à utiliser StorageGRID pour gérer les paramètres des buckets conformes existants ; toutefois, vous ne pouvez pas créer de nouveaux buckets conformes. Pour plus de détails, voir "[Base de connaissances NetApp : Gestion des buckets compatibles hérités dans StorageGRID 11.5](#)".

Étapes

1. Sélectionnez **CONFIGURATION > Système > Verrouillage d'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 apparaît et vous rappelle que vous ne pouvez pas désactiver le verrouillage d'objet S3 une fois qu'il est activé.

4. Si vous êtes sûr de vouloir activer de manière permanente le verrouillage des objets S3 pour l'ensemble de votre système, sélectionnez **OK**.

Lorsque vous sélectionnez **OK** :

- Si la règle par défaut de la politique 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 apparaît. Vous devez créer et activer une nouvelle stratégie ILM qui inclut une règle conforme comme règle par défaut. Sélectionnez **OK**. Ensuite, créez une nouvelle politique, simulez-la et activez-la. Voir "[Créer une politique ILM](#)" pour les instructions.

Résoudre les erreurs de cohérence lors de la mise à jour du verrouillage d'objet S3 ou de la configuration de conformité héritée

Si un site de centre de données ou plusieurs nœuds de stockage sur un site deviennent indisponibles, vous devrez peut-être aider les utilisateurs locataires S3 à appliquer les modifications apportées au verrouillage d'objet S3 ou à la configuration de conformité héritée.

Les utilisateurs locataires qui ont des buckets avec S3 Object Lock (ou conformité héritée) activé peuvent modifier certains paramètres. Par exemple, un utilisateur locataire utilisant S3 Object Lock peut avoir besoin de placer une version d'objet sous conservation légale.

Lorsqu'un utilisateur locataire met à jour les paramètres d'un bucket S3 ou d'une version d'objet, StorageGRID tente de mettre à jour immédiatement les métadonnées du bucket ou de l'objet sur la grille. Si le système ne parvient pas à mettre à jour les métadonnées parce qu'un site de centre de données ou plusieurs nœuds de stockage ne sont pas disponibles, il renvoie une erreur :

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 à nouveau disponibles dès que possible.
2. Si vous ne parvenez pas à rendre disponibles suffisamment de nœuds de stockage sur chaque site, contactez le support technique, qui peut vous aider à récupérer les nœuds et à garantir que les modifications sont appliquées de manière cohérente sur l'ensemble de la grille.
3. Une fois le problème sous-jacent résolu, rappelez à l'utilisateur locataire de réessayer ses modifications de configuration.

Informations connexes

- ["Utiliser un compte locataire"](#)
- ["Utiliser l'API REST S3"](#)
- ["Récupérer et entretenir"](#)

Exemples de règles et de politiques ILM

Exemple 1 : Règles et politique ILM pour le stockage d'objets

Vous pouvez utiliser les exemples de règles et de politiques suivants comme point de départ lors de la définition d'une politique ILM pour répondre à vos exigences de protection et de conservation d'objets.



Les règles et politiques ILM suivantes ne sont que des exemples. Il existe de nombreuses façons de configurer les règles ILM. Avant d'activer une nouvelle politique, simulez-la pour confirmer qu'elle fonctionnera comme prévu pour protéger le contenu contre la perte.

Règle ILM 1 pour l'exemple 1 : Copier les données d'objet sur deux sites

Cet exemple de règle ILM copie les données d'objet vers des pools de stockage sur deux sites.

Définition de la règle	Exemple de valeur
Pools de stockage sur un seul 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 la date définitive, 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.

Reference time

Ingest time

Time period and placements

Sort by start date

If you want a rule to apply only to specific objects, select **Previous** and add advanced filters. When objects are evaluated, the rule is applied if the object's metadata matches the criteria in the filter.

Time period 1

From Day 0

store

forever

Store objects by

replicating

1

copies at

Site 1

and store objects by

replicating

1

copies at

Site 2

Add other type or location

Add another time period

Retention diagram

Replicated copy

Rule analysis:

StorageGRID site-loss protection will apply for the duration of this rule.

Objects processed by this rule will not be deleted by ILM.

Reference time: Ingest time

Day 0

Day 0 - forever

1 replicated copy - Site 1

1 replicated copy - Site 2

Duration

Forever

Règle ILM 2 pour l'exemple 1 : Profil de codage d'effacement avec correspondance de compartiment

Cet exemple de règle ILM utilise un profil de codage d'effacement et un compartiment S3 pour déterminer où et combien de temps l'objet est stocké.

Définition de la règle	Exemple de valeur
Pool de stockage avec plusieurs sites	Un pool de stockage sur trois sites (sites 1, 2, 3) Utiliser le schéma de codage 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 nommé finance-records, créez une copie à codage d'effacement dans le pool spécifié par le profil de codage d'effacement. Gardez cette copie pour toujours.

Time period and placements

Sort by start date

If you want a rule to apply only to specific objects, select **Previous** and add advanced filters. When objects are evaluated, the rule is applied if the object's metadata matches the criteria in the filter.

Time period 1

From Day 0

store forever

×

Store objects by

erasure coding

using 6+3 EC scheme at Sites 1, 2, 3

✎

×

Add other type or location

Add another time period

Retention diagram

Erasure-coded (EC) copy

Rule analysis:

- StorageGRID site-loss protection will apply for the duration of this rule.
- Objects processed by this rule will not be deleted by ILM.

Reference time: Ingest time

Day 0

Day 0 - forever

EC 6+3 - Sites 1, 2, 3

Duration Forever

Politique ILM par exemple 1

En pratique, la plupart des politiques ILM sont simples, même si le système StorageGRID vous permet de concevoir des politiques ILM sophistiquées et complexes.

Une politique ILM typique pour une grille multi-sites peut inclure des règles ILM telles que les suivantes :

- Lors de l'ingestion, stockez tous les objets appartenant au bucket S3 nommé `finance-records` dans un pool de stockage contenant trois sites. Utilisez le codage d'effacement 6+3.
- Si un objet ne correspond pas à la première règle ILM, utilisez la règle ILM par défaut de la stratégie, Deux copies, deux centres de données, pour stocker une copie de cet objet sur le site 1 et une copie sur le site 2.

Proposed policy name

Object Storage Policy

Reason for change

example 1

Manage rules

1. Select the rules you want to add to the policy.
2. Determine the order in which the rules will be evaluated by dragging and dropping the rows. The default rule will be automatically placed at the end of the policy and cannot be moved.

Select rules

Rule order	Rule name	Filters
1	S3 Bucket finance-records	Tenant is Finance Bucket name is finance-records
Default	Two Copies Two Data Centers	—

Informations connexes

- ["Utiliser les politiques ILM"](#)
- ["Créer des politiques ILM"](#)

Exemple 2 : Règles et politique ILM pour le filtrage de la taille des objets EC

Vous pouvez utiliser les exemples de règles et de politiques suivants comme points de départ pour définir une politique ILM qui filtre par taille d'objet pour répondre aux exigences EC recommandées.



Les règles et politiques ILM suivantes ne sont que des exemples. Il existe de nombreuses façons de configurer les règles ILM. Avant d'activer une nouvelle politique, simulez-la pour confirmer qu'elle fonctionnera comme prévu pour protéger le contenu contre la perte.

Règle ILM 1 pour l'exemple 2 : utiliser EC pour les objets supérieurs à 1 Mo

Cet exemple de règle ILM efface les codes d'objets supérieurs à 1 Mo.



Le codage d'effacement est particulièrement adapté aux objets supérieurs à 1 Mo. N'utilisez pas le codage d'effacement pour les objets inférieurs à 200 Ko afin d'éviter la surcharge liée à la gestion de très petits fragments codés par effacement.

Définition de la 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

Définition de la règle	Exemple de valeur
Placements	Créer une copie codée à effacement 2+1 en utilisant trois sites

Filter group 1
Objects with all of following metadata will be evaluated by this rule:

Object size

greater than

1

MB

Règle ILM 2 pour l'exemple 2 : Deux copies répliquées

Cet exemple de règle ILM crée deux copies répliquées et ne filtre pas par taille d'objet. Cette règle est la règle par défaut de la politique. Étant donné que la première règle filtre tous les objets supérieurs à 1 Mo, cette règle s'applique uniquement aux objets de 1 Mo ou moins.

Définition de la 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 la date définitive, conservez une copie répliquée sur le site 1 et une copie répliquée sur le site 2.

Politique ILM pour l'exemple 2 : utiliser EC pour les objets supérieurs à 1 Mo

Cet exemple de politique ILM comprend deux règles ILM :

- La première règle efface les codes de tous les objets dont la taille est supérieure à 1 Mo.
- La deuxième règle ILM (par défaut) crée deux copies répliquées. Étant donné que les objets supérieurs à 1 Mo ont été filtrés par la règle 1, la règle 2 s'applique uniquement aux objets de 1 Mo ou moins.

Exemple 3 : Règles et politique ILM pour une meilleure protection des fichiers image

Vous pouvez utiliser les exemples de règles et de politiques suivants pour garantir que les images supérieures à 1 Mo sont codées par effacement et que deux copies d'images plus petites sont effectuées.



Les règles et politiques ILM suivantes ne sont que des exemples. Il existe de nombreuses façons de configurer les règles ILM. Avant d'activer une nouvelle politique, simulez-la pour confirmer qu'elle fonctionnera comme prévu pour protéger le contenu contre la perte.

Règle ILM 1 pour l'exemple 3 : utiliser EC pour les fichiers image supérieurs à 1 Mo

Cet exemple de règle ILM utilise un filtrage avancé pour effacer le code de tous les fichiers image supérieurs à 1 Mo.



Le codage d'effacement est particulièrement adapté aux objets supérieurs à 1 Mo. N'utilisez pas le codage d'effacement pour les objets inférieurs à 200 Ko afin d'éviter la surcharge liée à la gestion de très petits fragments codés par effacement.

Définition de la 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	Créer une copie codée à effacement 2+1 en utilisant trois sites

Filter group 1 Objects with all of following metadata will be evaluated by this rule: ✕

Object size ▼greater than ▼1 ⬆MB ▼✕

and Key ▼ends with ▼.jpg ✕

or **Filter group 2** Objects with all of following metadata will be evaluated by this rule: ✕

Object size ▼greater than ▼1 ⬆MB ▼✕

and Key ▼ends with ▼.png ✕

Étant donné que cette règle est configurée comme première règle de la stratégie, l'instruction de placement du codage d'effacement s'applique uniquement aux fichiers .jpg et .png supérieurs à 1 Mo.

Règle ILM 2 pour l'exemple 3 : créer 2 copies répliquées pour tous les fichiers image restants

Cet exemple de règle ILM utilise un filtrage avancé pour spécifier que des fichiers image plus petits doivent être répliqués. Étant donné que la première règle de la politique a déjà mis en correspondance des fichiers image supérieurs à 1 Mo, cette règle s'applique aux fichiers image de 1 Mo ou moins.

Définition de la règle	Exemple de valeur
Nom de la règle	2 copies pour les fichiers image
Heure de référence	Temps d'ingestion

731

Définition de la règle	Exemple de valeur
Filtres avancés pour la clé	• Se termine par .jpg • Se termine par .png
Placements	Créer 2 copies répliquées dans deux pools de stockage

Politique ILM pour l'exemple 3 : Meilleure protection des fichiers image

Cet exemple de politique ILM comprend trois règles :

- La première règle efface les codes de tous les fichiers image supérieurs à 1 Mo.
- La deuxième règle crée deux copies de tous les fichiers image restants (c'est-à-dire des images de 1 Mo ou moins).
- La règle par défaut s'applique à tous les objets restants (c'est-à-dire tous les fichiers non image).

Rule order	Rule name	Filters
1	↕ EC image files > 1 MB	Object size is greater than 1 MB
2	↕ 2 copies for small images	Object size is less than or equal to 200 KB
Default	Default rule	—

Exemple 4 : Règles et politique ILM pour les objets versionnés S3

Si vous disposez d'un compartiment S3 avec le contrôle de version activé, vous pouvez gérer les versions d'objet non actuelles en incluant des règles dans votre stratégie ILM qui utilisent « Heure non actuelle » comme heure de référence.



Si vous spécifiez une durée de conservation limitée pour les objets, ces objets seront supprimés définitivement une fois la période atteinte. Assurez-vous de bien comprendre combien de temps les objets seront conservés.

Comme le montre cet exemple, vous pouvez contrôler la quantité de stockage utilisée par les objets versionnés en utilisant différentes instructions de placement pour les versions d'objet non actuelles.



Les règles et politiques ILM suivantes ne sont que des exemples. Il existe de nombreuses façons de configurer les règles ILM. Avant d'activer une nouvelle politique, simulez-la pour confirmer qu'elle fonctionnera comme prévu pour protéger le contenu contre la perte.



Pour effectuer une simulation de stratégie ILM sur une version non actuelle d'un objet, vous devez connaître l'UUID ou le CBID de la version de l'objet. Pour trouver l'UUID et le CBID, utilisez "[recherche de métadonnées d'objet](#)" tant que l'objet est toujours d'actualité.

Informations connexes

["Comment les objets sont supprimés"](#)

Règle ILM 1 par exemple 4 : Conservez trois copies pendant 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 la règle	Exemple de valeur
Piscines de stockage	Trois pools de stockage, chacun composé de centres de données différents, nommés Site 1, Site 2 et Site 3.
Nom de la règle	Trois exemplaires dix ans
Heure de référence	Temps d'ingestion
Placements	Le jour 0, conservez trois copies répliquées pendant 10 ans (3 652 jours), une sur le site 1, une sur le site 2 et une sur le site 3. Au bout de 10 ans, supprimez toutes les copies de l'objet.

Règle ILM 2 pour l'exemple 4 : Conservez deux copies des versions non actuelles pendant 2 ans

Cet exemple de règle ILM stocke deux copies des versions non actuelles d'un objet versionné S3 pendant 2 ans.

Étant donné que la règle ILM 1 s'applique à toutes les versions de l'objet, vous devez créer une autre règle pour filtrer toutes les versions non actuelles.

Pour créer une règle qui utilise « Heure non actuelle » comme heure de référence, sélectionnez **Oui** pour la question « Appliquer cette règle uniquement aux anciennes versions d'objet (dans les compartiments S3 avec le contrôle de version activé) ? » à l'étape 1 (Saisir les détails) de l'assistant Créer une règle ILM. Lorsque vous sélectionnez **Oui**, *Heure non actuelle* est automatiquement sélectionné comme heure de référence et vous ne pouvez pas sélectionner une heure de référence différente.

1 Enter details
2 Define placements
3 Select ingest behavior

Rule name

Older Object Versions: Two Copies Two Years

Description (optional)

Older versions only

Basic filters (optional)

Specify which tenant accounts and buckets this rule applies to.

Tenant accounts ? Select tenant accounts

Bucket name ? matches all ▼

Apply this rule to older object versions only (in S3 buckets with versioning enabled)? ?

☐ No ☒ Yes

Dans cet exemple, seules deux copies des versions non actuelles sont stockées, et ces copies seront stockées pendant deux ans.

Définition de la règle	Exemple de valeur
Piscines de stockage	Deux pools de stockage, chacun dans des centres de données différents, Site 1 et Site 2.
Nom de la règle	Versions non actuelles : deux exemplaires, deux ans
Heure de référence	Temps non actuel Sélectionné automatiquement lorsque vous sélectionnez Oui pour la question « Appliquer cette règle uniquement aux anciennes versions d'objet (dans les compartiments S3 avec le contrôle de version activé) ? » dans l'assistant Créer une règle ILM.
Placements	Le jour 0 par rapport à la période non courante (c'est-à-dire à partir du jour où la version de l'objet devient la version non courante), conservez deux copies répliquées des versions de l'objet non courantes pendant 2 ans (730 jours), une sur le site 1 et une sur le site 2. Au bout de 2 ans, supprimez les versions non actuelles.

Politique ILM pour l'exemple 4 : objets versionnés S3

Si vous souhaitez gérer les anciennes versions d'un objet différemment de la version actuelle, les règles qui utilisent « Heure non actuelle » comme heure de référence doivent apparaître dans la stratégie ILM avant les règles qui s'appliquent à la version actuelle de l'objet.

Une politique ILM pour les objets versionnés S3 peut inclure des règles ILM telles que les suivantes :

- Conservez toutes les versions plus anciennes (non actuelles) de chaque objet pendant 2 ans, à compter du jour où la version est devenue non actuelle.



Les règles « Heure non actuelle » doivent apparaître dans la politique avant les règles qui s'appliquent à la version actuelle de l'objet. Dans le cas contraire, les versions d'objet non actuelles ne seront jamais mises en correspondance avec la règle « Heure non actuelle ».

- Lors de l'ingestion, créez trois copies répliquées et stockez une copie sur chacun des trois sites. Conservez des copies de la version actuelle de l'objet pendant 10 ans.

Lorsque vous simulez l'exemple de politique, vous vous attendez à ce que les objets de test soient évalués comme suit :

- Toutes les versions d'objet non actuelles seront mises en correspondance avec la première règle. Si une version d'objet non actuelle a plus de 2 ans, elle est définitivement supprimée par ILM (toutes les copies de la version non actuelle sont supprimées de la grille).
- La version actuelle de l'objet correspondrait à la deuxième règle. Lorsque la version actuelle de l'objet a été stockée pendant 10 ans, le processus ILM ajoute un marqueur de suppression comme version actuelle de l'objet et rend la version précédente de l'objet « non actuelle ». Lors de la prochaine évaluation ILM, cette version non actuelle correspond à la première règle. En conséquence, la copie du site 3 est purgée et les deux copies des sites 1 et 2 sont stockées pendant 2 ans supplémentaires.

Exemple 5 : Règles et politique ILM pour un comportement d'ingestion strict

Vous pouvez utiliser un filtre d'emplacement et le comportement d'ingestion strict dans une règle pour empêcher l'enregistrement d'objets à un emplacement de centre de données particulier.

Dans cet exemple, un locataire basé à Paris ne souhaite pas stocker certains objets en dehors de l'UE en raison de préoccupations réglementaires. D'autres objets, y compris tous les objets provenant d'autres comptes locataires, peuvent être stockés dans le centre de données de Paris ou dans le centre de données américain.



Les règles et politiques ILM suivantes ne sont que des exemples. Il existe de nombreuses façons de configurer les règles ILM. Avant d'activer une nouvelle politique, simulez-la pour confirmer qu'elle fonctionnera comme prévu pour protéger le contenu contre la perte.

Informations connexes

- ["Options d'ingestion"](#)
- ["Créer une règle ILM : sélectionner le comportement d'ingestion"](#)

Règle ILM 1 par exemple 5 : Ingestion stricte pour garantir le centre de données de Paris

Cet exemple de règle ILM utilise le comportement d'ingestion strict pour garantir que les objets enregistrés par

un locataire basé à Paris dans des buckets S3 avec la région définie sur la région eu-ouest-3 (Paris) ne sont jamais stockés dans le centre de données américain.

Cette règle s'applique aux objets appartenant au locataire Paris et dont la région de compartiment S3 est définie sur eu-west-3 (Paris).

Définition de la règle	Exemple de valeur
Compte locataire	Locataire parisien
Filtre avancé	La contrainte de localisation est égale à eu-ouest-3
Piscines de stockage	Site 1 (Paris)
Nom de la règle	Ingestion stricte pour garantir le centre de données de Paris
Heure de référence	Temps d'ingestion
Placements	Le jour 0, conserver deux copies répliquées pour toujours dans le site 1 (Paris)
Comportement d'ingestion	Strict. Utilisez toujours les placements de cette règle lors de l'ingestion. L'ingestion échoue s'il n'est pas possible de stocker deux copies de l'objet dans le centre de données de Paris.

Strict ingest to guarantee Paris data center

Compliant: Yes
Used in active policy: No
Used in proposed policy: No

Ingest behavior: Strict
Reference time: Ingest time

Clone Edit Remove

Filters

This rule applies if:
• Tenant is Paris tenant
And it only applies if objects have this metadata:
• Location constraint is eu-west-3

Time period and placements

Retention diagram Placement instructions

Sort placements by Time period Storage pool

● Replicated copy

Rule analysis:
• StorageGRID site-loss protection will not apply from Day 0 - Forever.
• Objects processed by this rule will not be deleted by ILM.

Reference time: Ingest time Ingest behavior: Strict

Day 0

Day 0 - forever

2 replicated copies - Site 1

Duration

Forever

Règle ILM 2 par exemple 5 : Ingestion équilibrée pour d'autres objets

Cet exemple de règle ILM utilise le comportement d'ingestion équilibré pour fournir une efficacité ILM optimale pour tous les objets ne correspondant pas à la première règle. Deux copies de tous les objets correspondant à cette règle seront stockées : une dans le centre de données américain et une dans le centre de données parisien. Si la règle ne peut pas être satisfaite immédiatement, des copies provisoires sont stockées à tout endroit disponible.

Cette règle s'applique aux objets appartenant à n'importe quel locataire et à n'importe quelle région.

Définition de la règle	Exemple de valeur
Compte locataire	Ignorer
Filtre avancé	Non spécifié
Piscines de stockage	Site 1 (Paris) et Site 2 (États-Unis)
Nom de la règle	2 copies 2 centres de données
Heure de référence	Temps d'ingestion

Définition de la règle	Exemple de valeur
Placements	Le jour 0, conservez deux copies répliquées pour toujours dans deux centres de données
Comportement d'ingestion	Équilibré. Les objets qui correspondent à cette règle sont placés conformément aux instructions de placement de la règle si possible. Dans le cas contraire, des copies provisoires sont réalisées à tout endroit disponible.

Politique ILM pour l'exemple 5 : Combinaison des comportements d'ingestion

L'exemple de politique ILM inclut deux règles qui ont des comportements d'ingestion différents.

Une politique ILM qui utilise deux comportements d'ingestion différents peut inclure des règles ILM telles que les suivantes :

- Stockez les objets appartenant au locataire de Paris et dont la région de compartiment S3 est définie sur eu-west-3 (Paris) uniquement dans le centre de données de Paris. Échec de l'ingestion si le centre de données de Paris n'est pas disponible.
- Stockez tous les autres objets (y compris ceux qui appartiennent au locataire de Paris mais qui ont une région de compartiment différente) dans le centre de données américain et dans le centre de données de Paris. Faites des copies provisoires dans n'importe quel endroit disponible si les instructions de placement ne peuvent pas être respectées.

Lorsque vous simulez l'exemple de politique, vous vous attendez à ce que les objets de test soient évalués comme suit :

- Tous les objets appartenant au locataire de Paris et dont la région de compartiment S3 est définie sur eu-west-3 correspondent à la première règle et sont stockés dans le centre de données de Paris. Étant donné que la première règle utilise l'ingestion stricte, ces objets ne sont jamais stockés dans le centre de données américain. Si les nœuds de stockage du centre de données de Paris ne sont pas disponibles, l'ingestion échoue.
- Tous les autres objets sont mis en correspondance avec la deuxième règle, y compris les objets qui appartiennent 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 centre de données. Cependant, comme la deuxième règle utilise l'ingestion équilibrée, si un centre de données n'est pas disponible, deux copies intermédiaires sont enregistrées à n'importe quel emplacement disponible.

Exemple 6 : Modifier une politique ILM

Si votre protection des données doit être modifiée ou si vous ajoutez de nouveaux sites, vous pouvez créer et activer une nouvelle politique ILM.

Avant de modifier une politique, vous devez comprendre comment les modifications apportées aux placements 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 stratégie 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](#)". Ensuite, vous devez "[simuler](#)" et puis "[activer](#)" la nouvelle politique.



Les règles et politiques ILM suivantes ne sont que des exemples. Il existe de nombreuses façons de configurer les règles ILM. Avant d'activer une nouvelle politique, simulez-la pour confirmer qu'elle fonctionnera comme prévu pour protéger le contenu contre la perte.

Comment la modification d'une politique ILM affecte les performances

Lorsque vous activez une nouvelle stratégie ILM, les performances de votre système StorageGRID peuvent être temporairement affectées, en particulier si les instructions de placement dans la nouvelle stratégie nécessitent le déplacement de nombreux objets existants vers de nouveaux emplacements.

Lorsque vous activez une nouvelle stratégie ILM, StorageGRID l'utilise pour gérer tous les objets, y compris les objets existants et les objets nouvellement ingérés. Avant d'activer une nouvelle stratégie ILM, vérifiez toutes les modifications apportées au placement des objets répliqués et codés par effacement existants. La modification de l'emplacement d'un objet existant peut entraîner des problèmes de ressources temporaires lorsque les nouveaux emplacements sont évalués et mis en œuvre.

Pour garantir qu'une nouvelle politique ILM n'affecte pas le placement des objets répliqués et codés par effacement existants, vous pouvez "[créer une règle ILM avec un filtre de temps d'ingestion](#)". Par exemple, **L'heure d'ingestion est le ou après <date et heure>**, 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 politique ILM qui peuvent affecter temporairement les performances de StorageGRID sont les suivants :

- Application d'un profil de codage d'effacement différent aux objets codés par effacement existants.



StorageGRID considère que chaque profil de codage d'effacement est unique et ne réutilise pas les fragments de codage d'effacement lorsqu'un nouveau profil est utilisé.

- Modification du type de copies requises pour les objets existants ; par exemple, conversion d'un pourcentage important d'objets répliqués en objets à code d'effacement.
- Déplacer des copies d'objets existants vers un emplacement complètement différent ; par exemple, déplacer un grand nombre d'objets vers ou depuis un pool de stockage cloud ou vers ou depuis un site distant.

Politique ILM active pour l'exemple 6 : Protection des données sur deux sites

Dans cet exemple, la stratégie ILM active a été initialement conçue pour un système StorageGRID à deux sites et utilise deux règles ILM.

Active policy

Policy history

Policy name:

Data Protection for Two Sites (2 rules)

Reason for change :

Data protection for two sites (using 2 rules)

Start date:

2022-10-11 10:37:11 MDT

Simulate

Policy rules

Retention diagram

Rule order ?	Rule name	Filters ?
1	One-Site Erasure Coding for Tenant A	Tenant is Tenant A
Default	Two-Site Replication for Other Tenants	—

Dans cette politique ILM, les objets appartenant au locataire A sont protégés par un codage d'effacement 2+1 sur un seul site, tandis que les objets appartenant à tous les autres locataires sont protégés sur deux sites à l'aide d'une réplication à 2 copies.

Règle 1 : Code d'effacement sur un seul site pour le locataire A

Définition de la règle	Exemple de valeur
Nom de la règle	Codage d'effacement sur un seul site pour le locataire A
Compte locataire	Locataire A
Piscine de stockage	Site 1
Placements	Codage 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 la règle	Exemple de valeur
Nom de la règle	Réplication sur deux sites pour d'autres locataires
Compte locataire	Ignorer
Piscines de stockage	Site 1 et Site 2
Placements	Deux copies répliquées du jour 0 jusqu'à toujours : une copie sur le site 1 et une copie sur le site 2.

Politique ILM pour l'exemple 6 : Protection des données sur trois sites

Dans cet exemple, la politique ILM est remplacée par une nouvelle politique 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). Ensuite, l'administrateur a créé deux nouvelles règles ILM et une nouvelle politique ILM, conçues pour protéger les données sur les trois sites.

Lorsque cette nouvelle politique ILM est activée, les objets appartenant au locataire A seront protégés par un codage d'effacement 2+1 sur trois sites, tandis que les objets appartenant à d'autres locataires (et les objets plus petits appartenant au locataire A) seront protégés sur trois sites à l'aide d'une réplication à 3 copies.

Règle 1 : Codage d'effacement à trois sites pour le locataire A

Définition de la règle	Exemple de valeur
Nom de la règle	Codage d'effacement à trois sites pour le locataire A
Compte locataire	Locataire A
Piscine de stockage	Les 3 sites (comprend le site 1, le site 2 et le site 3)
Placements	Codage d'effacement 2+1 sur les 3 sites du jour 0 à pour toujours

Règle 2 : Réplication sur trois sites pour d'autres locataires

Définition de la règle	Exemple de valeur
Nom de la règle	Réplication sur trois sites pour d'autres locataires
Compte locataire	Ignorer
Piscines de stockage	Site 1, Site 2 et Site 3
Placements	Trois copies répliquées du jour 0 jusqu'à 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 par exemple 6

Lorsque vous activez une nouvelle stratégie ILM, les objets existants peuvent être déplacés vers de nouveaux emplacements ou de nouvelles copies d'objets peuvent être créées pour les objets existants, en fonction des instructions de placement dans toutes les règles nouvelles ou mises à jour.



Des erreurs dans une politique ILM peuvent entraîner une perte de données irréversible. Examinez et simulez attentivement la politique avant de l'activer pour confirmer qu'elle fonctionnera comme prévu.



Lorsque vous activez une nouvelle stratégie ILM, StorageGRID l'utilise pour gérer tous les objets, y compris les objets existants et les objets nouvellement ingérés. Avant d'activer une nouvelle stratégie ILM, vérifiez toutes les modifications apportées au placement des objets répliqués et codés par effacement existants. La modification de l'emplacement d'un objet existant peut entraîner des problèmes de ressources temporaires lorsque les nouveaux emplacements sont évalués et mis en œuvre.

Que se passe-t-il lorsque les instructions de codage d'effacement changent

Dans la politique ILM actuellement active pour cet exemple, les objets appartenant au locataire A sont protégés à l'aide du codage d'effacement 2+1 sur le site 1. Dans la nouvelle politique ILM, les objets appartenant au locataire A seront protégés à l'aide du codage d'effacement 2+1 sur les sites 1, 2 et 3.

Lorsque la nouvelle politique 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 dans un site différent.
- Les objets existants appartenant au locataire A sont réévalués pendant le processus d'analyse ILM en cours. Étant donné que les instructions de placement ILM utilisent un nouveau profil de codage d'effacement, des fragments entièrement nouveaux codés par effacement sont créés et distribués aux trois sites.



Les fragments 2+1 existants sur le site 1 ne sont pas réutilisés. StorageGRID considère que chaque profil de codage d'effacement est unique et ne réutilise pas les fragments de codage d'effacement lorsqu'un nouveau profil est utilisé.

Que se passe-t-il lorsque les instructions de réplication changent

Dans la stratégie ILM actuellement active pour cet exemple, les objets appartenant à d'autres locataires sont protégés à l'aide de deux copies répliquées dans les pools de stockage des sites 1 et 2. Dans la nouvelle politique ILM, les objets appartenant à d'autres locataires seront protégés à l'aide de trois copies répliquées dans les pools de stockage des sites 1, 2 et 3.

Lorsque la nouvelle politique 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 enregistre une copie sur chaque site.
- Les objets existants appartenant à ces autres locataires sont réévalués pendant le processus d'analyse ILM en cours. Étant donné que les copies d'objet existantes sur le site 1 et le site 2 continuent de satisfaire aux exigences de réplication de la nouvelle règle ILM, StorageGRID n'a besoin de créer qu'une seule nouvelle copie de l'objet pour le site 3.

Impact sur les performances de l'activation de cette politique

Lorsque la politique ILM de cet exemple est activée, les performances globales de ce système StorageGRID seront temporairement affectées. Des niveaux de ressources de grille supérieurs à la normale seront nécessaires pour créer de nouveaux fragments codés par effacement pour les objets existants du locataire A et de nouvelles copies répliquées sur le site 3 pour les objets existants des autres locataires.

En raison du changement de politique ILM, les demandes de lecture et d'écriture des clients peuvent temporairement subir des latences supérieures à la normale. Les latences reviendront à des niveaux normaux une fois les instructions de placement entièrement implémentées sur la grille.

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 n'importe quelle règle susceptible de modifier l'emplacement d'un grand nombre d'objets existants. Définissez le temps d'ingestion comme étant supérieur ou égal à l'heure approximative à laquelle la nouvelle politique entrera en vigueur pour garantir que les objets existants ne sont pas déplacés inutilement.



Contactez le support technique si vous devez ralentir ou augmenter la vitesse à laquelle les objets sont traités après une modification de la politique ILM.

Exemple 7 : Politique ILM conforme pour le verrouillage d'objet S3

Vous pouvez utiliser le compartiment S3, les règles ILM et la stratégie ILM de cet exemple comme point de départ lors de la définition d'une stratégie ILM pour répondre aux exigences de protection et de conservation des objets dans les compartiments avec le verrouillage des objets S3 activé.



Si vous avez utilisé la fonctionnalité de conformité héritée dans les versions précédentes de StorageGRID , vous pouvez également utiliser cet exemple pour vous aider à gérer tous les buckets existants pour lesquels la fonctionnalité de conformité héritée est activée.



Les règles et politiques ILM suivantes ne sont que des exemples. Il existe de nombreuses façons de configurer les règles ILM. Avant d'activer une nouvelle politique, simulez-la pour confirmer qu'elle fonctionnera comme prévu pour protéger le contenu contre la perte.

Informations connexes

- ["Gérer les objets avec S3 Object Lock"](#)
- ["Créer une politique ILM"](#)

Exemple de bucket et d'objets pour le verrouillage d'objet S3

Dans cet exemple, un compte locataire S3 nommé Bank of ABC a utilisé Tenant Manager pour créer un bucket avec S3 Object Lock activé pour stocker les enregistrements bancaires critiques.

Définition du bucket	Exemple de valeur
Nom du compte du locataire	Banque ABC
Nom du bucket	relevés bancaires
Région du seau	us-east-1 (par défaut)

Chaque objet et version d'objet ajouté au compartiment des enregistrements bancaires utilisera les valeurs suivantes pour `retain-until-date` et `legal hold` paramètres.

Réglage pour chaque objet	Exemple de valeur
<code>retain-until-date</code>	30 décembre 2030 (2030-12-30T23:59:59Z) Chaque version d'objet possède sa propre <code>retain-until-date</code> paramètre. Ce paramètre peut être augmenté, mais pas diminué.
<code>legal hold</code>	"OFF" (sans effet) Une suspension légale peut être placée ou levée sur n'importe quelle version d'objet à tout moment pendant la période de conservation. Si un objet est sous une suspension légale, l'objet ne peut pas être supprimé même si le <code>retain-until-date</code> a été atteint.

Exemple de règle ILM 1 pour le verrouillage d'objet S3 : profil de codage d'effacement avec correspondance de compartiment

Cet exemple de règle ILM s'applique uniquement au compte locataire S3 nommé Bank of ABC. Il correspond à n'importe quel objet dans le `bank-records` bucket et utilise ensuite le codage d'effacement pour stocker l'objet sur des nœuds de stockage sur trois sites de centres de données à l'aide d'un profil de codage d'effacement 6+3. Cette règle répond aux exigences des buckets avec S3 Object Lock activé : une copie est conservée sur les nœuds de stockage du jour 0 à indéfiniment, en utilisant l'heure d'ingestion comme heure de référence.

Définition de la règle	Exemple de valeur
Nom de la règle	Règle de conformité : Objets EC dans le compartiment des enregistrements bancaires - Banque ABC
Compte locataire	Banque ABC
Nom du bucket	<code>bank-records</code>
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 moins.

Définition de la règle	Exemple de valeur
Heure de référence	Temps d'ingestion
Placements	À partir du jour 0, stockez pour toujours
Profil de codage d'effacement	- Créer une copie codée à effacement sur les nœuds de stockage de trois sites de centres de données - Utilise le schéma de codage d'effacement 6+3

Règle ILM 2 pour l'exemple de verrouillage d'objet S3 : règle non conforme

Cet exemple de règle ILM stocke initialement deux copies d'objets répliquées sur des nœuds de stockage. Après un an, il stocke une copie sur un pool de stockage cloud pour toujours. Étant donné que cette règle utilise un pool de stockage cloud, elle n'est pas conforme et ne s'appliquera pas aux objets des buckets avec le verrouillage d'objet S3 activé.

Définition de la règle	Exemple de valeur
Nom de la règle	Règle non conforme : utiliser le pool de stockage cloud
Comptes locataires	Non spécifié
Nom du bucket	Non spécifié, mais ne s'appliquera qu'aux buckets pour lesquels le verrouillage d'objet S3 (ou la fonctionnalité de conformité héritée) n'est pas activé.
Filtre avancé	Non spécifié

Définition de la règle	Exemple de valeur
Heure de référence	Temps d'ingestion
Placements	• Le jour 0, conservez deux copies répliquées sur les nœuds de stockage du centre de données 1 et du centre de données 2 pendant 365 jours • Après 1 an, conservez une copie répliquée dans un pool de stockage cloud pour toujours

Exemple de règle 3 ILM pour le verrouillage d'objet S3 : règle par défaut

Cet exemple de règle ILM copie les données d'objet dans des pools de stockage dans deux centres de données. Cette règle conforme est conçue pour être la règle par défaut dans la politique ILM. Il n'inclut aucun filtre, n'utilise pas l'heure de référence non actuelle et satisfait les exigences des buckets avec S3 Object Lock activé : deux copies d'objet sont conservées sur les nœuds de stockage du jour 0 à indéfiniment, en utilisant Ingest comme heure de référence.

Définition de la règle	Exemple de valeur
Nom de la règle	Règle de conformité par défaut : deux copies, deux centres de données
Compte locataire	Non spécifié
Nom du bucket	Non spécifié
Filtre avancé	Non spécifié

Définition de la règle	Exemple de valeur
Heure de référence	Temps d'ingestion
Placements	Du jour 0 à la fin des temps, conservez deux copies répliquées : une sur les nœuds de stockage du centre de données 1 et une sur les nœuds de stockage du centre de données 2.

Exemple de politique ILM conforme pour le verrouillage d'objet S3

Pour créer une stratégie ILM qui protégera efficacement tous les objets de votre système, y compris ceux des compartiments avec le verrouillage d'objet S3 activé, vous devez sélectionner des règles ILM qui répondent aux exigences de stockage de tous les objets. Ensuite, vous devez simuler et activer la politique.

Ajouter des règles à la politique

Dans cet exemple, la politique ILM comprend trois règles ILM, dans l'ordre suivant :

1. Une règle conforme qui utilise le codage d'effacement pour protéger les objets supérieurs à 1 Mo dans un compartiment spécifique avec le verrouillage d'objet S3 activé. Les objets sont stockés sur des nœuds de stockage du jour 0 jusqu'à toujours.
2. Une règle non conforme qui crée deux copies d'objet répliquées sur des nœuds de stockage pendant un an, puis déplace une copie d'objet vers un pool de stockage cloud pour toujours. Cette règle ne s'applique pas aux buckets avec S3 Object Lock activé, car il 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 pour toujours.

Simuler la politique

Après avoir ajouté des règles à votre stratégie, choisi une règle conforme par défaut et organisé les autres règles, vous devez simuler la stratégie en testant les objets du bucket avec le verrouillage d'objet S3 activé et d'autres buckets. Par exemple, lorsque vous simulez l'exemple de politique, vous vous attendez à ce que les objets de test soient évalués comme suit :

- La première règle correspondra uniquement aux objets de test dont la taille est supérieure à 1 Mo dans le bucket bank-records pour le locataire Bank of ABC.
- La deuxième règle correspondra à tous les objets de tous les compartiments non conformes pour tous les autres comptes locataires.
- La règle par défaut correspondra à ces objets :
 - Objets de 1 Mo ou moins dans le bucket bank-records pour le locataire de la Banque ABC.
 - Objets dans tout autre compartiment pour lequel le verrouillage d'objet S3 est activé pour tous les autres comptes de locataire.

Activer la politique

Lorsque vous êtes entièrement satisfait que la nouvelle politique protège les données de l'objet comme prévu, vous pouvez l'activer.

Exemple 8 : Priorités pour le cycle de vie du bucket S3 et la politique ILM

Selon la configuration de votre cycle de vie, les objets suivent les paramètres de conservation du cycle de vie du compartiment S3 ou d'une stratégie ILM.

Exemple de cycle de vie d'un bucket prioritaire sur la politique ILM

Politique ILM

- Règle basée sur une référence temporelle non courante : le jour 0, conserver X copies pendant 20 jours
- Règle basée sur la référence temporelle d'ingestion (par défaut) : le jour 0, conserver X copies pendant 50 jours

Cycle de vie du bucket

```
"Filter": {"Prefix": "docs/"}, "Expiration": {"Days": 100},  
"NoncurrentVersionExpiration": {"NoncurrentDays": 5}
```

Résultat

- Un objet nommé « docs/text » est ingéré. Il correspond au filtre de cycle de vie du bucket du préfixe « docs/ ».
 - Après 100 jours, un marqueur de suppression est créé et « docs/text » devient non actuel.
 - Après 5 jours, soit un total de 105 jours depuis l'ingestion, « docs/text » est supprimé.
 - Après 95 jours, soit un total de 200 jours depuis l'ingestion et 100 jours depuis la création du marqueur de suppression, le marqueur de suppression expiré est supprimé.
- Un objet nommé « vidéo/film » est ingéré. Il ne correspond pas au filtre et utilise la politique de rétention ILM.
 - Après 50 jours, un marqueur de suppression est créé et « vidéo/film » devient obsolète.
 - Après 20 jours, soit un total de 70 jours depuis l'ingestion, la « vidéo/le film » est supprimé.
 - Après 30 jours, un total de 100 jours depuis l'ingestion et 50 jours depuis la création du marqueur de suppression, le marqueur de suppression expiré est supprimé.

Exemple de cycle de vie d'un bucket implicitement conservé pour toujours

Politique ILM

- Règle basée sur une référence temporelle non courante : le jour 0, conserver X copies pendant 20 jours
- Règle basée sur la référence temporelle d'ingestion (par défaut) : le jour 0, conserver X copies pendant 50 jours

Cycle de vie du bucket

```
"Filter": {"Prefix": "docs/"}, "Expiration": {"ExpiredObjectDeleteMarker":  
true}
```

Résultat

- Un objet nommé « docs/text » est ingéré. Il correspond au filtre de cycle de vie du bucket du préfixe « docs/ ».

Le `Expiration` l'action s'applique uniquement aux marqueurs de suppression expirés, ce qui implique de conserver tout le reste pour toujours (en commençant par « docs/ »).

Les marqueurs de suppression commençant par « docs/ » sont supprimés lorsqu'ils expirent.

- Un objet nommé « vidéo/film » est ingéré. Il ne correspond pas au filtre et utilise la politique de rétention ILM.
 - Après 50 jours, un marqueur de suppression est créé et « vidéo/film » devient obsolète.
 - Après 20 jours, soit un total de 70 jours depuis l'ingestion, la « vidéo/le film » est supprimé.
 - Après 30 jours, un total de 100 jours depuis l'ingestion et 50 jours depuis la création du marqueur de suppression, le marqueur de suppression expiré est supprimé.

Exemple d'utilisation du cycle de vie du bucket pour dupliquer ILM et nettoyer les marqueurs de suppression expirés

Politique ILM

- Règle basée sur une référence temporelle non courante : le jour 0, conserver X copies pendant 20 jours
- Règle basée sur la référence temporelle d'ingestion (par défaut) : le jour 0, conserver X copies pour toujours

Cycle de vie du bucket

```
"Filter": {}, "Expiration": {"ExpiredObjectDeleteMarker": true},
"NoncurrentVersionExpiration": {"NoncurrentDays": 20}
```

Résultat

- La politique ILM est dupliquée dans le cycle de vie du bucket.
 - La règle permanente de la politique ILM est conçue pour supprimer manuellement les objets et nettoyer les versions non actuelles après 20 jours. Par conséquent, la règle d'ingestion conservera les marqueurs de suppression expirés pour toujours.
 - Le cycle de vie du bucket duplique le comportement de la politique ILM lors de l'ajout "ExpiredObjectDeleteMarker": true, qui supprime les marqueurs de suppression une fois qu'ils ont expiré
- Un objet est ingéré. L'absence de filtre signifie que le cycle de vie du bucket s'applique à tous les objets et remplace les paramètres de conservation ILM.
 - Lorsqu'un locataire émet une demande de suppression d'objet, un marqueur de suppression est créé et l'objet devient non actuel.
 - Après 20 jours, l'objet non actuel est supprimé et le marqueur de suppression devient expiré.
 - Peu de temps après, le marqueur de suppression expiré est supprimé.

Renforcement du système

Considérations générales pour le renforcement du système

Le renforcement du système est le processus consistant à éliminer autant de risques de sécurité que possible d'un système StorageGRID .

Lorsque vous installez et configurez StorageGRID, utilisez ces instructions pour vous aider à atteindre les objectifs de sécurité prescrits en matière de confidentialité, d'intégrité et de disponibilité.

Vous devriez déjà utiliser les meilleures pratiques standard de l'industrie pour le renforcement du système. Par exemple, vous utilisez des mots de passe forts pour StorageGRID, utilisez HTTPS au lieu de HTTP et activez l'authentification basée sur les certificats lorsqu'elle est disponible.

StorageGRID suit le ["Politique de gestion des vulnérabilités NetApp"](#) . Les vulnérabilités signalées sont

vérifiées et traitées conformément au processus de réponse aux incidents de sécurité du produit.

Lors du renforcement d'un système StorageGRID , tenez compte des éléments suivants :

- ***Lequel des trois réseaux StorageGRID * avez-vous implémenté ?** Tous les systèmes StorageGRID doivent utiliser le réseau Grid, mais vous pouvez également utiliser le réseau administrateur, le réseau client ou les deux. Chaque réseau a des considérations de sécurité différentes.
- **Le type de plates-formes** que vous utilisez pour les nœuds individuels de votre système StorageGRID . Les nœuds StorageGRID peuvent être déployés sur des machines virtuelles VMware, au sein d'un moteur de conteneur sur des hôtes Linux ou en tant qu'appliances matérielles dédiées. Chaque type de plateforme possède son propre ensemble de bonnes pratiques de renforcement.
- **Dans quelle mesure les comptes des locataires sont-ils fiables.** Si vous êtes un fournisseur de services avec des comptes locataires non approuvés, vous aurez des problèmes de sécurité différents de ceux que vous rencontreriez si vous utilisiez uniquement des locataires internes approuvés.
- **Quelles exigences et conventions de sécurité** votre organisation suit. Vous devrez peut-être vous conformer à des exigences réglementaires ou d'entreprise spécifiques.

Directives de renforcement pour les mises à niveau logicielles

Vous devez maintenir votre système StorageGRID et les services associés à jour pour vous défendre 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 majeure la plus récente ou vers la version majeure précédente. Maintenir StorageGRID à jour permet de réduire la durée pendant laquelle les vulnérabilités connues sont actives et réduit la surface d'attaque globale. De plus, les versions les plus récentes de StorageGRID contiennent souvent des fonctionnalités de renforcement de la sécurité qui ne sont pas incluses dans les versions précédentes.

Consultez le "[Outil de matrice d'interopérabilité NetApp](#)" (IMT) pour déterminer quelle version du logiciel StorageGRID vous devez utiliser. Lorsqu'un correctif est requis, NetApp donne la priorité à la création de mises à jour pour les versions les plus récentes. Certains correctifs peuvent ne pas être compatibles avec les versions antérieures.

- Pour télécharger les versions et correctifs les plus récents de StorageGRID , accédez à "[Téléchargements NetApp : StorageGRID](#)" .
- Pour mettre à niveau le logiciel StorageGRID , consultez le "[instructions de mise à niveau](#)" .
- Pour appliquer un correctif, consultez le "[Procédure de correctif logiciel StorageGRID](#)" .

Mises à niveau des services externes

Les services externes peuvent présenter des vulnérabilités qui affectent StorageGRID indirectement. Vous devez vous assurer que les services dont dépend StorageGRID sont maintenus à jour. Ces services incluent LDAP, KMS (ou serveur KMIP), DNS et NTP.

Pour une liste des versions prises en charge, consultez le "[Outil de matrice d'interopérabilité NetApp](#)" .

Mises à niveau des hyperviseurs

Si vos nœuds StorageGRID s'exécutent sur VMware ou un autre hyperviseur, vous devez vous assurer que le logiciel et le micrologiciel de l'hyperviseur sont à jour.

Pour une liste des versions prises en charge, consultez le ["Outil de matrice d'interopérabilité NetApp"](#) .

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 les mises à jour du noyau sont appliquées au système d'exploitation hôte. De plus, vous devez appliquer les mises à jour du micrologiciel au matériel vulnérable lorsque ces mises à jour sont disponibles.

Pour une liste des versions prises en charge, consultez le ["Outil de matrice d'interopérabilité NetApp"](#) .

Directives de renforcement pour les réseaux StorageGRID

Le système StorageGRID prend en charge jusqu'à trois interfaces réseau par nœud de grille, vous permettant de configurer la mise en réseau de chaque nœud de grille individuel afin de répondre à vos exigences de sécurité et d'accès.

Pour des informations détaillées sur les réseaux StorageGRID , consultez le ["Types de réseaux StorageGRID"](#) .

Lignes directrices pour le réseau de grille

Vous devez configurer un réseau Grid pour tout le trafic StorageGRID interne. Tous les nœuds de grille sont sur le réseau de grille et doivent pouvoir communiquer avec tous les autres nœuds.

Lors de la configuration du réseau Grid, suivez ces instructions :

- Assurez-vous que le réseau est sécurisé contre les clients non fiables, tels que ceux présents sur Internet ouvert.
- Dans la mesure du possible, utilisez le réseau Grid exclusivement pour le trafic interne. Le réseau d'administration et le réseau client disposent tous deux de restrictions de pare-feu supplémentaires 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 centres de données, utilisez un réseau privé virtuel (VPN) ou équivalent sur le réseau Grid pour fournir une protection supplémentaire au trafic interne.
- Certaines procédures de maintenance nécessitent un accès Secure Shell (SSH) sur le port 22 entre le nœud d'administration principal et tous les autres nœuds de grille. Utilisez un pare-feu externe pour restreindre l'accès SSH aux clients de confiance.

Directives pour le réseau d'administration

Le réseau d'administration est généralement utilisé pour les tâches administratives (employés de confiance utilisant Grid Manager ou SSH) et pour communiquer avec d'autres services de confiance tels que LDAP, DNS, NTP ou KMS (ou serveur KMIP). Cependant, StorageGRID n'applique pas cette utilisation en interne.

Si vous utilisez le réseau d'administration, suivez ces instructions :

- Bloquez tous les ports de trafic internes sur le réseau d'administration. Voir le ["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.

Lignes directrices pour le réseau de clients

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 plateforme. Cependant, StorageGRID n'applique pas cette utilisation en interne.

Si vous utilisez le réseau client, suivez ces directives :

- Bloquez tous les ports de trafic internes sur le réseau client. Voir le ["liste des ports internes"](#) .
- Acceptez le trafic client entrant uniquement sur les points de terminaison explicitement configurés. Voir les informations sur ["gestion des contrôles du pare-feu"](#) .

Directives de renforcement pour les nœuds StorageGRID

Les nœuds StorageGRID peuvent être déployés sur des machines virtuelles VMware, au sein d'un moteur de conteneur sur des hôtes Linux ou en tant qu'appliances matérielles dédiées. Chaque type de plateforme et chaque type de nœud possède son propre ensemble de bonnes pratiques de renforcement.

Contrôler l'accès IPMI à distance au BMC

Vous pouvez activer ou désactiver l'accès IPMI à distance pour tous les appareils contenant un BMC. L'interface IPMI distante permet l'accès matériel de bas niveau à vos appliances StorageGRID par toute personne disposant d'un compte BMC et d'un mot de passe. Si vous n'avez pas besoin d'un accès IPMI à distance au BMC, désactivez cette option.

- Pour contrôler l'accès IPMI à distance au BMC dans Grid Manager, accédez à **CONFIGURATION > Sécurité > Paramètres de sécurité > Appliances** :
 - Décochez la case **Activer l'accès IPMI à distance** pour désactiver l'accès IPMI au BMC.
 - Cochez la case **Activer l'accès IPMI à distance** pour activer l'accès IPMI au BMC.

Configuration du pare-feu

Dans le cadre du processus de renforcement du système, vous devez vérifier les configurations du pare-feu externe 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 inclut un pare-feu interne sur chaque nœud qui améliore la sécurité de votre grille en vous permettant de contrôler l'accès réseau au nœud. Tu devrais ["gérer les contrôles du pare-feu interne"](#) 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 que vous effectuez sur la page de contrôle du pare-feu sont déployées sur chaque nœud.

Plus précisément, vous pouvez gérer ces domaines :

- **Adresses privilégiées** : Vous pouvez autoriser les adresses IP ou les sous-réseaux sélectionnés 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 de protection supplémentaire contre certaines menaces courantes, il ne supprime pas le besoin d'un pare-feu externe.

Pour une liste de tous les ports internes et externes utilisés par StorageGRID, voir "[Référence du port réseau](#)".

Désactiver les services inutilisés

Pour tous les nœuds StorageGRID, vous devez désactiver ou bloquer l'accès aux services inutilisés. Par exemple, si vous ne prévoyez pas d'utiliser DHCP, utilisez le gestionnaire de grille pour fermer le port 68. Sélectionnez **CONFIGURATION > Contrôle du pare-feu > Gérer l'accès externe**. Modifiez ensuite le statut du port 68 de **Ouvert** à **Fermé**.

Virtualisation, conteneurs et matériel partagé

Pour tous les nœuds StorageGRID, évitez d'exécuter StorageGRID sur le même matériel physique que des logiciels non approuvés. Ne présumez pas que les protections de l'hyperviseur empêcheront 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 Spectre exploitent les vulnérabilités critiques des 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 via le réseau lorsque les nœuds sont en cours d'installation. Les nœuds ne sont pas totalement sécurisés tant qu'ils n'ont pas rejoint le réseau.

Directives pour les nœuds d'administration

Les nœuds d'administration fournissent des services de gestion tels que la configuration du système, la surveillance et la journalisation. Lorsque vous vous connectez au gestionnaire de grille ou au gestionnaire de locataires, vous vous connectez à un nœud d'administration.

Suivez ces instructions pour sécuriser les nœuds d'administration de votre système StorageGRID :

- Sécurisez tous les nœuds d'administration contre les clients non fiables, tels que ceux présents sur Internet ouvert. Assurez-vous qu'aucun client non approuvé ne peut accéder à un nœud d'administration sur le réseau de grille, 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 points de terminaison d'équilibrage de charge StorageGRID, utilisez des nœuds de passerelle au lieu des nœuds d'administration pour le trafic client non approuvé.
- Si vous avez des locataires non approuvés, ne leur permettez pas d'avoir un accès direct au gestionnaire de locataires ou à l'API de gestion des locataires. Au lieu de cela, demandez à tous les locataires non approuvés d'utiliser un portail de locataires ou un système de gestion de locataires externe, qui interagit avec l'API de gestion des locataires.
- Vous pouvez également utiliser un proxy d'administration pour un meilleur contrôle sur la communication AutoSupport des nœuds d'administration vers le support NetApp. Voir les étapes pour "[création d'un proxy d'administration](#)".
- Vous pouvez également utiliser les ports restreints 8443 et 9443 pour séparer les communications de Grid Manager et de Tenant Manager. Bloquez le port partagé 443 et limitez les demandes des locataires au port

9443 pour une protection supplémentaire.

- Vous pouvez également utiliser des nœuds d'administration distincts pour les administrateurs de grille et les utilisateurs locataires.

Pour plus d'informations, consultez les instructions pour [administrer StorageGRID](#) .

Directives pour les nœuds de stockage

Les nœuds de stockage gèrent et stockent les données et les métadonnées des objets. Suivez ces directives pour sécuriser les nœuds de stockage dans votre système StorageGRID .

- N'autorisez pas les clients non approuvés à se connecter directement aux nœuds de stockage. Utilisez un point de terminaison d'équilibrage de charge servi 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 d'un compte pour un locataire non approuvé, n'autorisez pas le locataire à utiliser sa propre source d'identité et n'autorisez pas l'utilisation des services de la plateforme. Voir les étapes pour [créer un compte locataire](#) .
- Utilisez un équilibreur de charge tiers pour le trafic client non fiable. L'équilibrage de charge tiers offre davantage de contrôle et des couches de protection supplémentaires contre les attaques.
- Vous pouvez également utiliser un proxy de stockage pour un meilleur contrôle sur les pools de stockage Cloud et la communication des services de plateforme des nœuds de stockage vers les services externes. Voir les étapes pour [création d'un proxy de stockage](#) .
- En option, connectez-vous à des services externes à l'aide du réseau client. Ensuite, sélectionnez **CONFIGURATION > Sécurité > Contrôle du pare-feu > Réseaux clients non approuvés** et indiquez que le réseau client sur le nœud de stockage n'est pas approuvé. Le nœud de stockage n'accepte plus aucun trafic entrant sur le réseau client, mais il continue d'autoriser les demandes sortantes pour les services de plate-forme.

Directives pour les nœuds de passerelle

Les nœuds de passerelle fournissent une interface d'équilibrage de charge facultative que les applications clientes peuvent utiliser pour se connecter à StorageGRID. Suivez ces directives pour sécuriser tous les nœuds de passerelle de votre système StorageGRID :

- Configurer et utiliser les points de terminaison de l'équilibreur 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 approuvé. L'équilibrage de charge tiers offre davantage de contrôle et des couches de protection supplémentaires contre les attaques. Si vous utilisez un équilibreur de charge tiers, le trafic réseau peut toujours être configuré pour passer par un point de terminaison d'équilibreur de charge interne ou être envoyé directement aux nœuds de stockage.
- Si vous utilisez des points de terminaison d'équilibrage de charge, vous pouvez éventuellement demander aux clients de se connecter via le réseau client. Ensuite, sélectionnez **CONFIGURATION > Sécurité > Contrôle du pare-feu > Réseaux clients non approuvés** et indiquez que le réseau client sur le nœud de passerelle n'est pas approuvé. Le nœud de passerelle accepte uniquement le trafic entrant sur les ports explicitement configurés comme points de terminaison d'équilibrage de charge.

Directives pour les nœuds d'appareils matériels

Les appareils matériels StorageGRID sont spécialement conçus pour être utilisés dans un système StorageGRID . Certains appareils peuvent être utilisés comme nœuds de stockage. D'autres appareils

peuvent être utilisés comme nœuds d'administration ou nœuds de passerelle. Vous pouvez combiner des nœuds d'appareils avec des nœuds basés sur des logiciels ou déployer des grilles entièrement conçues et composées d'appareils.

Suivez ces instructions pour sécuriser tous les nœuds d'appareils matériels de votre système StorageGRID :

- Si l'appliance utilise SANtricity System Manager pour la gestion du contrôleur de stockage, empêchez les clients non approuvés d'accéder à SANtricity System Manager via le réseau.
- Si l'appareil dispose d'un contrôleur de gestion de la carte mère (BMC), sachez que le port de gestion BMC permet un accès matériel de bas niveau. Connectez le port de gestion BMC uniquement à un réseau de gestion interne sécurisé et fiable. Si aucun réseau de ce type n'est disponible, laissez le port de gestion BMC déconnecté ou bloqué, sauf si une connexion BMC est demandée par le support technique.
- Si l'appareil 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 approuvé sur le port 623.



Vous pouvez activer ou désactiver l'accès IPMI à distance pour tous les appareils contenant un BMC. L'interface IPMI distante permet l'accès matériel de bas niveau à vos appliances StorageGRID par toute personne disposant d'un compte BMC et d'un mot de passe. Si vous n'avez pas besoin d'un accès IPMI à distance au BMC, désactivez cette option à l'aide de l'une des méthodes suivantes : + Dans Grid Manager, accédez à **CONFIGURATION > Sécurité > Paramètres de sécurité > Appliances** et décochez la case **Activer l'accès IPMI à distance**. + Dans l'API de gestion de grille, utilisez le point de terminaison privé : `PUT /private/bmc`.

- Pour les modèles d'appareils contenant des disques SED, FDE ou FIPS NL-SAS que vous gérez avec SANtricity System Manager, "[activer et configurer SANtricity Drive Security](#)".
- Pour les modèles d'appareils contenant des SSD NVMe SED ou FIPS que vous gérez à l'aide du programme d'installation de l'appareil StorageGRID et du gestionnaire de grille, "[activer et configurer le chiffrement du lecteur StorageGRID](#)".
- Pour les appareils sans lecteurs SED, FDE ou FIPS, activez et configurez le chiffrement des nœuds logiciels StorageGRID "[en utilisant un serveur de gestion de clés \(KMS\)](#)".

Directives de renforcement pour TLS et SSH

Vous devez remplacer les certificats par défaut créés lors de l'installation et sélectionner la politique 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 Web StorageGRID n'est pas conforme à leurs politiques de sécurité des informations. 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** : utilisé pour sécuriser l'accès aux nœuds de stockage et aux nœuds de passerelle, que

les applications clientes S3 utilisent pour télécharger et charger 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 points de terminaison de l'équilibreur de charge. Pour configurer les certificats d'équilibrage de charge, voir "[Configurer les points de terminaison de l'équilibreur de charge](#)".

Lorsque vous utilisez des certificats de serveur personnalisés, suivez ces instructions :

- Les certificats doivent avoir un `subjectAltName` qui correspond aux entrées DNS pour StorageGRID. Pour plus de détails, voir la section 4.2.1.6, « Nom alternatif du sujet », dans "[RFC 5280 : Certificat PKIX et profil CRL](#)".
- Dans la mesure du possible, évitez l'utilisation de certificats génériques. Une exception à cette directive est le certificat d'un point de terminaison de style hébergé virtuel S3, qui 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 modèle générique tel que `*.s3.example.com`, et n'utilisez pas le `s3.example.com` suffixe pour d'autres applications. Ce modèle fonctionne également avec l'accès S3 de type chemin, tel que `dc1-s1.s3.example.com/mybucket`.
- Définissez les délais d'expiration des certificats sur une durée courte (par exemple, 2 mois) et utilisez l'API Grid Management pour automatiser la rotation des certificats. Ceci est particulièrement important pour les certificats génériques.

De plus, les clients doivent utiliser une vérification stricte du nom d'hôte lors de la communication avec StorageGRID.

Directives de renforcement des politiques TLS et SSH

Vous pouvez sélectionner une politique de sécurité pour déterminer quels protocoles et chiffrements sont utilisés pour établir des connexions TLS sécurisées avec les applications clientes et des connexions SSH sécurisées aux services StorageGRID internes.

La politique de sécurité contrôle la manière dont TLS et SSH chiffrent les données en mouvement. En tant que bonne pratique, vous devez désactiver les options de chiffrement qui ne sont pas nécessaires à la compatibilité des applications. Utilisez la politique moderne par défaut, sauf si votre système doit être conforme aux critères communs ou si vous devez utiliser d'autres chiffrements.

Voir "[Gérer la politique TLS et SSH](#)" pour plus de détails et d'instructions.

Autres directives de durcissement

En plus de suivre les directives de renforcement pour les réseaux et les nœuds StorageGRID, vous devez suivre les directives de renforcement pour les autres zones du système StorageGRID.

Mot de passe d'installation temporaire

Pour sécuriser le système StorageGRID pendant l'installation, définissez un mot de passe sur la page de mot de passe du programme d'installation temporaire dans l'interface utilisateur d'installation de StorageGRID ou dans l'API d'installation. Une fois défini, ce mot de passe s'applique à toutes les méthodes d'installation de StorageGRID, y compris l'interface utilisateur, l'API d'installation et `configure-storagegrid.py` scénario.

Pour plus d'informations, reportez-vous à :

- ["Installer StorageGRID sur Red Hat Enterprise Linux"](#)
- ["Installer StorageGRID sur Ubuntu ou Debian"](#)
- ["Installer StorageGRID sur VMware"](#)
- ["Installer l'appliance 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. De plus, les informations et les détails contenus dans les journaux StorageGRID et dans la sortie des messages d'audit sont généralement de nature sensible.

Configurez StorageGRID pour envoyer des événements de sécurité à un serveur syslog externe. Si vous utilisez l'exportation Syslog, sélectionnez TLS et RELP/TLS pour les protocoles de transport.

Voir le ["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 fonctionnalité AutoSupport de StorageGRID vous permet de surveiller de manière proactive l'état de votre système et d'envoyer automatiquement des packages au site de support NetApp , à l'équipe de support interne de votre organisation ou à un partenaire de support. Par défaut, l'envoi de packages AutoSupport à NetApp est activé lorsque StorageGRID est configuré pour la première fois.

La fonction AutoSupport peut être désactivée. Cependant, NetApp recommande de l'activer car AutoSupport permet d'accélérer l'identification et la résolution des problèmes en cas de problème sur votre système StorageGRID .

AutoSupport prend en charge HTTPS, HTTP et SMTP pour les protocoles de transport. En raison de la nature sensible des packages AutoSupport , NetApp recommande fortement d'utiliser HTTPS comme protocole de transport par défaut pour l'envoi de packages AutoSupport à NetApp.

Partage de ressources inter-origines (CORS)

Vous pouvez configurer le partage de ressources inter-origines (CORS) pour un bucket S3 si vous souhaitez que ce bucket et les objets qu'il contient soient accessibles aux applications Web d'autres domaines. En général, n'activez pas CORS à moins que cela ne soit nécessaire. Si CORS est requis, limitez-le aux origines fiables.

Voir les étapes pour ["configuration du partage de ressources inter-origines \(CORS\)"](#) .

Dispositifs de sécurité externes

Une solution de renforcement complète doit aborder les mécanismes de sécurité en dehors de StorageGRID. L'utilisation de périphériques d'infrastructure supplémentaires pour filtrer et limiter l'accès à StorageGRID est un moyen efficace d'établir et de maintenir une posture de sécurité stricte. Ces dispositifs de sécurité externes comprennent des pare-feu, des systèmes de prévention des intrusions (IPS) et d'autres dispositifs de sécurité.

Un équilibreur de charge tiers est recommandé pour le trafic client non fiable. L'équilibrage de charge tiers offre davantage de contrôle et des couches de protection supplémentaires contre les attaques.

Atténuation des risques de ransomware

Aidez à protéger vos données d'objet contre les attaques de ransomware en suivant les recommandations de ["Défense contre les ransomwares avec StorageGRID"](#) .

Configurer StorageGRID pour FabricPool

Configurer StorageGRID pour FabricPool

Si vous utilisez le logiciel NetApp ONTAP , vous pouvez utiliser NetApp FabricPool pour hiérarchiser les données inactives vers un système de stockage d'objets NetApp StorageGRID .

Utilisez ces instructions pour :

- Découvrez les considérations et les meilleures pratiques pour configurer StorageGRID pour une charge de travail FabricPool .
- Découvrez comment configurer un système de stockage d'objets StorageGRID à utiliser avec FabricPool.
- Découvrez comment fournir les valeurs requises à ONTAP lors de la connexion de StorageGRID en tant que niveau cloud FabricPool .

Démarrage rapide pour la configuration de StorageGRID pour FabricPool

1

Planifiez votre configuration

- Décidez quelle stratégie de hiérarchisation des volumes FabricPool vous utiliserez pour hiérarchiser les données ONTAP inactives vers StorageGRID.
- Planifiez et installez un système StorageGRID pour répondre à vos besoins de capacité de stockage et de performances.
- Familiarisez-vous avec le logiciel système StorageGRID , y compris le ["Gestionnaire de grille"](#) et le ["Gestionnaire de locataires"](#) .
- Consultez les meilleures pratiques de FabricPool pour ["groupes HA"](#) , ["équilibre de charge"](#) , ["ILM"](#) , et ["plus"](#) .
- Consultez ces ressources supplémentaires, qui fournissent des détails sur l'utilisation et la configuration ONTAP et de FabricPool:

["TR-4598 : Bonnes pratiques FabricPool dans ONTAP"](#)

["Documentation ONTAP pour FabricPool"](#)

2

Effectuer les tâches prérequis

Obtenez le ["informations nécessaires pour attacher StorageGRID en tant que niveau cloud"](#) , y compris:

- adresses IP
- noms de domaine
- Certificat SSL

En option, configurez ["fédération d'identité"](#) et ["authentification unique"](#) .

3

Configurer les paramètres de StorageGRID

Utilisez StorageGRID pour obtenir les valeurs dont ONTAP a besoin pour se connecter à la grille.

En utilisant le ["Assistant de configuration de FabricPool"](#) est le moyen recommandé et le plus rapide pour configurer tous les éléments, mais vous pouvez également configurer chaque entité manuellement, si nécessaire.

4

Configurer ONTAP et DNS

Utilisez ONTAP pour ["ajouter un niveau cloud"](#) qui utilise les valeurs StorageGRID . Alors, ["configurer les entrées DNS"](#) pour associer des adresses IP à tous les noms de domaine que vous prévoyez d'utiliser.

5

Surveiller et gérer

Lorsque votre système est opérationnel, effectuez des tâches continues dans ONTAP et StorageGRID pour gérer et surveiller la hiérarchisation 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 hautes performances comme niveau de performance et un magasin d'objets comme niveau cloud. L'utilisation d'agrégats compatibles FabricPool vous aide à réduire les coûts de stockage sans compromettre les performances, l'efficacité ou 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 à l'intérieur de FabricPool peuvent ensuite profiter de la hiérarchisation en conservant les données actives (chaudes) sur un stockage hautes performances (le niveau local) et en désactivant les données (froides) sur le magasin d'objets externe (le niveau cloud).

Aucune modification architecturale n'est requise et vous pouvez continuer à gérer vos données et votre environnement d'application à partir du système de stockage central ONTAP .

Qu'est-ce que StorageGRID?

NetApp StorageGRID est une architecture de stockage qui gère les données sous forme d'objets, contrairement à d'autres architectures de stockage telles que le stockage de fichiers ou de blocs. Les objets sont conservés dans un seul conteneur (tel qu'un bucket) et ne sont pas imbriqués en tant que fichiers dans un répertoire à l'intérieur d'autres répertoires. Bien que le stockage d'objets offre généralement des performances inférieures à celles du stockage de fichiers ou de blocs, il est nettement plus évolutif. Les buckets StorageGRID peuvent contenir des pétaoctets de données et des milliards d'objets.

Pourquoi utiliser StorageGRID comme niveau cloud FabricPool ?

FabricPool peut hiérarchiser les données ONTAP vers un certain nombre de fournisseurs de stockage d'objets, notamment StorageGRID. Contrairement aux clouds publics qui peuvent définir un nombre maximal d'opérations d'entrée/sortie prises en charge par seconde (IOPS) au niveau du bucket ou du conteneur, les performances de StorageGRID évoluent en fonction du nombre de nœuds d'un système. L'utilisation de StorageGRID comme niveau cloud FabricPool vous permet de conserver vos données froides dans votre

propre cloud privé pour des performances optimales et un contrôle complet sur vos données.

De plus, une licence FabricPool n'est pas requise lorsque vous utilisez StorageGRID comme niveau cloud.

Informations nécessaires pour attacher StorageGRID en tant que niveau cloud

Avant de pouvoir attacher StorageGRID en tant que niveau cloud pour FabricPool, vous devez effectuer des étapes de configuration dans StorageGRID et obtenir certaines valeurs à utiliser dans ONTAP.

De quelles valeurs ai-je besoin ?

Le tableau suivant indique les valeurs que vous devez configurer dans StorageGRID et comment 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)	StorageGRID > Groupe HA	Entrée DNS
Port	StorageGRID > Point de terminaison de l'équilibreur de charge	Gestionnaire système ONTAP > Ajouter un niveau de cloud
Certificat SSL	StorageGRID > Point de terminaison de l'équilibreur de charge	Gestionnaire système ONTAP > Ajouter un niveau de cloud
Nom du serveur (FQDN)	StorageGRID > Point de terminaison de l'équilibreur de charge	Entrée DNS
ID de clé d'accès et clé d'accès secrète	StorageGRID > Locataire et bucket	Gestionnaire système ONTAP > Ajouter un niveau de cloud
Nom du seau/conteneur	StorageGRID > Locataire et bucket	Gestionnaire système ONTAP > Ajouter un niveau de cloud

Comment puis-je obtenir ces valeurs ?

Selon vos besoins, vous pouvez procéder de l'une des manières suivantes pour obtenir les informations dont vous avez besoin :

- Utilisez le ["Assistant de configuration de FabricPool"](#) . L'assistant de configuration FabricPool vous aide à configurer rapidement les valeurs requises dans StorageGRID et génère un fichier que vous pouvez utiliser pour configurer ONTAP System Manager. L'assistant vous guide à travers les étapes requises et vous aide à garantir que vos paramètres sont conformes aux meilleures pratiques de StorageGRID et FabricPool .
- Configurez chaque élément manuellement. Ensuite, saisissez les valeurs dans ONTAP System Manager ou dans l' ONTAP CLI. Suivez ces étapes :
 - a. ["Configurer un groupe de haute disponibilité \(HA\) pour FabricPool"](#) .

- b. ["Créer un point de terminaison d'équilibrage de charge pour FabricPool"](#) .
- c. ["Créer un compte locataire pour FabricPool"](#) .
- d. Sign in au compte locataire et ["créer le bucket et les clés d'accès pour l'utilisateur root"](#) .
- e. Créez une règle ILM pour les données FabricPool et ajoutez-la à vos stratégies ILM actives. Voir ["Configurer ILM pour les données FabricPool"](#) .
- f. En option, ["créer une politique de classification du trafic pour FabricPool"](#) .

Utiliser l'assistant de configuration de FabricPool

Utiliser l'assistant de configuration de FabricPool : considérations et exigences

Vous pouvez utiliser l'assistant de configuration FabricPool pour configurer StorageGRID comme système de stockage d'objets pour un niveau cloud FabricPool . Une fois l'assistant de configuration terminé, vous pouvez saisir les détails requis dans ONTAP System Manager.

Quand utiliser l'assistant de configuration FabricPool

L'assistant de configuration de FabricPool vous guide à travers chaque étape de la configuration de StorageGRID pour une utilisation avec FabricPool et configure automatiquement certaines entités pour vous, telles que les stratégies ILM et de classification du trafic. Dans le cadre de l'exécution 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 vous assurer que vos paramètres sont conformes aux meilleures pratiques de StorageGRID et FabricPool .

En supposant que vous disposez de l'autorisation d'accès root, vous pouvez terminer l'assistant de configuration de FabricPool lorsque vous commencez à utiliser StorageGRID Grid Manager, ou vous pouvez accéder à l'assistant et le terminer à tout moment ultérieurement. Selon vos besoins, vous pouvez également configurer manuellement certains ou tous les éléments requis, puis utiliser l'assistant pour assembler les valeurs dont ONTAP a besoin dans un seul fichier.



Utilisez l'assistant de configuration FabricPool , sauf si vous savez que vous avez des exigences particulières ou que votre implémentation nécessitera une personnalisation importante.

Avant d'utiliser l'assistant

Confirmez que vous avez terminé ces étapes préalables.

Revoir les meilleures pratiques

- Vous avez une compréhension générale de la ["informations nécessaires pour attacher StorageGRID en tant que niveau cloud"](#) .
- Vous avez examiné les meilleures pratiques de FabricPool pour :
 - ["Groupes de haute disponibilité \(HA\)"](#)
 - ["Équilibrage de charge"](#)
 - ["Règles et politique de l'ILM"](#)

Obtenir des adresses IP et configurer des interfaces VLAN

Si vous configurez un groupe HA, vous savez à quels nœuds ONTAP se connectera et quel réseau StorageGRID sera utilisé. Vous savez également quelles valeurs saisir pour le sous-réseau CIDR, l'adresse IP de la passerelle et les adresses IP virtuelles (VIP).

Si vous prévoyez d'utiliser un réseau local virtuel pour séparer le trafic FabricPool, vous avez déjà configuré l'interface VLAN. Voir ["Configurer les interfaces VLAN"](#).

Configurer la fédération d'identité et l'authentification unique

Si vous prévoyez d'utiliser la fédération d'identité ou l'authentification unique (SSO) pour votre système StorageGRID, vous avez activé ces fonctionnalités. Vous savez également quel groupe fédéré doit avoir un accès root pour le compte locataire ONTAP utilisera. Voir ["Utiliser la fédération d'identité"](#) 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 du serveur de noms de domaine (DNS) mapperont ce nom de domaine complet aux adresses IP virtuelles (VIP) du groupe HA que vous créez à l'aide de l'assistant. Voir ["Configurer le serveur DNS"](#).
- Si vous prévoyez d'utiliser des requêtes de type hébergé virtuel S3, vous devez ["noms de domaine de point de terminaison S3 configurés"](#). ONTAP utilise des URL de type chemin par défaut, mais l'utilisation de requêtes de type hébergé virtuellement est recommandée.

Examiner les exigences relatives à l'équilibreur de charge et aux certificats de sécurité

Si vous prévoyez d'utiliser l'équilibreur de charge StorageGRID, vous avez examiné les instructions générales ["considérations pour 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 point de terminaison d'équilibrage de charge externe (tiers), vous disposez du nom de domaine complet (FQDN), du port et du certificat pour cet équilibreur de charge.

Confirmer la configuration du pool de stockage ILM

si vous avez initialement installé StorageGRID 11.6 ou une version antérieure, 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 les données ONTAP.



Cette condition préalable ne s'applique pas si vous avez initialement installé StorageGRID 11.7 ou 11.8. Lorsque vous installez initialement l'une de ces versions, des 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 de cloud StorageGRID unique qui comprend un locataire StorageGRID, un ensemble de clés d'accès et un bucket StorageGRID. Vous pouvez attacher 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, en fonction de vos besoins, vous souhaitez peut-être utiliser plusieurs buckets ou même plusieurs locataires StorageGRID pour les niveaux locaux dans un seul cluster. L'utilisation de différents buckets et locataires vous permet d'isoler les données et l'accès aux données entre les niveaux locaux ONTAP.

, mais est un peu plus complexe à configurer et à gérer.

NetApp ne recommande pas d'attacher un seul niveau de cloud à des niveaux locaux dans plusieurs clusters.



Pour connaître les meilleures pratiques d'utilisation de StorageGRID avec NetApp MetroCluster™ et FabricPool Mirror, consultez "[TR-4598 : Bonnes pratiques FabricPool dans ONTAP](#)".

Facultatif : utilisez un bucket différent pour chaque niveau local

Pour utiliser plusieurs buckets pour les niveaux locaux dans un cluster ONTAP, ajoutez plusieurs niveaux cloud StorageGRID dans ONTAP. Chaque niveau de cloud partage le même groupe HA, le même point de terminaison d'équilibrage de charge, le même locataire et les mêmes clés d'accès, mais utilise un conteneur différent (bucket StorageGRID). Suivez ces étapes générales :

1. Depuis StorageGRID Grid Manager, terminez l'assistant de configuration de FabricPool pour le premier niveau de cloud.
2. Depuis ONTAP System Manager, ajoutez un niveau cloud et utilisez le fichier que vous avez téléchargé depuis StorageGRID pour fournir les valeurs requises.
3. Depuis StorageGRID Tenant Manager, connectez-vous au locataire créé par l'assistant et créez un deuxième bucket.
4. Terminez à nouveau l'assistant FabricPool. Sélectionnez le groupe HA existant, le point de terminaison de l'équilibreur de charge et le locataire. Ensuite, sélectionnez le nouveau bucket que vous avez créé manuellement. Créez une nouvelle règle ILM pour le nouveau bucket et activez une stratégie ILM pour inclure cette règle.
5. Depuis ONTAP, ajoutez un deuxième niveau de cloud, mais indiquez le nouveau nom de bucket.

Facultatif : utiliser un locataire et un bucket différents pour chaque niveau local

Pour utiliser plusieurs locataires et différents ensembles de clés d'accès pour les niveaux locaux dans un cluster ONTAP, ajoutez plusieurs niveaux de cloud StorageGRID dans ONTAP. Chaque niveau de cloud partage le même groupe HA, le même point de terminaison d'équilibrage de charge, mais utilise un locataire, des clés d'accès et un conteneur différents (bucket StorageGRID). Suivez ces étapes générales :

1. Depuis StorageGRID Grid Manager, terminez l'assistant de configuration de FabricPool pour le premier niveau de cloud.
2. Depuis ONTAP System Manager, ajoutez un niveau cloud et utilisez le fichier que vous avez téléchargé depuis StorageGRID pour fournir les valeurs requises.
3. Terminez à nouveau l'assistant FabricPool. Sélectionnez le groupe HA existant et le point de terminaison de l'équilibreur de charge. Créez un nouveau locataire et un bucket. Créez une nouvelle règle ILM pour le nouveau bucket et activez une stratégie ILM pour inclure cette règle.
4. Depuis ONTAP, ajoutez un deuxième niveau de cloud, mais fournissez la nouvelle clé d'accès, la clé secrète et le nom du bucket.

Accéder et terminer l'assistant de configuration de FabricPool

Vous pouvez utiliser l'assistant de configuration FabricPool pour configurer StorageGRID comme système de stockage d'objets pour un niveau cloud FabricPool.

Avant de commencer

- Vous avez examiné 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, accédez à ["Utiliser l'assistant de configuration S3"](#) .

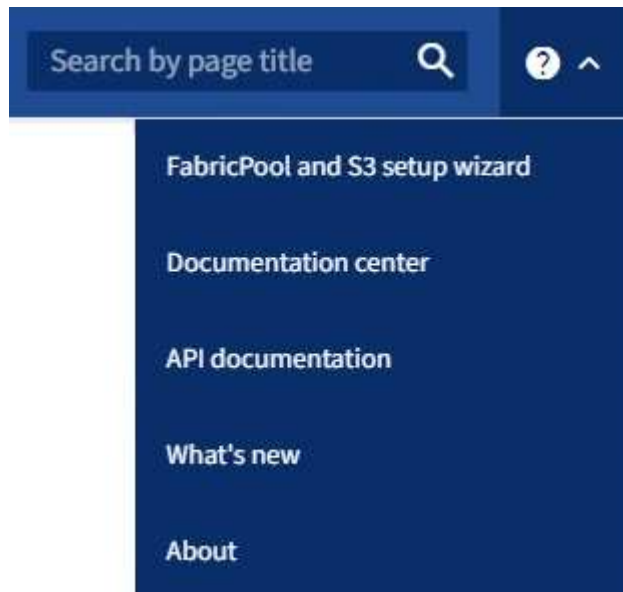
- Vous avez le ["Autorisation d'accès root"](#) .

Accéder à l'assistant

Vous pouvez terminer l'assistant de configuration de FabricPool lorsque vous commencez à utiliser StorageGRID Grid Manager, ou vous pouvez accéder à l'assistant et le terminer à tout moment ultérieurement.

Étapes

1. Sign in au Grid Manager à l'aide d'un ["navigateur Web pris en charge"](#) .
2. Si la bannière * Assistant de configuration FabricPool et S3* apparaît sur le tableau de bord, sélectionnez le lien dans la bannière. Si la bannière n'apparaît plus, sélectionnez l'icône d'aide dans la barre d'en-tête du gestionnaire de grille et sélectionnez * Assistant de configuration FabricPool et S3*.



3. Dans la section FabricPool de la page de l'assistant de configuration de FabricPool et S3, sélectionnez **Configurer maintenant**.

Étape 1 sur 9 : Configurer le groupe HA apparaît.

Étape 1 sur 9 : Configurer le groupe HA

Un groupe haute disponibilité (HA) est un ensemble de nœuds contenant chacun le service StorageGRID Load Balancer. Un groupe HA peut contenir des nœuds de passerelle, des nœuds d'administration ou les deux.

Vous pouvez utiliser un groupe HA pour aider à maintenir les connexions de données FabricPool disponibles. Un groupe HA utilise des adresses IP virtuelles (VIP) pour fournir un accès hautement disponible au service Load Balancer. Si l'interface active du groupe HA échoue, une interface de sauvegarde peut gérer la charge de travail avec peu d'impact sur les opérations FabricPool

Pour plus de détails sur cette tâche, voir ["Gérer les groupes de haute disponibilité"](#) et ["Bonnes pratiques pour"](#)

les groupes de haute disponibilité" .

Étapes

1. Si vous prévoyez d'utiliser un équilibreur de charge externe, vous n'avez pas besoin de créer un groupe HA. Sélectionnez **Ignorer cette étape** et accédez à [Étape 2 sur 9 : Configurer le point de terminaison de l'équilibreur de charge](#) .
2. Pour utiliser l'équilibreur de charge StorageGRID , créez un nouveau groupe HA ou utilisez un groupe HA existant.

Créer un groupe HA

- a. Pour créer un nouveau groupe HA, sélectionnez **Créer un groupe HA**.
- b. Pour l'étape **Entrer les détails**, remplissez les champs suivants.

Champ	Description
Nom du groupe HA	Un nom d'affichage unique pour ce groupe HA.
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 HA.

Utilisez les en-têtes de colonnes pour trier les lignes ou saisissez 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 **Prioriser les interfaces**, déterminez l'interface principale et toutes les interfaces de sauvegarde pour ce groupe HA.

Faites glisser les lignes pour modifier les valeurs dans 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 panne.

Si le groupe HA comprend plusieurs interfaces et que l'interface active échoue, les adresses IP virtuelles (VIP) se déplacent vers la première interface de secours dans l'ordre de priorité. Si cette interface échoue, les adresses VIP se déplacent vers l'interface de sauvegarde suivante, et ainsi de suite. Une fois les échecs résolus, les adresses VIP reviennent à l'interface la plus prioritaire disponible.

- e. Pour l'étape **Saisir les adresses IP**, remplissez les champs suivants.

Champ	Description
Sous-réseau CIDR	L'adresse du sous-réseau VIP en notation CIDR : une adresse IPv4 suivie d'une barre oblique et de la longueur du sous-réseau (0-32). L'adresse réseau ne doit avoir aucun bit d'hôte défini. Par exemple : 192.16.0.0/22 .
Adresse IP de la passerelle (facultatif)	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 , saisissez 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	Saisissez au moins une et pas plus de dix adresses VIP pour l'interface active dans le 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. En option, vous pouvez spécifier des adresses IPv4 et IPv6 supplémentaires.

f. Sélectionnez **Créer un groupe HA**, puis sélectionnez **Terminer** pour revenir à l'assistant de configuration de FabricPool .

g. Sélectionnez **Continuer** pour accéder à l'étape de l'équilibrage de charge.

Utiliser le groupe HA 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 accéder à l'étape de l'équilibrage de charge.

Étape 2 sur 9 : Configurer le point de terminaison de l'équilibreur de charge

StorageGRID utilise un équilibreur de charge pour gérer la charge de travail des applications clientes, telles que FabricPool. L'équilibrage de charge maximise la vitesse et la capacité de connexion sur plusieurs nœuds de stockage.

Vous pouvez utiliser le service d'équilibrage de charge StorageGRID , qui existe sur tous les nœuds de passerelle et d'administration, ou vous connecter à un équilibreur de charge externe (tiers). L'utilisation de l'équilibreur de charge StorageGRID est recommandée.

Pour plus de détails sur cette tâche, consultez le général "[considérations pour l'équilibrage de charge](#)" et le "[meilleures pratiques d'équilibrage de charge pour FabricPool](#)" .

Étapes

1. Sélectionnez ou créez un point de terminaison d'équilibrage de charge StorageGRID ou utilisez un équilibreur de charge externe.

Créer un point de terminaison

- a. Sélectionnez **Créer un point de terminaison**.
- b. Pour l'étape **Saisir les détails du point de terminaison**, remplissez les champs suivants.

Champ	Description
Nom	Un nom descriptif pour le point de terminaison.
Port	Le port StorageGRID que vous souhaitez utiliser pour l'équilibrage de charge. Ce champ est défini par défaut sur 10433 pour le premier point de terminaison que vous créez, mais vous pouvez saisir n'importe quel port externe inutilisé. Si vous entrez 80 ou 443, le point de terminaison est configuré uniquement sur les nœuds de passerelle, car ces ports sont réservés sur les nœuds d'administration. Remarque : les ports utilisés par d'autres services de grille ne sont pas autorisés. Voir le "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 non recommandée.

- c. Pour l'étape **Sélectionner le mode de liaison**, spécifiez le mode de liaison. Le mode de liaison contrôle la manière dont le point de terminaison est accessible à l'aide de n'importe quelle adresse IP ou à l'aide d'adresses IP et d'interfaces réseau spécifiques.

Mode	Description
Global (par défaut)	Les clients peuvent accéder au point de terminaison à l'aide de l'adresse IP de n'importe quel nœud de passerelle ou nœud d'administration, de l'adresse IP virtuelle (VIP) de n'importe quel groupe HA sur n'importe quel réseau ou d'un nom de domaine complet correspondant. Utilisez le paramètre Global (par défaut) sauf si vous devez restreindre l'accessibilité de ce point de terminaison.
IP virtuelles des groupes HA	Les clients doivent utiliser une adresse IP virtuelle (ou un nom de domaine complet correspondant) d'un groupe HA pour accéder à ce point de terminaison. Les points de terminaison avec ce mode de liaison peuvent tous utiliser le même numéro de port, à condition que les groupes HA que vous sélectionnez pour les points de terminaison ne se chevauchent pas.

Mode	Description
Interfaces de nœuds	Les clients doivent utiliser les adresses IP (ou les noms de domaine complets correspondants) des interfaces de nœuds sélectionnées pour accéder à ce point de terminaison.
Type de nœud	En fonction du type de nœud que vous sélectionnez, les clients doivent utiliser soit l'adresse IP (ou le nom de domaine complet correspondant) de n'importe quel nœud d'administration, soit l'adresse IP (ou le nom de domaine complet correspondant) de n'importe quel nœud de passerelle pour accéder à ce point de terminaison.

d. Pour l'étape **Accès locataire**, sélectionnez l'une des options suivantes :

Champ	Description
Autoriser tous les locataires (par défaut)	Tous les comptes locataires peuvent utiliser ce point de terminaison pour accéder à leurs buckets. Autoriser tous les locataires est presque toujours l'option appropriée pour le point de terminaison de l'équilibreur de charge utilisé pour FabricPool. Vous devez sélectionner cette option si vous utilisez l'assistant de configuration FabricPool pour un nouveau système StorageGRID et que vous n'avez pas encore créé de comptes de locataire.
Autoriser les locataires sélectionnés	Seuls les comptes locataires sélectionnés peuvent utiliser ce point de terminaison pour accéder à leurs compartiments.
Bloquer les locataires sélectionnés	Les comptes locataires sélectionnés ne peuvent pas utiliser ce point de terminaison pour accéder à leurs compartiments. Tous les autres locataires peuvent utiliser ce point de terminaison.

e. Pour l'étape **Joindre le 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.
Générer un certificat	Utilisez cette option pour générer un certificat auto-signé. Voir " Configurer les points de terminaison de l'équilibreur de charge " pour plus de détails sur ce qu'il faut saisir.
Utiliser le certificat StorageGRID S3	Cette option n'est disponible que si vous avez déjà téléchargé ou généré une version personnalisée du certificat global StorageGRID . Voir " Configurer les certificats API S3 " pour plus de détails.

f. Sélectionnez **Terminer** pour revenir à l'assistant de configuration de FabricPool .

g. Sélectionnez **Continuer** pour accéder à l'étape du locataire et du bucket.



Les modifications apportées à un certificat de point de terminaison peuvent prendre jusqu'à 15 minutes pour être appliquées à tous les nœuds.

Utiliser le point de terminaison de l'équilibreur de charge existant

a. Sélectionnez le nom d'un point de terminaison existant dans la liste déroulante **Sélectionner un point de terminaison d'équilibrage de charge**.

b. Sélectionnez **Continuer** pour accéder à l'étape du locataire et du bucket.

Utiliser un équilibreur de charge externe

a. Remplissez les champs suivants pour l'équilibreur de charge externe.

Champ	Description
Nom de domaine complet	Le 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 du locataire et du bucket.

Étape 3 sur 9 : Le locataire et le seau

Un locataire est une entité qui peut utiliser des applications S3 pour stocker et récupérer des objets dans StorageGRID. Chaque locataire possède ses propres utilisateurs, clés d'accès, buckets, objets et un ensemble spécifique de fonctionnalités. Vous devez créer un locataire StorageGRID avant de pouvoir créer le bucket que FabricPool utilisera.

Un bucket est un conteneur utilisé pour stocker les objets et les métadonnées d'objet d'un locataire. Bien que certains locataires puissent avoir plusieurs compartiments, l'assistant vous permet de créer ou de sélectionner un seul locataire et un seul compartiment à la fois. Vous pouvez utiliser le gestionnaire de locataires ultérieurement pour ajouter les compartiments supplémentaires dont vous avez besoin.

Vous pouvez créer un nouveau locataire et un nouveau bucket pour l'utilisation de FabricPool , ou vous pouvez sélectionner un locataire et un bucket 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 de détails sur cette tâche, voir "[Créer un compte locataire pour FabricPool](#)" et "[Créez un bucket S3 et obtenez une clé d'accès](#)".

Étapes

Créez un nouveau locataire et un bucket ou sélectionnez un locataire existant.

Nouveau locataire et seau

1. Pour créer un nouveau locataire et un nouveau bucket, saisissez un **Nom de locataire**. Par exemple : `FabricPool tenant`.
2. Définissez l'accès root pour le compte locataire, selon que votre système StorageGRID utilise "fédération d'identité", "authentification unique (SSO)", ou les deux.

Option	Fais ceci
Si la fédération d'identité n'est pas activée	Spécifiez le mot de passe à utiliser lors de la connexion au locataire en tant qu'utilisateur root local.
Si la fédération d'identité est activée	a. Sélectionnez un groupe fédéré existant pour disposer de l'autorisation d'accès root pour le locataire. b. Vous pouvez également spécifier le mot de passe à utiliser lors de la connexion au locataire en tant qu'utilisateur root local.
Si la fédération d'identité et l'authentification unique (SSO) sont activées	Sélectionnez un groupe fédéré existant pour disposer de l'autorisation d'accès root pour le locataire. Aucun utilisateur local ne peut se connecter.

3. Pour **Nom du bucket**, saisissez le nom du bucket que FabricPool utilisera pour stocker les données ONTAP. Par exemple : `fabricpool-bucket`.



Vous ne pouvez pas modifier le nom du bucket après l'avoir créé.

4. Sélectionnez la **Région** pour ce bucket.

Utiliser la région par défaut(`us-east-1`) sauf si vous prévoyez d'utiliser ILM à l'avenir pour filtrer les objets en fonction de la région du bucket.

5. Sélectionnez **Créer et continuer** pour créer le locataire et le bucket et pour accéder à l'étape de téléchargement des données

Sélectionnez le locataire et le bucket

Le compte locataire existant doit avoir au moins un bucket pour lequel le contrôle de version n'est pas activé. Vous ne pouvez pas sélectionner un compte de locataire existant si aucun bucket n'existe pour ce locataire.

1. Sélectionnez le locataire existant dans la liste déroulante **Nom du locataire**.
2. Sélectionnez le bucket existant dans la liste déroulante **Nom du bucket**.

FabricPool ne prend pas en charge le contrôle de version des objets. Par conséquent, les buckets pour lesquels le contrôle de version est activé ne sont pas affichés.



Ne sélectionnez pas un bucket sur lequel le verrouillage d'objet S3 est activé pour une utilisation avec 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. En option, sélectionnez l'icône de copie () pour copier à la fois 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 souhaitez peut-être 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` Le fichier contient les informations dont vous avez besoin pour configurer StorageGRID comme système de stockage d'objets pour un niveau cloud FabricPool , notamment :

- Détails de connexion de l'équilibreur de charge, y compris le nom du serveur (FQDN), le port et le certificat
- Nom du bucket
- ID de clé d'accès et clé d'accès secrète pour l'utilisateur root du compte 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 clés ne seront plus disponibles après avoir fermé cette page. Assurez-vous de sauvegarder ces informations dans un endroit sûr, 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 : Sélectionner 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 à partir d' 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 d' ONTAP.
2. Dans la liste déroulante **Pool de stockage**, sélectionnez le pool de stockage pour ce site.

Le pool de stockage d'un site comprend tous les nœuds de stockage de ce site.

- Sélectionnez **Continuer** pour accéder à l'étape de la règle ILM.

Étape 6 sur 9 : Vérifier 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 de configuration de FabricPool crée automatiquement la règle ILM recommandée pour l'utilisation de FabricPool . Cette règle s'applique uniquement au bucket que vous avez spécifié. Il utilise le codage d'effacement 2+1 sur un seul site pour stocker les données hiérarchisées à partir d' ONTAP.

Pour plus de détails sur cette étape, voir "[Créer une règle ILM](#)" et "[Bonnes pratiques pour l'utilisation d'ILM avec les données FabricPool](#)".

Étapes

- Consultez les détails de la règle.

Champ	Description
Nom de la règle	Généré automatiquement et ne peut pas être modifié
Description	Généré automatiquement et ne peut pas être modifié
Filtre	Le nom du bucket Cette règle s'applique uniquement aux objets enregistrés dans le bucket que vous avez spécifié.
Heure de référence	Temps d'ingestion L'instruction de placement démarre lorsque les objets sont initialement enregistrés dans le bucket.
Instructions de placement	Utiliser le codage d'effacement 2+1

- Triez le diagramme de rétention par **Période** et **Pool de stockage** pour confirmer l'instruction de placement.
 - La **période de temps** pour la règle est **Jour 0 - pour toujours**. **Jour 0** signifie que la règle est appliquée lorsque les données sont hiérarchisées à partir d' ONTAP. **Pour toujours** signifie que StorageGRID ILM ne supprimera pas les données qui ont été hiérarchisées à partir d' 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 codage 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.
- Sélectionnez **Créer et continuer** pour créer cette règle et accéder à l'étape de la politique ILM.

Étape 7 sur 9 : Réviser et activer la politique ILM

Une fois que l'assistant de configuration de FabricPool a créé la règle ILM pour l'utilisation de FabricPool , il crée une stratégie ILM. Vous devez simuler et examiner attentivement cette politique avant de l'activer.

Pour plus de détails sur cette étape, voir "[Créer une politique ILM](#)" et "[Bonnes pratiques pour l'utilisation d'ILM avec les données FabricPool](#)".



Lorsque vous activez une nouvelle stratégie ILM, StorageGRID utilise cette stratégie 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 politique 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 niveau cloud FabricPool. Définissez la période de conservation sur **pour toujours** pour garantir que les objets FabricPool ne sont pas supprimés par StorageGRID ILM.

Étapes

1. Vous pouvez également mettre à jour le **Nom de la politique** généré par le système. Par défaut, le système ajoute « + FabricPool » au nom de votre politique active ou inactive, mais vous pouvez fournir votre propre nom.
2. Consultez la liste des règles de la politique inactive.
 - Si votre grille ne dispose pas d'une politique ILM inactive, l'assistant crée une politique inactive en clonant votre politique active et en ajoutant la nouvelle règle en haut.
 - Si votre grille dispose déjà d'une politique ILM inactive et que cette politique utilise les mêmes règles et le même ordre que la politique ILM active, l'assistant ajoute la nouvelle règle en haut de la politique inactive.
 - Si votre politique inactive contient des règles différentes ou un ordre différent de la politique active, l'assistant crée une nouvelle politique inactive en clonant votre politique active et en ajoutant la nouvelle règle en haut.
3. Revoyez l'ordre des règles dans la nouvelle politique inactive.

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 stratégie ne soient évaluées. Les objets dans tous les autres compartiments sont placés selon les règles ultérieures de la politique.

4. Consultez le diagramme de rétention pour savoir comment différents objets seront conservés.
 - a. Sélectionnez **Développer tout** pour voir un diagramme de rétention pour chaque règle de la politique inactive.
 - b. Sélectionnez **Période** et **Pool de stockage** pour consulter le diagramme de rétention. Confirmez que toutes les règles qui s'appliquent au bucket ou au locataire FabricPool conservent les objets **pour toujours**.
5. Une fois que vous avez examiné la politique inactive, sélectionnez **Activer et continuer** pour activer la politique et passer à l'étape de classification du trafic.



Des erreurs dans une politique ILM peuvent entraîner une perte de données irréparable. Lisez attentivement la politique avant de l'activer.

Étape 8 sur 9 : Créer une politique de classification du trafic

En option, l'assistant de configuration FabricPool peut créer une stratégie de classification du trafic que vous pouvez utiliser pour surveiller la charge de travail FabricPool. La politique créée par le système utilise une règle de correspondance pour identifier tout le trafic réseau lié au bucket que vous avez créé. Cette politique

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 politique de classification du trafic pour FabricPool](#)".

Étapes

1. Revoir la politique.
2. Si vous souhaitez créer cette politique de classification du trafic, sélectionnez **Créer et continuer**.

Dès que FabricPool commence à hiérarchiser les données vers StorageGRID, vous pouvez accéder à la page Stratégies de classification du trafic pour afficher les mesures de trafic réseau pour cette stratégie. Plus tard, vous pouvez également ajouter des règles pour limiter d'autres charges de travail et garantir que la charge de travail FabricPool dispose de la majeure partie de la bande passante.

3. Sinon, sélectionnez **Ignorer cette étape**.

Étape 9 sur 9 : Récapitulatif de l'examen

Le résumé fournit des détails sur les éléments que vous avez configurés, notamment le nom de l'équilibreur de charge, du locataire et du bucket, la politique de classification du trafic et la politique ILM active,

Étapes

1. Consultez le résumé.
2. Sélectionnez **Terminer**.

Prochaines étapes

Après avoir terminé l'assistant FabricPool, effectuez ces étapes supplémentaires.

Étapes

1. Aller à "[Configurer ONTAP System Manager](#)" pour saisir les valeurs enregistrées et terminer le côté ONTAP de la connexion. Vous devez ajouter StorageGRID en tant que niveau cloud, attacher le niveau cloud à un niveau local pour créer un FabricPool et définir des stratégies de hiérarchisation des volumes.
2. Aller à "[Configurer le serveur DNS](#)" et assurez-vous que le DNS inclut un enregistrement pour associer le nom du serveur StorageGRID (nom de domaine complet) à chaque adresse IP StorageGRID que vous utiliserez.
3. Aller à "[Autres bonnes pratiques pour StorageGRID et FabricPool](#)" pour découvrir les meilleures pratiques pour les journaux d'audit StorageGRID et d'autres options de configuration globales.

Configurer StorageGRID manuellement

Créer un groupe haute disponibilité (HA) pour FabricPool

Lors de la configuration de StorageGRID pour une utilisation avec FabricPool, vous pouvez éventuellement créer un ou plusieurs groupes de haute disponibilité (HA). Un groupe HA est un ensemble de nœuds contenant chacun le service StorageGRID Load Balancer. Un groupe HA peut contenir des nœuds de passerelle, des nœuds d'administration ou les deux.

Vous pouvez utiliser un groupe HA pour aider à maintenir les connexions de données FabricPool disponibles. Un groupe HA utilise des adresses IP virtuelles (VIP) pour fournir un accès hautement disponible au service Load Balancer. Si l'interface active du groupe HA échoue, une interface de sauvegarde peut gérer la charge

de travail avec peu d'impact sur les opérations FabricPool .

Pour plus de détails sur cette tâche, voir "[Gérer les groupes de haute disponibilité](#)". Pour utiliser l'assistant de configuration FabricPool pour effectuer cette tâche, accédez à "[Accéder et terminer l'assistant de configuration de FabricPool](#)".

Avant de commencer

- Vous avez examiné le "[meilleures pratiques pour les groupes de haute disponibilité](#)".
- Vous êtes connecté au Grid Manager à l'aide d'un "[navigateur Web pris en charge](#)".
- Vous avez le "[Autorisation d'accès root](#)".
- Si vous prévoyez d'utiliser un VLAN, vous avez créé l'interface VLAN. Voir "[Configurer les interfaces VLAN](#)".

Étapes

1. Sélectionnez **CONFIGURATION > Réseau > Groupes de haute disponibilité**.
2. Sélectionnez **Créer**.
3. Pour l'étape **Entrer les détails**, remplissez les champs suivants.

Champ	Description
Nom du groupe HA	Un nom d'affichage unique pour ce groupe HA.
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 HA.

Utilisez les en-têtes de colonnes pour trier les lignes ou saisissez 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 **Prioriser les interfaces**, déterminez l'interface principale et toutes les interfaces de sauvegarde pour ce groupe HA.

Faites glisser les lignes pour modifier les valeurs dans 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 panne.

Si le groupe HA comprend plusieurs interfaces et que l'interface active échoue, les adresses IP virtuelles (VIP) se déplacent vers la première interface de secours dans l'ordre de priorité. Si cette interface échoue, les adresses VIP se déplacent vers l'interface de sauvegarde suivante, et ainsi de suite. Une fois les échecs résolus, les adresses VIP reviennent à l'interface la plus prioritaire disponible.

6. Pour l'étape **Saisir les adresses IP**, remplissez les champs suivants.

Champ	Description
Sous-réseau CIDR	L'adresse du sous-réseau VIP en notation CIDR : une adresse IPv4 suivie d'une barre oblique et de la longueur du sous-réseau (0-32). L'adresse réseau ne doit avoir aucun bit d'hôte défini. Par exemple : 192.16.0.0/22 .
Adresse IP de la passerelle (facultatif)	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 , saisissez l'adresse IP de la passerelle locale VIP StorageGRID . L'adresse IP de la passerelle locale doit se trouver dans le sous-réseau VIP.
Adresse IP virtuelle	Saisissez au moins une et pas plus de dix adresses VIP pour l'interface active dans le groupe HA. Toutes les adresses VIP doivent se trouver dans le sous-réseau VIP. Au moins une adresse doit être IPv4. En option, vous pouvez spécifier des adresses IPv4 et IPv6 supplémentaires.

7. Sélectionnez **Créer un groupe HA** puis sélectionnez **Terminer**.

Créer un point de terminaison d'équilibrage de charge pour FabricPool

StorageGRID utilise un équilibreur de charge pour gérer la charge de travail des applications clientes, telles que FabricPool. L'équilibrage de charge maximise 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 de terminaison d'équilibrage de charge et télécharger ou générer un certificat de point de terminaison d'équilibrage de charge, qui est utilisé pour sécuriser la connexion entre ONTAP et StorageGRID.

Pour utiliser l'assistant de configuration FabricPool pour effectuer cette tâche, accédez à ["Accéder et terminer l'assistant de configuration de FabricPool"](#) .

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 root"](#) .
- Vous avez examiné le général ["considérations pour l'équilibrage de charge"](#) ainsi que le ["meilleures pratiques d'équilibrage de charge pour FabricPool"](#) .

Étapes

1. Sélectionnez **CONFIGURATION > Réseau > Points de terminaison de l'équilibreur de charge**.
2. Sélectionnez **Créer**.
3. Pour l'étape **Saisir les détails du point de terminaison**, remplissez les champs suivants.

Champ	Description
Nom	Un nom descriptif pour le point de terminaison.
Port	Le port StorageGRID que vous souhaitez utiliser pour l'équilibrage de charge. Ce champ est défini par défaut sur 10433 pour le premier point de terminaison que vous créez, mais vous pouvez saisir n'importe quel port externe inutilisé. Si vous entrez 80 ou 443, le point de terminaison est configuré uniquement sur les nœuds de passerelle. Ces ports sont réservés sur les nœuds d'administration. Remarque : les ports utilisés par d'autres services de grille ne sont pas autorisés. Voir le "Référence du port réseau". Vous fournirez ce numéro à ONTAP lorsque vous attachez StorageGRID en tant que 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 non recommandée.

4. Pour l'étape **Sélectionner le mode de liaison**, spécifiez le mode de liaison. Le mode de liaison contrôle la manière dont le point de terminaison est accessible à l'aide de n'importe quelle adresse IP ou à l'aide d'adresses IP et d'interfaces réseau spécifiques.

Mode	Description
Global (par défaut)	Les clients peuvent accéder au point de terminaison à l'aide de l'adresse IP de n'importe quel nœud de passerelle ou nœud d'administration, de l'adresse IP virtuelle (VIP) de n'importe quel groupe HA sur n'importe quel réseau ou d'un nom de domaine complet correspondant. Utilisez le paramètre Global (par défaut) sauf si vous devez restreindre l'accessibilité de ce point de terminaison.
IP virtuelles des groupes HA	Les clients doivent utiliser une adresse IP virtuelle (ou un nom de domaine complet correspondant) d'un groupe HA pour accéder à ce point de terminaison. Les points de terminaison avec ce mode de liaison peuvent tous utiliser le même numéro de port, à condition que les groupes HA que vous sélectionnez pour les points de terminaison ne se chevauchent pas.
Interfaces de nœuds	Les clients doivent utiliser les adresses IP (ou les noms de domaine complets correspondants) des interfaces de nœuds sélectionnées pour accéder à ce point de terminaison.

Mode	Description
Type de nœud	En fonction du type de nœud que vous sélectionnez, les clients doivent utiliser soit l'adresse IP (ou le nom de domaine complet correspondant) de n'importe quel nœud d'administration, soit l'adresse IP (ou le nom de domaine complet correspondant) de n'importe quel nœud de passerelle pour accéder à ce point de terminaison.

5. Pour l'étape **Accès locataire**, sélectionnez l'une des options suivantes :

Champ	Description
Autoriser tous les locataires (par défaut)	Tous les comptes locataires peuvent utiliser ce point de terminaison pour accéder à leurs buckets. Autoriser tous les locataires est presque toujours l'option appropriée pour le point de terminaison de l'équilibreur de charge utilisé pour FabricPool. Vous devez sélectionner cette option si vous n'avez pas encore créé de compte locataire.
Autoriser les locataires sélectionnés	Seuls les comptes locataires sélectionnés peuvent utiliser ce point de terminaison pour accéder à leurs compartiments.
Bloquer les locataires sélectionnés	Les comptes locataires sélectionnés ne peuvent pas utiliser ce point de terminaison pour accéder à leurs compartiments. Tous les autres locataires peuvent utiliser ce point de terminaison.

6. Pour l'étape **Joindre le 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.
Générer un certificat	Utilisez cette option pour générer un certificat auto-signé. Voir " Configurer les points de terminaison de l'équilibreur de charge " pour plus de détails sur ce qu'il faut saisir.
Utiliser le certificat StorageGRID S3	Cette option n'est disponible que si vous avez déjà téléchargé ou généré une version personnalisée du certificat global StorageGRID . Voir " Configurer les certificats API S3 " pour plus de détails.

7. Sélectionnez **Créer**.



Les modifications apportées à un certificat de point de terminaison peuvent prendre jusqu'à 15 minutes pour être appliquées à tous les nœuds.

Créer un compte locataire pour FabricPool

Vous devez créer un compte locataire dans Grid Manager pour utiliser FabricPool .

Les comptes locataires permettent aux applications clientes de stocker et de récupérer des objets sur StorageGRID. Chaque compte locataire possède son propre ID de compte, ses propres groupes et utilisateurs autorisés, ses compartiments et ses objets.

Pour plus de détails sur cette tâche, voir "[Créer un compte locataire](#)". Pour utiliser l'assistant de configuration FabricPool pour effectuer cette tâche, accédez à "[Accéder et terminer l'assistant de configuration de FabricPool](#)".

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "[navigateur Web pris en charge](#)".
- Tu as "[autorisations d'accès spécifiques](#)".

Étapes

1. Sélectionnez **LOCATAIRES**.
2. Sélectionnez **Créer**.
3. Pour les étapes de saisie des détails, saisissez les informations suivantes.

Champ	Description
Nom	Un nom pour le compte locataire. Les noms des locataires n'ont pas besoin d'être uniques. Lorsque le compte locataire est créé, 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 plateforme**.

Les locataires FabricPool n'ont généralement pas besoin d'utiliser des services de plateforme, tels que la réplication CloudMirror.

- b. En option, sélectionnez **Utiliser votre propre source d'identité**.

- c. Ne sélectionnez pas **Autoriser la sélection S3**.

Les locataires FabricPool n'ont généralement pas besoin d'utiliser S3 Select.

- d. En option, sélectionnez **Utiliser la connexion à la fédération de grille** pour permettre au locataire d'utiliser une "[connexion à la fédération de réseau](#)" pour le clonage de compte et la réplication inter-grille. Ensuite, sélectionnez la connexion de fédération de grille à utiliser.

5. Pour l'étape Définir l'accès root, spécifiez quel utilisateur disposera de l'autorisation d'accès root initiale pour le compte locataire, selon que votre système StorageGRID utilise "[fédération d'identité](#)".

, ["authentification unique \(SSO\)"](#) , ou les deux.

Option	Fais ceci
Si la fédération d'identité n'est pas activée	Spécifiez le mot de passe à utiliser lors de la connexion au locataire en tant qu'utilisateur root local.
Si la fédération d'identité est activée	a. Sélectionnez un groupe fédéré existant pour disposer de l'autorisation d'accès root pour le locataire. b. Vous pouvez également spécifier le mot de passe à utiliser lors de la connexion au locataire en tant qu'utilisateur root local.
Si la fédération d'identité et l'authentification unique (SSO) sont activées	Sélectionnez un groupe fédéré existant pour disposer de l'autorisation d'accès root pour le locataire. Aucun utilisateur local ne peut se connecter.

6. Sélectionnez **Créer un locataire**.

Créez un bucket S3 et obtenez des clés d'accès

Avant d'utiliser StorageGRID avec une charge de travail FabricPool , vous devez créer un bucket S3 pour vos données FabricPool . Vous devez également obtenir une clé d'accès et une clé d'accès secrète pour le compte locataire que vous utiliserez pour FabricPool.

Pour plus de détails sur cette tâche, voir ["Créer un bucket S3"](#) et ["Créez vos propres clés d'accès S3"](#) . Pour utiliser l'assistant de configuration FabricPool pour effectuer cette tâche, accédez à ["Accéder et terminer l'assistant de configuration de FabricPool"](#) .

Avant de commencer

- Vous avez créé un compte locataire pour l'utilisation de FabricPool .
- Vous disposez d'un accès root au compte locataire.

Étapes

1. Sign in au gestionnaire de locataires.

Vous pouvez effectuer l'une des opérations suivantes :

- Depuis la page Comptes locataires du Gestionnaire de grille, sélectionnez le lien * Sign in* pour le locataire et saisissez vos informations d'identification.
- Saisissez l'URL du compte locataire dans un navigateur Web et saisissez vos informations d'identification.

2. Créez un bucket S3 pour les données FabricPool .

Vous devez créer un bucket unique pour chaque cluster ONTAP que vous prévoyez d'utiliser.

- a. Sélectionnez **Afficher les buckets** dans le tableau de bord ou sélectionnez **STOCKAGE (S3) > Buckets**.
- b. Sélectionnez **Créer un bucket**.
- c. Saisissez le nom du bucket StorageGRID que vous souhaitez utiliser avec FabricPool. Par exemple :

fabricpool-bucket .



Vous ne pouvez pas modifier le nom du bucket après l'avoir créé.

d. Sélectionnez la région pour ce bucket.

Par défaut, tous les buckets sont créés dans le `us-east-1` région.

e. Sélectionnez **Continuer**.

f. Sélectionnez **Créer un bucket**.



Ne sélectionnez pas **Activer le contrôle de version des objets** pour le bucket FabricPool . De même, ne modifiez pas un bucket FabricPool pour utiliser **Disponible** ou une cohérence non par défaut. La cohérence de compartiment recommandée pour les compartiments FabricPool est **Lecture après nouvelle écriture**, qui est la cohérence par défaut pour un nouveau compartiment.

3. Créez une clé d'accès et une clé d'accès secrète.

a. Sélectionnez **STOCKAGE (S3) > Mes clés d'accès**.

b. Sélectionnez **Créer une clé**.

c. Sélectionnez **Créer une clé d'accès**.

d. Copiez l'ID de clé d'accès et la clé d'accès secrète dans un emplacement sûr ou sélectionnez **Télécharger .csv** pour enregistrer un fichier de feuille de calcul contenant l'ID de clé d'accès et la clé d'accès secrète.

Vous saisirez ces valeurs dans ONTAP lorsque vous configurerez StorageGRID en tant que niveau cloud FabricPool .



Si vous générez une nouvelle clé d'accès et une clé d'accès secrète dans StorageGRID à l'avenir, saisissez les nouvelles clés dans ONTAP avant de supprimer les anciennes valeurs de StorageGRID. Dans le cas contraire, ONTAP risque de perdre temporairement son accès à StorageGRID.

Configurer ILM pour les données FabricPool

Vous pouvez utiliser cet exemple simple de politique comme point de départ pour vos propres règles et politiques ILM.

Cet exemple suppose que vous concevez les règles ILM et une politique ILM pour un système StorageGRID doté de quatre nœuds de stockage dans un seul centre de données à Denver, Colorado. Les données FabricPool dans cet exemple utilisent un bucket nommé `fabricpool-bucket` .



Les règles et politiques ILM suivantes ne sont que des exemples. Il existe de nombreuses façons de configurer les règles ILM. Avant d'activer une nouvelle politique, simulez-la pour confirmer qu'elle fonctionnera comme prévu pour protéger le contenu contre la perte. Pour en savoir plus, voir "[Gérer les objets avec ILM](#)" .



Pour éviter toute perte de données, n'utilisez pas de règle ILM qui expirera ou supprimera les données de niveau cloud FabricPool . Définissez la période de conservation sur **pour toujours** pour garantir que les objets FabricPool ne sont pas supprimés par StorageGRID ILM.

Avant de commencer

- Vous avez examiné le ["meilleures pratiques pour utiliser ILM avec les données FabricPool"](#) .
- Vous êtes connecté au Grid Manager à l'aide d'un ["navigateur Web pris en charge"](#) .
- Vous avez le ["Autorisation d'accès ILM ou Root"](#) .
- Si vous avez effectué une mise à niveau vers StorageGRID 11.9 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.



Cette condition préalable ne s'applique pas si vous avez initialement installé StorageGRID 11.7 ou 11.8. Lorsque vous installez initialement l'une de ces versions, des pools de stockage sont automatiquement créés pour chaque site.

Étapes

1. Créez une règle ILM qui s'applique uniquement aux données dans `fabricpool-bucket` Cet exemple de règle crée des copies à code d'effacement.

Définition de la règle	Exemple de valeur
Nom de la règle	Codage d'effacement 2 + 1 pour les données FabricPool
Nom du bucket	<code>fabricpool-bucket</code> Vous pouvez également filtrer sur le compte locataire 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 codage d'effacement.
Heure de référence	Temps d'ingestion
Période et emplacements	À partir du jour 0, stockez pour toujours Stockez les objets par codage d'effacement à l'aide du schéma EC 2+1 à Denver et conservez ces objets dans StorageGRID pour toujours.  Pour éviter toute perte de données, n'utilisez pas de règle ILM qui expirera ou supprimera les données de niveau cloud FabricPool .
Comportement d'ingestion	Équilibré

2. Créez une règle ILM par défaut qui créera deux copies répliquées de tous les objets ne correspondant pas à la première règle. Ne sélectionnez pas de filtre de base (compte locataire ou nom de bucket) ni de filtres avancés.

Définition de la règle	Exemple de valeur
Nom de la règle	Deux copies répliquées
Nom du bucket	<i>aucun</i>
Filtres avancés	<i>aucun</i>
Heure de référence	Temps d'ingestion
Période et emplacements	À partir du jour 0, stockez pour toujours Stockez les objets en répliquant 2 copies à Denver.
Comportement d'ingestion	Équilibré

3. Créez une politique ILM et sélectionnez les deux règles. Étant donné que la règle de réplication n'utilise aucun filtre, elle peut être la règle par défaut (dernière) de la politique.
4. Ingérer les objets de test dans la grille.
5. Simulez la politique avec les objets de test pour vérifier le comportement.
6. Activer la politique.

Lorsque cette politique est activée, StorageGRID place les données d'objet comme suit :

- Les données hiérarchisées à partir de FabricPool dans `fabricpool-bucket` sera codé par effacement en utilisant le schéma de codage par effacement 2+1. Deux fragments de données et un fragment de parité seront placés sur trois nœuds de stockage différents.
- Tous les objets de tous les autres buckets seront répliqués. Deux copies seront créées et placées sur deux nœuds de stockage différents.
- Les copies seront conservées dans StorageGRID pour toujours. StorageGRID ILM ne supprimera pas ces objets.

Créer une politique de classification du trafic pour FabricPool

Vous pouvez éventuellement concevoir une stratégie de classification du trafic StorageGRID pour optimiser la qualité de service pour la charge de travail FabricPool .

Pour plus de détails sur cette tâche, voir "[Gérer les politiques de classification du trafic](#)". Pour utiliser l'assistant de configuration FabricPool pour effectuer cette tâche, accédez à "[Accéder et terminer l'assistant de configuration de FabricPool](#)".

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 root](#)".

À propos de cette tâche

Les meilleures pratiques pour créer une politique de classification du trafic pour FabricPool dépendent de la charge de travail, comme suit :

- Si vous prévoyez de hiérarchiser les données de charge de travail principales de FabricPool vers StorageGRID, vous devez vous assurer que la charge de travail de FabricPool dispose de la majeure partie de la bande passante. Vous pouvez créer une politique de classification du trafic pour limiter toutes les autres charges de travail.



En général, les opérations de lecture de FabricPool sont plus importantes à prioriser que les opérations d'écriture.

Par exemple, si d'autres clients S3 utilisent ce système StorageGRID, vous devez créer une stratégie de classification du trafic. Vous pouvez limiter le trafic réseau pour les autres buckets, locataires, sous-réseaux IP ou points de terminaison d'équilibrage de charge.

- En règle générale, 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 imposées aux autres charges de travail doivent tenir compte du comportement de ces charges de travail. Les limites imposées varieront également en fonction de la taille et des capacités de votre réseau et de la quantité d'utilisation prévue.

Étapes

1. Sélectionnez **CONFIGURATION > Réseau > Classification du trafic**.
2. Sélectionnez **Créer**.
3. Saisissez un nom et une description (facultatif) pour la politique et sélectionnez **Continuer**.
4. Pour l'étape Ajouter des règles de correspondance, ajoutez au moins une règle.
 - a. Sélectionnez **Ajouter une règle**
 - b. Pour Type, sélectionnez **Point de terminaison de l'équilibreur de charge**, puis sélectionnez le point de terminaison de l'équilibreur de charge que vous avez créé pour FabricPool.

Vous pouvez également sélectionner le compte locataire ou le bucket FabricPool .
 - c. Si vous souhaitez que cette politique de trafic limite le trafic pour les autres points de terminaison, sélectionnez **Correspondance inverse**.
5. Vous pouvez également ajouter une ou plusieurs limites pour contrôler le trafic réseau correspondant à la règle.



StorageGRID collecte des métriques même si vous n'ajoutez aucune limite, afin que vous puissiez 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 révisiez 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 politique, sélectionnez **Enregistrer et continuer**.

Après votre finition

["Afficher les mesures du trafic réseau"](#) pour vérifier que les policiers appliquent les limites de circulation que vous attendez.

Configurer ONTAP System Manager

Après avoir obtenu les informations StorageGRID requises, vous pouvez accéder à ONTAP pour ajouter StorageGRID en tant que niveau cloud.

Avant de commencer

- Si vous avez terminé l'assistant de configuration de FabricPool, vous disposez de `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) du groupe HA StorageGRID, du numéro de port du point de terminaison de l'équilibreur de charge, du certificat de l'équilibreur de charge, de l'ID de clé d'accès et de la clé secrète de l'utilisateur root du compte de locataire, ainsi que du nom du bucket ONTAP utilisera dans ce locataire.

Gestionnaire du système Access ONTAP

Ces instructions décrivent comment utiliser ONTAP System Manager pour ajouter StorageGRID en tant que niveau cloud. Vous pouvez effectuer la même configuration à l'aide de l'interface de ligne de commande ONTAP. Pour obtenir des instructions, rendez-vous sur ["Documentation ONTAP pour FabricPool"](#).

Étapes

1. Accédez au gestionnaire système pour le cluster ONTAP que vous souhaitez hiérarchiser vers StorageGRID.
2. Sign in en tant qu'administrateur du cluster.
3. Accédez à **STOCKAGE > Niveaux > Ajouter un niveau Cloud**.
4. Sélectionnez * StorageGRID* dans la liste des fournisseurs de magasins d'objets.

Entrer les valeurs StorageGRID

Voir ["Documentation ONTAP pour FabricPool"](#) pour plus d'informations.

Étapes

1. Remplissez le formulaire Ajouter un niveau de cloud en utilisant le `ONTAP_FabricPool_settings_bucketname.txt` fichier ou les valeurs que vous avez obtenues manuellement.

Champ	Description
Nom	Saisissez un nom unique pour ce niveau de cloud. Vous pouvez accepter la valeur par défaut.

Champ	Description
Style d'URL	Si tu "noms de domaine de point de terminaison S3 configurés", sélectionnez URL de style hébergé virtuellement. Path-Style URL est la valeur par défaut pour ONTAP, mais l'utilisation de requêtes de style hébergé virtuel est recommandée pour StorageGRID. Vous devez utiliser URL de style chemin si vous fournissez une adresse IP au lieu d'un nom de domaine pour le champ Nom du serveur (FQDN).
Nom du serveur (FQDN)	Saisissez le nom de domaine complet (FQDN) que vous utilisez pour StorageGRID ou l'adresse IP virtuelle (VIP) du groupe HA StorageGRID . Par exemple : <code>s3.storagegrid.company.com</code> . 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 point de terminaison 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 point de terminaison de l'équilibreur de charge StorageGRID , y compris : -----BEGIN CERTIFICATE----- et -----END CERTIFICATE----- . Remarque : si une autorité de certification intermédiaire a émis le certificat StorageGRID , vous devez fournir le certificat de l'autorité de certification intermédiaire. Si le certificat StorageGRID a été émis directement par l'autorité de certification racine, vous devez fournir le certificat de l'autorité de certification racine.
Port	Saisissez le port utilisé par le point de terminaison de l'équilibreur de charge StorageGRID . ONTAP utilisera ce port lorsqu'il se connectera à StorageGRID. Par exemple, 10433.
Clé d'accès et clé secrète	Saisissez l'ID de clé d'accès et la clé d'accès secrète pour l'utilisateur root du compte locataire StorageGRID . Astuce : si vous générez une nouvelle clé d'accès et une clé d'accès secrète dans StorageGRID à l'avenir, saisissez les nouvelles clés dans ONTAP avant de supprimer les anciennes valeurs de StorageGRID. Dans le cas contraire, ONTAP risque de perdre temporairement son accès à StorageGRID.
Nom du conteneur	Saisissez le nom du bucket StorageGRID que vous avez créé pour l'utiliser avec ce niveau ONTAP .

2. Terminez la configuration finale de FabricPool dans ONTAP.
 - a. Attachez un ou plusieurs agrégats au niveau cloud.
 - b. Vous pouvez également créer une stratégie de hiérarchisation des volumes.

Configurer le serveur DNS

Après avoir configuré les groupes de haute disponibilité, les points de terminaison d'équilibrage de charge et les noms de domaine de point de terminaison S3, vous devez vous assurer que le DNS inclut les entrées nécessaires pour StorageGRID. Vous devez inclure une entrée DNS pour chaque nom dans le 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 saisissez dans le DNS dépendent du fait que vous utilisez ou non un groupe HA de nœuds d'équilibrage de charge :

- Si vous avez configuré un groupe HA, ONTAP se connectera aux adresses IP virtuelles de ce groupe HA.
- Si vous n'utilisez pas de groupe HA, ONTAP peut se connecter au service StorageGRID Load Balancer à l'aide de l'adresse IP de n'importe quel nœud de passerelle ou nœud d'administration.
- Si le nom du serveur correspond à plusieurs adresses IP, ONTAP établit des connexions client avec toutes les adresses IP (jusqu'à un maximum de 16 adresses IP). Les adresses IP sont récupérées selon une méthode circulaire lorsque les connexions sont établies.

Entrées DNS pour les requêtes de type hébergement virtuel

Si vous avez défini "[Noms de domaine de point de terminaison S3](#)" et vous utiliserez des requêtes de type hébergé virtuel, ajoutez des entrées DNS pour tous les noms de domaine de point de terminaison S3 requis, y compris tous les noms génériques.

Bonnes pratiques StorageGRID pour FabricPool

Bonnes pratiques pour les groupes à haute disponibilité (HA)

Avant d'associer StorageGRID en tant que niveau cloud FabricPool, découvrez les groupes haute disponibilité (HA) StorageGRID et examinez les meilleures pratiques d'utilisation des groupes HA avec FabricPool.

Qu'est-ce qu'un groupe HA ?

Un groupe haute disponibilité (HA) est un ensemble d'interfaces provenant de plusieurs nœuds de passerelle StorageGRID, nœuds d'administration ou les deux. Un groupe HA permet de maintenir les connexions de données client disponibles. Si l'interface active du groupe HA échoue, une interface de sauvegarde peut gérer la charge de travail avec peu d'impact sur les opérations FabricPool.

Chaque groupe HA fournit un accès hautement disponible aux services partagés sur les nœuds associés. Par exemple, un groupe HA composé d'interfaces uniquement sur des nœuds de passerelle ou sur des nœuds

d'administration et des nœuds de passerelle fournit un accès hautement disponible au service d'équilibrage de charge partagé.

Pour en savoir plus sur les groupes de haute disponibilité, consultez ["Gérer les groupes de haute disponibilité \(HA\)"](#) .

Utilisation des groupes HA

Les meilleures pratiques pour créer un groupe StorageGRID HA pour FabricPool dépendent de la charge de travail.

- Si vous prévoyez d'utiliser FabricPool avec des données de charge de travail principales, vous devez créer un groupe HA qui inclut au moins deux nœuds d'équilibrage de charge pour éviter toute interruption de la récupération des données.
- Si vous prévoyez d'utiliser la stratégie de hiérarchisation des volumes de snapshots FabricPool uniquement ou des niveaux de performances locaux non principaux (par exemple, des emplacements de reprise après sinistre ou des destinations NetApp SnapMirror®), vous pouvez configurer un groupe HA avec un seul nœud.

Ces instructions décrivent la configuration d'un groupe HA pour la HA de sauvegarde active (un nœud est actif et un nœud est de sauvegarde). Cependant, vous préférerez peut-être utiliser DNS Round Robin ou Active-Active HA. Pour connaître les avantages de ces autres configurations HA, consultez ["Options de configuration pour les groupes HA"](#) .

Bonnes pratiques d'équilibrage de charge pour FabricPool

Avant d'attacher StorageGRID en tant que niveau cloud FabricPool , passez en revue les meilleures pratiques d'utilisation des équilibreurs de charge avec FabricPool.

Pour obtenir des informations générales sur l'équilibreur de charge StorageGRID et le certificat de l'équilibreur de charge, consultez ["Considérations relatives à l'équilibrage de charge"](#) .

Bonnes pratiques pour l'accès des locataires au point de terminaison de l'équilibreur de charge utilisé pour FabricPool

Vous pouvez contrôler quels locataires peuvent utiliser un point de terminaison d'équilibrage de charge spécifique pour accéder à leurs buckets. Vous pouvez autoriser tous les locataires, autoriser certains locataires ou bloquer certains locataires. Lors de la création d'un point de terminaison d'équilibrage de charge pour l'utilisation de FabricPool , sélectionnez **Autoriser tous les locataires**. ONTAP crypte les données placées dans les buckets StorageGRID , donc peu de sécurité supplémentaire serait fournie par cette couche de sécurité supplémentaire.

Bonnes pratiques pour le certificat de sécurité

Lorsque vous créez un point de terminaison d'équilibrage de charge StorageGRID pour l'utilisation de 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 cryptage TLS (Transport Layer Security). L'utilisation de FabricPool sans cryptage TLS est prise en charge mais non recommandée. Lorsque vous sélectionnez le protocole réseau pour le point de terminaison 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 de terminaison d'équilibrage de charge :

- ["Gérer les certificats de sécurité"](#)
- ["Considérations relatives à l'équilibrage de charge"](#)
- ["Directives de renforcement pour les certificats de serveur"](#)

Ajouter un certificat à ONTAP

Lorsque vous ajoutez StorageGRID en tant que niveau cloud FabricPool , vous devez installer le même certificat sur le cluster ONTAP , y compris les certificats racine et tous les certificats d'autorité de certification (CA) subordonnés.

Gérer l'expiration des certificats



Si le certificat utilisé pour sécuriser la connexion entre ONTAP et StorageGRID expire, FabricPool cessera temporairement de fonctionner et ONTAP perdra temporairement l'accès aux données hiérarchisées sur StorageGRID.

Pour éviter les problèmes d'expiration des certificats, suivez ces bonnes pratiques :

- Surveillez attentivement toutes les alertes qui avertissent de l'approche de la date d'expiration du certificat, telles que les alertes **Expiration du certificat du point de terminaison de l'équilibreur de charge** et **Expiration du certificat du serveur global pour l'API S3**.
- Gardez toujours les versions StorageGRID et ONTAP du certificat synchronisées. Si vous remplacez ou renouvelez le certificat utilisé pour un point de terminaison d'équilibrage de charge, vous devez remplacer ou renouveler le certificat équivalent utilisé par ONTAP pour le niveau cloud.
- Utilisez un certificat CA 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. Cela vous permet de remplacer les certificats sur le point d'expirer sans interruption.
- Si vous avez généré un certificat StorageGRID auto-signé et que ce certificat est sur le point d'expirer, vous devez remplacer manuellement le certificat dans StorageGRID et dans ONTAP avant l'expiration du certificat existant. 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 auto-signé StorageGRID sur un déploiement ONTAP FabricPool existant"](#) pour les instructions.

Bonnes pratiques pour l'utilisation d'ILM avec les données FabricPool

Si vous utilisez FabricPool pour hiérarchiser les données vers StorageGRID, vous devez comprendre les exigences d'utilisation de la gestion du cycle de vie des informations (ILM) de StorageGRID avec les données FabricPool .



FabricPool n'a aucune connaissance des règles ou politiques ILM de StorageGRID . Une perte de données peut se produire si la stratégie ILM StorageGRID est mal configurée. Pour des informations détaillées, voir ["Utiliser les règles ILM pour gérer les objets"](#) et ["Créer des politiques ILM"](#) .

Directives d'utilisation d'ILM avec FabricPool

Lorsque vous utilisez l'assistant de configuration FabricPool , l'assistant crée automatiquement une nouvelle règle ILM pour chaque compartiment S3 que vous créez et ajoute cette règle à une stratégie inactive. Vous

êtes invité à activer la politique. La règle créée automatiquement suit les meilleures pratiques recommandées : elle utilise le codage d'effacement 2+1 sur un seul site.

Si vous configurez StorageGRID manuellement au lieu d'utiliser l'assistant de configuration FabricPool, consultez ces instructions pour vous assurer que vos règles ILM et votre stratégie ILM sont adaptées aux données FabricPool et aux besoins de votre entreprise. Vous devrez peut-être créer de nouvelles règles et mettre à jour vos politiques ILM actives pour respecter ces directives.

- Vous pouvez utiliser n'importe quelle combinaison de règles de réplication et de codage d'effacement pour protéger les données de niveau cloud.

La meilleure pratique recommandée consiste à utiliser le codage d'effacement 2+1 au sein d'un site pour une protection des données rentable. Le codage d'effacement utilise plus de CPU, mais offre une capacité de stockage nettement inférieure à celle de la réplication. Les schémas 4+1 et 6+1 utilisent moins de capacité que le schéma 2+1. Cependant, les schémas 4+1 et 6+1 sont moins flexibles si vous devez ajouter des nœuds de stockage lors de l'extension du réseau. Pour plus de détails, consultez la section ["Ajouter une capacité de stockage pour les objets à code d'effacement"](#).

- Chaque règle appliquée aux données FabricPool doit soit utiliser le codage d'effacement, soit créer au moins deux copies répliquées.



Une règle ILM qui crée une seule copie répliquée pour une période donnée expose les données à un risque de perte permanente. Si une seule copie répliquée d'un objet existe, cet objet est perdu si un nœud de stockage échoue ou présente une erreur importante. Vous perdez également temporairement l'accès à l'objet pendant les procédures de maintenance telles que les mises à niveau.

- Si vous avez besoin de ["supprimer les données FabricPool de StorageGRID"](#), utilisez ONTAP pour récupérer toutes les données du volume FabricPool et les promouvoir au niveau de performance.



Pour éviter toute perte de données, n'utilisez pas de règle ILM qui expirera ou supprimera les données de niveau cloud FabricPool. Définissez la période de conservation dans chaque règle ILM sur **pour toujours** pour garantir que les objets FabricPool ne sont pas supprimés par StorageGRID ILM.

- Ne créez pas de règles qui déplaceront les données de niveau cloud FabricPool hors du bucket vers un autre emplacement. Vous ne pouvez pas utiliser un pool de stockage cloud pour déplacer les données FabricPool vers un autre magasin d'objets.



L'utilisation de pools de stockage Cloud avec FabricPool n'est pas prise en charge en raison de la latence supplémentaire nécessaire pour récupérer un objet à partir de la cible du pool de stockage Cloud.

- À partir d'ONTAP 9.8, vous pouvez éventuellement créer des balises d'objet pour aider à classer et trier les données hiérarchisées pour une gestion plus facile. Par exemple, vous pouvez définir des balises uniquement sur les volumes FabricPool attachés à StorageGRID. Ensuite, lorsque vous créez des règles ILM dans StorageGRID, vous pouvez utiliser le filtre avancé de balise d'objet pour sélectionner et placer ces données.

Autres bonnes pratiques pour StorageGRID et FabricPool

Lors de la configuration d'un système StorageGRID à utiliser avec FabricPool, vous devrez peut-être modifier d'autres options StorageGRID. Avant de modifier un paramètre

global, réfléchissez à la manière dont la modification affectera les autres applications S3.

Destinations des messages d'audit et des journaux

Les charges de travail FabricPool ont souvent un taux élevé d'opérations de lecture, ce qui peut générer un volume élevé de messages d'audit.

- Si vous n'avez pas besoin d'un enregistrement des opérations de lecture client pour FabricPool ou toute autre application S3, accédez éventuellement à **CONFIGURATION > Surveillance > Serveur d'audit et syslog**. Modifiez le paramètre **Lectures client** sur **Erreur** pour réduire le nombre de messages d'audit enregistrés dans le journal d'audit. Voir "[Configurer les messages d'audit et les destinations des journaux](#)" pour plus de détails.
- 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 minimise 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 de détails.

Chiffrement d'objet

Lors de la configuration de StorageGRID, vous pouvez éventuellement activer le "[option globale pour le chiffrement des objets stockés](#)" si le cryptage des données est requis pour d'autres clients StorageGRID. Les données hiérarchisées de FabricPool vers StorageGRID sont déjà chiffrées, l'activation du paramètre StorageGRID n'est donc pas requise. Les clés de chiffrement côté client appartiennent à ONTAP.

Compression d'objets

Lors de la configuration de StorageGRID, n'activez pas le "[option globale pour compresser les objets stockés](#)". Les données hiérarchisées de FabricPool vers StorageGRID sont déjà compressées. L'utilisation de l'option StorageGRID ne réduira pas davantage la taille d'un objet.

Consistance du seau

Pour les buckets FabricPool, la cohérence de bucket recommandée est **Lecture après nouvelle écriture**, qui est la cohérence par défaut pour un nouveau bucket. Ne modifiez pas les buckets FabricPool pour utiliser **Disponible** ou **Strong-site**.

Hiérarchisation de FabricPool

Si un nœud StorageGRID utilise le stockage attribué à partir d'un système NetApp ONTAP, vérifiez que le volume n'a pas de stratégie de hiérarchisation FabricPool activée. Par exemple, si un nœud StorageGRID s'exécute sur un hôte VMware, assurez-vous que le volume qui sauvegarde la banque de données pour le nœud StorageGRID n'a pas de stratégie de hiérarchisation FabricPool activée. La désactivation de la hiérarchisation FabricPool pour les volumes utilisés avec les nœuds StorageGRID simplifie le dépannage et les opérations de stockage.



N'utilisez jamais FabricPool pour hiérarchiser les données liées à StorageGRID vers StorageGRID lui-même. La hiérarchisation des données StorageGRID vers StorageGRID augmente le dépannage et la complexité opérationnelle.

Supprimer les données FabricPool de StorageGRID

Si vous devez supprimer les données FabricPool actuellement stockées dans

StorageGRID, vous devez utiliser ONTAP pour récupérer toutes les données du volume FabricPool et les promouvoir au niveau de performance.

Avant de commencer

- Vous avez examiné les instructions et les considérations dans ["Promouvoir les données vers le niveau 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 locataire FabricPool qui possède le ["Gérer tous les buckets ou l'autorisation d'accès root"](#) .

À propos de cette tâche

Ces instructions expliquent comment déplacer les données de StorageGRID vers FabricPool. Vous effectuez cette procédure à l'aide ONTAP et de StorageGRID Tenant Manager.

Étapes

1. Depuis ONTAP, émettez le `volume modify` commande.

Ensemble `tiering-policy` à `none` pour arrêter la nouvelle hiérarchisation et définir `cloud-retrieval-policy` à `promote` pour renvoyer toutes les données qui étaient précédemment hiérarchisées vers StorageGRID.

Voir ["Promouvoir toutes les données d'un volume FabricPool vers le niveau de performance"](#) .

2. Attendez que l'opération soit terminée.

Vous pouvez utiliser le `volume object-store` commande avec le `tiering` option pour ["vérifier l'état de la promotion du niveau de performance"](#) .

3. Une fois l'opération de promotion terminée, connectez-vous à StorageGRID Tenant Manager pour le compte locataire FabricPool .
4. Sélectionnez **Afficher les buckets** dans le tableau de bord ou sélectionnez **STOCKAGE (S3) > Buckets**.
5. Confirmez que le bucket FabricPool est désormais vide.
6. Si le seau est vide, ["supprimer le bucket"](#) .

Après avoir terminé

Lorsque vous supprimez le bucket, la hiérarchisation de FabricPool vers StorageGRID ne peut plus continuer. Cependant, étant donné que le niveau local est toujours attaché au niveau cloud StorageGRID , ONTAP System Manager renvoie des messages d'erreur indiquant que le bucket est inaccessible.

Pour éviter ces messages d'erreur, effectuez l'une des opérations suivantes :

- Utilisez FabricPool Mirror pour attacher un niveau de cloud différent à l'agrégat.
- Déplacez les données de l'agrégat FabricPool vers un agrégat non FabricPool , puis supprimez l'agrégat inutilisé.

Voir le ["Documentation ONTAP pour FabricPool"](#) pour les instructions.

Utiliser les locataires et les clients StorageGRID

Utiliser un compte locataire

Utiliser un compte locataire

Un compte locataire vous permet d'utiliser l'API REST Simple Storage Service (S3) ou l'API REST Swift pour stocker et récupérer des objets dans un système StorageGRID .

Qu'est-ce qu'un compte locataire ?

Chaque compte locataire possède ses propres groupes fédérés ou locaux, utilisateurs, buckets S3 ou conteneurs Swift et objets.

Les comptes locataires peuvent être utilisés pour séparer les objets stockés par différentes entités. Par exemple, plusieurs comptes locataires peuvent être utilisés pour l'un ou l'autre de ces cas d'utilisation :

- **Cas d'utilisation d'entreprise** : si le système StorageGRID est utilisé au sein d'une entreprise, le stockage d'objets de la grille peut être séparé par les différents services de l'organisation. Par exemple, il peut y avoir des comptes locataires pour le service marketing, le service d'assistance clientèle, le service des ressources humaines, etc.



Si vous utilisez le protocole client S3, vous pouvez également utiliser des buckets S3 et des stratégies de bucket pour séparer les objets entre les services d'une entreprise. Vous n'avez pas besoin de créer des comptes locataires distincts. Voir les instructions de mise en œuvre "[Buckets S3 et politiques de buckets](#)" pour plus d'informations.

- **Cas d'utilisation du fournisseur de services** : si le système StorageGRID est utilisé par un fournisseur de services, le stockage d'objets de la grille peut être séparé par les différentes entités qui louent le stockage. Par exemple, il peut y avoir des comptes locataires pour la société A, la société B, la société C, etc.

Comment créer un compte locataire

Les comptes locataires sont créés par un "[Administrateur de grille StorageGRID utilisant Grid Manager](#)". Lors de la création d'un compte locataire, l'administrateur du réseau spécifie les éléments suivants :

- Informations de base, notamment le nom du locataire, le type de client (S3) et le quota de stockage facultatif.
- Autorisations pour le compte locataire, par exemple si le compte locataire peut utiliser les services de la plateforme S3, configurer sa propre source d'identité, utiliser S3 Select ou utiliser une connexion de fédération de grille.
- L'accès root initial pour le locataire, selon que le système StorageGRID utilise des groupes et des utilisateurs locaux, une fédération d'identité ou une authentification unique (SSO).

De plus, les administrateurs de grille peuvent activer le paramètre de verrouillage d'objet S3 pour le système StorageGRID si les comptes de locataire S3 doivent se conformer aux exigences réglementaires. Lorsque le verrouillage d'objet S3 est activé, tous les comptes de locataire S3 peuvent créer et gérer des compartiments conformes.

Configurer les locataires S3

Après un ["Le compte locataire S3 est créé"](#) , vous pouvez accéder au gestionnaire de locataires pour effectuer des tâches telles que les suivantes :

- Configurer la fédération d'identité (sauf si la source d'identité est partagée avec la grille)
- Gérer les groupes et les utilisateurs
- Utiliser la fédération de grille pour le clonage de compte et la réplication inter-grille
- Gérer les clés d'accès S3
- Créer et gérer des buckets S3
- Utiliser les services de la plateforme S3
- Utiliser S3 Select
- Surveiller l'utilisation du stockage



Bien que vous puissiez créer et gérer des buckets S3 avec Tenant Manager, vous devez utiliser un ["Client S3"](#) ou ["Console S3"](#) pour ingérer et gérer des objets.

Comment se connecter et se déconnecter

Sign in à Tenant Manager

Vous accédez au Tenant Manager en saisissant l'URL du locataire dans la barre d'adresse d'un ["navigateur Web pris en charge"](#) .

Avant de commencer

- Vous avez vos identifiants de connexion.
- Vous disposez d'une URL pour accéder au gestionnaire de locataires, fournie par votre administrateur de réseau. L'URL ressemblera à 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 HA de nœuds d'administration. Il peut également inclure un numéro de port, l'ID de compte 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 a ["autorisations d'accès spécifiques"](#) .

Étapes

1. Lancer un ["navigateur Web pris en charge"](#) .

2. Dans la barre d'adresse du navigateur, saisissez l'URL permettant d'accéder à Tenant Manager.
3. Si une alerte de sécurité s'affiche, installez le certificat à l'aide de l'assistant d'installation du navigateur.
4. Sign in au gestionnaire de locataires.

L'écran de connexion qui s'affiche dépend de l'URL que vous avez saisie et de la configuration de l'authentification unique (SSO) pour StorageGRID.

Ne pas utiliser SSO

Si StorageGRID n'utilise pas SSO, l'un des écrans suivants s'affiche :

- La page de connexion de Grid Manager. Sélectionnez le lien **Connexion du locataire**.



NetApp StorageGRID®

Grid Manager

Username

Password

[Sign in](#)

[Tenant sign in](#) | [NetApp support](#) | [NetApp.com](#)

- La page de connexion du gestionnaire de locataires. Le champ **Compte** est peut-être déjà rempli, comme indiqué ci-dessous.

The screenshot shows the NetApp StorageGRID Tenant Manager login interface. At the top is the NetApp StorageGRID logo. Below it is the title 'Tenant Manager'. The form includes a 'Recent' dropdown menu currently showing '-- Optional --'. Below that is an 'Account' field containing the ID '64600207336181242061'. This is followed by 'Username' and 'Password' input fields. A blue 'Sign in' button is positioned below the password field. At the bottom of the form, there is a link for 'NetApp support | NetApp.com'.

- i. Si l'ID de compte à 20 chiffres du locataire n'est pas affiché, sélectionnez le nom du compte du locataire s'il apparaît dans la liste des comptes récents ou saisissez l'ID de compte.
- ii. Entrez votre nom d'utilisateur et votre mot de passe.
- iii. Sélectionnez * Sign in*.

Le tableau de bord du gestionnaire de locataires apparaît.

- iv. Si vous avez reçu un mot de passe initial de quelqu'un d'autre, sélectionnez **username > Modifier le mot de passe** 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:

Sign in with your organizational account

Sign in

Saisissez vos identifiants SSO standard et sélectionnez * Sign in*.

- La page de connexion SSO du gestionnaire de locataires.

NetApp StorageGRID®

Tenant Manager

Recent

S3 tenant ▼

Account

62984032838045582045

Sign in

[NetApp support](#) | [NetApp.com](#)

- Si l'ID de compte à 20 chiffres du locataire n'est pas affiché, sélectionnez le nom du compte du locataire s'il apparaît dans la liste des comptes récents ou saisissez l'ID de compte.
- Sélectionnez * Sign in*.
- Sign in avec vos informations d'identification SSO standard sur la page de connexion SSO de votre organisation.

Le tableau de bord du gestionnaire de locataires apparaît.

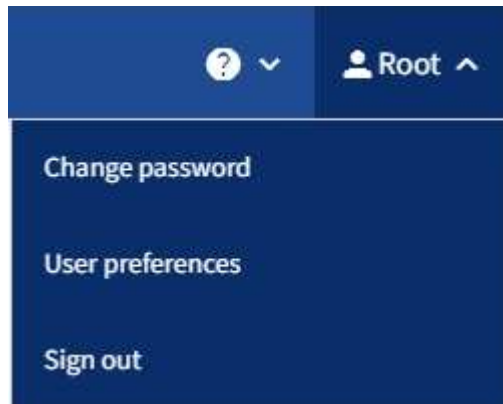
Déconnexion de Tenant Manager

Une fois que vous avez terminé de travailler avec le gestionnaire de locataires, vous

devez vous déconnecter pour garantir que les utilisateurs non autorisés ne peuvent pas accéder au système StorageGRID . La fermeture de votre navigateur peut ne pas vous déconnecter du système, en fonction des paramètres de cookies du navigateur.

Étapes

1. Localisez la liste déroulante du 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 du 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 accédez. La page de Sign in StorageGRID s'affiche. Le nom du compte locataire auquel vous venez d'accéder est répertorié par défaut dans la liste déroulante **Comptes récents** et l'**ID de compte** du locataire est affiché.



Si SSO est activé et que vous êtes également connecté au Gestionnaire de grille, vous devez également vous déconnecter du Gestionnaire de grille pour vous déconnecter de SSO.

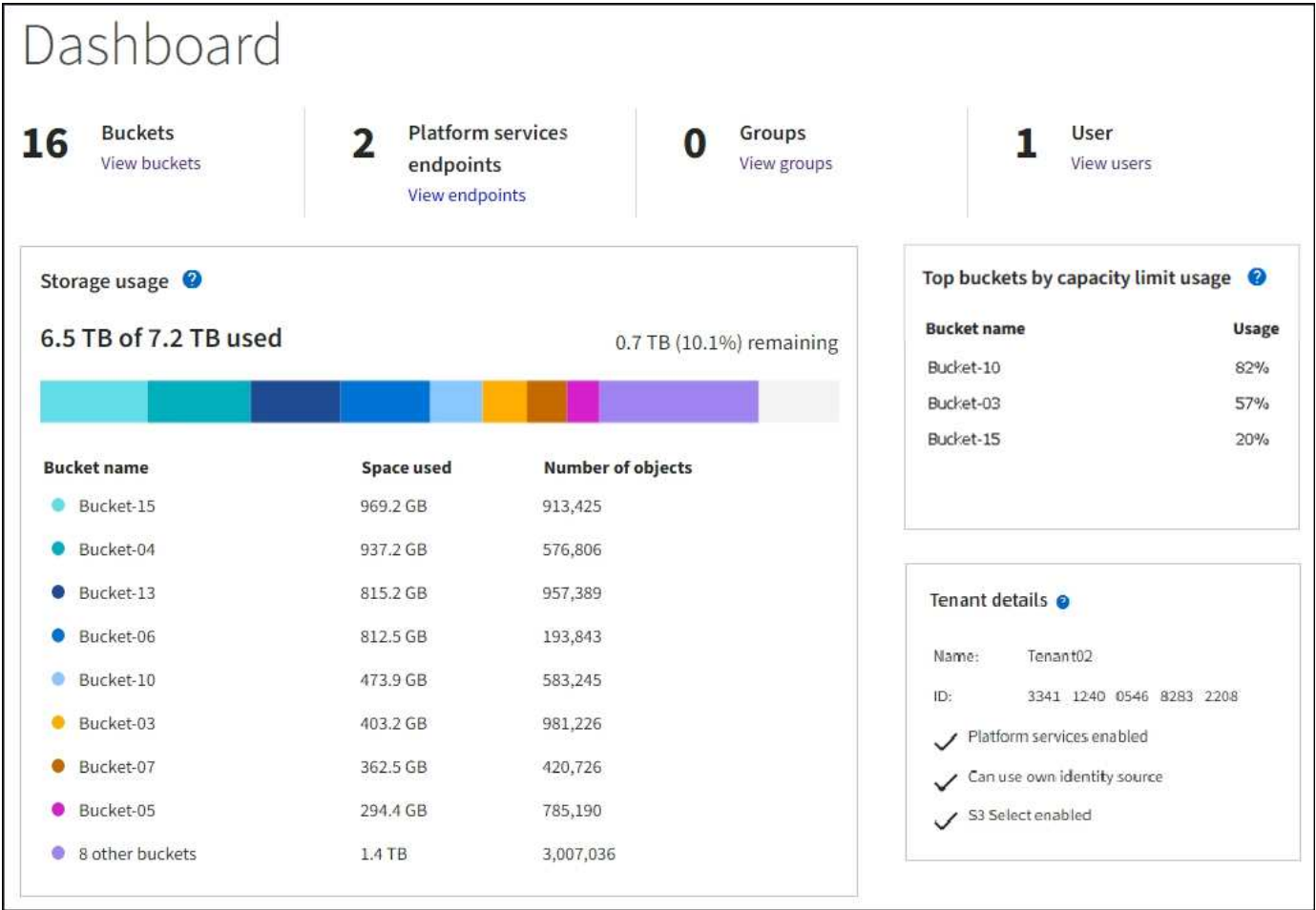
Comprendre le tableau de bord du Tenant Manager

Le tableau de bord du gestionnaire de locataires fournit un aperçu de la configuration d'un compte de locataire et de la quantité d'espace utilisée par les objets dans les compartiments (S3) ou les conteneurs (Swift) du locataire. Si le locataire dispose d'un quota, le tableau de bord indique la part du quota utilisée et la part restante. S'il y a des erreurs liées au compte locataire, les erreurs sont affichées sur le tableau de bord.



Les valeurs de l'espace utilisé sont des estimations. Ces estimations sont affectées par le moment des ingestions, la connectivité réseau et l'état du nœud.

Une fois les objets téléchargés, le tableau de bord ressemble à l'exemple suivant :





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 télécharger des objets et rejette les nouvelles acquisitions si le locataire a dépassé le quota. Cependant, StorageGRID ne prend pas en compte la taille du téléchargement actuel pour déterminer si le quota a été dépassé. Si des objets sont supprimés, un locataire peut être temporairement empêché de télécharger de nouveaux objets jusqu'à ce que l'utilisation du quota soit recalculée. Les calculs d'utilisation des quotas peuvent prendre 10 minutes ou plus.

- Un graphique à barres qui représente les tailles relatives des plus grands seaux ou conteneurs.

Vous pouvez placer votre curseur sur l'un des segments du graphique pour afficher l'espace total consommé par ce bucket ou ce conteneur.



- Pour correspondre au graphique à barres, une liste des plus grands compartiments ou conteneurs, y compris la quantité totale de données d'objet et le nombre d'objets pour chaque compartiment 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 seaux ou conteneurs, tous les autres seaux 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 de quota ont été activées dans le gestionnaire de grille, ces alertes apparaîtront 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 **Utilisation élevée du quota du locataire** est déclenchée.

Pensez à demander à votre administrateur de réseau d'augmenter le quota.

- Si vous dépassez votre quota, une notification vous indique que vous ne pouvez pas télécharger de nouveaux objets.

Utilisation de la limite de capacité

Si vous avez défini une limite de capacité pour vos compartiments, le tableau de bord du gestionnaire de locataires affiche une liste des compartiments principaux par utilisation de la limite de capacité.

Si aucune limite n'est définie pour un bucket, sa capacité est illimitée. Cependant, si votre compte locataire dispose d'un quota de stockage total et que ce quota est atteint, vous ne pourrez pas ingérer davantage d'objets, quelle que soit la limite de capacité restante sur un bucket.

Erreurs de point de terminaison

Si vous avez utilisé Grid Manager pour configurer un ou plusieurs points de terminaison à utiliser avec les services de plateforme, le tableau de bord Tenant Manager affiche une alerte si des erreurs de point de terminaison se sont produites au cours des sept derniers jours.

 One or more endpoints have experienced an error and might not be functioning properly. Go to the [Endpoints](#) page to view the error details. The last error occurred 2 hours ago.

Pour voir les détails sur "[erreurs de point de terminaison des services de plateforme](#)", sélectionnez **Points de terminaison** pour afficher la page Points de terminaison.

API de gestion des locataires

Comprendre l'API de gestion des locataires

Vous pouvez effectuer des tâches de gestion du système à l'aide de l'API REST de gestion des locataires au lieu de l'interface utilisateur du gestionnaire des locataires. Par exemple, vous souhaitez peut-être utiliser l'API pour automatiser des opérations ou créer plusieurs entités, telles que des utilisateurs, plus rapidement.

L'API de gestion des locataires :

- Utilise la plateforme 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 de Swagger fournit des détails complets et une documentation pour chaque opération API.
- Utilisations "[gestion des versions pour prendre en charge les mises à niveau non perturbatrices](#)".

Pour accéder à la documentation Swagger pour l'API de gestion des locataires :

1. Sign in au gestionnaire de locataires.
2. En haut du gestionnaire de locataires, sélectionnez l'icône d'aide et sélectionnez **Documentation API**.

Opérations 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 permettant d'effectuer l'authentification de la session utilisateur.

L'API de gestion des locataires prend en charge le schéma d'authentification du jeton porteur. Pour une connexion locataire, vous fournissez un nom d'utilisateur, un mot de passe et un accountId dans le corps JSON de la demande d'authentification (c'est-à-dire, `POST /api/v3/authorize`). Si l'utilisateur est authentifié avec succès, un jeton de sécurité est renvoyé. Ce jeton doit être fourni dans l'en-tête des requêtes API ultérieures (« Autorisation : jeton porteur »).

Pour plus d'informations sur l'amélioration de la sécurité de l'authentification, consultez ["Protection contre la falsification de requêtes intersites"](#).



Si l'authentification unique (SSO) est activée pour le système StorageGRID, vous devez effectuer différentes étapes pour vous authentifier. Voir le ["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 répertorier la version du produit et les principales versions de l'API prises en charge par cette version.
- **conteneurs** : opérations sur les buckets S3 ou les conteneurs Swift.
- **fonctionnalités désactivées** : opérations permettant d'afficher les fonctionnalités qui pourraient avoir été désactivées.
- **points de terminaison** : opérations permettant de gérer un point de terminaison. Les points de terminaison permettent à un bucket 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 inter-grille.
- **groupes** : opérations de gestion des groupes de locataires locaux et de récupération des groupes de locataires fédérés à partir d'une source d'identité externe.
- **identity-source** : opérations permettant de configurer une source d'identité externe et de synchroniser manuellement les informations des groupes fédérés et des utilisateurs.
- **ilm** : opérations sur les paramètres de gestion du cycle de vie de l'information (ILM).
- **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 permettant d'afficher et de gérer les utilisateurs locataires.

Détails de l'opération

Lorsque vous développez chaque opération API, vous pouvez voir son action HTTP, l'URL du point de terminaison, une liste de tous les paramètres obligatoires ou facultatifs, un exemple du corps de la requête (si nécessaire) et les réponses possibles.

groups Operations on groups

GET `/org/groups` Lists Tenant User Groups

Parameters Try it out

Name	Description
<code>type</code> string (query)	filter by group type
<code>limit</code> integer (query)	maximum number of results
<code>marker</code> string (query)	marker-style pagination offset (value is Group's URN)
<code>includeMarker</code> boolean (query)	if set, the marker element is also returned
<code>order</code> string (query)	pagination order (desc requires marker)

Responses Response content type `application/json`

Code	Description
200	Example Value Model <pre>{ "responseTime": "2018-02-01T16:22:31.066Z", "status": "success", "apiVersion": "2.3" }</pre>

Émettre des requêtes API



Toutes les opérations API que vous effectuez à l'aide de la page Web de documentation API 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 voir les détails de la demande.

2. Déterminez si la demande nécessite des paramètres supplémentaires, tels qu'un ID de groupe ou d'utilisateur. Ensuite, obtenez ces valeurs. Vous devrez peut-être d'abord émettre une demande d'API différente pour obtenir les informations dont vous avez besoin.
3. Déterminez si vous devez modifier le corps de la demande d'exemple. Si tel est le cas, vous pouvez sélectionner **Modèle** pour connaître les exigences de chaque champ.
4. Sélectionnez **Essayer**.
5. Fournissez tous les paramètres requis ou modifiez le corps de la demande selon vos besoins.
6. Sélectionnez **Exécuter**.
7. Consultez 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 le contrôle de version pour prendre en charge les mises à niveau sans interruption.

Par exemple, cette URL de demande spécifie la version 4 de l'API.

`https://hostname_or_ip_address/api/v4/authorize`

La version principale de l'API est mise à jour lorsque des modifications sont apportées qui ne sont pas compatibles avec les versions plus anciennes. La version mineure de l'API est mise à jour lorsque des modifications sont apportées qui sont *compatibles* avec les versions plus anciennes. Les modifications compatibles incluent l'ajout de nouveaux points de terminaison ou de nouvelles propriétés.

L'exemple suivant illustre comment la version de l'API est augmentée en fonction du type de modifications apportées.

Type de modification de l'API	Ancienne version	Nouvelle version
Compatible avec les anciennes versions	2,1	2,2
Non compatible avec les anciennes versions	2,1	3,0

Lorsque vous installez le logiciel StorageGRID pour la première fois, seule la version la plus récente de l'API est activée. Cependant, lorsque vous effectuez une mise à niveau vers une nouvelle version de fonctionnalité de StorageGRID, vous continuez à avoir accès à l'ancienne version de l'API pour au moins une version de fonctionnalité de StorageGRID .



Vous pouvez configurer les versions prises en charge. Consultez la section **config** de la documentation de l'API Swagger pour le "[API de gestion de grille](#)" pour plus d'informations. Vous devez désactiver la prise en charge de l'ancienne version après avoir mis à jour tous les clients API pour utiliser la version la plus récente.

Les demandes obsolètes sont marquées comme obsolètes 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 v2 API at POST "/api/v2/authorize"
```

Déterminer quelles versions d'API sont prises en charge dans la version actuelle

Utilisez le GET /versions Requête d'API pour renvoyer une liste des versions majeures d'API prises en charge. Cette demande se trouve dans la section **config** de la documentation de l'API Swagger.

```
GET https://{{IP-Address}}/api/versions
{
  "responseTime": "2023-06-27T22:13:50.750Z",
  "status": "success",
  "apiVersion": "4.0",
  "data": [
    2,
    3,
    4
  ]
}
```

Spécifier une version d'API pour une requête

Vous pouvez spécifier la version de l'API à l'aide d'un paramètre de chemin(/api/v4) ou un en-tête(Api-Version: 4). Si vous fournissez les deux valeurs, la valeur de l'en-tête remplace la valeur du chemin.

```
curl https://[IP-Address]/api/v4/grid/accounts

curl -H "Api-Version: 4" https://[IP-Address]/api/grid/accounts
```

Protection contre la falsification de requêtes intersites (CSRF)

Vous pouvez contribuer à vous protéger contre les attaques de falsification de requête intersite (CSRF) contre StorageGRID en utilisant des jetons CSRF pour améliorer l'authentification qui utilise des cookies. Le gestionnaire de grille et le gestionnaire de locataires activent automatiquement cette fonctionnalité de sécurité ; les autres clients API peuvent choisir de l'activer ou non lorsqu'ils se connectent.

Un attaquant capable de déclencher une requête vers un autre site (par exemple avec un formulaire HTTP POST) peut provoquer l'exécution de certaines requêtes à l'aide des cookies de l'utilisateur connecté.

StorageGRID aide à se protéger contre les attaques CSRF en utilisant des jetons CSRF. Lorsqu'elle 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 fonctionnalité, définissez le `csrfToken` paramètre à `true` lors de 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"
```

Lorsque c'est vrai, un `GridCsrfToken` Le cookie est défini avec une valeur aléatoire pour les connexions au Grid Manager, et le `AccountCsrfToken` le cookie est défini avec une valeur aléatoire pour les connexions au Tenant Manager.

Si le cookie est présent, toutes les requêtes pouvant modifier l'état du système (POST, PUT, PATCH, DELETE) doivent inclure l'un des éléments suivants :

- Le `X-Csrf-Token` en-tête, avec la valeur de l'en-tête définie sur la valeur du cookie de jeton CSRF.
- Pour les points de terminaison qui acceptent un corps codé par formulaire : A `csrfToken` paramètre de corps de requête codé par formulaire.

Pour configurer la protection CSRF, utilisez le ["API de gestion de grille"](#) ou ["API de gestion des locataires"](#).



Les requêtes qui ont un cookie de jeton CSRF défini appliqueront également l'en-tête « Content-Type : application/json » pour toute requête qui attend un corps de requête JSON comme protection supplémentaire contre les attaques CSRF.

Utiliser les connexions de la fédération de grille

Cloner des groupes de locataires et des utilisateurs

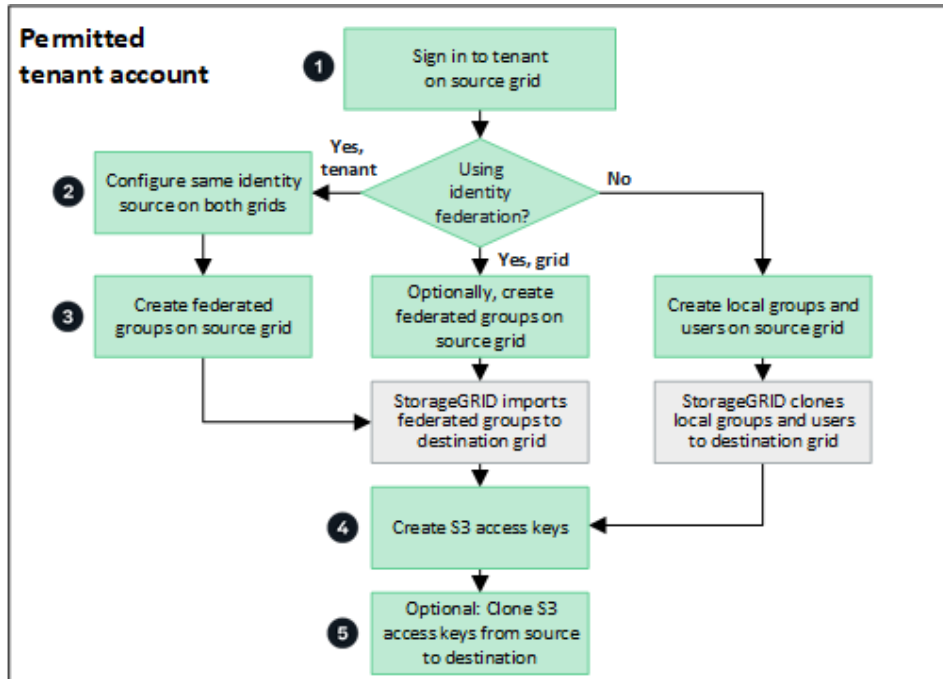
Si un locataire a été créé ou modifié pour utiliser une connexion de fédération de grille, ce locataire est répliqué d'un système StorageGRID (le locataire source) vers un autre système StorageGRID (le locataire réplique). Une fois le locataire répliqué, tous les groupes et utilisateurs ajoutés au locataire source sont clonés sur le locataire répliqué.

Le système StorageGRID dans lequel le locataire est créé à l'origine est la *grille source* du locataire. Le système StorageGRID sur lequel le locataire est répliqué est la *grille de destination* du locataire. Les deux comptes locataires ont le même ID de compte, le même nom, la même description, le même quota de stockage et les mêmes 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 clonage de compte"](#) et ["Gérer les locataires autorisés"](#).

Le clonage des informations du compte locataire est requis pour ["réplication inter-réseaux"](#) d'objets de seau. Le fait d'avoir les mêmes groupes de locataires et utilisateurs sur les deux grilles garantit que vous pouvez accéder aux compartiments et objets correspondants sur l'une ou l'autre grille.

Flux de travail du locataire pour le clonage de compte

Si votre compte locataire dispose de l'autorisation **Utiliser la connexion à la fédération de grille**, consultez le diagramme de flux de travail pour voir les étapes que vous effectuerez pour cloner des groupes, des utilisateurs et des clés d'accès S3.



Voici les principales étapes du flux de travail :

1

Sign in au locataire

Sign in au compte locataire sur la grille source (la grille où le locataire a été initialement créé).

2

En option, configurer la fédération d'identité

Si votre compte locataire dispose de l'autorisation **Utiliser sa propre source d'identité** pour utiliser des groupes et des utilisateurs fédérés, configurez la même source d'identité (avec les mêmes paramètres) pour les comptes locataires source et de destination. Les groupes et utilisateurs fédérés ne peuvent pas être clonés à moins que les deux grilles n'utilisent la même source d'identité. Pour les instructions, voir ["Utiliser la fédération d'identité"](#).

3

Créer des groupes et des utilisateurs

Lors de la création de groupes et d'utilisateurs, commencez toujours par la grille source du locataire. Lorsque vous ajoutez un nouveau groupe, StorageGRID le clone automatiquement sur la grille de destination.

- Si la fédération d'identité est configurée pour l'ensemble du système StorageGRID ou pour votre compte locataire, ["créer de nouveaux groupes de locataires"](#) en important des groupes fédérés à partir de la source d'identité.
- Si vous n'utilisez pas la fédération d'identité, ["créer de nouveaux groupes locaux"](#) et puis ["créer des utilisateurs locaux"](#).

4

Créer des clés d'accès S3

Tu peux "[créer vos propres clés d'accès](#)" ou à "[créer les clés d'accès d'un autre utilisateur](#)" sur la grille source ou sur la grille de destination pour accéder aux buckets sur cette grille.

5

En option, clonez les clés d'accès S3

Si vous devez accéder à des buckets avec les mêmes clés d'accès sur les deux grilles, créez les clés d'accès sur la grille source, puis utilisez l'API Tenant Manager pour les cloner manuellement sur la grille de destination. Pour les instructions, voir "[Cloner les clés d'accès S3 à l'aide de l'API](#)".

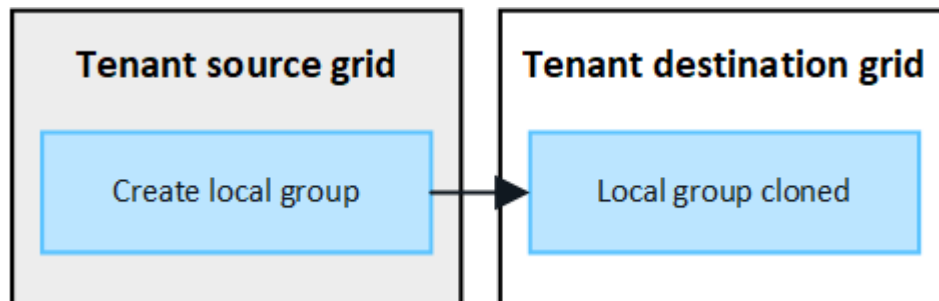
Comment les groupes, les utilisateurs et les clés d'accès S3 sont-ils clonés ?

Consultez cette section pour comprendre comment les groupes, les utilisateurs et les clés d'accès S3 sont clonés entre la grille source du locataire et la grille de destination du locataire.

Les groupes locaux créés sur 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 vers la grille de destination du locataire.

Le groupe d'origine et son clone ont le même mode d'accès, les mêmes autorisations de groupe et la même stratégie de groupe S3. Pour les instructions, voir "[Créer des groupes pour le locataire S3](#)".

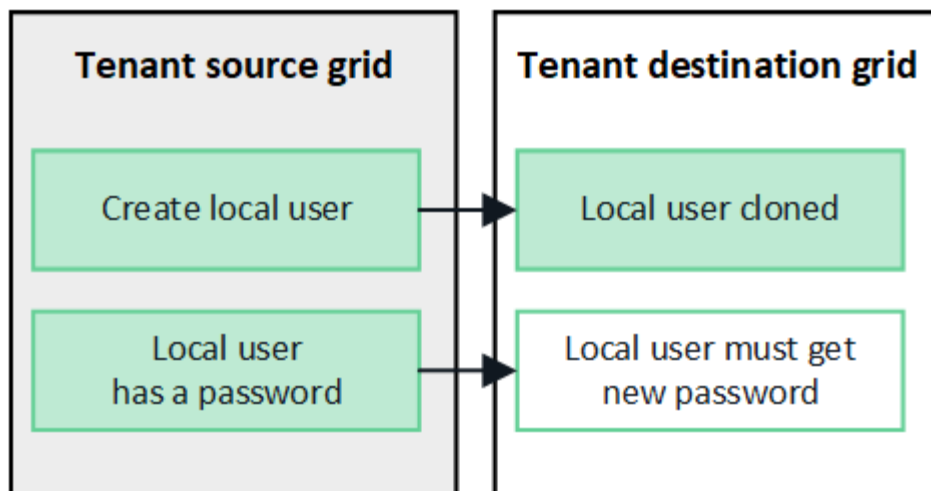


Tous les utilisateurs que vous sélectionnez lorsque vous créez un groupe local sur la grille source ne sont pas inclus lorsque le groupe est cloné sur la grille de destination. Pour cette raison, ne sélectionnez pas d'utilisateurs lorsque vous créez le groupe. Sélectionnez plutôt le groupe lorsque vous créez les utilisateurs.

Les utilisateurs locaux créés sur la grille source sont clonés

Lorsque vous créez un nouvel utilisateur local sur la grille source, StorageGRID clone automatiquement cet utilisateur sur la grille de destination. L'utilisateur d'origine et son clone ont le même nom complet, le même nom d'utilisateur et le même paramètre **Refuser l'accès**. Les deux utilisateurs appartiennent également aux mêmes groupes. Pour les instructions, voir "[Gérer 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 à Tenant Manager sur la grille de destination, l'utilisateur root du compte locataire doit ajouter un mot de passe pour cet utilisateur sur la grille de destination. Pour les instructions, voir "[Gérer les utilisateurs locaux](#)".

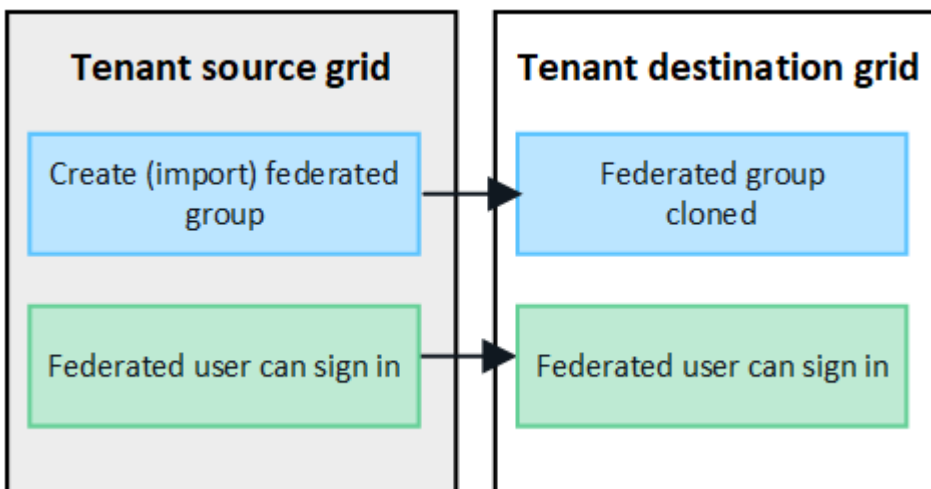


Les groupes fédérés créés sur la grille source sont clonés

En supposant que les exigences pour l'utilisation du clonage de compte avec ["authentification unique"](#) et ["fédération d'identité"](#) ont été rencontrés, les groupes fédérés que vous créez (importez) pour le locataire sur la grille source sont automatiquement clonés sur le locataire sur la grille de destination.

Les deux groupes ont le même mode d'accès, les mêmes autorisations de groupe et la même stratégie de groupe S3.

Une fois les groupes fédérés créés pour le locataire source et clonés vers le locataire de destination, les utilisateurs fédérés peuvent se connecter au locataire sur l'une ou l'autre grille.

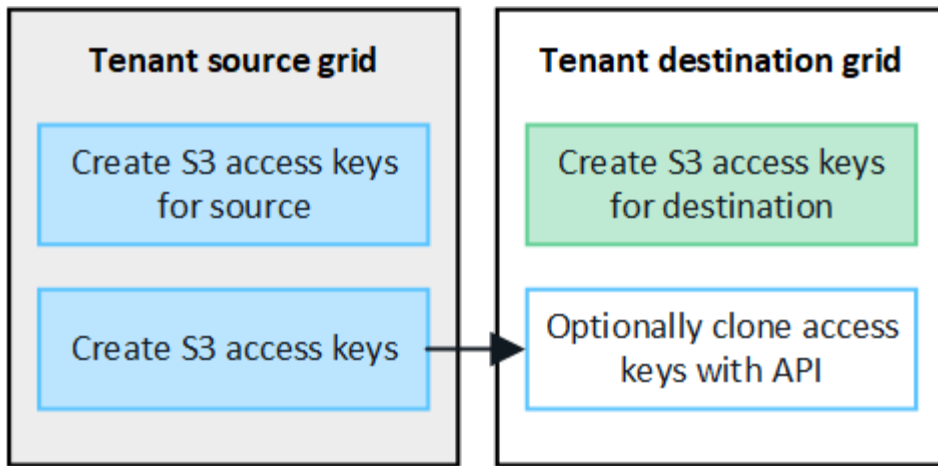


Les clés d'accès S3 peuvent être clonées manuellement

StorageGRID ne clone pas automatiquement les clés d'accès S3 car la sécurité est améliorée en ayant des clés différentes sur chaque grille.

Pour gérer les clés d'accès sur les deux grilles, vous pouvez effectuer l'une des opérations suivantes :

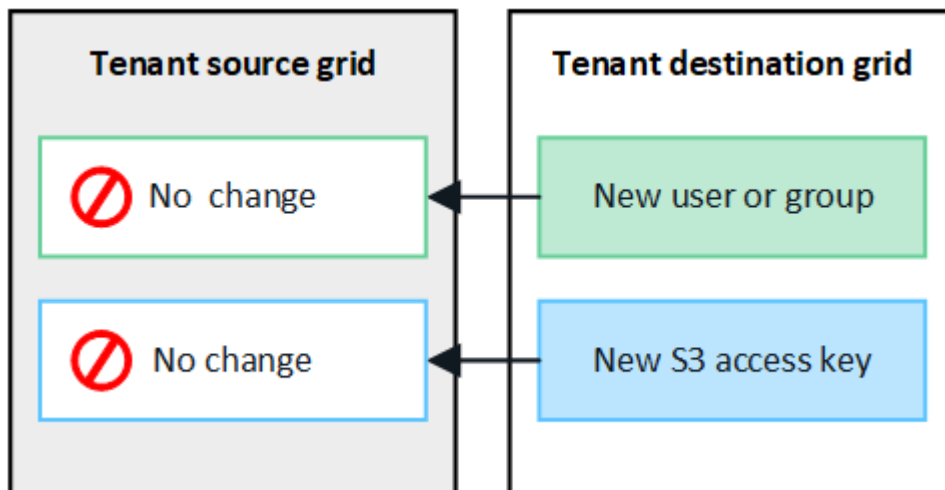
- Si vous n'avez pas besoin d'utiliser les mêmes clés pour chaque grille, vous pouvez ["créer vos propres clés d'accès"](#) ou ["créer les clés d'accès d'un autre utilisateur"](#) sur chaque grille.
- Si vous devez utiliser les mêmes clés sur les deux grilles, vous pouvez créer des clés sur la grille source, puis utiliser l'API Tenant Manager pour les utiliser manuellement. ["cloner les clés"](#) vers la grille de destination.



Lorsque vous clonez des clés d'accès S3 pour un utilisateur fédéré, l'utilisateur et les clés d'accès S3 sont clonés sur le locataire de destination.

Les groupes et les utilisateurs ajoutés à la grille de destination ne sont pas clonés

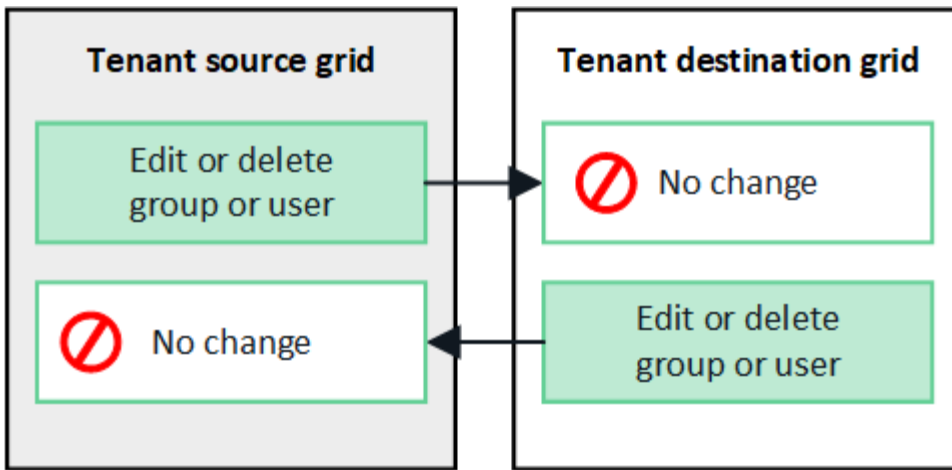
Le clonage se produit uniquement à partir de la grille source du locataire vers la grille de destination du locataire. Si vous créez ou importez des groupes et des utilisateurs sur la grille de destination du locataire, StorageGRID ne clonera pas ces éléments dans la grille source du locataire.



Les groupes, utilisateurs et clés d'accès modifiés ou supprimés ne sont pas clonés

Le clonage se produit 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 à la fédération de grille**, vous pouvez utiliser l'API de gestion des locataires pour cloner manuellement les clés d'accès S3 du locataire sur la grille source vers le locataire sur la grille de destination.

Avant de commencer

- Le compte locataire dispose de l'autorisation **Utiliser la connexion à la fédération de grille**.
- La connexion à la fédération de grille a un **statut 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 autorisation d'accès root"](#).
- Si vous clonez des clés d'accès pour un utilisateur local, l'utilisateur existe déjà sur les deux grilles.



Lorsque vous clonez des clés d'accès S3 pour un utilisateur fédéré, l'utilisateur et les clés d'accès S3 sont ajoutés 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. En utilisant le gestionnaire de locataires sur la grille source, ["créez vos propres clés d'accès"](#) et téléchargez le `.csv` déposer.
2. En haut du gestionnaire de locataires, sélectionnez l'icône d'aide et sélectionnez **Documentation API**.
3. Dans la section **s3**, sélectionnez le point de terminaison suivant :

```
POST /org/users/current-user/replicate-s3-access-key
```

POST

`/org/users/current-user/replicate-s3-access-key` Clone the current user's S3 key to the other grids.



4. Sélectionnez **Essayer**.
5. Dans la zone de texte **body**, remplacez les exemples d'entrées pour **accessKey** et **secretAccessKey** par les valeurs du fichier **.csv** que vous avez téléchargé.

Assurez-vous de conserver les guillemets doubles autour de chaque chaîne.



The screenshot shows a REST client interface with a field labeled 'body' marked as '* required'. Below the label, there are tabs for 'Edit Value' and 'Model'. The 'Edit Value' tab is active, displaying a JSON object: { "accessKey": "AKIAIOSFODNN7EXAMPLE", "secretAccessKey": "wJalrXUtnFEMI/K7MDENG/bPxrFiCYEXAMPLEKEY", "expires": "2028-09-04T00:00:00.000Z" }.

6. Si la clé expire, remplacez l'exemple d'entrée pour **expires** par la date et l'heure d'expiration sous forme de chaîne au format de données-heure 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. Confirmez que le code de réponse du serveur est **204**, indiquant que la clé a été clonée avec succès sur 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.

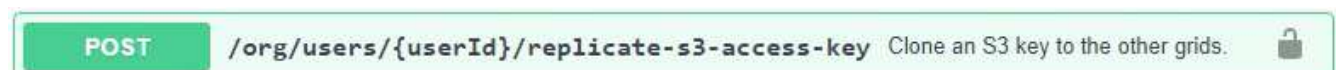
Étapes

1. En utilisant le gestionnaire de locataires sur la grille source, "[créer les clés d'accès S3 de l'autre utilisateur](#)" et téléchargez le **.csv** déposer.
2. En haut du gestionnaire de locataires, sélectionnez l'icône d'aide et sélectionnez **Documentation API**.
3. Obtenir l'ID utilisateur. Vous aurez besoin de cette valeur pour cloner les clés d'accès de l'autre utilisateur.
 - a. Dans la section **utilisateurs**, sélectionnez le point de terminaison suivant :
4. Dans la section **s3**, sélectionnez le point de terminaison suivant :

```
GET /org/users
```

- b. Sélectionnez **Essayer**.
- 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**.

```
POST /org/users/{userId}/replicate-s3-access-key
```



The screenshot shows a REST client interface with a green button labeled 'POST' and a text field containing the URL '/org/users/{userId}/replicate-s3-access-key'. To the right of the text field, there is a description 'Clone an S3 key to the other grids.' and a lock icon.

5. Sélectionnez **Essayer**.

6. Dans la zone de texte **userid**, collez l'ID utilisateur que vous avez copié.
7. Dans la zone de texte **corps**, remplacez les exemples d'entrées pour **exemple de clé d'accès** et **clé d'accès secrète** par les valeurs du fichier **.csv** pour cet utilisateur.

Assurez-vous de conserver les guillemets doubles autour de la chaîne.

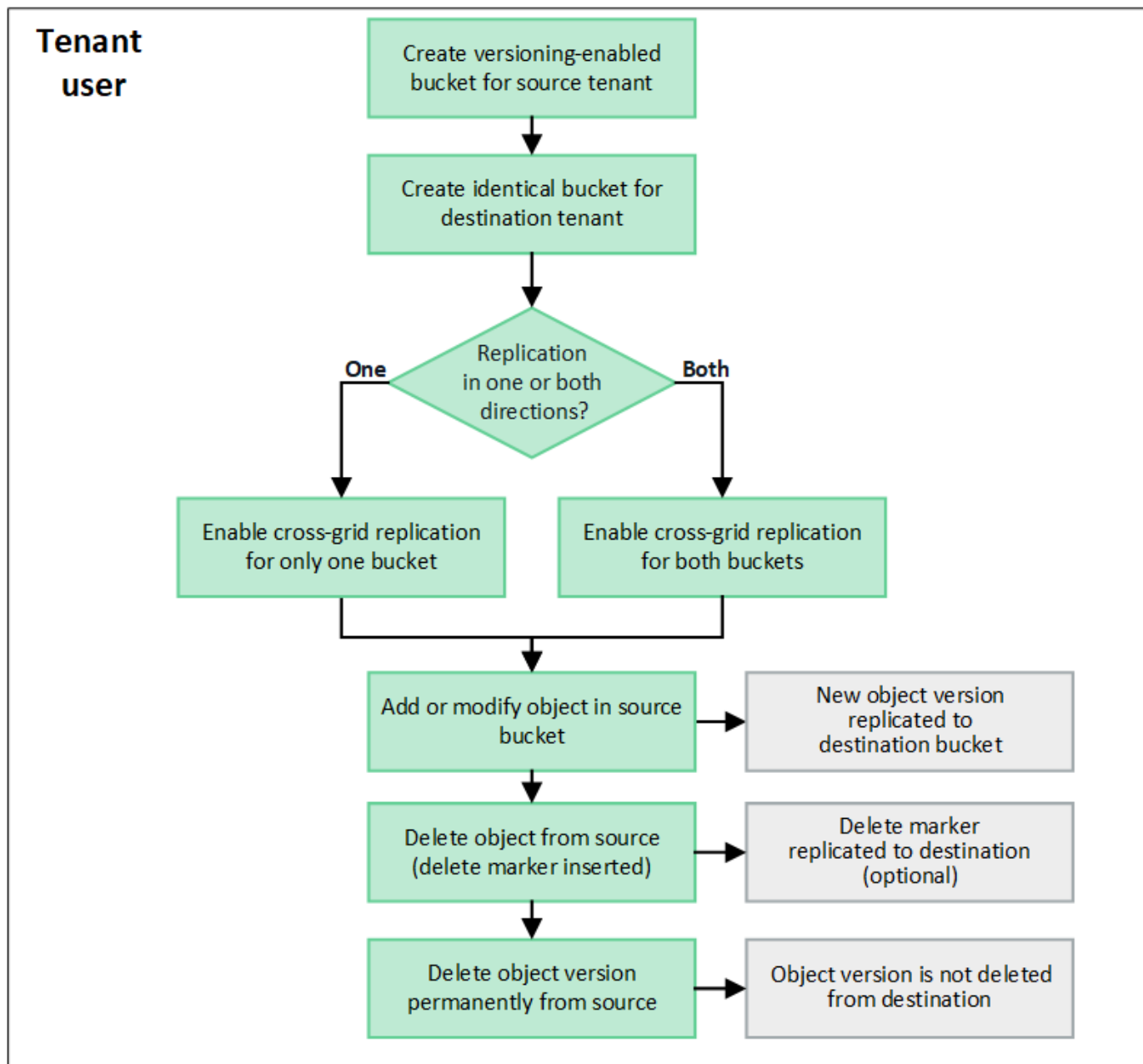
8. Si la clé expire, remplacez l'exemple d'entrée pour **expires** par la date et l'heure d'expiration sous forme de chaîne au format de données-heure ISO 8601 (par exemple, `2023-02-28T22:46:33-08:00`). Si la clé n'expire pas, entrez **null** comme valeur pour l'entrée **expires** (ou supprimez la ligne **Expires** et la virgule précédente).
9. Sélectionnez **Exécuter**.
10. Confirmez que le code de réponse du serveur est **204**, indiquant que la clé a été clonée avec succès sur la grille de destination.

Gérer la réplication inter-réseaux

Si l'autorisation **Utiliser la connexion à la fédération de grille** a été attribuée à votre compte de locataire lors de sa création, vous pouvez utiliser la réplication inter-grille pour répliquer automatiquement les objets entre les buckets de la grille source du locataire et les buckets de la grille de destination du locataire. La réplication inter-grille peut se produire dans un sens ou dans les deux sens.

Flux de travail pour la réplication inter-grille

Le diagramme de flux de travail résume les étapes que vous effectuerez pour configurer la réplication inter-grille entre les buckets sur deux grilles. Ces étapes sont décrites plus en détail ci-dessous.



Configurer la réplication inter-grille

Avant de pouvoir utiliser la réplication inter-grille, vous devez vous connecter aux comptes locataires correspondants sur chaque grille et créer des buckets identiques. Ensuite, vous pouvez activer la réplication inter-grille sur l'un ou les deux buckets.

Avant de commencer

- Vous avez examiné les exigences relatives à la réplication inter-réseaux. Voir ["Qu'est-ce que la réplication inter-réseau"](#).
- Vous utilisez un ["navigateur Web pris en charge"](#).
- Le compte locataire dispose de l'autorisation **Utiliser la connexion à la fédération de grille** et des comptes locataires identiques existent sur les deux grilles. Voir ["Gérer les locataires autorisés pour la connexion à la fédération de réseau"](#).
- L'utilisateur locataire avec lequel vous vous connecterez existe déjà sur les deux grilles et appartient à un groupe d'utilisateurs qui possède le ["Autorisation d'accès root"](#).

- 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 buckets identiques

Dans un premier temps, connectez-vous aux comptes locataires correspondants sur chaque grille et créez des buckets identiques.

Étapes

1. À partir de l'une ou l'autre des grilles de la connexion à la fédération de grilles, créez un nouveau bucket :
 - a. Sign in au compte locataire à l'aide des informations d'identification d'un utilisateur locataire 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, confirmez que l'utilisateur root du compte locataire a défini un mot de passe pour votre compte utilisateur.

- b. Suivez les instructions pour "[créer un bucket S3](#)".
 - c. Dans l'onglet **Gérer les paramètres de l'objet**, sélectionnez **Activer le contrôle de version de l'objet**.
 - d. Si le verrouillage d'objet S3 est activé pour votre système StorageGRID, n'activez pas le verrouillage d'objet S3 pour le bucket.
 - e. Sélectionnez **Créer un bucket**.
 - f. Sélectionnez **Terminer**.
2. Répétez ces étapes pour créer un bucket identique pour le même compte locataire sur l'autre grille dans la connexion de fédération de grille.



Selon les besoins, chaque bucket peut utiliser une région différente.

Activer la réplication inter-réseaux

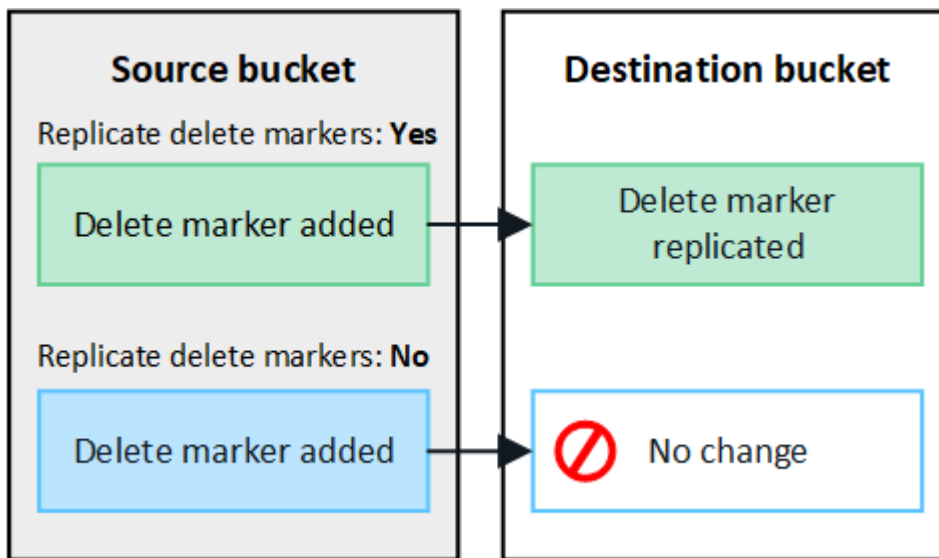
Vous devez effectuer ces étapes avant d'ajouter des objets à l'un ou l'autre des compartiments.

Étapes

1. À partir d'une grille dont vous souhaitez répliquer les objets, activez "[réplication inter-grille dans une direction](#)" :
 - a. Sign in au compte locataire du bucket.
 - b. Sélectionnez **Afficher les buckets** dans le tableau de bord ou sélectionnez **STOCKAGE (S3) > Buckets**.
 - c. Sélectionnez le nom du bucket dans le tableau pour accéder à la page des détails du bucket.
 - d. Sélectionnez l'onglet **Réplication inter-grille**.
 - e. Sélectionnez **Activer** et examinez la liste des exigences.
 - f. Si toutes les exigences sont remplies, sélectionnez la connexion à la fédération de réseau que vous souhaitez utiliser.
 - g. Vous pouvez également modifier le paramètre **Répliquer les marqueurs de suppression** pour déterminer ce qui se passe sur la grille de destination si un client S3 émet une demande de

suppression vers la grille source qui n'inclut pas d'ID de version :

- **Oui** (par défaut) : un marqueur de suppression est ajouté au bucket source et répliqué vers le bucket de destination.
- **Non** : un marqueur de suppression est ajouté au bucket source mais n'est pas répliqué dans le bucket de destination.



Si la demande de suppression inclut un ID de version, cette version d'objet est définitivement supprimée du bucket source. StorageGRID ne réplique pas les demandes de suppression qui incluent un ID de version, donc la même version d'objet n'est pas supprimée de la destination.

Voir ["Qu'est-ce que la réplication inter-réseau"](#) pour plus de détails.

- a. Vous pouvez également modifier le paramètre de la catégorie d'audit **Réplication inter-grille** pour gérer le volume des messages d'audit :
 - **Erreur** (par défaut) : seules les demandes de réplication inter-grille ayant échoué sont incluses dans la sortie d'audit.
 - **Normal** : toutes les demandes de réplication inter-grille sont incluses, ce qui augmente considérablement le volume de sortie d'audit.
- b. Revoyez vos sélections. Vous ne pouvez pas modifier ces paramètres à moins que les deux compartiments soient vides.
- c. Sélectionnez **Activer et tester**.

Après quelques instants, un message de réussite apparaît. Les objets ajoutés à ce bucket seront désormais automatiquement répliqués sur l'autre grille. La **réplication inter-grille** est affichée comme une fonctionnalité activée sur la page des détails du bucket.

2. En option, accédez au bucket correspondant sur l'autre grille et ["activer la réplication inter-réseau dans les deux sens"](#).

Réplication des tests entre les grilles

Si la réplication inter-grille est activée pour un bucket, vous devrez peut-être vérifier que la connexion et la réplication inter-grille fonctionnent correctement et que les buckets source et de destination répondent toujours

à toutes les exigences (par exemple, le contrôle de version est toujours activé).

Avant de commencer

- Vous utilisez un ["navigateur Web pris en charge"](#) .
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Autorisation d'accès root"](#) .

Étapes

1. Sign in au compte locataire du bucket.
2. Sélectionnez **Afficher les buckets** dans le tableau de bord ou sélectionnez **STOCKAGE (S3) > Buckets**.
3. Sélectionnez le nom du bucket dans le tableau pour accéder à la page des détails du bucket.
4. Sélectionnez l'onglet **Réplication inter-grille**.
5. Sélectionnez **Tester la connexion**.

Si la connexion est saine, une bannière de réussite apparaît. Sinon, un message d'erreur s'affiche, que vous et l'administrateur du réseau pouvez utiliser pour résoudre le problème. Pour plus de détails, consultez la section ["Résoudre les erreurs de fédération de grille"](#) .

6. Si la réplication inter-grille est configurée pour se produire dans les deux sens, accédez au bucket 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 inter-grille

Vous pouvez arrêter définitivement la réplication inter-grille si vous ne souhaitez plus copier d'objets vers l'autre grille.

Avant de désactiver la réplication inter-grille, notez les points suivants :

- La désactivation de la réplication inter-grille ne supprime aucun objet qui a déjà été copié entre les grilles. Par exemple, les objets dans `my-bucket` sur la grille 1 qui ont été copiés sur `my-bucket` sur la grille 2 ne sont pas supprimés si vous désactivez la réplication inter-grille pour ce bucket. Si vous souhaitez supprimer ces objets, vous devez les supprimer manuellement.
- Si la réplication inter-grille a été activée pour chacun des buckets (c'est-à-dire si la réplication se produit dans les deux sens), vous pouvez désactiver la réplication inter-grille pour l'un ou les deux buckets. Par exemple, vous souhaitez peut-être 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 de `my-bucket` sur la grille 2 à `my-bucket` sur la grille 1.
- Vous devez désactiver la réplication inter-grille 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-grille pour un bucket contenant des objets, vous ne pourrez pas réactiver la réplication inter-grille, sauf si vous supprimez tous les objets des buckets source et de destination.



Vous ne pouvez pas réactiver la réplication à moins que les deux buckets ne soient 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 root"](#) .

Étapes

1. En partant de la grille dont vous ne souhaitez plus répliquer les objets, arrêtez la réplication inter-grille pour le bucket :
 - a. Sign in au compte locataire du bucket.
 - b. Sélectionnez **Afficher les buckets** dans le tableau de bord ou sélectionnez **STOCKAGE (S3) > Buckets**.
 - c. Sélectionnez le nom du bucket dans le tableau pour accéder à la page des détails du bucket.
 - d. Sélectionnez l'onglet **Réplication inter-grille**.
 - e. Sélectionnez **Désactiver la réplication**.
 - f. Si vous êtes sûr de vouloir désactiver la réplication inter-grille pour ce bucket, saisissez **Oui** dans la zone de texte et sélectionnez **Désactiver**.

Après quelques instants, un message de réussite apparaît. Les nouveaux objets ajoutés à ce bucket ne peuvent plus être automatiquement répliqués sur l'autre grille. La **réplication inter-grille** n'est plus affichée comme une fonctionnalité activée sur la page Buckets.

2. Si la réplication inter-grille a été configurée pour se produire dans les deux sens, accédez au bucket correspondant sur l'autre grille et arrêtez la réplication inter-grille dans l'autre sens.

Afficher les connexions de la fédération de grille

Si votre compte locataire dispose de l'autorisation **Utiliser la connexion à la fédération de grille**, vous pouvez afficher les connexions autorisées.

Avant de commencer

- Le compte locataire dispose de l'autorisation **Utiliser la connexion à la fédération de grille**.
- Vous êtes connecté au Tenant Manager à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Autorisation d'accès root"](#).

Étapes

1. Sélectionnez **STOCKAGE (S3) > Connexions de fédération de grille**.

La page de connexion à la fédération Grid apparaît et inclut un tableau qui résume les informations suivantes :

Colonne	Description
Nom de la connexion	Les connexions de la fédération de grille que ce locataire est autorisé à utiliser.
Buckets avec réplication inter-grille	Pour chaque connexion de fédération de grille, les buckets de locataire pour lesquels la réplication inter-grille est activée. Les objets ajoutés à ces buckets seront répliqués sur l'autre grille de la connexion.
Dernière erreur	Pour chaque connexion de fédération de grille, l'erreur la plus récente survenue, le cas échéant, lors de la réplication des données sur l'autre grille. Voir Effacer la dernière erreur .

2. Vous pouvez également sélectionner un nom de bucket pour "[afficher les détails du godet](#)".

Effacer la dernière erreur

Une erreur peut apparaître dans la colonne **Dernière erreur** pour l'une des raisons suivantes :

- La version de l'objet source n'a pas été trouvée.
- Le bucket source n'a pas été trouvé.
- Le bucket de destination a été supprimé.
- Le bucket de destination a été recréé par un compte différent.
- Le contrôle de version du bucket de destination est suspendu.
- Le bucket de destination a été recréé par le même compte mais n'est désormais plus versionné.



Cette colonne affiche uniquement la dernière erreur de réplication inter-grille survenue ; les erreurs précédentes qui auraient pu se produire 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 bucket de destination pour la réplication inter-grille était dans un état non valide, probablement parce que le contrôle de version a été suspendu ou que le verrouillage d'objet S3 a été activé.

Grid federation connections

Clear error

Displaying one result

Connection name	Buckets with cross-grid replication	Last error
☐ Grid 1-Grid 2	my-cgr-bucket	2022-12-07 16:02:20 MST Cross-grid replication has encountered an error. Failed to send cross-grid replication request from source bucket 'my-cgr-bucket' to destination bucket 'my-cgr-bucket'. Error code: DestinationRequestError. Detail: InvalidBucketState. Confirm that the source and destination buckets have object versioning enabled and S3 Object Lock disabled. (logID 4791585492825418592)

2. Effectuez toutes les actions recommandées. Par exemple, si le contrôle de version a été suspendu sur le bucket de destination pour la réplication inter-grille, réactivez le contrôle de version pour ce bucket.
3. Sélectionnez la connexion dans le tableau.
4. Sélectionnez **Effacer l'erreur**.
5. Sélectionnez **Oui** pour effacer le message et mettre à jour l'état du système.
6. Attendez 5 à 6 minutes, puis ingérez un nouvel objet dans le seau. 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 du message avant d'ingérer un nouvel objet.

7. Pour déterminer si des objets n'ont pas pu être répliqués en raison de l'erreur de compartiment, consultez "[Identifier et réessayer les opérations de réplication ayant échoué](#)".

Gérer les groupes et les utilisateurs

Utiliser la fédération d'identité

L'utilisation de la fédération d'identité accélère la configuration des groupes de locataires et des utilisateurs et permet aux utilisateurs locataires de se connecter au compte locataire à l'aide d'informations d'identification familières.

Configurer la fédération d'identité pour Tenant Manager

Vous pouvez configurer la fédération d'identité pour Tenant Manager si vous souhaitez que les groupes de locataires et les utilisateurs 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 Tenant Manager à l'aide d'un ["navigateur Web pris en charge"](#) .
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Autorisation d'accès root"](#) .
- Vous utilisez Active Directory, Azure AD, OpenLDAP ou Oracle Directory Server comme fournisseur d'identité.



Si vous souhaitez utiliser un service LDAP v3 qui n'est pas répertorié, contactez le support technique.

- Si vous prévoyez d'utiliser OpenLDAP, vous devez configurer le serveur OpenLDAP. Voir [Directives pour la configuration du serveur OpenLDAP](#) .
- Si vous prévoyez d'utiliser Transport Layer Security (TLS) pour les communications avec le serveur LDAP, le fournisseur d'identité doit utiliser TLS 1.2 ou 1.3. Voir ["Chiffres pris en charge pour les connexions TLS sortantes"](#) .

À propos de cette tâche

La possibilité de configurer un service de fédération d'identité pour votre locataire dépend de la façon dont votre compte de locataire a été configuré. Votre locataire peut partager le service de fédération d'identité qui a été configuré pour Grid Manager. Si vous voyez ce message lorsque vous accédez à la page Fédération d'identité, vous ne pouvez pas configurer une source d'identité fédérée distincte 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.

Entrer la configuration

Lorsque vous configurez l'identification de la fédération, vous fournissez les valeurs dont StorageGRID a besoin pour se connecter à un service LDAP.

Étapes

1. Sélectionnez **GESTION DES ACCÈS > Fédération d'identité**.
2. Sélectionnez **Activer la fédération d'identité**.
3. Dans la section Type de service LDAP, sélectionnez le type de service LDAP que vous souhaitez configurer.

LDAP service type

Select the type of LDAP service you want to configure.

Active Directory	Azure	OpenLDAP	Other

Sélectionnez **Autre** pour configurer les valeurs d'un serveur LDAP qui utilise Oracle Directory Server.

4. Si vous avez sélectionné **Autre**, remplissez les champs de la section Attributs LDAP. , passez à l'étape suivante.
 - **Nom unique de l'utilisateur** : le 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 utilisateur** : le 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 du groupe** : le 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** : le nom de l'attribut qui contient l'identifiant 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, saisissez les informations de serveur LDAP et de connexion réseau 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** : Le port utilisé pour se connecter au serveur LDAP.



Le port par défaut pour STARTTLS est 389 et le port par défaut pour LDAPS est 636. Cependant, vous pouvez utiliser n'importe quel port à condition que votre pare-feu soit correctement configuré.

- **Nom d'utilisateur** : le 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 de niveau inférieur ou le nom d'utilisateur principal.

L'utilisateur spécifié doit avoir l'autorisation de répertorier les groupes et les utilisateurs et d'accéder aux attributs suivants :

- `sAMAccountName` ou `uid`

- objectGUID, entryUUID, ou nsuniqueid
 - cn
 - memberOf`ou `isMemberOf
 - **Active Directory:** objectSid, primaryGroupID, userAccountControl, et userPrincipalName
 - **Azuré:** accountEnabled et userPrincipalName
- **Mot de passe :** Le mot de passe associé au nom d'utilisateur.



Si vous modifiez le mot de passe à l'avenir, vous devez le mettre à jour sur cette page.

- **DN de base du groupe :** le chemin complet du nom distinctif (DN) d'une sous-arborescence LDAP dans laquelle vous souhaitez 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=example,DC=com) peuvent être utilisés comme groupes fédérés.



Les valeurs **Nom unique du groupe** doivent être uniques dans le **DN de base du groupe** auquel elles appartiennent.

- **DN de base utilisateur :** le chemin complet du nom distinctif (DN) d'une sous-arborescence LDAP dans laquelle vous souhaitez rechercher des utilisateurs.



Les valeurs **Nom unique de l'utilisateur** doivent être uniques dans le **DN de base de l'utilisateur** auquel elles appartiennent.

- * **Format de nom d'utilisateur de liaison *** (facultatif) : le modèle de nom d'utilisateur par défaut que StorageGRID doit utiliser si le modèle ne peut pas être déterminé automatiquement.

Il est recommandé de fournir le **format de nom d'utilisateur de liaison** car il peut permettre aux utilisateurs de se connecter si StorageGRID ne parvient pas à se lier au compte de service.

Saisissez l'un de ces modèles :

- **Modèle UserPrincipalName (Active Directory et Azure):** [USERNAME]@example.com
- **Modèle de nom de connexion de niveau inférieur (Active Directory et Azure):**
example\[USERNAME]
- **Modèle de nom distinctif:** CN=[USERNAME],CN=Users,DC=example,DC=com

Incluez [USERNAME] exactement comme écrit.

6. Dans la section Sécurité de la couche de transport (TLS), sélectionnez un paramètre de sécurité.

- **Utiliser 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.
- **Utiliser 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.
 - **Utiliser le certificat CA du système d'exploitation** : utilisez le certificat CA Grid par défaut installé sur le système d'exploitation pour sécuriser les connexions.
 - **Utiliser un certificat CA 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.

Tester la connexion et enregistrer 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 du nom d'utilisateur de liaison, 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 de connexion réussi » s'affiche si les paramètres de connexion sont valides. Sélectionnez **Enregistrer** pour enregistrer la configuration.
 - Un message « La connexion de test n'a pas pu être établie » s'affiche si les paramètres de connexion ne sont pas valides. Sélectionnez **Fermer**. Ensuite, résolvez tous les problèmes et testez à nouveau la connexion.
3. Si vous avez fourni un format de nom d'utilisateur de liaison, saisissez le nom d'utilisateur et le mot de passe d'un utilisateur fédéré valide.

Par exemple, entrez votre propre nom d'utilisateur et votre mot de passe. N'incluez aucun caractère spécial dans le nom d'utilisateur, tel que @ ou /.

Test Connection

To test the connection and the bind username format, enter the username and password of a federated user. For example, enter your own federated username and password. The test values are not saved.

Test username

The username of a federated user.

Test password

[Cancel](#) [Test Connection](#)

- Un message « Test de connexion réussi » 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 de test ne sont pas valides. Résolvez tous les problèmes et testez à nouveau la connexion.

Forcer la synchronisation avec la source d'identité

Le système StorageGRID synchronise périodiquement les groupes fédérés et les utilisateurs à partir de la source d'identité. Vous pouvez forcer le démarrage de la synchronisation si vous souhaitez activer ou restreindre les autorisations des utilisateurs le plus rapidement possible.

Étapes

1. Accédez à la page Fédération d'identité.
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 la synchronisation de la fédération d'identité** est déclenchée s'il y a un problème de synchronisation des groupes fédérés et des utilisateurs à partir de la source d'identité.

Désactiver la fédération d'identité

Vous pouvez désactiver temporairement ou définitivement la fédération d'identité pour les groupes et les utilisateurs. Lorsque la fédération d'identité est désactivée, il n'y a aucune communication entre StorageGRID et la source d'identité. Cependant, tous les paramètres que vous avez configurés sont conservés, ce qui vous permet de réactiver facilement la fédération d'identité à l'avenir.

À propos de cette tâche

Avant de désactiver la fédération d'identité, vous devez tenir compte des points suivants :

- Les utilisateurs fédérés ne pourront pas se connecter.
- Les utilisateurs fédérés actuellement connectés conserveront 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 la source d'identité n'aura pas lieu et les alertes ne seront pas générées pour les comptes qui n'ont pas été synchronisés.
- La case à cocher **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 d'authentification unique doit être **Désactivé** avant de pouvoir désactiver la fédération d'identité. Voir "[Désactiver l'authentification unique](#)".

Étapes

1. Accédez à la page Fédération d'identité.
2. Décochez la case **Activer la fédération d'identité**.

Directives pour la configuration du serveur OpenLDAP

Si vous souhaitez utiliser un serveur OpenLDAP pour la fédération d'identité, vous devez configurer des paramètres spécifiques sur le serveur OpenLDAP.



Pour les sources 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 toutes les clés S3 de l'utilisateur ou supprimez l'utilisateur de tous les groupes.

Superpositions Memberof et refint

Les superpositions memberof et refint doivent être activées. Pour plus d'informations, consultez les instructions relatives à la maintenance de l'appartenance à un groupe inversé dans <http://www.openldap.org/doc/admin24/index.html> ["Documentation OpenLDAP : Guide de l'administrateur version 2.4"] .

Indexage

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.

Consultez les informations sur la maintenance de l'appartenance à un groupe inversé dans <http://www.openldap.org/doc/admin24/index.html> ["Documentation OpenLDAP : Guide de l'administrateur version 2.4"] .

Gérer les groupes de locataires

Créer 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 Tenant Manager à l'aide d'un ["navigateur Web pris en charge"](#) .
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Autorisation d'accès root"](#) .
- Si vous envisagez d'importer un groupe fédéré, vous devez ["fédération d'identité configurée"](#) , et le groupe fédéré existe déjà dans la source d'identité configurée.
- Si votre compte locataire dispose de l'autorisation **Utiliser la connexion à la 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.

Accéder à l'assistant de création de groupe

Dans un premier temps, accédez à l'assistant de création de groupe.

Étapes

1. Sélectionnez **GESTION DES ACCÈS > Groupes**.

2. Si votre compte locataire dispose de l'autorisation **Utiliser la connexion à la fédération de grille**, confirmez qu'une bannière bleue apparaît, 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 êtes peut-être connecté à la grille de destination du locataire.

3. Sélectionnez **Créer un 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 de la source d'identité précédemment configurée.

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 des applications clientes pour gérer les ressources du locataire, en fonction des autorisations de groupe.

2. Entrez le nom du groupe.

- **Groupe local** : saisissez un nom d'affichage et un nom unique. Vous pouvez modifier le nom d'affichage ultérieurement.



Si votre compte locataire dispose de l'autorisation **Utiliser la connexion à la fédération de grille**, une erreur de clonage se produira 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 au sAMAccountName attribut. Pour OpenLDAP, le nom unique est le nom associé au uid attribut.

3. Sélectionnez **Continuer**.

Gérer les autorisations de groupe

Les autorisations de groupe contrôlent les tâches que les utilisateurs peuvent effectuer dans Tenant Manager et l'API Tenant Management.

Étapes

1. Pour le **Mode d'accès**, sélectionnez l'une des options suivantes :

- **Lecture-écriture** (par défaut) : les utilisateurs peuvent se connecter à Tenant Manager et gérer la configuration du locataire.
- **Lecture seule** : les utilisateurs peuvent uniquement afficher les paramètres et les fonctionnalités. Ils ne peuvent apporter aucune modification ni effectuer aucune opération dans l'API Tenant Manager ou Tenant 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 aura un accès en lecture seule à tous les paramètres et fonctionnalités sélectionnés.

2. Sélectionnez une ou plusieurs autorisations pour ce groupe.

Voir "[Autorisations de gestion des locataires](#)".

3. Sélectionnez **Continuer**.

Définir la stratégie de groupe S3

La stratégie de groupe détermine les autorisations d'accès S3 dont disposeront les utilisateurs.

Étapes

1. Sélectionnez la politique que vous souhaitez utiliser pour ce groupe.

Politique de groupe	Description
Pas d'accès S3	Défaut. Les utilisateurs de ce groupe n'ont pas accès aux ressources S3, sauf si l'accès est accordé avec une stratégie de compartiment. Si vous sélectionnez cette option, seul l'utilisateur root aura accès aux ressources S3 par défaut.
Accès en lecture seule	Les utilisateurs de ce groupe ont un accès en lecture seule aux ressources S3. Par exemple, les utilisateurs de ce groupe peuvent répertorier les objets et lire les données d'objet, les métadonnées et les balises. Lorsque vous sélectionnez cette option, la chaîne JSON d'une stratégie de groupe en lecture seule apparaît dans la zone de texte. Vous ne pouvez pas modifier cette chaîne.
Accès complet	Les utilisateurs de ce groupe ont un accès complet aux ressources S3, y compris les buckets. Lorsque vous sélectionnez cette option, la chaîne JSON d'une stratégie de groupe à accès complet apparaît dans la zone de texte. Vous ne pouvez pas modifier cette chaîne.

Politique de groupe	Description
Atténuation des ransomwares	Cet exemple de politique s'applique à tous les compartiments de ce locataire. Les utilisateurs de ce groupe peuvent effectuer des actions courantes, mais ne peuvent pas supprimer définitivement les objets des buckets pour lesquels le contrôle de version des objets est activé. Les utilisateurs de Tenant Manager qui disposent 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) lorsqu'elle est disponible.
Coutume	Les utilisateurs du groupe bénéficient des autorisations que vous spécifiez dans la zone de texte.

- Si vous avez sélectionné **Personnalisé**, saisissez la stratégie de groupe. Chaque stratégie de groupe a une limite de taille de 5 120 octets. Vous devez saisir une chaîne formatée JSON valide.

Pour des informations détaillées sur les stratégies de groupe, y compris la syntaxe du langage et des exemples, voir ["Exemples de stratégies de groupe"](#).

- Si vous créez un groupe local, sélectionnez **Continuer**. Si vous créez un groupe fédéré, sélectionnez **Créer un 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 déjà existants.



Si votre compte locataire dispose de l'autorisation **Utiliser la connexion à la 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 sur 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

- Vous pouvez également sélectionner un ou plusieurs utilisateurs locaux pour ce groupe.
- Sélectionnez **Créer un 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 à la fédération de grille** et que vous êtes sur la grille source du locataire, le nouveau groupe est cloné sur la grille de destination du locataire. **Succès** apparaît comme **Statut de clonage** dans la section Présentation de la page de détails du groupe.

Créer des groupes pour un locataire Swift

Vous pouvez gérer les autorisations d'accès pour un compte 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 locataire Swift.



La prise en charge des applications clientes Swift est obsolète et sera supprimée dans une prochaine version.

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un ["navigateur Web pris en charge"](#) .
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Autorisation d'accès root"](#) .
- Si vous envisagez d'importer un groupe fédéré, vous devez ["fédération d'identité configurée"](#) , et le groupe fédéré existe déjà dans la source d'identité configurée.

Accéder à l'assistant de création de groupe

Étapes

Dans un premier temps, accédez à l'assistant de création de groupe.

1. Sélectionnez **GESTION DES ACCÈS > Groupes**.
2. Sélectionnez **Créer un 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 de la source d'identité précédemment configurée.

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 des applications clientes pour gérer les ressources du locataire, en fonction des autorisations de groupe.

2. Entrez le nom du groupe.
 - **Groupe local** : saisissez 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 au sAMAccountName attribut. Pour OpenLDAP, le nom unique est le nom associé au uid attribut.
3. Sélectionnez **Continuer**.

Gérer les autorisations de groupe

Les autorisations de groupe contrôlent les tâches que les utilisateurs peuvent effectuer dans Tenant Manager et l'API Tenant Management.

Étapes

1. Pour le **Mode d'accès**, sélectionnez l'une des options suivantes :
 - **Lecture-écriture** (par défaut) : les utilisateurs peuvent se connecter à Tenant Manager et gérer la configuration du locataire.

- **Lecture seule** : les utilisateurs peuvent uniquement afficher les paramètres et les fonctionnalités. Ils ne peuvent apporter aucune modification ni effectuer aucune opération dans l'API Tenant Manager ou Tenant 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 aura un accès en lecture seule à tous les paramètres et fonctionnalités sélectionnés.

2. Cochez la case **Accès root** si les utilisateurs du groupe doivent se connecter au gestionnaire de locataires ou à l'API de gestion des locataires.
3. Sélectionnez **Continuer**.

Définir la politique de groupe Swift

Les utilisateurs de Swift ont besoin d'une autorisation d'administrateur pour s'authentifier dans l'API REST Swift afin de créer des conteneurs et d'ingérer des objets.

1. Cochez la case **Administrateur Swift** 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 un 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 déjà existants.

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 "[Gérer les utilisateurs locaux](#)".

2. Sélectionnez **Créer un 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, réfléchissez aux 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 se 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 qui peuvent se connecter peuvent effectuer les tâches suivantes :

- Afficher le tableau de bord
- Changer leur 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 peuvent uniquement afficher les paramètres et fonctionnalités associés.



Si un utilisateur appartient à plusieurs groupes et qu'un groupe est défini sur Lecture seule, l'utilisateur aura un accès en lecture seule à tous les paramètres et fonctionnalités sélectionnés.

Vous pouvez attribuer les autorisations suivantes à un groupe. Notez que les locataires S3 et les locataires Swift ont des autorisations de groupe différentes.

Autorisation	Description	Détails
Accès root	Fournit un accès complet au gestionnaire de locataires et à l'API de gestion des locataires.	Les utilisateurs Swift doivent disposer de l'autorisation d'accès root pour se connecter au compte locataire.
Administrateur	Locataires rapides seulement. Fournit un accès complet aux conteneurs et objets Swift pour ce compte locataire	Les utilisateurs Swift doivent disposer de l'autorisation d'administrateur Swift pour effectuer des opérations avec l'API REST Swift.
Gérez vos propres 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 STOCKAGE (S3) > Mes clés d'accès S3 .
Voir tous les seaux	• Locataires S3 * : permet aux utilisateurs d'afficher tous les buckets et configurations de buckets. • Locataires Swift * : permet aux utilisateurs Swift d'afficher tous les conteneurs et configurations de conteneurs à l'aide de l'API de gestion des locataires.	Les utilisateurs qui ne disposent pas de l'autorisation Afficher tous les buckets ou Gérer tous les buckets ne voient pas l'option de menu Buckets. Cette autorisation est remplacée par l'autorisation Gérer tous les buckets. Cela n'affecte pas les stratégies de groupe ou de compartiment S3 utilisées par les clients S3 ou la console S3. Vous ne pouvez attribuer cette autorisation qu'aux groupes Swift à partir de l'API de gestion des locataires. Vous ne pouvez pas attribuer cette autorisation aux groupes Swift à l'aide du gestionnaire de locataires.

Autorisation	Description	Détails
Gérer 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 pour gérer les paramètres de tous les compartiments S3 du compte de locataire, quels que soient les compartiments S3 ou les stratégies de groupe. - Locataires Swift * : permet aux utilisateurs Swift de contrôler la cohérence des conteneurs Swift à l'aide de l'API de gestion des locataires.	Les utilisateurs qui ne disposent pas de l'autorisation Afficher tous les buckets ou Gérer tous les buckets ne voient pas l'option de menu Buckets. Cette autorisation remplace l'autorisation Afficher tous les buckets. Cela n'affecte pas les stratégies de groupe ou de compartiment S3 utilisées par les clients S3 ou la console S3. Vous ne pouvez attribuer cette autorisation qu'aux groupes Swift à partir de l'API de gestion des locataires. Vous ne pouvez pas attribuer cette autorisation aux groupes Swift à l'aide du gestionnaire de locataires.
Gérer les points de terminaison	Permet aux utilisateurs d'utiliser Tenant Manager ou l'API Tenant Management pour créer ou modifier des points de terminaison 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 Points de terminaison des services de plateforme .
Utiliser l'onglet Console S3	Associée à l'autorisation Afficher tous les buckets ou Gérer tous les buckets, cette option permet aux utilisateurs d'afficher et de gérer les objets à partir de l'onglet Console S3 sur la page de détails d'un bucket.	

Gérer les groupes

Gérez vos groupes de locataires selon vos besoins pour afficher, modifier ou dupliquer un groupe, et bien plus encore.

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un ["navigateur Web pris en charge"](#) .
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Autorisation d'accès root"](#) .

Afficher ou modifier le groupe

Vous pouvez afficher et modifier les informations de base et les détails de chaque groupe.

Étapes

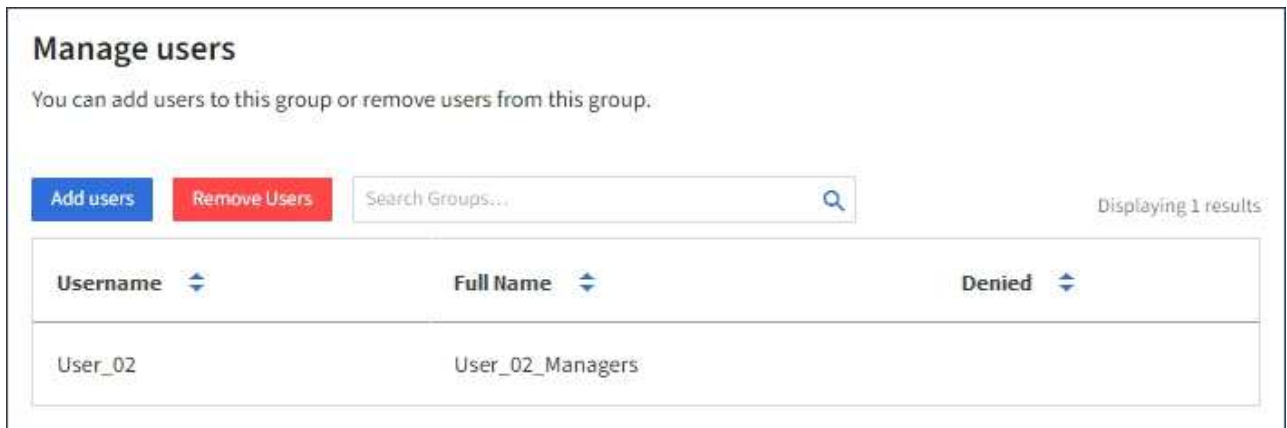
- Sélectionnez **GESTION DES ACCÈS > Groupes**.
- Consultez les informations fournies sur la page Groupes, qui répertorie les informations de base pour tous les groupes locaux et fédérés pour ce compte locataire.

Si le compte locataire dispose de l'autorisation **Utiliser la connexion à la fédération de grille** et que vous

visualisez les groupes sur la grille source du locataire :

- Un message de bannière indique que si vous modifiez ou supprimez un groupe, vos modifications ne seront pas synchronisées avec l'autre grille.
 - Si nécessaire, un message de bannière indique si les groupes n'ont pas été clonés sur le locataire sur la grille de destination. Tu peux [réessayer un clonage de groupe](#) ça a échoué.
3. Si vous souhaitez modifier le nom du groupe :
- a. Cochez la case correspondant au groupe.
 - b. Sélectionnez **Actions > Modifier le nom du groupe**.
 - c. Entrez 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 correspondant au groupe, puis sélectionnez **Actions > Afficher les détails du groupe**.
5. Consultez la section Présentation, qui affiche les informations suivantes pour chaque groupe :
- Nom d'affichage
 - Nom unique
 - Type
 - Mode d'accès
 - Autorisations
 - Politique S3
 - Nombre d'utilisateurs dans ce groupe
 - Champs supplémentaires si le compte locataire dispose de l'autorisation **Utiliser la connexion à la fédération de grille** et que vous visualisez le groupe sur la grille source du locataire :
 - Statut du 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 du groupe selon vos besoins. Voir "[Créer des groupes pour un locataire S3](#)" et "[Créer des groupes pour un locataire Swift](#)" pour plus de détails sur ce qu'il faut saisir.
- a. Dans la section Aperçu, 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 éventuellement une autre stratégie de groupe S3 ou saisissez la chaîne JSON d'une stratégie personnalisée, selon vos besoins.
 - Si vous modifiez un groupe Swift, cochez ou décochez éventuellement la case **Administrateur Swift**.
7. Pour ajouter un ou plusieurs utilisateurs locaux existants au groupe :

- a. Sélectionnez l'onglet Utilisateurs.



Manage users

You can add users to this group or remove users from this group.

Add users **Remove Users** Search Groups... Displaying 1 results

Username	Full Name	Denied
User_02	User_02_Managers	

- b. Sélectionnez **Ajouter des utilisateurs**.

- c. Sélectionnez les utilisateurs existants que vous souhaitez ajouter, puis sélectionnez **Ajouter des utilisateurs**.

Un message de réussite apparaît dans le coin supérieur droit.

8. Pour supprimer les utilisateurs locaux du groupe :

- a. Sélectionnez l'onglet Utilisateurs.

- b. Sélectionnez **Supprimer les utilisateurs**.

- c. Sélectionnez les utilisateurs que vous souhaitez supprimer, puis sélectionnez **Supprimer les utilisateurs**.

Un message de réussite apparaît dans le coin supérieur droit.

9. Confirmez que vous avez sélectionné **Enregistrer les modifications** pour chaque section que vous avez modifiée.

Groupe en double

Vous pouvez dupliquer un groupe existant pour créer de nouveaux groupes plus rapidement.



Si votre compte locataire dispose de l'autorisation **Utiliser la connexion à la fédération de grille** et que vous dupliquez un groupe à partir de la grille source du locataire, le groupe dupliqué sera cloné sur la grille de destination du locataire.

Étapes

1. Sélectionnez **GESTION DES ACCÈS > Groupes**.
2. Cochez la case correspondant au groupe que vous souhaitez dupliquer.
3. Sélectionnez **Actions > Dupliquer le groupe**.
4. Voir "[Créer des groupes pour un locataire S3](#)" ou "[Créer des groupes pour un locataire Swift](#)" pour plus de détails sur ce qu'il faut saisir.
5. Sélectionnez **Créer un groupe**.

Réessayer le clonage du groupe

Pour réessayer un clonage qui a échoué :

1. Sélectionnez chaque groupe qui indique (*Échec du clonage*) sous le nom du groupe.
2. Sélectionnez **Actions** > **Cloner les groupes**.
3. Affichez l'état de l'opération de clonage à partir de la page de détails de chaque groupe que vous clonez.

Pour plus d'informations, voir ["Cloner des groupes de locataires et des utilisateurs"](#) .

Supprimer un ou plusieurs groupes

Vous pouvez supprimer un ou plusieurs groupes. Tous les utilisateurs appartenant uniquement à un groupe supprimé ne pourront plus se connecter au gestionnaire de locataires ni utiliser le compte de locataire.



Si votre compte locataire dispose de l'autorisation **Utiliser la connexion à la 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 **GESTION DES ACCÈS** > **Groupes**.
2. Cochez la case correspondant à chaque groupe que vous souhaitez supprimer.
3. Sélectionnez **Actions** > **Supprimer le groupe** ou **Actions** > **Supprimer les groupes**.

Une boîte de dialogue de confirmation apparaît.

4. Sélectionnez **Supprimer le groupe** ou **Supprimer les groupes**.

Gérer les utilisateurs locaux

Vous pouvez créer des utilisateurs locaux et les affecter à des groupes locaux pour déterminer les fonctionnalités 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 root.



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 Tenant Manager à l'aide d'un ["navigateur Web pris en charge"](#) .
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Autorisation d'accès root"](#) .
- Si votre compte locataire dispose de l'autorisation **Utiliser la connexion à la 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.

Créer un utilisateur local

Vous pouvez créer un utilisateur local et l'affecter à un ou plusieurs groupes locaux pour contrôler ses autorisations d'accès.

Les utilisateurs S3 qui n'appartiennent à aucun groupe ne disposent pas d'autorisations de gestion ni de stratégies de groupe S3 qui leur sont appliquées. Ces utilisateurs peuvent bénéficier d'un accès au compartiment S3 accordé via une politique de compartiment.

Les utilisateurs Swift qui n'appartiennent à aucun groupe ne disposent pas d'autorisations de gestion ni d'accès au conteneur Swift.

Accéder à l'assistant de création d'utilisateur

Étapes

1. Sélectionnez **GESTION DES ACCÈS > Utilisateurs**.

Si votre compte locataire dispose de l'autorisation **Utiliser la connexion à la 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 sur l'autre grille de la connexion.

2. Sélectionnez **Créer un utilisateur**.

Entrez les informations d'identification

Étapes

1. Pour l'étape **Saisir les informations d'identification de l'utilisateur**, remplissez les champs suivants.

Champ	Description
Nom et prénom	Le nom complet de cet utilisateur, par exemple, le prénom et le nom d'une personne ou le nom d'une application.

Champ	Description
Nom d'utilisateur	Le 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 de locataire dispose de l'autorisation Utiliser la connexion à la fédération de grille, une erreur de clonage se produira si le même Nom d'utilisateur existe déjà pour le locataire sur la grille de destination.
Mot de passe et confirmation du mot de passe	Le mot de passe que l'utilisateur utilisera initialement lors de la connexion.
Refuser l'accès	Sélectionnez Oui pour empêcher cet utilisateur de se connecter au compte locataire, même s'il appartient toujours à un ou plusieurs groupes. Par exemple, sélectionnez Oui pour suspendre temporairement la possibilité pour un utilisateur de se connecter.

2. Sélectionnez **Continuer**.

Affecter à des groupes

Étapes

1. Affectez l'utilisateur à un ou plusieurs groupes locaux pour déterminer les tâches qu'il peut effectuer.

L'affectation d'un utilisateur à des groupes est facultative. Si vous préférez, vous pouvez sélectionner des utilisateurs lorsque vous créez ou modifiez des groupes.

Les utilisateurs qui n'appartiennent à aucun groupe n'auront aucune autorisation de gestion. Les autorisations sont cumulatives. Les utilisateurs disposeront de toutes les autorisations pour tous les groupes auxquels ils appartiennent. Voir "[Autorisations de gestion des locataires](#)".

2. Sélectionnez **Créer un utilisateur**.

Si votre compte locataire dispose de l'autorisation **Utiliser la connexion à la fédération de grille** et que vous êtes sur la grille source du locataire, le nouvel utilisateur local est cloné sur la grille de destination du locataire. **Succès** apparaît comme **Statut de clonage** dans la section Présentation de la page de détails de l'utilisateur.

3. Sélectionnez **Terminer** pour revenir à la page Utilisateurs.

Afficher ou modifier l'utilisateur local

Étapes

1. Sélectionnez **GESTION DES ACCÈS > Utilisateurs**.

2. Consultez les informations fournies sur la page Utilisateurs, qui répertorie les informations de base pour tous les utilisateurs locaux et fédérés de ce compte locataire.

Si le compte locataire dispose de l'autorisation **Utiliser la connexion à la fédération de grille** et que vous visualisez l'utilisateur sur la grille source du locataire :

- Un message de bannière indique que si vous modifiez ou supprimez un utilisateur, vos modifications ne seront pas synchronisées avec l'autre grille.
 - Si nécessaire, un message de bannière indique si les utilisateurs n'ont pas été clonés sur le locataire sur la grille de destination. Vous pouvez [réessayer un clone d'utilisateur qui a échoué](#) .
3. Si vous souhaitez modifier le nom complet de l'utilisateur :
 - a. Cochez la case correspondant à l'utilisateur.
 - b. Sélectionnez **Actions > Modifier le nom complet**.
 - c. Entrez 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 correspondant à l'utilisateur, puis sélectionnez **Actions > Afficher les détails de l'utilisateur**.
 5. Consultez la section Présentation, qui affiche les informations suivantes pour chaque utilisateur :
 - Nom et prénom
 - Nom d'utilisateur
 - Type d'utilisateur
 - Accès refusé
 - Mode d'accès
 - Adhésion au groupe
 - Champs supplémentaires si le compte locataire dispose de l'autorisation **Utiliser la connexion à la fédération de grille** et que vous visualisez l'utilisateur sur la grille source du locataire :
 - Statut du 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 de détails sur ce qu'il faut saisir.
 - a. Dans la section Aperçu, modifiez le nom complet en sélectionnant le nom ou l'icône de modification  .

Vous ne pouvez pas changer 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 autoriser l'utilisateur à se connecter ou sélectionnez **Oui** pour empêcher l'utilisateur de se connecter. Ensuite, sélectionnez **Enregistrer les modifications**.
 - d. Dans l'onglet **Clés d'accès**, sélectionnez **Créer une clé** et suivez les instructions pour "[créer les 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. Ensuite, sélectionnez **Enregistrer les modifications**.
 7. Confirmez que vous avez sélectionné **Enregistrer les modifications** pour chaque section que vous avez modifiée.

Utilisateur local en double

Vous pouvez dupliquer un utilisateur local pour créer un nouvel utilisateur plus rapidement.



Si votre compte locataire dispose de l'autorisation **Utiliser la connexion à la fédération de grille** et que vous dupliquez un utilisateur à partir de la grille source du locataire, l'utilisateur dupliqué sera cloné sur la grille de destination du locataire.

Étapes

1. Sélectionnez **GESTION DES ACCÈS > Utilisateurs**.
2. Cochez la case correspondant à l'utilisateur que vous souhaitez dupliquer.
3. Sélectionnez **Actions > Dupliquer l'utilisateur**.
4. Voir [Créer un utilisateur local](#) pour plus de détails sur ce qu'il faut saisir.
5. Sélectionnez **Créer un utilisateur**.

Réessayer le clonage de l'utilisateur

Pour réessayer un clonage qui a échoué :

1. Sélectionnez chaque utilisateur qui indique (*Échec du clonage*) sous le nom d'utilisateur.
2. Sélectionnez **Actions > Cloner les utilisateurs**.
3. Affichez l'état de l'opération de clonage à partir de la page de détails de chaque utilisateur que vous clonez.

Pour plus d'informations, voir "[Cloner des groupes de locataires et des utilisateurs](#)".

Supprimer un ou plusieurs utilisateurs locaux

Vous pouvez supprimer définitivement un ou plusieurs utilisateurs locaux qui n'ont plus besoin d'accéder au compte locataire StorageGRID .



Si votre compte locataire dispose de l'autorisation **Utiliser la connexion à la 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 la source d'identité fédérée pour supprimer les utilisateurs fédérés.

Étapes

1. Sélectionnez **GESTION DES ACCÈS > Utilisateurs**.
2. Cochez la case correspondant à chaque utilisateur que vous souhaitez supprimer.
3. Sélectionnez **Actions > Supprimer l'utilisateur** ou **Actions > Supprimer les utilisateurs**.

Une boîte de dialogue de confirmation apparaît.

4. Sélectionnez **Supprimer l'utilisateur** ou **Supprimer les utilisateurs**.

Gérer les clés d'accès S3

Gérer les clés d'accès S3

Chaque utilisateur d'un compte 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 comme suit :

- 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 **Accès root** peuvent gérer les clés d'accès pour le compte root S3 et tous les autres utilisateurs. Les clés d'accès racine fournissent un accès complet à tous les compartiments et objets du locataire, sauf si elles sont explicitement désactivées par une stratégie de compartiment.

StorageGRID prend en charge l'authentification Signature Version 2 et Signature Version 4. L'accès entre comptes n'est pas autorisé, sauf s'il est explicitement activé par une politique 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 buckets et objets.

Avant de commencer

- Vous êtes connecté au Tenant Manager 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 autorisation d'accès root"](#) .

À propos de cette tâche

Vous pouvez créer une ou plusieurs clés d'accès S3 qui vous permettent de créer et de gérer des buckets pour votre compte 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 qu'elle est sur le point d'expirer, créez une nouvelle clé avant l'expiration de l'ancienne, puis supprimez l'ancienne.

Chaque clé peut avoir une date d'expiration spécifique ou aucune date d'expiration. Suivez ces directives concernant le délai d'expiration :

- Définissez une heure 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 vos risques si votre ID de clé d'accès et votre clé d'accès secrète sont accidentellement exposés. 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 périodiquement de nouvelles clés, vous n'avez pas besoin de définir un délai d'expiration pour vos clés. Si vous décidez ultérieurement de créer de nouvelles clés, supprimez les anciennes clés manuellement.



Les compartiments et objets S3 appartenant à votre compte sont accessibles à l'aide de l'ID de clé d'accès et de la clé d'accès secrète affichées pour votre compte dans le gestionnaire de locataires. Pour cette raison, protégez les clés d'accès comme vous le feriez avec un mot de passe. Faites tourner régulièrement les clés d'accès, supprimez toutes les clés inutilisées de votre compte et ne les partagez jamais avec d'autres utilisateurs.

Étapes

1. Sélectionnez **STOCKAGE (S3) > Mes clés d'accès**.

La page Mes clés d'accès apparaît et répertorie toutes les clés d'accès existantes.

2. Sélectionnez **Créer une clé**.

3. Effectuez l'une des opérations suivantes :

- Sélectionnez **Ne pas définir de délai d'expiration** pour créer une clé qui n'expirera pas. (Défaut)
- Sélectionnez **Définir 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. Le délai 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, répertoriant votre ID de clé d'accès et votre clé d'accès secrète.

5. Copiez l'ID de clé d'accès et la clé d'accès secrète dans un emplacement sûr ou sélectionnez **Télécharger .csv** pour enregistrer un fichier de feuille de calcul contenant l'ID de clé d'accès et la clé d'accès secrète.



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 des clés une fois la boîte de dialogue fermée.

6. Sélectionnez **Terminer**.

La nouvelle clé est répertoriée sur la page Mes clés d'accès.

7. Si votre compte de locataire dispose de l'autorisation **Utiliser la connexion à la fédération de grille**, utilisez éventuellement l'API de gestion des locataires pour cloner manuellement les clés d'accès S3 du locataire sur la grille source vers le locataire sur la grille de destination. Voir "[Cloner les clés d'accès S3 à l'aide de l'API](#)".

Afficher vos clés d'accès S3

Si vous utilisez un locataire S3 et que vous avez le "[autorisation appropriée](#)", vous pouvez afficher une liste de vos clés d'accès S3. Vous pouvez trier la liste par heure d'expiration, afin de déterminer quelles clés expireront bientôt. Au besoin, vous pouvez "[créer de nouvelles clés](#)" ou "[touches de suppression](#)" que vous n'utilisez plus.



Les compartiments et objets S3 appartenant à votre compte sont accessibles à l'aide de l'ID de clé d'accès et de la clé d'accès secrète affichées pour votre compte dans le gestionnaire de locataires. Pour cette raison, protégez les clés d'accès comme vous le feriez avec un mot de passe. Faites tourner régulièrement les clés d'accès, supprimez toutes les clés inutilisées de votre compte et ne les partagez jamais avec d'autres utilisateurs.

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un ["navigateur Web pris en charge"](#) .
- Vous appartenez à un groupe d'utilisateurs disposant de l'autorisation Gérer vos propres informations d'identification S3 ["autorisation"](#) .

Étapes

1. Sélectionnez **STOCKAGE (S3) > Mes clés d'accès**.
2. Depuis la page Mes clés d'accès, triez toutes les clés d'accès existantes par **Délai d'expiration** ou **ID de clé d'accès**.
3. Selon vos besoins, créez de nouvelles clés ou supprimez celles 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 de l'autorisation appropriée, vous pouvez supprimer vos propres clés d'accès S3. Une fois qu'une clé d'accès est supprimée, elle ne peut plus être utilisée pour accéder aux objets et aux buckets du compte locataire.

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un ["navigateur Web pris en charge"](#) .
- Vous avez le ["Gérez vos propres autorisations d'informations d'identification S3"](#) .



Les compartiments et objets S3 appartenant à votre compte sont accessibles à l'aide de l'ID de clé d'accès et de la clé d'accès secrète affichées pour votre compte dans le gestionnaire de locataires. Pour cette raison, protégez les clés d'accès comme vous le feriez avec un mot de passe. Faites tourner régulièrement les clés d'accès, supprimez toutes les clés inutilisées de votre compte et ne les partagez jamais avec d'autres utilisateurs.

Étapes

1. Sélectionnez **STOCKAGE (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 **Touche Suppr.**
4. Dans la boîte de dialogue de confirmation, sélectionnez **Touche Supprimer**.

Un message de confirmation apparaît dans le coin supérieur droit de la page.

Créer les clés d'accès S3 d'un autre utilisateur

Si vous utilisez un locataire S3 et que vous disposez de l'autorisation appropriée, vous pouvez créer des clés d'accès S3 pour d'autres utilisateurs, tels que les applications qui ont besoin d'accéder aux buckets et aux objets.

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Autorisation d'accès root"](#).

À propos de cette tâche

Vous pouvez créer une ou plusieurs clés d'accès S3 pour d'autres utilisateurs afin qu'ils puissent créer et gérer des buckets pour leur compte 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 nécessaire pour l'utilisateur et supprimez les clés qui ne sont pas utilisées. Si vous n'avez qu'une seule clé et qu'elle est sur le point d'expirer, créez une nouvelle clé avant l'expiration de l'ancienne, puis supprimez l'ancienne.

Chaque clé peut avoir une date d'expiration spécifique ou aucune date d'expiration. Suivez ces directives concernant le délai 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 les risques si l'ID de clé d'accès et la clé d'accès secrète sont accidentellement exposés. 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 périodiquement de nouvelles clés, vous n'avez pas besoin de définir un délai d'expiration pour les clés. Si vous décidez ultérieurement de créer de nouvelles clés, supprimez les anciennes clés manuellement.



Les compartiments et objets S3 appartenant à un utilisateur sont accessibles à l'aide de l'ID de clé d'accès et de la clé d'accès secrète affichées 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 tourner régulièrement les clés d'accès, supprimez toutes les clés inutilisées du compte et ne les partagez jamais avec d'autres utilisateurs.

Étapes

1. Sélectionnez **GESTION DES ACCÈS > Utilisateurs**.
2. Sélectionnez l'utilisateur dont vous souhaitez gérer les clés d'accès S3.

La page de détails de l'utilisateur apparaît.

3. Sélectionnez **Clés d'accès**, puis sélectionnez **Créer une clé**.
4. Effectuez l'une des opérations suivantes :
 - Sélectionnez **Ne pas définir de délai d'expiration** pour créer une clé qui n'expire pas. (Défaut)
 - Sélectionnez **Définir 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. Le délai 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, répertoriant l'ID de la clé d'accès et la clé d'accès secrète.

6. Copiez l'ID de clé d'accès et la clé d'accès secrète dans un emplacement sûr ou sélectionnez **Télécharger .csv** pour enregistrer un fichier de feuille de calcul contenant l'ID de clé d'accès et la clé d'accès secrète.



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 des clés une fois la boîte de dialogue fermée.

7. Sélectionnez **Terminer**.

La nouvelle clé est répertoriée dans l'onglet Clés d'accès de la page des détails de l'utilisateur.

8. Si votre compte de locataire dispose de l'autorisation **Utiliser la connexion à la fédération de grille**, utilisez éventuellement l'API de gestion des locataires pour cloner manuellement les clés d'accès S3 du locataire sur la grille source vers le locataire sur 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 afin de déterminer quelles clés expireront bientôt. Selon vos besoins, vous pouvez créer de nouvelles clés et supprimer des clés qui ne sont plus utilisées.

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un "[navigateur Web pris en charge](#)".
- Vous avez le "[Autorisation d'accès root](#)".



Les compartiments et objets S3 appartenant à un utilisateur sont accessibles à l'aide de l'ID de clé d'accès et de la clé d'accès secrète affichées 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 tourner régulièrement les clés d'accès, supprimez toutes les clés inutilisées du compte et ne les partagez jamais avec d'autres utilisateurs.

Étapes

1. Sélectionnez **GESTION DES ACCÈS > Utilisateurs**.
2. Depuis la page Utilisateurs, sélectionnez l'utilisateur dont vous souhaitez afficher les clés d'accès S3.
3. Depuis la page Détails de l'utilisateur, sélectionnez **Clés d'accès**.
4. Trier les clés par **Délai d'expiration** ou **ID de clé d'accès**.
5. Selon les besoins, créez de nouvelles clés et supprimez manuellement les clés qui ne sont plus utilisées.

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 connexes

- ["Créer les clés d'accès S3 d'un autre utilisateur"](#)
- ["Supprimer les clés d'accès S3 d'un autre utilisateur"](#)

Supprimer 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 qu'une clé d'accès est supprimée, elle ne peut plus être utilisée pour accéder aux objets et aux buckets du compte locataire.

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous avez le ["Autorisation d'accès root"](#).



Les compartiments et objets S3 appartenant à un utilisateur sont accessibles à l'aide de l'ID de clé d'accès et de la clé d'accès secrète affichées 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 tourner régulièrement les clés d'accès, supprimez toutes les clés inutilisées du compte et ne les partagez jamais avec d'autres utilisateurs.

Étapes

1. Sélectionnez **GESTION DES ACCÈS > Utilisateurs**.
2. Depuis la page Utilisateurs, sélectionnez l'utilisateur dont vous souhaitez gérer les clés d'accès S3.
3. Sur la page Détails de l'utilisateur, sélectionnez **Clés d'accès**, puis cochez la case correspondant à chaque clé d'accès que vous souhaitez supprimer.
4. Sélectionnez **Actions > Supprimer la clé sélectionnée**.
5. Dans la boîte de dialogue de confirmation, sélectionnez **Touche Supprimer**.

Un message de confirmation apparaît dans le coin supérieur droit de la page.

Gérer les buckets S3

Créer un bucket S3

Vous pouvez utiliser Tenant Manager pour créer des compartiments S3 pour les données d'objet.

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous appartenez à un groupe d'utilisateurs disposant de l'accès Root ou Gérer tous les buckets ["autorisation"](#). Ces autorisations remplacent les paramètres d'autorisations dans les stratégies de groupe ou de compartiment.



Les autorisations permettant 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 politique de groupe"](#).

- Si vous prévoyez d'activer le verrouillage d'objet S3 pour un bucket, un administrateur de grille a activé le paramètre global de verrouillage d'objet S3 pour le système StorageGRID et vous avez examiné les exigences pour les buckets et objets de verrouillage d'objet S3.
- Si chaque locataire dispose de 5 000 buckets, chaque nœud de stockage de la grille dispose d'un minimum de 64 Go de RAM.



Chaque grille peut contenir un maximum de 100 000 buckets.

Accéder à l'assistant

Étapes

1. Sélectionnez **Afficher les buckets** dans le tableau de bord ou sélectionnez **STOCKAGE (S3) > Buckets**.
2. Sélectionnez **Créer un bucket**.

Entrez les détails

Étapes

1. Saisissez les détails du bucket.

Champ	Description
Nom du bucket	Un nom pour le bucket qui respecte ces règles : • Doit être unique sur chaque système StorageGRID (pas seulement unique au sein du compte locataire). • Doit être conforme au DNS. • Doit contenir au moins 3 et pas plus de 63 caractères. • Chaque étiquette doit commencer et se terminer par une lettre minuscule ou un chiffre et ne peut utiliser que des lettres minuscules, des chiffres et des traits d'union. • Ne doit pas contenir de points dans les demandes de style hébergé virtuellement. Les points entraîneront des problèmes avec la vérification du certificat générique du serveur. Pour plus d'informations, consultez le "Documentation d'Amazon Web Services (AWS) sur les règles de dénomination des buckets". Remarque : vous ne pouvez pas modifier le nom du bucket après l'avoir créé.
Région	La région du seau. Votre administrateur StorageGRID gère les régions disponibles. La région d'un bucket peut affecter la politique de protection des données appliquée aux objets. Par défaut, tous les buckets sont créés dans le us-east-1 région. Remarque : vous ne pouvez pas modifier la région après avoir créé le bucket.

2. Sélectionnez **Continuer**.

Étapes

1. Vous pouvez également activer le contrôle de version des objets pour le bucket.

Activez le contrôle de version des objets si vous souhaitez stocker chaque version de chaque objet dans ce bucket. Vous pouvez ensuite récupérer les versions précédentes d'un objet selon vos besoins. Vous devez activer le contrôle de version des objets si le bucket doit être utilisé pour la réplication inter-grille.

2. Si le paramètre global de verrouillage d'objet S3 est activé, activez éventuellement le verrouillage d'objet S3 pour que le bucket stocke les objets à l'aide d'un modèle WORM (écriture unique, lecture multiple).

Activez le verrouillage d'objet S3 pour un bucket uniquement si vous devez conserver des objets pendant une durée déterminée, par exemple pour répondre à certaines exigences réglementaires. S3 Object Lock est un paramètre permanent qui vous aide à empêcher la suppression ou l'écrasement d'objets pendant une durée déterminée ou indéfiniment.



Une fois le paramètre de verrouillage d'objet S3 activé pour un bucket, il ne peut pas être désactivé. Toute personne disposant des autorisations appropriées peut ajouter des objets à ce bucket qui ne peuvent pas être modifiés. Vous ne pourrez peut-être pas supprimer ces objets ni le bucket lui-même.

Si vous activez le verrouillage d'objet S3 pour un bucket, le contrôle de version du bucket est activé automatiquement.

3. Si vous avez sélectionné **Activer le verrouillage d'objet S3**, activez éventuellement la **Rétention par défaut** pour ce bucket.



Votre administrateur de réseau doit vous donner la permission de ["utiliser les fonctionnalités spécifiques de S3 Object Lock"](#) .

Lorsque la **rétention par défaut** est activée, les nouveaux objets ajoutés au bucket seront automatiquement protégés contre la suppression ou l'écrasement. Le paramètre **Conservation par défaut** ne s'applique pas aux objets qui ont leurs propres périodes de conservation.

- a. Si la **Rétention par défaut** est activée, spécifiez un **Mode de rétention par défaut** pour le bucket.

Mode de rétention par défaut	Description
Gouvernance	• Les utilisateurs avec le <code>s3:BypassGovernanceRetention</code> l'autorisation peut utiliser le <code>x-amz-bypass-governance-retention: true</code> en-tête de demande pour contourner les paramètres de conservation. • Ces utilisateurs peuvent supprimer une version d'objet avant que sa date de conservation ne soit atteinte. • Ces utilisateurs peuvent augmenter, diminuer ou supprimer la date de conservation d'un objet.

Mode de rétention par défaut	Description
Conformité	• L'objet ne peut pas être supprimé tant que sa date de conservation n'est pas atteinte. • La date de conservation de l'objet peut être augmentée, mais elle ne peut pas être diminuée. • La date de conservation de l'objet ne peut pas être supprimée tant que cette date n'est pas atteinte. Remarque : votre administrateur de réseau doit vous autoriser à utiliser le mode de conformité.

- b. Si la **Conservation par défaut** est activée, spécifiez la **Période de conservation par défaut** pour le bucket.

La **Période de conservation par défaut** indique la durée pendant laquelle les nouveaux objets ajoutés à ce bucket doivent être conservés, à compter du moment où ils sont ingérés. Spécifiez une valeur inférieure ou égale à la période de conservation maximale du locataire, telle que définie par l'administrateur de la grille.

Une période de conservation *maximale*, qui peut être une valeur comprise entre 1 jour et 100 ans, est définie lorsque l'administrateur de la grille crée le locataire. Lorsque vous définissez une période de conservation par défaut, elle ne peut pas dépasser la valeur définie pour la période de conservation maximale. Si nécessaire, demandez à votre administrateur de réseau d'augmenter ou de diminuer la période de conservation maximale.

4. Vous pouvez également sélectionner **Activer la limite de capacité**.

La limite de capacité est la capacité maximale disponible pour les objets de ce bucket. Cette valeur représente une quantité logique (taille de l'objet), et non une quantité physique (taille sur le disque).

Si aucune limite n'est définie, la capacité de ce bucket est illimitée. Consultez ["Utilisation de la limite de capacité"](#) pour plus d'informations.

5. Sélectionnez **Créer un bucket**.

Le bucket est créé et ajouté au tableau sur la page Buckets.

6. En option, sélectionnez **Accéder à la page des détails du bucket** pour ["afficher les détails du godet"](#) et effectuer une configuration supplémentaire.

Afficher les détails du godet

Vous pouvez afficher les buckets dans votre compte locataire.

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Accès root, autorisation Gérer tous les buckets ou Afficher tous les buckets"](#). Ces autorisations remplacent les paramètres d'autorisation dans les stratégies de groupe ou de compartiment.

Étapes

1. Sélectionnez **Afficher les buckets** dans le tableau de bord ou sélectionnez **STOCKAGE (S3) > Buckets**.

La page Buckets apparaît.

2. Consultez le tableau récapitulatif pour chaque compartiment.

Selon vos besoins, vous pouvez trier les informations par colonne ou parcourir la liste en avant et en arrière.



Les valeurs de nombre d'objets, d'espace utilisé et d'utilisation affichées sont des estimations. Ces estimations sont affectées par le moment des ingestions, la connectivité réseau et l'état du nœud. Si le contrôle de version est activé pour les buckets, les versions d'objet supprimées sont incluses dans le nombre d'objets.

Nom

Le nom unique du bucket, qui ne peut pas être modifié.

Fonctionnalités activées

La liste des fonctionnalités activées pour le bucket.

Verrouillage d'objet S3

Si le verrouillage d'objet S3 est activé pour le bucket.

Cette colonne apparaît uniquement si le verrouillage d'objet S3 est activé pour la grille. Cette colonne affiche également des informations sur tous les buckets conformes hérités.

Région

La région du bucket, qui ne peut pas être modifiée. Cette colonne est masquée par défaut.

Nombre d'objets

Le nombre d'objets dans ce bucket. Si le contrôle de version est activé pour les buckets, les versions d'objet non actuelles sont incluses dans cette valeur.

Lorsque des objets sont ajoutés ou supprimés, cette valeur peut ne pas être mise à jour immédiatement.

Espace utilisé

La taille logique de tous les objets dans le bucket. La taille logique n'inclut pas l'espace réel requis pour les copies répliquées ou codées par effacement ou pour les métadonnées de l'objet.

La mise à jour de cette valeur peut prendre jusqu'à 10 minutes.

Usage

Le pourcentage utilisé de la limite de capacité du bucket, si elle a été définie.

La valeur d'utilisation est basée sur des estimations internes et peut être dépassée dans certains cas. Par exemple, StorageGRID vérifie la limite de capacité (si définie) lorsqu'un locataire commence à télécharger des objets et rejette les nouvelles ingestions dans ce bucket si le locataire a dépassé la limite de capacité. Cependant, StorageGRID ne prend pas en compte la taille du téléchargement actuel pour déterminer si la limite de capacité a été dépassée. Si des objets sont supprimés, un locataire peut être temporairement empêché de télécharger de nouveaux objets dans ce bucket jusqu'à ce que l'utilisation de la limite de capacité soit recalculée. Les calculs peuvent prendre 10 minutes ou plus.

Cette valeur indique la taille logique, et non la taille physique nécessaire pour stocker les objets et leurs métadonnées.

Capacité

Si défini, la limite de capacité du bucket.

Date de création

La date et l'heure de création du bucket. Cette colonne est masquée par défaut.

3. Pour afficher les détails d'un bucket spécifique, sélectionnez le nom du bucket dans le tableau.
 - a. Consultez les informations récapitulatives en haut de la page Web pour confirmer les détails du bucket, tels que la région et le nombre d'objets.
 - b. Afficher la barre d'utilisation de la limite de capacité. Si l'utilisation est de 100 % ou proche de 100 %, envisagez d'augmenter la limite ou de supprimer certains objets.
 - c. Si nécessaire, sélectionnez **Supprimer les objets dans le bucket** et **Supprimer le bucket**.



Portez une attention particulière aux avertissements qui s'affichent lorsque vous sélectionnez chacune de ces options. Pour plus d'informations, reportez-vous à :

- ["Supprimer tous les objets d'un bucket"](#)
- ["Supprimer un bucket"](#)(le seau doit être vide)

- d. Affichez ou modifiez les paramètres du bucket dans chacun des onglets selon vos besoins.
 - **Console S3** : Afficher les objets du bucket. Pour plus d'informations, reportez-vous à ["Utiliser la console S3"](#) .
 - **Options du bucket** : afficher ou modifier les paramètres des options. Certains paramètres, tels que le verrouillage d'objet S3, ne peuvent pas être modifiés une fois le bucket créé.
 - ["Gérer la cohérence des buckets"](#)
 - ["Mises à jour de l'heure du dernier accès"](#)
 - ["Limite de capacité"](#)
 - ["Versionnage d'objet"](#)
 - ["Verrouillage d'objet S3"](#)
 - ["Rétention du bucket par défaut"](#)
 - ["Gérer la réplication inter-réseaux"](#)(si autorisé pour le locataire)
 - **Services de la plateforme**:["Gérer les services de la plateforme"](#) (si autorisé pour le locataire)
 - **Accès au bucket** : afficher ou modifier les paramètres des options. Vous devez disposer d'autorisations d'accès spécifiques.
 - Configurez ["Partage des ressources inter-origines \(CORS\)"](#) ainsi, le bucket et les objets qu'il contient seront accessibles aux applications Web dans d'autres domaines.
 - ["Contrôler l'accès des utilisateurs"](#) pour un bucket S3 et les objets dans ce bucket.

Appliquer une balise de stratégie ILM à un bucket

Choisissez une balise de stratégie ILM à appliquer à un bucket en fonction de vos besoins de stockage d'objets.

La politique ILM contrôle où les données de l'objet sont stockées et si elles sont supprimées après une certaine période. Votre administrateur de réseau crée des stratégies ILM et les attribue à des balises de stratégie ILM lors de l'utilisation de plusieurs stratégies actives.



Évitez de réaffecter fréquemment la balise de stratégie d'un bucket. Dans le cas contraire, des problèmes de performances pourraient survenir.

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un ["navigateur Web pris en charge"](#) .
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Accès root, autorisation Gérer tous les buckets ou Afficher tous les buckets"](#) . Ces autorisations remplacent les paramètres d'autorisation dans les stratégies de groupe ou de compartiment.

Étapes

1. Sélectionnez **Afficher les buckets** dans le tableau de bord ou sélectionnez **STOCKAGE (S3) > Buckets**.

La page Buckets apparaît. Selon vos besoins, vous pouvez trier les informations par colonne ou parcourir la liste en avant et en arrière.

2. Sélectionnez le nom du bucket auquel vous souhaitez attribuer une balise de stratégie ILM.

Vous pouvez également modifier l'attribution de balise de stratégie ILM pour un bucket auquel une balise est déjà attribuée.



Les valeurs affichées pour le nombre d'objets et l'espace utilisé sont des estimations. Ces estimations sont affectées par le moment des ingestions, la connectivité réseau et l'état du nœud. Si le contrôle de version est activé pour les buckets, les versions d'objet supprimées sont incluses dans le nombre d'objets.

3. Dans l'onglet Options du compartiment, développez l'accordéon de balise de stratégie ILM. Cet accordéon n'apparaît que si votre administrateur de grille a activé l'utilisation de balises de stratégie personnalisées.
4. Lisez la description de chaque balise de stratégie pour déterminer quelle balise doit être appliquée au bucket.



La modification de la balise de politique ILM pour un bucket déclenchera la réévaluation ILM de tous les objets du bucket. Si la nouvelle politique conserve les objets pendant une durée limitée, les objets plus anciens seront supprimés.

5. Sélectionnez le bouton radio correspondant à la balise que vous souhaitez attribuer au bucket.
6. Sélectionnez **Enregistrer les modifications**. Une nouvelle balise de compartiment S3 sera définie sur le compartiment avec la clé `NTAP-SG-ILM-BUCKET-TAG` et la valeur du nom de la balise de politique ILM.



Assurez-vous que vos applications S3 ne remplacent pas ou ne suppriment pas accidentellement la nouvelle balise de compartiment. Si cette balise est omise lors de l'application d'un nouveau TagSet au bucket, les objets du bucket seront à nouveau évalués par rapport à la stratégie ILM par défaut.



Définissez et modifiez les balises de stratégie ILM à l'aide uniquement de Tenant Manager ou de l'API Tenant Manager où la balise de stratégie ILM est validée. Ne pas modifier le NTAP-SG-ILM-BUCKET-TAG Balise de stratégie ILM utilisant l'API S3 PutBucketTagging ou l'API S3 DeleteBucketTagging.



La modification de la balise de stratégie attribuée à un bucket a un impact temporaire sur les performances pendant que les objets sont réévalués à l'aide de la nouvelle stratégie ILM.

Gérer la politique de compartiment

Vous pouvez contrôler l'accès des utilisateurs à un compartiment S3 et aux objets de ce compartiment.

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Autorisation d'accès root"](#). Les autorisations Afficher tous les compartiments et Gérer tous les compartiments permettent uniquement l'affichage.
- Vous avez vérifié que le nombre requis de nœuds de stockage et de sites est disponible. Si deux ou plusieurs nœuds de stockage ne sont pas disponibles sur un site, ou si un site n'est pas disponible, les modifications apportées à ces paramètres peuvent ne pas être disponibles.

Étapes

1. Sélectionnez **Buckets**, puis sélectionnez le bucket que vous souhaitez gérer.
2. Sur la page des détails du bucket, sélectionnez **Accès au bucket > Politique du bucket**.
3. Effectuez l'une des opérations suivantes :
 - Saisissez une politique de compartiment en cochant la case **Activer la politique**. Saisissez ensuite une chaîne formatée JSON valide.

Chaque politique de compartiment a une limite de taille de 20 480 octets.
 - Modifier une politique existante en modifiant la chaîne.
 - Désactivez une politique en désélectionnant **Activer la politique**.

Pour des informations détaillées sur les politiques de bucket, y compris la syntaxe du langage et des exemples, voir ["Exemples de politiques de compartiment"](#).

Gérer la cohérence des buckets

Les valeurs de cohérence peuvent être utilisées pour spécifier la disponibilité des modifications des paramètres de bucket ainsi que pour fournir un équilibre entre la disponibilité des objets dans un bucket et la cohérence de ces objets sur différents nœuds de stockage et sites. Vous pouvez modifier les valeurs de cohérence pour qu'elles soient différentes des valeurs par défaut afin que les applications clientes puissent répondre à leurs besoins opérationnels.

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un ["navigateur Web pris en charge"](#).

- Vous appartenez à un groupe d'utilisateurs qui possède le "[Gérer tous les buckets ou l'autorisation d'accès root](#)". Ces autorisations remplacent les paramètres d'autorisations dans les stratégies de groupe ou de compartiment.

Directives relatives à la cohérence des seaux

La cohérence du bucket est utilisée pour déterminer la cohérence des applications clientes affectant les objets dans ce bucket S3. En général, vous devez utiliser la cohérence **Lecture après nouvelle écriture** pour vos buckets.

Modifier la cohérence du bucket

Si la cohérence **Lecture après nouvelle écriture** ne répond pas aux exigences de l'application cliente, vous pouvez modifier la cohérence en définissant la cohérence du compartiment ou en utilisant le Consistency-Control en-tête. Le Consistency-Control l'en-tête remplace la cohérence du bucket.



Lorsque vous modifiez la cohérence d'un bucket, seuls les objets ingérés après la modification sont assurés de respecter le paramètre révisé.

Étapes

1. Sélectionnez **Afficher les buckets** dans le tableau de bord ou sélectionnez **STOCKAGE (S3) > Buckets**.
2. Sélectionnez le nom du bucket dans le tableau.

La page des détails du bucket apparaît.

3. Dans l'onglet **Options du bucket**, sélectionnez l'accordéon **.
4. Sélectionnez une cohérence pour les opérations effectuées sur les objets de ce bucket.
 - **Tous** : Offre le plus haut niveau de cohérence. Tous les nœuds reçoivent les données immédiatement, sinon la demande échouera.
 - **Strong-global** : garantit la cohérence de lecture après écriture pour toutes les demandes client sur tous les sites.
 - **Strong-site** : garantit la cohérence de lecture après écriture pour toutes les requêtes client au sein d'un site.
 - **Lecture après nouvelle écriture** (par défaut) : assure la cohérence de lecture après écriture pour les nouveaux objets et la cohérence éventuelle pour les mises à jour d'objets. Offre des garanties de haute disponibilité et de protection des données. Recommandé dans la plupart des cas.
 - **Disponible** : Fournit une cohérence éventuelle pour les nouveaux objets et les mises à jour d'objets. Pour les buckets S3, utilisez-les uniquement si nécessaire (par exemple, pour un bucket contenant des valeurs de journal rarement lues ou pour des opérations HEAD ou GET sur des clés qui n'existent pas). Non pris en charge pour les buckets S3 FabricPool .
5. Sélectionnez **Enregistrer les modifications**.

Que se passe-t-il lorsque vous modifiez les paramètres du bucket

Les buckets ont plusieurs paramètres qui affectent le comportement des buckets et des objets qu'ils contiennent.

Les paramètres de bucket suivants utilisent une cohérence **forte** par défaut. Si deux ou plusieurs nœuds de stockage ne sont pas disponibles sur un site, ou si un site n'est pas disponible, les modifications apportées à ces paramètres peuvent ne pas être disponibles.

- ["Suppression du bucket vide en arrière-plan"](#)
- ["Heure du dernier accès"](#)
- ["Cycle de vie du bucket"](#)
- ["Politique de compartiment"](#)
- ["Étiquetage des buckets"](#)
- ["Gestion des versions de buckets"](#)
- ["Verrouillage d'objet S3"](#)
- ["Chiffrement du bucket"](#)



La valeur de cohérence pour le contrôle de version du bucket, le verrouillage d'objet S3 et le chiffrement du bucket ne peut pas être définie sur une valeur qui n'est pas fortement cohérente.

Les paramètres de compartiment suivants n'utilisent pas de cohérence forte et ont une plus grande disponibilité pour les modifications. Les modifications apportées à ces paramètres peuvent prendre un certain temps avant d'avoir un effet.

- ["Configuration des services de la plateforme : intégration des notifications, de la réplication ou de la recherche"](#)
- ["Configuration CORS"](#)
- [Modifier la cohérence du bucket](#)



Si la cohérence par défaut utilisée lors de la modification des paramètres de compartiment ne répond pas aux exigences de l'application cliente, vous pouvez modifier la cohérence à l'aide de l' `Consistency-Control` en-tête pour le ["API REST S3"](#) ou en utilisant le `reducedConsistency` ou `force` options dans le ["API de gestion des locataires"](#) .

Activer ou désactiver les mises à jour de l'heure du dernier accès

Lorsque les administrateurs de grille créent les règles de gestion du cycle de vie des informations (ILM) pour un système StorageGRID , ils peuvent éventuellement spécifier que l'heure du dernier accès d'un objet soit utilisée pour déterminer s'il faut déplacer cet objet vers un autre emplacement de stockage. Si vous utilisez un locataire S3, vous pouvez tirer parti de ces règles en activant les mises à jour de l'heure du dernier accès pour les objets d'un compartiment S3.

Ces instructions s'appliquent uniquement aux systèmes StorageGRID qui incluent au moins une règle ILM qui utilise l'option **Dernière heure d'accès** 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 de détails.

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un ["navigateur Web pris en charge"](#) .
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Gérer tous les buckets ou l'autorisation d'accès root"](#) . Ces autorisations remplacent les paramètres d'autorisations dans les stratégies de groupe ou de compartiment.

À propos de cette tâche

L'heure du dernier accès est l'une des options disponibles pour l'instruction de placement **Heure de référence** pour une règle ILM. La définition de l'heure de référence d'une règle sur l'heure du dernier accès permet aux administrateurs de grille de spécifier que les objets doivent être placés dans certains emplacements de stockage en fonction du moment où ces objets ont été récupérés pour la dernière fois (lus ou visualisés).

Par exemple, pour garantir que les objets récemment consultés restent sur un stockage plus rapide, un administrateur de grille peut créer une règle ILM spécifiant les éléments suivants :

- 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 mois dernier 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 **Dernière heure d'accès** et que vous souhaitez que cette option s'applique aux objets de ce compartiment, vous devez activer les mises à jour de la dernière heure d'accès pour les compartiments S3 spécifiés dans cette règle.



La mise à jour de l'heure du dernier accès lors de la récupération d'un objet peut réduire les performances de StorageGRID , en particulier pour les petits objets.

Un impact sur les performances se produit avec les mises à jour de l'heure du dernier accès, car StorageGRID doit effectuer ces étapes supplémentaires à chaque fois que des objets sont récupérés :

- Mettre à jour les objets avec de nouveaux horodatages
- Ajoutez les objets à la file d'attente ILM afin qu'ils puissent être réévalués par rapport aux règles et politiques ILM actuelles

Le tableau résume 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	
	Dernière heure d'accès mise à jour ?	Objet ajouté à la file d'attente d'évaluation ILM ?	Dernière heure d'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

Demande de liste d'objets ou de versions d'objets	Non	Non	Non	Non
Demande de copie d'un objet d'un bucket 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
Demande de finalisation d'un téléchargement en plusieurs parties	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 buckets** dans le tableau de bord ou sélectionnez **STOCKAGE (S3) > Buckets**.
2. Sélectionnez le nom du bucket dans le tableau.

La page des détails du bucket apparaît.

3. Dans l'onglet **Options du bucket**, sélectionnez l'accordéon **Dernières mises à jour de l'heure d'accès**.
4. Activer ou désactiver les mises à jour de l'heure du dernier accès.
5. Sélectionnez **Enregistrer les modifications**.

Modifier la version d'objet pour un bucket

Si vous utilisez un locataire S3, vous pouvez modifier l'état de contrôle de version des buckets S3.

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Gérer tous les buckets ou l'autorisation d'accès root"](#). Ces autorisations remplacent les paramètres d'autorisations dans les stratégies de groupe ou de compartiment.
- Vous avez vérifié que le nombre requis de nœuds de stockage et de sites est disponible. Si deux ou plusieurs nœuds de stockage ne sont pas disponibles sur un site, ou si un site n'est pas disponible, les modifications apportées à ces paramètres peuvent ne pas être disponibles.

À propos de cette tâche

Vous pouvez activer ou suspendre le contrôle de version d'objet pour un bucket. Une fois que vous avez activé le contrôle de version pour un bucket, celui-ci ne peut pas revenir à un état non versionné. Cependant, vous pouvez suspendre le contrôle de version du bucket.

- Désactivé : le contrôle de version n'a jamais été activé
- Activé : le contrôle de version est activé
- Suspendu : le contrôle de version était précédemment activé et est suspendu

Pour plus d'informations, consultez les éléments suivants :

- ["Versionnage d'objet"](#)
- ["Règles et politiques ILM pour les objets versionnés S3 \(exemple 4\)"](#)
- ["Comment les objets sont supprimés"](#)

Étapes

1. Sélectionnez **Afficher les buckets** dans le tableau de bord ou sélectionnez **STOCKAGE (S3) > Buckets**.
2. Sélectionnez le nom du bucket dans le tableau.

La page des détails du bucket apparaît.

3. Dans l'onglet **Options du bucket**, sélectionnez l'accordéon **Versionnement d'objet**.
4. Sélectionnez un état de version pour les objets de ce bucket.

Le contrôle de version des objets doit rester activé pour un bucket utilisé pour la réplication inter-grille. Si le verrouillage d'objet S3 ou la conformité héritée est activé, les options **Versionnage d'objet** sont désactivées.

Option	Description
Activer le contrôle de version	Activez le contrôle de version des objets si vous souhaitez stocker chaque version de chaque objet dans ce bucket. Vous pouvez ensuite récupérer les versions précédentes d'un objet selon vos besoins. Les objets qui étaient déjà dans le bucket seront versionnés lorsqu'ils seront modifiés par un utilisateur.
Suspendre le contrôle de version	Suspendez le contrôle de version des objets si vous ne souhaitez plus que de nouvelles versions d'objets soient créées. Vous pouvez toujours récupérer toutes les versions d'objet existantes.

5. Sélectionnez **Enregistrer les modifications**.

Utilisez S3 Object Lock pour conserver les objets

Vous pouvez utiliser S3 Object Lock si les buckets et les objets doivent être conformes aux exigences réglementaires en matière de conservation.



Votre administrateur de grille doit vous donner l'autorisation d'utiliser des fonctionnalités spécifiques de S3 Object Lock.

Qu'est-ce que S3 Object Lock ?

La fonctionnalité StorageGRID S3 Object Lock est une solution de protection d'objets équivalente à S3 Object Lock dans Amazon Simple Storage Service (Amazon S3).

Lorsque le paramètre global de verrouillage d'objet S3 est activé pour un système StorageGRID , un compte de locataire S3 peut créer des buckets avec ou sans verrouillage d'objet S3 activé. Si le verrouillage d'objet S3 est activé pour un bucket, le contrôle de version du bucket est requis et est activé automatiquement.

Un bucket sans verrouillage d'objet S3 ne peut contenir que des objets sans paramètres de conservation spécifiés. Aucun objet ingéré n'aura de paramètres de rétention.

Un bucket avec verrouillage d'objet S3 peut contenir des objets avec et sans paramètres de rétention spécifiés par les applications clientes S3. Certains objets ingérés auront des paramètres de rétention.

Un bucket avec verrouillage d'objet S3 et rétention par défaut configuré peut contenir des objets téléchargés avec des paramètres de rétention spécifiés et de nouveaux objets sans paramètres de rétention. Les nouveaux objets utilisent le paramètre par défaut, car le paramètre de rétention n'a pas été configuré au niveau de l'objet.

En effet, tous les objets nouvellement ingérés ont des paramètres de rétention lorsque la rétention par défaut est configurée. Les objets existants sans paramètres de conservation d'objets restent inchangés.

Modes de rétention

La fonctionnalité 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 rétention d'Amazon S3.

- En mode conformité :
 - L'objet ne peut pas être supprimé tant que sa date de conservation n'est pas atteinte.
 - La date de conservation de l'objet peut être augmentée, mais elle ne peut pas être diminuée.
 - La date de conservation de l'objet 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 que sa date de conservation ne soit atteinte.
 - 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 d'objet S3 activé, les utilisateurs peuvent utiliser l'application cliente S3 pour spécifier éventuellement les paramètres de conservation suivants pour chaque objet ajouté au compartiment :

- **Mode de conservation** : Soit la conformité, soit la gouvernance.
- **Date de conservation jusqu'à** : si la date de conservation jusqu'à d'une version d'objet est dans le futur, l'objet peut être récupéré, mais il ne peut pas être supprimé.
- **Conservation légale** : L'application d'une conservation légale à une version d'objet verrouille immédiatement cet objet. Par exemple, vous pourriez avoir besoin de suspendre légalement un objet lié à une enquête ou à un litige juridique. Une conservation légale n'a pas de date d'expiration, mais reste en place jusqu'à ce qu'elle soit explicitement supprimée. Les conservations légales sont indépendantes de la date de conservation.



Si un objet est sous conservation légale, personne ne peut supprimer l'objet, quel que soit son mode de conservation.

Pour plus de détails sur les paramètres de l'objet, voir ["Utiliser l'API REST S3 pour configurer le"](#)

Paramètre de rétention par défaut pour les buckets

Si un bucket est créé avec le verrouillage d'objet S3 activé, les utilisateurs peuvent éventuellement spécifier les paramètres par défaut suivants pour le bucket :

- **Mode de conservation par défaut** : Conformité ou gouvernance.
- **Période de conservation par défaut** : durée pendant laquelle les nouvelles versions d'objet ajoutées à ce bucket doivent être conservées, à compter du jour de leur ajout.

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 bucket S3"](#) et ["Mettre à jour la conservation par défaut du verrouillage des objets S3"](#) .

Tâches de verrouillage d'objet S3

Les listes suivantes destinées aux administrateurs de grille et aux utilisateurs locataires contiennent les tâches de haut niveau pour l'utilisation de la fonctionnalité de verrouillage d'objet S3.

Administrateur de réseau

- Activez le paramètre de verrouillage d'objet S3 global pour l'ensemble du système StorageGRID .
- Assurez-vous que les politiques de gestion du cycle de vie de l'information (ILM) sont *conformes* ; c'est-à-dire qu'elles répondent aux ["exigences des buckets avec S3 Object Lock activé"](#) .
- Si nécessaire, autorisez un locataire à utiliser la conformité comme mode de conservation. Sinon, seul le mode Gouvernance est autorisé.
- Si nécessaire, définissez une période de conservation maximale pour un locataire.

Utilisateur locataire

- Passez en revue les considérations relatives aux buckets et aux objets avec S3 Object Lock.
- Si nécessaire, contactez l'administrateur de la grille pour activer le paramètre de verrouillage d'objet S3 global et définir les autorisations.
- Créez des buckets avec le verrouillage d'objet S3 activé.
- Vous pouvez également configurer les paramètres de conservation par défaut pour un bucket :
 - Mode de conservation par défaut : Gouvernance ou Conformité, si autorisé par l'administrateur du réseau.
 - Période de conservation par défaut : doit être inférieure ou égale à la période de conservation maximale définie par l'administrateur du réseau.
- Utilisez l'application client S3 pour ajouter des objets et éventuellement définir une conservation spécifique à l'objet :
 - Mode de rétention. Gouvernance ou conformité, si autorisée par l'administrateur du réseau.
 - Date de conservation : doit être inférieure ou égale à ce qui est autorisé par la période de conservation maximale définie par l'administrateur de la grille.

Exigences pour les buckets avec S3 Object Lock activé

- Si le paramètre global de verrouillage d'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 buckets avec le verrouillage d'objets S3 activé.
- Si vous prévoyez d'utiliser S3 Object Lock, vous devez activer S3 Object Lock lorsque vous créez le bucket. Vous ne pouvez pas activer le verrouillage d'objet S3 pour un bucket existant.
- Lorsque le verrouillage d'objet S3 est activé pour un bucket, StorageGRID active automatiquement le contrôle de version pour ce bucket. Vous ne pouvez pas désactiver le verrouillage d'objet S3 ou suspendre le contrôle de version du bucket.
- Vous pouvez également spécifier un mode de conservation par défaut et une période de conservation pour chaque compartiment à l'aide du gestionnaire de locataires, de l'API de gestion des locataires ou de l'API REST S3. Les paramètres de conservation par défaut du bucket s'appliquent uniquement aux nouveaux objets ajoutés au bucket 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 pour chaque version d'objet lors de son téléchargement.
- La configuration du cycle de vie du bucket est prise en charge pour les buckets avec S3 Object Lock activé.
- La réplication CloudMirror n'est pas prise en charge pour les buckets avec S3 Object Lock activé.

Exigences relatives aux objets dans les compartiments avec le verrouillage d'objet S3 activé

- Pour protéger une version d'objet, vous pouvez spécifier des paramètres de rétention par défaut pour le compartiment ou spécifier des paramètres de rétention pour chaque version d'objet. Les paramètres de conservation au niveau de l'objet peuvent être spécifiés à l'aide de l'application cliente 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 une date de conservation et un paramètre de conservation légale, l'un mais pas l'autre, ou aucun des deux. La spécification d'une date de conservation ou d'un paramètre de conservation légale 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 les buckets avec S3 Object Lock activé

Chaque objet enregistré dans un bucket avec S3 Object Lock activé passe par ces étapes :

1. Objet ingéré

Lorsqu'une version d'objet est ajoutée à un bucket sur lequel le verrouillage d'objet S3 est activé, les paramètres de rétention sont appliqués comme suit :

- Si des paramètres de conservation sont spécifiés pour l'objet, les paramètres au niveau de l'objet sont appliqués. Tous les paramètres de bucket 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 S3 Object Lock.

Si les paramètres de conservation sont appliqués, l'objet et toutes les métadonnées définies par l'utilisateur S3 sont protégés.

2. Conservation et suppression d'objets

Plusieurs copies de chaque objet protégé sont stockées par StorageGRID pendant la période de conservation spécifiée. Le nombre et le type exacts de copies d'objets ainsi que les emplacements de stockage sont déterminés par les règles de conformité des politiques ILM actives. La possibilité de supprimer un objet protégé avant que sa date de conservation ne soit atteinte dépend de son mode de conservation.

- Si un objet est sous conservation légale, personne ne peut supprimer l'objet, quel que soit son mode de conservation.

Puis-je toujours gérer les buckets conformes hérités ?

La fonctionnalité de verrouillage d'objet S3 remplace la fonctionnalité de conformité qui était disponible dans les versions précédentes de StorageGRID . Si vous avez créé des buckets conformes à l'aide d'une version précédente de StorageGRID, vous pouvez continuer à gérer les paramètres de ces buckets ; toutefois, vous ne pouvez plus créer de nouveaux buckets conformes. Pour les instructions, voir https://kb.netapp.com/Advice_and_Troubleshooting/Hybrid_Cloud_Infrastructure/StorageGRID/How_to_manage_legacy_Compliant_buckets_in_StorageGRID_11.5 [Base de connaissances NetApp : Gestion des buckets compatibles hérités dans StorageGRID 11.5].

Mettre à jour la conservation par défaut du verrouillage des objets S3

Si vous avez activé le verrouillage d'objet S3 lors de la création du bucket, vous pouvez modifier le bucket pour modifier les paramètres de rétention par défaut. Vous pouvez activer (ou désactiver) la conservation par défaut et définir un mode de conservation par défaut et une période de conservation.

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un ["navigateur Web pris en charge"](#) .
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Gérer tous les buckets ou l'autorisation d'accès root"](#) . Ces autorisations remplacent les paramètres d'autorisations dans les stratégies de groupe ou de compartiment.
- 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 bucket. Voir ["Utilisez S3 Object Lock pour conserver les objets"](#) .

Étapes

1. Sélectionnez **Afficher les buckets** dans le tableau de bord ou sélectionnez **STOCKAGE (S3) > Buckets**.
2. Sélectionnez le nom du bucket dans le tableau.

La page des détails du bucket apparaît.

3. Dans l'onglet **Options du bucket**, sélectionnez l'accordéon **Verrouillage d'objet S3**.
4. En option, activez ou désactivez la **Rétention par défaut** pour ce bucket.

Les modifications apportées à ce paramètre ne s'appliquent pas aux objets déjà présents dans le bucket ni aux objets susceptibles d'avoir leurs propres périodes de conservation.

5. Si la **Rétention par défaut** est activée, spécifiez un **Mode de rétention par défaut** pour le bucket.

Mode de rétention par défaut	Description
Gouvernance	• Les utilisateurs avec le <code>s3:BypassGovernanceRetention</code> l'autorisation peut utiliser le <code>x-amz-bypass-governance-retention: true</code> en-tête de demande pour contourner les paramètres de conservation. • Ces utilisateurs peuvent supprimer une version d'objet avant que sa date de conservation ne soit atteinte. • Ces utilisateurs peuvent augmenter, diminuer ou supprimer la date de conservation d'un objet.
Conformité	• L'objet ne peut pas être supprimé tant que sa date de conservation n'est pas atteinte. • La date de conservation de l'objet peut être augmentée, mais elle ne peut pas être diminuée. • La date de conservation de l'objet ne peut pas être supprimée tant que cette date n'est pas atteinte. Remarque : votre administrateur de réseau doit vous autoriser à utiliser le mode de conformité.

6. Si la **Conservation par défaut** est activée, spécifiez la **Période de conservation par défaut** pour le bucket.

La **Période de conservation par défaut** indique la durée pendant laquelle les nouveaux objets ajoutés à ce bucket doivent être conservés, à compter du moment où ils sont ingérés. Spécifiez une valeur inférieure ou égale à la période de conservation maximale du locataire, telle que définie par l'administrateur de la grille.

Une période de conservation *maximale*, qui peut être une valeur comprise entre 1 jour et 100 ans, est définie lorsque l'administrateur de la grille crée le locataire. Lorsque vous définissez une période de conservation par défaut, elle ne peut pas dépasser la valeur définie pour la période de conservation maximale. Si nécessaire, demandez à votre administrateur de réseau d'augmenter ou de diminuer la période de conservation maximale.

7. Sélectionnez **Enregistrer les modifications**.

Configurer le partage de ressources inter-origines (CORS)

Vous pouvez configurer le partage de ressources inter-origines (CORS) pour un bucket S3 si vous souhaitez que ce bucket et les objets qu'il contient soient accessibles aux applications Web d'autres domaines.

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un ["navigateur Web pris en charge"](#).
- Pour les demandes de configuration GET CORS, vous appartenez à un groupe d'utilisateurs qui possède le ["Autorisation de gérer tous les compartiments ou d'afficher tous les compartiments"](#). Ces autorisations remplacent les paramètres d'autorisations dans les stratégies de groupe ou de compartiment.
- Pour les demandes de configuration PUT CORS, vous appartenez à un groupe d'utilisateurs qui possède

le ["Gérer toutes les autorisations des buckets"](#) . Cette autorisation remplace les paramètres d'autorisations dans les stratégies de groupe ou de compartiment.

- Le ["Autorisation d'accès root"](#) donne accès à toutes les demandes de configuration CORS.

À propos de cette tâche

Le partage de ressources inter-origines (CORS) est un mécanisme de sécurité qui permet aux applications Web clientes d'un domaine d'accéder aux ressources d'un domaine différent. Par exemple, supposons que vous utilisiez un bucket S3 nommé `Images` pour stocker des graphiques. En configurant CORS pour le `Images` bucket, vous pouvez autoriser l'affichage des images de ce bucket sur le site Web `http://www.example.com`.

Activer CORS pour un bucket

Étapes

1. Utilisez un éditeur de texte pour créer le XML requis. Cet exemple montre le XML utilisé pour activer CORS pour un bucket S3. Spécifiquement:
 - Permet à n'importe quel domaine d'envoyer des requêtes GET au bucket
 - Autorise uniquement le `http://www.example.com` domaine pour envoyer des requêtes GET, POST et DELETE
 - Tous les en-têtes de requête 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 de l'utilisateur d'Amazon Simple Storage Service"](#) .

2. Sélectionnez **Afficher les buckets** dans le tableau de bord ou sélectionnez **STOCKAGE (S3) > Buckets**.
3. Sélectionnez le nom du bucket dans le tableau.

La page des détails du bucket apparaît.

4. Dans l'onglet **Accès au bucket**, sélectionnez l'accordéon **Partage de ressources inter-origines (CORS)**.
5. Cochez la case **Activer CORS**.

6. Collez le 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**.

Supprimer les objets dans le bucket

Vous pouvez utiliser le gestionnaire de locataires pour supprimer les objets dans un ou plusieurs compartiments.

Considérations et exigences

Avant d'effectuer ces étapes, notez les points suivants :

- Lorsque vous supprimez les objets d'un bucket, StorageGRID supprime définitivement tous les objets et toutes les versions d'objets de chaque bucket sélectionné de tous les nœuds et sites de votre système StorageGRID . StorageGRID supprime également toutes les métadonnées d'objet associées. Vous ne pourrez pas récupérer ces informations.
- La suppression de tous les objets d'un bucket peut prendre des minutes, des jours, voire des semaines, en fonction du nombre d'objets, de copies d'objets et d'opérations simultanées.
- Si un seau a "**Verrouillage d'objet S3 activé**" , il pourrait rester dans l'état **Suppression d'objets : lecture seule** pendant *années*.



Un bucket qui utilise S3 Object Lock restera dans 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 conservations légales soient supprimées.

- Pendant la suppression des objets, l'état du bucket est **Suppression d'objets : lecture seule**. Dans cet état, vous ne pouvez pas ajouter de nouveaux objets au bucket.
- Lorsque tous les objets ont été supprimés, le bucket reste en état de lecture seule. Vous pouvez effectuer l'une des opérations suivantes :
 - Remettre le bucket en mode écriture et le réutiliser pour de nouveaux objets
 - Supprimer le bucket
 - Gardez le bucket en mode lecture seule pour réserver son nom pour une utilisation ultérieure
- Si le contrôle de version d'objet est activé pour un bucket, les marqueurs de suppression créés dans StorageGRID 11.8 ou version ultérieure peuvent être supprimés à l'aide des opérations Supprimer des objets dans le bucket.
- Si le contrôle de version d'objet est activé pour un bucket, l'opération de suppression d'objets ne

supprimera pas les marqueurs de suppression créés dans StorageGRID 11.7 ou une version antérieure. Consultez les informations sur la suppression d'objets dans un bucket dans ["Comment les objets versionnés S3 sont supprimés"](#).

- Si vous utilisez ["réplication inter-réseaux"](#), notez ce qui suit :
 - L'utilisation de cette option ne supprime aucun objet du bucket sur l'autre grille.
 - Si vous sélectionnez cette option pour le bucket source, l'alerte **Échec de la réplication inter-grille** sera déclenchée si vous ajoutez des objets au bucket de destination sur l'autre grille. Si vous ne pouvez pas garantir que personne n'ajoutera d'objets au seau sur l'autre grille, ["désactiver la réplication inter-grille"](#) pour ce bucket avant de supprimer tous les objets du bucket.

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Autorisation d'accès root"](#). Cette autorisation remplace les paramètres d'autorisations dans les stratégies de groupe ou de compartiment.

Étapes

1. Sélectionnez **Afficher les buckets** dans le tableau de bord ou sélectionnez **STOCKAGE (S3) > Buckets**.

La page Buckets apparaît et affiche tous les buckets S3 existants.

2. Utilisez le menu **Actions** ou la page de détails pour un bucket spécifique.

Menu Actions

- a. Cochez la case correspondant à chaque compartiment dont vous souhaitez supprimer des objets.
- b. Sélectionnez **Actions > Supprimer les objets dans le bucket**.

Page de détails

- a. Sélectionnez un nom de bucket pour afficher ses détails.
- b. Sélectionnez **Supprimer les objets dans le bucket**.

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.

Après quelques minutes :

- Une bannière d'état jaune apparaît sur la page des détails du bucket. La barre de progression représente le pourcentage d'objets supprimés.
- **(lecture seule)** apparaît après le nom du bucket sur la page des détails du bucket.
- **(Suppression d'objets : lecture seule)** apparaît à côté du nom du bucket sur la page Buckets.

Buckets > my-bucket

my-bucket (read-only)

Region: us-east-1

Date created: 2022-12-14 10:09:50 MST

Object count: 3

View bucket contents in Experimental S3 Console

Delete bucket

 **All bucket objects are being deleted**

StorageGRID is deleting all copies of the objects in this bucket, which might take days or weeks. While objects are being deleted, the bucket is read only. To stop the operation, select **Stop deleting objects**. You cannot restore objects that have already been deleted.

0% (0 of 3 objects deleted)

Stop deleting objects

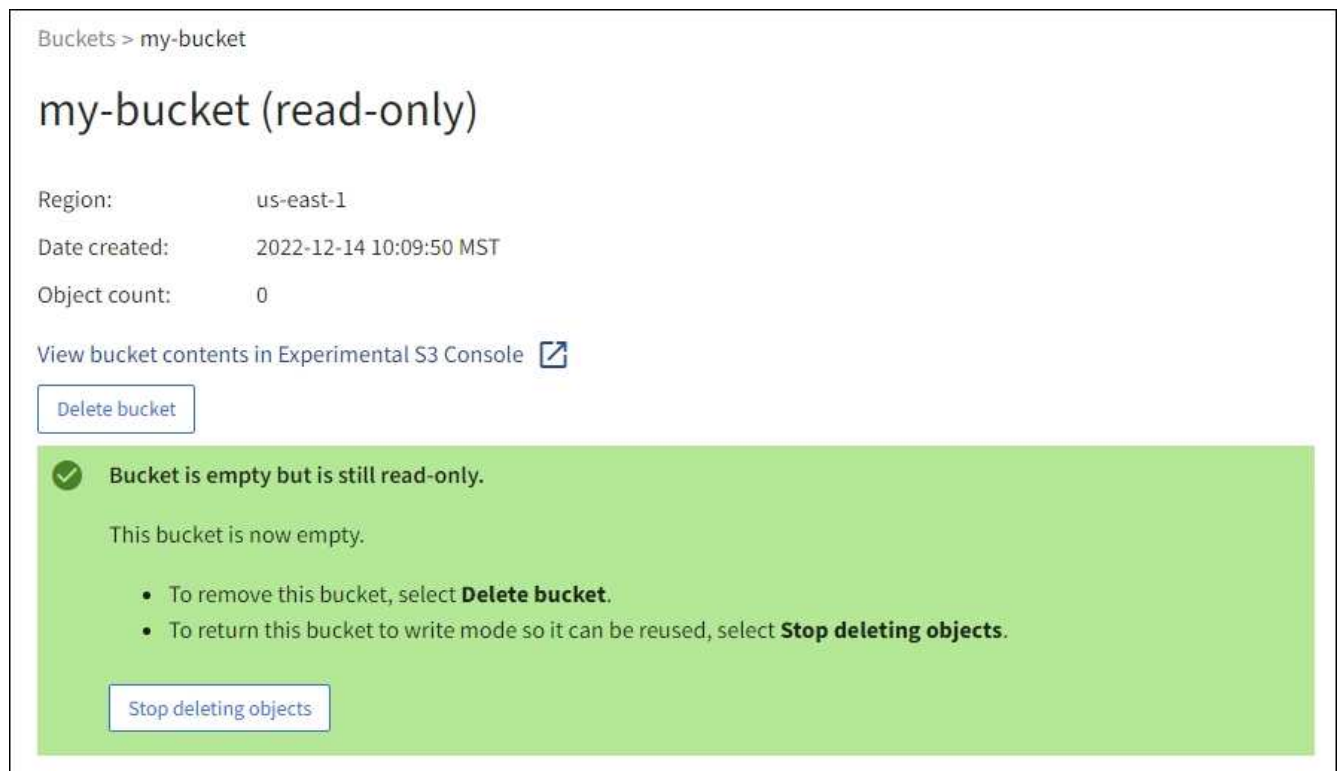
Success
Starting to delete objects from one bucket.

5. Si nécessaire, pendant que l'opération est en cours, sélectionnez **Arrêter la suppression des objets** pour arrêter le processus. Ensuite, si vous le souhaitez, sélectionnez **Supprimer les objets dans le bucket** pour reprendre le processus.

Lorsque vous sélectionnez **Arrêter la suppression des objets**, le bucket revient en mode écriture ; cependant, vous ne pouvez pas accéder ni restaurer les objets qui ont été supprimés.

6. Attendez que l'opération soit terminée.

Lorsque le bucket est vide, la bannière d'état est mise à jour, mais le bucket reste en lecture seule.



7. Effectuez l'une des opérations suivantes :

- Quittez la page pour conserver le bucket en mode lecture seule. Par exemple, vous pouvez conserver un bucket vide en mode lecture seule pour réserver le nom du bucket pour une utilisation ultérieure.
- Supprimer le bucket. Vous pouvez sélectionner **Supprimer le bucket** pour supprimer un seul bucket ou revenir à la page Buckets et sélectionner **Actions > Supprimer** les buckets pour supprimer plusieurs buckets.



Si vous ne parvenez pas à supprimer un bucket versionné après la suppression de tous les objets, des marqueurs de suppression peuvent rester. Pour supprimer le bucket, vous devez supprimer tous les marqueurs de suppression restants.

- Remettez le bucket en mode écriture et réutilisez-le éventuellement pour de nouveaux objets. Vous pouvez sélectionner **Arrêter la suppression des objets** pour un seul bucket ou revenir à la page Buckets et sélectionner **Action > Arrêter la suppression des objets** pour plusieurs buckets.

Supprimer le compartiment S3

Vous pouvez utiliser le gestionnaire de locataires pour supprimer un ou plusieurs compartiments S3 vides.

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un ["navigateur Web pris en charge"](#) .
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Gérer tous les buckets ou l'autorisation d'accès root"](#) . Ces autorisations remplacent les paramètres d'autorisations dans les stratégies de groupe ou de compartiment.
- Les buckets que vous souhaitez supprimer sont vides. Si les buckets que vous souhaitez supprimer ne sont pas vides, ["supprimer des objets du bucket"](#) .

À propos de cette tâche

Ces instructions décrivent comment supprimer un compartiment S3 à l'aide du gestionnaire de locataires. Vous pouvez également supprimer des compartiments S3 à l'aide de la ["API de gestion des locataires"](#) ou le ["API REST S3"](#).

Vous ne pouvez pas supprimer un compartiment S3 s'il contient des objets, des versions d'objet non actuelles ou des marqueurs de suppression. Pour plus d'informations sur la manière dont les objets versionnés S3 sont supprimés, consultez ["Comment les objets sont supprimés"](#).

Étapes

1. Sélectionnez **Afficher les buckets** dans le tableau de bord ou sélectionnez **STOCKAGE (S3) > Buckets**.

La page Buckets apparaît et affiche tous les buckets S3 existants.

2. Utilisez le menu **Actions** ou la page de détails pour un bucket spécifique.

Menu Actions

- a. Cochez la case correspondant à chaque compartiment que vous souhaitez supprimer.
- b. Sélectionnez **Actions > Supprimer les buckets**.

Page de détails

- a. Sélectionnez un nom de bucket pour afficher ses détails.
- b. Sélectionnez **Supprimer le bucket**.

3. Lorsque la boîte de dialogue de confirmation apparaît, sélectionnez **Oui**.

StorageGRID confirme que chaque bucket est vide, puis supprime chaque bucket. Cette opération peut prendre quelques minutes.

Si un bucket n'est pas vide, un message d'erreur s'affiche. Vous devez ["supprimer tous les objets et tous les marqueurs de suppression dans le bucket"](#) avant de pouvoir supprimer le bucket.

Utiliser la console S3

Vous pouvez utiliser la console S3 pour afficher et gérer les objets dans un bucket S3.

La console S3 vous permet de :

- Télécharger, renommer, copier, déplacer et supprimer des objets
- Afficher, rétablir, télécharger et supprimer les versions d'objets
- Rechercher des objets par préfixe
- Gérer les balises d'objet
- Afficher les métadonnées de l'objet
- Afficher, créer, renommer, copier, déplacer et supprimer des dossiers

La console S3 offre une expérience utilisateur améliorée pour les cas les plus courants. Il n'est pas conçu pour remplacer les opérations CLI ou API dans toutes les situations.



Si l'utilisation de la console S3 entraîne des opérations qui prennent trop de temps (par exemple, des minutes ou des heures), tenez compte des éléments suivants :

- Réduire le nombre d'objets sélectionnés
- Utiliser des méthodes non graphiques (API ou CLI) pour accéder à vos données

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un ["navigateur Web pris en charge"](#) .
- Si vous souhaitez gérer des objets, vous appartenez à un groupe d'utilisateurs disposant de l'autorisation d'accès Root. Vous pouvez également appartenir à un groupe d'utilisateurs disposant de l'autorisation Utiliser l'onglet Console S3 et de l'autorisation Afficher tous les buckets ou Gérer tous les buckets. Voir ["Autorisations de gestion des locataires"](#) .
- Une stratégie de groupe ou de compartiment S3 a été configurée pour l'utilisateur. Voir ["Utiliser des politiques d'accès aux buckets et aux groupes"](#) .
- Vous connaissez l'ID de la clé d'accès et la clé d'accès secrète de l'utilisateur. En option, vous disposez d'un .csv fichier contenant ces informations. Voir le ["instructions pour créer des clés d'accès"](#) .

Étapes

1. Sélectionnez **STOCKAGE > Compartiments > nom du compartiment**.
2. Sélectionnez l'onglet Console S3.
3. Collez l'ID de la clé d'accès et la clé d'accès secrète dans les champs. Sinon, sélectionnez **Télécharger les clés d'accès** et sélectionnez votre .csv déposer.
4. Sélectionnez * Sign in*.
5. Le tableau des objets du bucket apparaît. Vous pouvez gérer les objets selon vos besoins.

Informations Complémentaires

- **Recherche par préfixe** : La fonction de recherche par préfixe recherche uniquement les objets commençant par un mot spécifique relatif au dossier actuel. La recherche n'inclut pas les objets qui contiennent le mot ailleurs. Cette règle s'applique également aux objets contenus dans les dossiers. Par exemple, une recherche de folder1/folder2/somefile- renverrait les objets qui sont dans le folder1/folder2/ dossier et commencer par le mot somefile- .
- **Glisser-déposer** : vous pouvez glisser-déposer des fichiers du gestionnaire de fichiers de votre ordinateur vers la console S3. Cependant, vous ne pouvez pas télécharger de dossiers.
- **Opérations sur les dossiers** : Lorsque vous déplacez, copiez ou renommez un dossier, tous les objets du dossier sont mis à jour un par un, ce qui peut prendre du temps.
- **Suppression permanente lorsque le contrôle de version du bucket est désactivé** : lorsque vous écrasez ou supprimez un objet dans un bucket avec le contrôle de version désactivé, l'opération est permanente. Voir ["Modifier la version d'objet pour un bucket"](#) .

Gérer les services de la plateforme S3

Services de la plateforme S3

Présentation et considérations relatives aux services de la plateforme

Avant d'implémenter les services de plateforme, consultez la présentation et les considérations relatives à l'utilisation de ces services.

Pour plus d'informations sur S3, voir ["Utiliser l'API REST S3"](#) .

Aperçu des services de la plateforme

Les services de la plateforme StorageGRID peuvent vous aider 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'objets vers des destinations externes.

Étant donné que l'emplacement cible des services de plateforme est généralement externe à votre déploiement StorageGRID , les services de plateforme vous offrent la puissance et la flexibilité qui découlent de l'utilisation de ressources de stockage externes, de services de notification et de services de recherche ou d'analyse pour vos données.

N'importe quelle combinaison de services de plateforme peut être configurée pour un seul compartiment S3. Par exemple, vous pouvez configurer à la fois le ["Service CloudMirror"](#) et ["notifications"](#) sur un bucket StorageGRID S3 afin que vous puissiez mettre en miroir des objets spécifiques sur Amazon Simple Storage Service (S3), 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 plateforme doit être activée pour chaque compte de locataire par un administrateur StorageGRID à l'aide de Grid Manager ou de l'API Grid Management.

Comment les services de la plateforme sont configurés

Les services de plateforme communiquent avec des points de terminaison externes que vous configurez à l'aide de l'["Gestionnaire de locataires"](#) ou le ["API de gestion des locataires"](#) . Chaque point de terminaison représente une destination externe, telle qu'un bucket StorageGRID S3, un bucket Amazon Web Services, une rubrique Amazon SNS ou un cluster Elasticsearch hébergé localement, sur AWS ou ailleurs.

Après avoir créé un point de terminaison externe, vous pouvez activer un service de plateforme pour un bucket en ajoutant une configuration XML au bucket. La configuration XML identifie les objets sur lesquels le bucket doit agir, l'action que le bucket doit entreprendre et le point de terminaison que le bucket doit utiliser pour le service.

Vous devez ajouter des configurations XML distinctes pour chaque service de plateforme que vous souhaitez configurer. Par exemple:

- Si vous voulez tous les objets dont les clés commencent par `/images` pour être répliqué vers un compartiment Amazon S3, vous devez ajouter une configuration de réplication au compartiment source.
- Si vous souhaitez également envoyer des notifications lorsque ces objets sont stockés dans le bucket, vous devez ajouter une configuration de notifications.
- Si vous souhaitez 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 implémenter les services de la plateforme StorageGRID :

Service de plateforme	API REST S3	Se référer à
Réplication CloudMirror	• Réplication GetBucket • Réplication de PutBucket	• "Réplication CloudMirror" • "Opérations sur les godets"
Notifications	• Configuration de GetBucketNotification • Configuration de PutBucketNotification	• "Notifications" • "Opérations sur les godets"
Intégration de la recherche	• Configuration de la notification des métadonnées du bucket GET • Configuration des notifications de métadonnées du compartiment PUT	• "Intégration de la recherche" • "Opérations personnalisées StorageGRID"

Considérations relatives à l'utilisation des services de plateforme

Considération	Détails
Surveillance du point de terminaison de destination	Vous devez surveiller la disponibilité de chaque point de terminaison de destination. Si la connectivité au point de terminaison de destination est perdue pendant une période prolongée et qu'un important arriéré de demandes existe, les demandes client supplémentaires (telles que les demandes PUT) adressées à StorageGRID échoueront. Vous devez réessayer ces demandes ayant échoué lorsque le point de terminaison redevient accessible.
Limitation du point de terminaison de destination	Le logiciel StorageGRID peut limiter les requêtes S3 entrantes pour un bucket si la vitesse à laquelle les requêtes sont envoyées dépasse la vitesse à laquelle le point de terminaison de destination peut recevoir les requêtes. La limitation se produit uniquement lorsqu'il existe un arriéré de requêtes en attente d'être envoyées au point de terminaison de destination. Le seul effet visible est que les requêtes S3 entrantes prendront plus de temps à s'exécuter. Si vous commencez à détecter des performances nettement plus lentes, vous devez réduire le taux d'ingestion ou utiliser un point de terminaison avec une capacité supérieure. Si l'arriéré des demandes continue de croître, les opérations S3 du client (telles que les demandes PUT) finiront par échouer. Les requêtes CloudMirror sont plus susceptibles d'être affectées par les performances du point de terminaison de destination, car ces requêtes impliquent généralement plus de transfert de données que les requêtes d'intégration de recherche ou de notification d'événements.

Considération	Détails
Garanties de commande	StorageGRID garantit l'ordre des opérations sur un objet au sein d'un site. Tant que toutes les opérations sur un objet se déroulent sur le même site, l'état final de l'objet (pour la réplication) sera toujours égal à l'état dans StorageGRID. StorageGRID fait de son mieux pour ordonner les demandes lorsque des opérations sont effectuées sur les sites StorageGRID . Par exemple, si vous écrivez initialement un objet sur le site A, puis écrasez ultérieurement le même objet sur le site B, il n'est pas garanti que l'objet final répliqué par CloudMirror vers le bucket de destination soit l'objet le plus récent.
Suppressions d'objets pilotées par ILM	Pour correspondre au comportement de suppression d'AWS CRR et d'Amazon Simple Notification Service, les demandes de notification d'événements et CloudMirror ne sont pas envoyées lorsqu'un objet dans le compartiment source est supprimé en raison des règles StorageGRID ILM. Par exemple, aucune demande de notification CloudMirror ou d'événement n'est envoyée si une règle ILM supprime un objet après 14 jours. En revanche, les demandes d'intégration de recherche sont envoyées lorsque des objets sont supprimés en raison de l'ILM.
Utilisation des points de terminaison Kafka	Pour les points de terminaison Kafka, le protocole TLS mutuel n'est pas pris en charge. Par conséquent, si vous avez <code>ssl.client.auth</code> réglé sur <code>required</code> dans la configuration de votre courtier Kafka, cela peut entraîner des problèmes de configuration du point de terminaison Kafka. L'authentification des points de terminaison Kafka utilise les types d'authentification suivants. Ces types sont différents de ceux utilisés pour l'authentification d'autres points de terminaison, tels qu'Amazon SNS, et nécessitent des informations d'identification de nom d'utilisateur et de mot de passe. • SASL/PLAIN • SASL/SCRAM-SHA-256 • SASL/SCRAM-SHA-512 Remarque : les paramètres de proxy de stockage configurés ne s'appliquent pas aux points de terminaison des services de la plateforme Kafka.

Considérations relatives à l'utilisation du service de réplication CloudMirror

Considération	Détails
État de réplication	StorageGRID ne prend pas en charge le <code>x-amz-replication-status</code> en-tête.

Considération	Détails
Taille de l'objet	La taille maximale des objets pouvant être répliqués vers un bucket de destination par le service de réplication CloudMirror est de 5 Tio, ce qui correspond à la taille maximale de l'objet <i>pris en charge</i>. Remarque : la taille maximale <i>recommandée</i> pour une seule opération PutObject est de 5 Gio (5 368 709 120 octets). Si vous avez des objets dont la taille est supérieure à 5 Gio, utilisez plutôt le téléchargement en plusieurs parties.
Gestion des versions de bucket et identifiants de version	Si le contrôle de version est activé pour le bucket S3 source dans StorageGRID , vous devez également activer le contrôle de version pour le bucket de destination. Lorsque vous utilisez le contrôle de version, notez que l'ordre des versions d'objet dans le compartiment de destination est le meilleur effort et n'est pas garanti par le service CloudMirror, en raison des limitations du protocole S3. Remarque : les ID de version du bucket source dans StorageGRID ne sont pas liés aux ID de version du bucket de destination.
Balisateur des versions d'objet	Le service CloudMirror ne réplique aucune requête PutObjectTagging ou DeleteObjectTagging qui fournit 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'existe aucun moyen de garantir qu'une mise à jour de balise vers un ID de version spécifique sera répliquée. En revanche, le service CloudMirror réplique les requêtes PutObjectTagging ou DeleteObjectTagging qui ne spécifient pas d'ID de version. Ces requêtes mettent à jour les balises de la dernière clé (ou de la dernière version si le bucket est versionné). Les ingestions normales avec des balises (pas de mises à jour de balisage) sont également répliquées.
Téléchargements en plusieurs parties et ETag valeurs	Lors de la mise en miroir d'objets téléchargés à l'aide d'un téléchargement en plusieurs parties, le service CloudMirror ne conserve pas les parties. En conséquence, le ETag la valeur de l'objet en miroir sera différente de la ETag valeur de l'objet d'origine.
Objets chiffrés 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 bucket source pour la réplication CloudMirror et que la requête inclut les en-têtes de requête SSE-C, l'opération échoue.
Bucket avec verrouillage d'objet S3 activé	La réplication n'est pas prise en charge pour les buckets source ou de destination avec le verrouillage d'objet S3 activé.

Comprendre le service de réplication CloudMirror

Vous pouvez activer la réplication CloudMirror pour un bucket S3 si vous souhaitez que StorageGRID réplique les objets spécifiés ajoutés au bucket vers un ou plusieurs buckets de destination externes.

Par exemple, vous pouvez utiliser la réplication CloudMirror pour mettre en miroir des enregistrements clients spécifiques dans Amazon S3, puis exploiter les services AWS pour effectuer des analyses sur vos données.



La réplication CloudMirror n'est pas prise en charge si le verrouillage d'objet S3 est activé pour le compartiment source.

CloudMirror et ILM

La réplication CloudMirror fonctionne indépendamment des politiques ILM actives de la grille. Le service CloudMirror réplique les objets au fur et à mesure qu'ils sont stockés dans le bucket source et les livre au bucket de destination dès que possible. La livraison des objets répliqués est déclenchée lorsque l'ingestion de l'objet réussit.

CloudMirror et réplication inter-grille

La réplication CloudMirror présente des similitudes et des différences importantes avec la fonctionnalité de réplication inter-grille. "[Comparer la réplication inter-grille et la réplication CloudMirror](#)".

CloudMirror et buckets S3

La réplication CloudMirror est généralement configurée pour utiliser un bucket S3 externe comme destination. Cependant, vous pouvez également configurer la réplication pour utiliser un autre déploiement StorageGRID ou tout service compatible S3.

Buckets existants

Lorsque vous activez la réplication CloudMirror pour un bucket existant, seuls les nouveaux objets ajoutés à ce bucket sont répliqués. Tous les objets existants dans le bucket 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 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.

Plusieurs buckets de destination

Pour répliquer des objets d'un seul bucket vers plusieurs buckets de destination, spécifiez la destination de chaque règle dans le XML de configuration de réplication. Vous ne pouvez pas répliquer un objet dans plusieurs buckets en même temps.

Buckets versionnés ou non versionnés

Vous pouvez configurer la réplication CloudMirror sur des buckets versionnés ou non versionnés. Les buckets de destination peuvent être versionnés ou non. Vous pouvez utiliser n'importe quelle combinaison de buckets versionnés et non versionnés. Par exemple, vous pouvez spécifier un bucket versionné comme destination pour un bucket source non versionné, ou vice versa. Vous pouvez également effectuer une réplication entre des buckets non versionnés.

Suppression, boucles de réplication et événements

Comportement de suppression

Il s'agit du même comportement de suppression que le service Amazon S3, la réplication interrégionale (CRR). La suppression d'un objet dans un bucket source ne supprime jamais un objet répliqué dans la

destination. Si les buckets source et de destination sont tous deux versionnés, le marqueur de suppression est répliqué. Si le bucket de destination n'est pas versionné, la suppression d'un objet dans le bucket source ne réplique pas le marqueur de suppression dans le bucket de destination ni ne supprime l'objet de destination.

Protection contre les boucles de réplication

Lorsque les objets sont répliqués vers le bucket de destination, StorageGRID les marque comme « répliqués ». Un bucket StorageGRID de destination ne répliquera plus les objets marqués comme répliqués, vous protégeant ainsi des boucles de réplication accidentelles. Ce marquage de réplication est interne à StorageGRID et ne vous empêche pas d'exploiter 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.

Événements dans le bucket de destination

L'unicité et l'ordre des événements dans le bucket de destination ne sont pas garantis. Plusieurs copies identiques d'un objet source peuvent être livrées à la destination à la suite d'opérations effectuées pour garantir la réussite de la livraison. Dans de rares cas, lorsque le même objet est mis à jour simultanément à partir de deux ou plusieurs sites StorageGRID différents, l'ordre des opérations sur le bucket de destination peut ne pas correspondre à l'ordre des événements sur le bucket source.

Comprendre les notifications pour les buckets

Vous pouvez activer la notification d'événement pour un compartiment S3 si vous souhaitez que StorageGRID envoie des notifications sur des événements spécifiés à un cluster Kafka de destination ou à Amazon Simple Notification Service.

Par exemple, vous pouvez configurer des alertes à envoyer aux administrateurs pour chaque objet ajouté à un bucket, où les objets représentent des fichiers journaux associés à un événement système critique.

Les notifications d'événements sont créées dans le bucket source comme spécifié dans la configuration de notification et sont livrées à la destination. Si un événement associé à un objet réussit, une notification concernant cet événement est créée et mise en file d'attente pour livraison.

L'unicité et l'ordre des notifications ne sont pas garantis. Plusieurs notifications d'un événement peuvent être délivrées à la destination à la suite d'opérations effectuées pour garantir le succès de la livraison. Et comme la livraison est asynchrone, il n'est pas garanti que l'ordre temporel des notifications à la destination corresponde à l'ordre des événements sur le bucket source, en particulier pour les opérations provenant de différents sites StorageGRID. Vous pouvez utiliser le `sequencer` saisissez le message d'événement pour déterminer l'ordre des événements pour un objet particulier, comme décrit dans la documentation Amazon S3.

Les notifications d'événements StorageGRID suivent l'API Amazon S3 avec certaines limitations.

- Les types d'événements suivants sont pris en charge :
 - s3 : Objet créé :
 - s3:ObjetCréé:Mettre
 - s3 : Objet créé : Publication
 - s3:ObjetCréé:Copier
 - s3 : Objet créé : Téléchargement multi-parties complet

- s3 : Objet supprimé :
- s3:ObjectRemoved:Supprimer
- s3 : Objet supprimé : Supprimer le marqueur créé
- s3 : Restauration d'objet : Publication
- Les notifications d'événements envoyées depuis StorageGRID utilisent le format JSON standard mais n'incluent pas certaines clés et utilisent des valeurs spécifiques pour d'autres, comme indiqué dans le tableau :

Nom de la clé	Valeur StorageGRID
Source de l'événement	sgws:s3
Région AWS	<i>non inclus</i>
x-amz-id-2	<i>non inclus</i>
arn	urn:sgws:s3:::bucket_name

Comprendre le service d'intégration de recherche

Vous pouvez activer l'intégration de la recherche pour un compartiment S3 si vous souhaitez utiliser un service de recherche et d'analyse de données externe pour les métadonnées de votre objet.

Le service d'intégration de recherche est un service StorageGRID personnalisé qui envoie automatiquement et de manière asynchrone les métadonnées d'objet S3 à un point de terminaison de destination chaque fois qu'un objet est créé ou supprimé, ou que ses métadonnées ou balises sont mises à jour. Vous pouvez ensuite utiliser des outils sophistiqués de recherche, d'analyse de données, de visualisation ou d'apprentissage automatique fournis par le service de destination pour rechercher, analyser et obtenir des informations à partir des données de vos objets.

Par exemple, vous pouvez configurer vos buckets pour envoyer des métadonnées d'objet S3 à un service Elasticsearch distant. Vous pouvez ensuite utiliser Elasticsearch pour effectuer des recherches dans plusieurs compartiments et effectuer des analyses sophistiquées des modèles présents dans les métadonnées de votre objet.

Bien que l'intégration Elasticsearch puisse être configurée sur un bucket avec S3 Object Lock activé, les métadonnées S3 Object Lock (y compris la date de conservation et le statut de conservation légale) des objets ne seront pas incluses dans les métadonnées envoyées à Elasticsearch.



Étant donné que le service d'intégration de recherche provoque l'envoi des métadonnées d'objet vers une destination, sa configuration XML est appelée « XML de configuration de notification *metadata* ». Ce XML de configuration est différent du « XML de configuration de notification » utilisé pour activer les notifications d'événements.

Intégration de la recherche et buckets S3

Vous pouvez activer le service d'intégration de recherche pour n'importe quel bucket versionné ou non versionné. L'intégration de la recherche est configurée en associant la configuration XML de notification de

métadonnées au bucket qui spécifie les objets sur lesquels agir et la destination des métadonnées de l'objet.

Les notifications de métadonnées sont générées sous la forme d'un document JSON nommé avec le nom du bucket, 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 des métadonnées utilisateur.



Pour les balises et les métadonnées utilisateur, StorageGRID transmet des dates et des nombres à Elasticsearch sous forme de chaînes ou de notifications d'événements S3. Pour configurer Elasticsearch afin d'interpréter ces chaînes comme des dates ou des nombres, suivez les instructions Elasticsearch pour le mappage de champs dynamiques et pour le mappage des formats de date. Vous devez activer les mappages de champs dynamiques sur l'index avant de configurer le service d'intégration de recherche. Une fois qu'un document est indexé, vous ne pouvez pas modifier les types de champs du document dans l'index.

Notifications de recherche

Les notifications de métadonnées sont générées et mises en file d'attente pour être envoyées chaque fois que :

- Un objet est créé.
- Un objet est supprimé, y compris lorsque des objets sont supprimés suite au fonctionnement de la politique ILM de la grille.
- Les métadonnées ou balises d'objet sont ajoutées, mises à jour ou supprimées. L'ensemble complet des métadonnées et des balises est toujours envoyé lors de la mise à jour, pas seulement les valeurs modifiées.

Une fois que vous avez ajouté une configuration XML de notification de métadonnées à un bucket, des notifications sont envoyées pour tous les nouveaux objets que vous créez et pour tous les objets que vous modifiez en mettant à jour ses données, ses métadonnées utilisateur ou ses balises. Cependant, les notifications ne sont pas envoyées pour les objets qui se trouvaient déjà dans le bucket. Pour garantir que les métadonnées d'objet pour tous les objets du bucket sont envoyées à la destination, vous devez effectuer l'une des opérations suivantes :

- Configurez le service d'intégration de recherche immédiatement après la création du bucket et avant d'ajouter des objets.
- Exécutez une action sur tous les objets déjà présents dans le bucket qui déclenchera l'envoi d'un message de notification de métadonnées à la destination.

Service d'intégration de recherche et Elasticsearch

Le service d'intégration de recherche StorageGRID prend en charge un cluster Elasticsearch comme destination. Comme pour les autres services de plateforme, la destination est spécifiée dans le point de terminaison dont l'URN est utilisée dans le XML de configuration du service. Utilisez le "[Outil de matrice d'interopérabilité NetApp](#)" pour déterminer les versions prises en charge d'Elasticsearch.

Gérer les points de terminaison des services de la plateforme

Configurer les points de terminaison des services de la plateforme

Avant de pouvoir configurer un service de plateforme pour un bucket, vous devez configurer au moins un point de terminaison comme destination du service de plateforme.

L'accès aux services de la plateforme est activé pour chaque locataire par un administrateur StorageGRID . Pour créer ou utiliser un point de terminaison de services de plateforme, vous devez être un utilisateur locataire avec l'autorisation d'accès Gérer les points de terminaison ou Racine, dans une grille dont la mise en réseau a été configurée pour permettre aux nœuds de stockage d'accéder aux ressources de point de terminaison externes. Pour un seul locataire, vous pouvez configurer un maximum de 500 points de terminaison de services de plateforme. Contactez votre administrateur StorageGRID pour plus d'informations.

Qu'est-ce qu'un point de terminaison de services de plateforme ?

Un point de terminaison de services de plateforme spécifie les informations dont StorageGRID a besoin pour accéder à la destination externe.

Par exemple, si vous souhaitez répliquer des objets d'un compartiment StorageGRID vers un compartiment Amazon S3, vous créez un point de terminaison de services de plateforme qui inclut les informations et les informations d'identification dont StorageGRID a besoin pour accéder au compartiment de destination sur Amazon.

Chaque type de service de plateforme nécessite son propre point de terminaison. Vous devez donc configurer au moins un point de terminaison pour chaque service de plateforme que vous prévoyez d'utiliser. Après avoir défini un point de terminaison de services de plateforme, vous utilisez l'URN du point de terminaison comme destination dans le XML de configuration utilisé pour activer le service.

Vous pouvez utiliser le même point de terminaison comme destination pour plusieurs buckets sources. Par exemple, vous pouvez configurer plusieurs buckets sources pour envoyer des métadonnées d'objet au même point de terminaison d'intégration de recherche afin de pouvoir effectuer des recherches dans plusieurs buckets. Vous pouvez également configurer un bucket source pour utiliser plusieurs points de terminaison comme cible, ce qui vous permet d'effectuer des opérations telles que l'envoi de notifications sur la création d'objets à une rubrique Amazon Simple Notification Service (Amazon SNS) et de notifications sur la suppression d'objets à une deuxième rubrique Amazon SNS.

Points de terminaison pour la réplication CloudMirror

StorageGRID prend en charge les points de terminaison de réplication qui représentent des buckets S3. Ces buckets peuvent être hébergés sur Amazon Web Services, le même déploiement StorageGRID ou un déploiement distant, ou un autre service.

Points de terminaison pour les notifications

StorageGRID prend en charge les points de terminaison Amazon SNS et Kafka. Les points de terminaison Simple Queue Service (SQS) ou AWS Lambda ne sont pas pris en charge.

Pour les points de terminaison Kafka, le protocole TLS mutuel n'est pas pris en charge. Par conséquent, si vous avez `ssl.client.auth` réglé sur `required` dans la configuration de votre courtier Kafka, cela peut entraîner des problèmes de configuration du point de terminaison Kafka.

Points de terminaison pour le service d'intégration de recherche

StorageGRID prend en charge les points de terminaison d'intégration de recherche qui représentent les clusters Elasticsearch. Ces clusters Elasticsearch peuvent être situés dans un centre de données local ou hébergés dans un cloud AWS ou ailleurs.

Le point de terminaison d'intégration de recherche fait référence à un index et un type Elasticsearch spécifiques. Vous devez créer l'index dans Elasticsearch avant de créer le point de terminaison dans StorageGRID, sinon la création du point de terminaison échouera. Vous n'avez pas besoin de créer le type avant de créer le point de terminaison. StorageGRID créera le type si nécessaire lorsqu'il envoie les

métadonnées de l'objet au point de terminaison.

Informations connexes

["Administrer StorageGRID"](#)

Spécifier l'URN pour le point de terminaison des services de la plateforme

Lorsque vous créez un point de terminaison de services de plateforme, vous devez spécifier un nom de ressource unique (URN). Vous utiliserez l'URN pour référencer le point de terminaison lorsque vous créerez un XML de configuration pour le service de plateforme. L'URN de chaque point de terminaison doit être unique.

StorageGRID valide les points de terminaison des services de la plateforme au fur et à mesure que vous les créez. Avant de créer un point de terminaison de services de plateforme, confirmez que la ressource spécifiée dans le point de terminaison existe et qu'elle est accessible.

éléments URN

L'URN d'un point de terminaison de services de plateforme doit commencer par `arn:aws` ou `urn:mysite`, comme suit :

- Si le service est hébergé sur Amazon Web Services (AWS), utilisez `arn:aws`
- Si le 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 d'un point de terminaison CloudMirror hébergé sur StorageGRID, l'URN peut commencer par `urn:sgws`.

L'élément suivant de l'URN spécifie le type de service de plateforme, comme suit :

Service	Type
Réplication CloudMirror	s3
Notifications	sns`ou `kafka
Intégration de la recherche	es

Par exemple, pour continuer à spécifier l'URN d'un point de terminaison CloudMirror hébergé sur StorageGRID, vous devez ajouter `s3` obtenir `urn:sgws:s3`.

L'élément final de l'URN identifie la ressource cible spécifique à l'URI de destination.

Service	Ressource spécifique
Réplication CloudMirror	bucket-name
Notifications	sns-topic-name`ou `kafka-topic-name

Service	Ressource spécifique
Intégration de la recherche	domain-name/index-name/type-name Remarque : si le cluster Elasticsearch n'est pas configuré pour créer des index automatiquement, vous devez créer l'index manuellement avant de créer le point de terminaison.

URN 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 point de terminaison d'intégration de recherche AWS, le domain-name doit inclure la chaîne littérale domain/ , comme indiqué ici.

URN pour les services hébergés localement

Lorsque vous utilisez des services hébergés localement au lieu de services cloud, vous pouvez spécifier l'URN de toute manière qui crée un URN valide et unique, à condition que l'URN inclue les éléments requis dans les troisième et dernière positions. Vous pouvez laisser les éléments indiqués par facultatif vides, ou vous pouvez les spécifier de toute manière qui vous aide à identifier la ressource et à rendre l'URN unique. Par exemple:

- Réplication CloudMirror :

```
urn:mysite:s3:optional:optional:bucket-name
```

Pour un point de terminaison CloudMirror hébergé sur StorageGRID, vous pouvez spécifier un URN valide qui commence par urn:sgws :

```
urn:sgws:s3:optional:optional:bucket-name
```

- Notifications:

Spécifiez un point de terminaison Amazon Simple Notification Service :

```
urn:mysite:sns:optional:optional:sns-topic-name
```

Spécifiez un point de terminaison Kafka :

```
urn:mysite:kafka:optional:optional:kafka-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 à condition que l'URN du point de terminaison soit unique.

Créer un point de terminaison des services de plateforme

Vous devez créer au moins un point de terminaison du type correct avant de pouvoir activer un service de plateforme.

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un ["navigateur Web pris en charge"](#) .
- Les services de plateforme ont été activés pour votre compte locataire par un administrateur StorageGRID .
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Gérer les points de terminaison ou l'autorisation d'accès root"](#) .
- La ressource référencée par le point de terminaison des services de la plateforme a été créée :
 - Réplication CloudMirror : compartiment S3
 - Notification d'événement : Amazon Simple Notification Service (Amazon SNS) ou rubrique Kafka
 - Notification de recherche : index Elasticsearch, si le cluster de destination n'est pas configuré pour créer automatiquement des index.
- Vous avez les informations sur la ressource de destination :
 - Hôte et port pour l'identifiant de ressource uniforme (URI)



Si vous prévoyez d'utiliser un bucket 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)

"Spécifier l'URN pour le point de terminaison des services de la plateforme"

- Informations d'authentification (si nécessaire) :

Points de terminaison d'intégration de recherche

Pour les points de terminaison d'intégration de recherche, vous pouvez utiliser les informations d'identification suivantes :

- Clé d'accès : ID de clé d'accès et clé d'accès secrète
- HTTP de base : nom d'utilisateur et mot de passe

Points de terminaison de réplication CloudMirror

Pour les points de terminaison de réplication CloudMirror, vous pouvez utiliser les informations d'identification suivantes :

- Clé d'accès : ID de clé d'accès et clé d'accès secrète
- CAP (portail d'accès C2S) : URL d'informations d'identification temporaires, certificats serveur et client, clés client et une phrase secrète de clé privée client facultative.

Points de terminaison Amazon SNS

Pour les points de terminaison Amazon SNS, vous pouvez utiliser les informations d'identification suivantes :

- Clé d'accès : ID de clé d'accès et clé d'accès secrète

Points de terminaison Kafka

Pour les points de terminaison Kafka, vous pouvez utiliser les informations d'identification suivantes :

- SASL/PLAIN : Nom d'utilisateur et mot de passe
- SASL/SCRAM-SHA-256 : Nom d'utilisateur et mot de passe
- SASL/SCRAM-SHA-512 : Nom d'utilisateur et mot de passe

- Certificat de sécurité (si vous utilisez un certificat CA personnalisé)

- Si les fonctionnalités de sécurité Elasticsearch sont activées, vous disposez du privilège de surveillance du cluster pour les tests de connectivité, ainsi que du privilège d'écriture d'index ou des privilèges d'index et de suppression d'index pour les mises à jour de documents.

Étapes

1. Sélectionnez **STOCKAGE (S3) > Points de terminaison des services de plateforme**. La page Points de terminaison des services de la plateforme s'affiche.
2. Sélectionnez **Créer un point de terminaison**.
3. Saisissez un nom d'affichage pour décrire brièvement le point de terminaison et son objectif.

Le type de service de plateforme pris en charge par le point de terminaison est affiché à côté du nom du point de terminaison lorsqu'il est répertorié sur la page Points de terminaison. Vous n'avez donc pas besoin d'inclure ces informations dans le nom.

4. Dans le champ **URI**, spécifiez l'identifiant de ressource unique (URI) du point de terminaison.

Utilisez l'un des formats suivants :

```
https://host:port  
http://host:port
```

Si vous ne spécifiez pas de port, les ports par défaut suivants sont utilisés :

- Port 443 pour les URI HTTPS et port 80 pour les URI HTTP (la plupart des points de terminaison)
- Port 9092 pour les URI HTTPS et HTTP (points de terminaison Kafka uniquement)

Par exemple, l'URI d'un bucket hébergé sur StorageGRID pourrait être :

```
https://s3.example.com:10443
```

Dans cet exemple, `s3.example.com` représente l'entrée DNS pour l'IP virtuelle (VIP) du groupe haute disponibilité (HA) StorageGRID , et `10443` représente le port défini dans le point de terminaison de l'équilibreur de charge.



Dans la mesure du possible, vous devez vous connecter à un groupe HA de nœuds d'équilibrage de charge pour éviter un point de défaillance unique.

De même, l'URI d'un bucket hébergé sur AWS pourrait être :

```
https://s3-aws-region.amazonaws.com
```



Si le point de terminaison est utilisé pour le service de réplication CloudMirror, n'incluez pas le nom du bucket dans l'URI. Vous incluez le nom du bucket dans le champ **URN**.

5. Saisissez le nom de ressource unique (URN) pour le point de terminaison.



Vous ne pouvez pas modifier l'URN d'un point de terminaison une fois le point de terminaison créé.

6. Sélectionnez **Continuer**.

7. Sélectionnez une valeur pour **Type d'authentification**.

Points de terminaison d'intégration de recherche

Saisissez ou téléchargez les informations d'identification d'un point de terminaison d'intégration de recherche.

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 points de terminaison dont la sécurité est désactivée.	Aucune authentification.
Clé d'accès	Utilise les informations d'identification de style AWS pour authentifier les connexions avec la destination.	• ID de la 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

Points de terminaison de réplication CloudMirror

Saisissez ou téléchargez les informations d'identification d'un point de terminaison de réplication CloudMirror.

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 points de terminaison dont la sécurité est désactivée.	Aucune authentification.
Clé d'accès	Utilise les informations d'identification de style AWS pour authentifier les connexions avec la destination.	• ID de la clé d'accès • Clé d'accès secrète

Type d'authentification	Description	Informations d'identification
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 d'autorité de certification du serveur (téléchargement de fichier PEM) • Certificat client (téléchargement de fichier PEM) • Clé privée du client (téléchargement de fichier PEM, format crypté OpenSSL ou format de clé privée non cryptée) • Mot de passe de la clé privée du client (facultatif)

Points de terminaison Amazon SNS

Saisissez ou téléchargez les informations d'identification d'un point de terminaison Amazon SNS.

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 points de terminaison dont la sécurité est désactivée.	Aucune authentification.
Clé d'accès	Utilise les informations d'identification de style AWS pour authentifier les connexions avec la destination.	• ID de la clé d'accès • Clé d'accès secrète

Points de terminaison Kafka

Saisissez ou téléchargez les informations d'identification d'un point de terminaison Kafka.

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 points de terminaison dont la sécurité est désactivée.	Aucune authentification.

Type d'authentification	Description	Informations d'identification
SASL/PLAIN	Utilise un nom d'utilisateur et un mot de passe en texte brut pour authentifier les connexions à la destination.	- Nom d'utilisateur - Mot de passe
SASL/SCRAM-SHA-256	Utilise un nom d'utilisateur et un mot de passe à l'aide d'un protocole de défi-réponse et d'un hachage SHA-256 pour authentifier les connexions à la destination.	- Nom d'utilisateur - Mot de passe
SASL/SCRAM-SHA-512	Utilise un nom d'utilisateur et un mot de passe à l'aide d'un protocole de défi-réponse et d'un hachage SHA-512 pour authentifier les connexions à la destination.	- Nom d'utilisateur - Mot de passe

Sélectionnez **Utiliser l'authentification par délégation** si le nom d'utilisateur et le mot de passe sont dérivés d'un jeton de délégation obtenu à partir d'un cluster Kafka.

8. Sélectionnez **Continuer**.

9. Sélectionnez un bouton radio pour **Vérifier le serveur** pour choisir comment la connexion TLS au point de terminaison est vérifiée.

Type de vérification du certificat	Description
Utiliser un certificat CA 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 Grid CA par défaut installé sur le système d'exploitation pour sécuriser les connexions.
Ne pas vérifier le certificat	Le certificat utilisé pour la connexion TLS n'est pas vérifié. Cette option n'est pas sécurisée.

10. Sélectionnez **Tester et créer un point de terminaison**.

- Un message de réussite s'affiche si le point de terminaison peut être atteint à l'aide des informations d'identification spécifiées. La connexion au point de terminaison est validée à partir d'un nœud sur chaque site.
- Un message d'erreur s'affiche si la validation du point de terminaison échoue. Si vous devez modifier le point de terminaison pour corriger l'erreur, sélectionnez **Retour aux détails du point de terminaison** et mettez à jour les informations. Ensuite, sélectionnez **Tester et créer un point de terminaison**.



La création du point de terminaison échoue si les services de plateforme ne sont pas activés pour votre compte locataire. Contactez votre administrateur StorageGRID .

Après avoir configuré un point de terminaison, vous pouvez utiliser son URN pour configurer un service de plateforme.

Informations connexes

- ["Spécifier l'URN pour le point de terminaison des services de la plateforme"](#)
- ["Configurer la réplication CloudMirror"](#)
- ["Configurer les notifications d'événements"](#)
- ["Configurer le service d'intégration de recherche"](#)

Tester la connexion pour le point de terminaison des services de la plateforme

Si la connexion à un service de plateforme a changé, vous pouvez tester la connexion pour le point de terminaison afin de valider que la ressource de destination existe et qu'elle est accessible à l'aide des informations d'identification que vous avez spécifiées.

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un ["navigateur Web pris en charge"](#) .
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Gérer les points de terminaison ou l'autorisation d'accès root"](#) .

À propos de cette tâche

StorageGRID ne valide pas que les informations d'identification disposent des autorisations correctes.

Étapes

1. Sélectionnez **STOCKAGE (S3) > Points de terminaison des services de plateforme**.

La page Points de terminaison des services de plateforme s'affiche et affiche la liste des points de terminaison des services de plateforme qui ont déjà été configurés.

2. Sélectionnez le point de terminaison dont vous souhaitez tester la connexion.

La page des détails du point de terminaison s'affiche.

3. Sélectionnez **Tester la connexion**.

- Un message de réussite s'affiche si le point de terminaison peut être atteint à l'aide des informations d'identification spécifiées. La connexion au point de terminaison est validée à partir d'un nœud sur chaque site.
- Un message d'erreur s'affiche si la validation du point de terminaison échoue. Si vous devez modifier le point de terminaison pour corriger l'erreur, sélectionnez **Configuration** et mettez à jour les informations. Ensuite, sélectionnez **Tester et enregistrer les modifications**.

Modifier le point de terminaison des services de la plateforme

Vous pouvez modifier la configuration d'un point de terminaison de services de plateforme pour modifier son nom, son URI ou d'autres détails. Par exemple, vous devrez peut-être mettre à jour des informations d'identification expirées ou modifier l'URI pour

pointer vers un index Elasticsearch de sauvegarde pour le basculement. Vous ne pouvez pas modifier l'URN d'un point de terminaison de services de plateforme.

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un ["navigateur Web pris en charge"](#) .
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Gérer les points de terminaison ou l'autorisation d'accès root"](#) .

Étapes

1. Sélectionnez **STOCKAGE (S3) > Points de terminaison des services de plateforme**.

La page Points de terminaison des services de plateforme s'affiche et affiche la liste des points de terminaison des services de plateforme qui ont déjà été configurés.

2. Sélectionnez le point de terminaison que vous souhaitez modifier.

La page des détails du point de terminaison s'affiche.

3. Sélectionnez **Configuration**.
4. Selon les besoins, modifiez la configuration du point de terminaison.



Vous ne pouvez pas modifier l'URN d'un point de terminaison une fois le point de terminaison créé.

- a. Pour modifier le nom d'affichage du point de terminaison, sélectionnez l'icône de modification  .
- b. Si nécessaire, modifiez l'URL.
- c. Si nécessaire, modifiez le type d'authentification.
 - Pour l'authentification par clé d'accès, modifiez la clé si nécessaire en sélectionnant **Modifier la clé S3** et en collant un nouvel ID de clé d'accès et une clé d'accès secrète. Si vous devez annuler vos modifications, sélectionnez **Annuler la modification de la clé S3**.
 - Pour l'authentification CAP (portail d'accès C2S), modifiez l'URL des informations d'identification temporaires ou la phrase secrète de la clé privée facultative du client et téléchargez de nouveaux fichiers de certificat et de clé selon les besoins.



La clé privée du client doit être au format crypté OpenSSL ou au format de clé privée non cryptée.

- 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 point de terminaison peut être atteint à l'aide des informations d'identification spécifiées. La connexion au point de terminaison est vérifiée à partir d'un nœud sur chaque site.
 - Un message d'erreur s'affiche si la validation du point de terminaison échoue. Modifiez le point de terminaison pour corriger l'erreur, puis sélectionnez **Tester et enregistrer les modifications**.

Supprimer le point de terminaison des services de la plateforme

Vous pouvez supprimer un point de terminaison si vous ne souhaitez plus utiliser le service de plateforme associé.

Avant de commencer

- Vous êtes connecté au Tenant Manager à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Gérer les points de terminaison ou l'autorisation d'accès root"](#).

Étapes

1. Sélectionnez **STOCKAGE (S3) > Points de terminaison des services de plateforme**.

La page Points de terminaison des services de plateforme s'affiche et affiche la liste des points de terminaison des services de plateforme qui ont déjà été configurés.

2. Cochez la case correspondant à chaque point de terminaison que vous souhaitez supprimer.



Si vous supprimez un point de terminaison de services de plateforme en cours d'utilisation, le service de plateforme associé sera désactivé pour tous les buckets qui utilisent le point de terminaison. Toutes les demandes qui n'ont pas encore été traitées seront abandonnées. Toutes les nouvelles demandes continueront d'être générées jusqu'à ce que vous modifiez la configuration de votre bucket pour ne plus référencer l'URN supprimée. StorageGRID signalera ces demandes comme des erreurs irrécupérables.

3. Sélectionnez **Actions > Supprimer le point de terminaison**.

Un message de confirmation apparaît.

4. Sélectionnez **Supprimer le point de terminaison**.

Résoudre les erreurs de point de terminaison des services de plateforme

Si une erreur se produit lorsque StorageGRID tente de communiquer avec un point de terminaison de services de plateforme, un message s'affiche sur le tableau de bord. Sur la page Points de terminaison des services de la plateforme, la colonne Dernière erreur indique depuis combien de temps l'erreur s'est produite. Aucune erreur ne s'affiche si les autorisations associées aux informations d'identification d'un point de terminaison sont incorrectes.

Déterminer si une erreur s'est produite

Si des erreurs de point de terminaison des 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 Points de terminaison des services de la plateforme pour voir plus de détails sur l'erreur.



One or more endpoints have experienced an error and might not be functioning properly. Go to the [Endpoints](#) page to view the error details. The last error occurred 2 hours ago.

La même erreur qui apparaît sur le tableau de bord apparaît également en haut de la page Points de terminaison des services de la plateforme. Pour afficher un message d'erreur plus détaillé :

Étapes

1. Dans la liste des points de terminaison, sélectionnez le point de terminaison qui présente l'erreur.
2. Sur la page des détails du point de terminaison, sélectionnez **Connexion**. Cet onglet affiche uniquement

l'erreur la plus récente pour un point de terminaison et indique depuis combien de temps l'erreur s'est produite. Erreurs qui incluent l'icône X rouge  survenu au cours des 7 derniers jours.

Vérifiez si l'erreur est toujours d'actualité

Certaines erreurs peuvent continuer à s'afficher dans la colonne **Dernière erreur** même après avoir été résolues. Pour voir si une erreur est actuelle ou pour forcer la suppression d'une erreur résolue du tableau :

Étapes

1. Sélectionnez le point de terminaison.

La page des détails du point de terminaison s'affiche.

2. Sélectionnez **Connexion > Tester la connexion**.

La sélection de **Tester la connexion** amène StorageGRID à valider que le point de terminaison des services de la plateforme existe et qu'il est accessible avec les informations d'identification actuelles. La connexion au point de terminaison est validée à partir d'un nœud sur chaque site.

Résoudre les erreurs de point de terminaison

Vous pouvez utiliser le message **Dernière erreur** sur la page des détails du point de terminaison pour vous aider à déterminer la cause de l'erreur. Certaines erreurs peuvent nécessiter de modifier le point de terminaison pour résoudre le problème. Par exemple, une erreur CloudMirroring peut se produire si StorageGRID ne peut pas accéder au bucket S3 de destination car il ne dispose pas des autorisations d'accès appropriées ou si la clé d'accès a expiré. Le message est « Les informations d'identification du point de terminaison ou l'accès à la destination doivent être mis à jour » et les détails sont « AccessDenied » ou « InvalidAccessKeyId ».

Si vous devez modifier le point de terminaison pour résoudre une erreur, la sélection de **Tester et enregistrer les modifications** amène StorageGRID à valider le point de terminaison mis à jour et à confirmer qu'il est accessible avec les informations d'identification actuelles. La connexion au point de terminaison est validée à partir d'un nœud sur chaque site.

Étapes

1. Sélectionnez le point de terminaison.
2. Sur la page des détails du point de terminaison, sélectionnez **Configuration**.
3. Modifiez la configuration du point de terminaison selon vos besoins.
4. Sélectionnez **Connexion > Tester la connexion**.

Informations d'identification du point de terminaison avec des autorisations insuffisantes

Lorsque StorageGRID valide un point de terminaison de services de plateforme, il confirme que les informations d'identification du point de terminaison peuvent être utilisées pour contacter la ressource de destination et effectue une vérification des 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 lorsque vous tentez d'utiliser un service de plateforme (par exemple « 403 Forbidden »), vérifiez les autorisations associées aux informations d'identification du point de terminaison.

Informations connexes

- [Administrer StorageGRID > Résoudre les problèmes des services de la plateforme](#)

- ["Créer un point de terminaison des services de plateforme"](#)
- ["Tester la connexion pour le point de terminaison des services de la plateforme"](#)
- ["Modifier le point de terminaison des services de la plateforme"](#)

Configurer la réplication CloudMirror

Pour activer la réplication CloudMirror pour un bucket, vous créez et appliquez un XML de configuration de réplication de bucket valide.

Avant de commencer

- Les services de plateforme ont été activés pour votre compte locataire par un administrateur StorageGRID.
- Vous avez déjà créé un bucket pour servir de source de réplication.
- Le point de terminaison que vous souhaitez utiliser comme destination pour la réplication CloudMirror existe déjà et vous disposez de son URN.
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Gérer tous les buckets ou l'autorisation d'accès root"](#). Ces autorisations remplacent les paramètres d'autorisation dans les stratégies de groupe ou de compartiment lors de la configuration du compartiment à l'aide du gestionnaire de locataires.

À propos de cette tâche

La réplication CloudMirror copie les objets d'un bucket source vers un bucket de destination spécifié dans un point de terminaison.

Pour obtenir des informations générales sur la réplication de bucket et comment la configurer, consultez ["Documentation Amazon Simple Storage Service \(S3\) : Réplication d'objets"](#). Pour plus d'informations sur la manière dont StorageGRID implémente GetBucketReplication, DeleteBucketReplication et PutBucketReplication, consultez le ["Opérations sur les godets"](#).



La réplication CloudMirror présente des similitudes et des différences importantes avec la fonctionnalité de réplication inter-grille. Pour en savoir plus, voir ["Comparer la réplication inter-grille et la réplication CloudMirror"](#).

Notez les exigences et caractéristiques suivantes lors de la configuration de la réplication CloudMirror :

- Lorsque vous créez et appliquez un XML de configuration de réplication de compartiment valide, il doit utiliser l'URN d'un point de terminaison de compartiment S3 pour chaque destination.
- La réplication n'est pas prise en charge pour les buckets source ou de destination avec le verrouillage d'objet S3 activé.
- Si vous activez la réplication CloudMirror sur un bucket contenant des objets, les nouveaux objets ajoutés au bucket sont répliqués, mais les objets existants dans le bucket ne sont pas répliqués. Vous devez mettre à jour les objets existants pour déclencher la réplication.
- Si vous spécifiez une classe de stockage dans le XML de configuration de réplication, StorageGRID utilise cette classe lors de l'exécution d'opérations sur le point de terminaison S3 de destination. Le point de terminaison de destination doit également prendre en charge la classe de stockage spécifiée. Assurez-vous de suivre toutes les recommandations fournies par le fournisseur du système de destination.

Étapes

1. Activer la réplication pour votre bucket 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 la version V1 de la configuration de réplication. Cela signifie que StorageGRID ne prend pas en charge l'utilisation du `Filter` élément pour les règles et suit les conventions V1 pour la suppression des versions d'objet. Consultez la documentation Amazon sur la configuration de la réplication pour plus de détails.
- Utilisez l'URN d'un point de terminaison de compartiment S3 comme destination.
- Ajoutez éventuellement le `<StorageClass>` élément et spécifiez l'un des éléments suivants :
 - `STANDARD`: La classe de stockage par défaut. Si vous ne spécifiez pas de classe de stockage lorsque vous téléchargez 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 on accède moins fréquemment, mais qui nécessitent néanmoins un accès rapide en cas de besoin.
 - `REDUCED_REDUNDANCY`: Utilisez cette classe de stockage pour les données non critiques et reproductibles qui peuvent être stockées avec moins de redondance que les `STANDARD` classe de stockage.
- Si vous spécifiez un `Role` dans la configuration XML, 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 buckets** dans le tableau de bord ou sélectionnez **STOCKAGE (S3) > Buckets**.
3. Sélectionnez le nom du bucket source.

La page des détails du bucket apparaît.

4. Sélectionnez **Services de plateforme > Réplication**.
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 Grid Management. Contactez votre administrateur StorageGRID si une erreur se produit lorsque vous enregistrez le XML de configuration.

7. Vérifiez que la réplication est correctement configurée :

- a. Ajoutez un objet au bucket source qui répond aux exigences de réplication telles que spécifiées dans la configuration de réplication.

Dans l'exemple présenté précédemment, les objets correspondant au préfixe « 2020 » sont répliqués.

- b. Confirmez que l'objet a été répliqué dans le bucket de destination.

Pour les petits objets, la réplication se produit rapidement.

Informations connexes

["Créer un point de terminaison des services de plateforme"](#)

Configurer les notifications d'événements

Vous activez les notifications pour un bucket en créant un XML de configuration de notification et en utilisant le gestionnaire de locataires pour appliquer le XML à un bucket.

Avant de commencer

- Les services de plateforme ont été activés pour votre compte locataire par un administrateur StorageGRID .
- Vous avez déjà créé un bucket pour servir de source de notifications.
- Le point de terminaison que vous souhaitez utiliser comme destination pour les notifications d'événements existe déjà et vous disposez de son URN.
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Gérer tous les buckets ou l'autorisation d'accès root"](#) . Ces autorisations remplacent les paramètres d'autorisation dans les stratégies de groupe ou de compartiment lors de la configuration du compartiment à l'aide du gestionnaire de locataires.

À propos de cette tâche

Vous configurez les notifications d'événements en associant le XML de configuration de notification à un bucket source. Le XML de configuration de notification suit les conventions S3 pour la configuration des notifications de compartiment, avec la rubrique de destination Kafka ou Amazon SNS spécifiée comme URN d'un point de terminaison.

Pour obtenir des informations générales sur les notifications d'événements et comment les configurer, reportez-vous à la ["Documentation Amazon"](#) . Pour plus d'informations sur la manière dont StorageGRID implémente l'API de configuration des notifications de compartiment S3, reportez-vous à la ["instructions pour la mise en œuvre des applications clientes S3"](#) .

Notez les exigences et caractéristiques suivantes lors de la configuration des notifications d'événements pour un bucket :

- Lorsque vous créez et appliquez un XML de configuration de notification valide, il doit utiliser l'URN d'un point de terminaison de notifications d'événements pour chaque destination.
- Bien que la notification d'événement puisse être configurée sur un bucket avec le verrouillage d'objet S3 activé, les métadonnées du verrouillage d'objet S3 (y compris la date de conservation et le statut de conservation légale) des objets ne seront pas incluses dans les messages de notification.
- Une fois que vous avez 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 Amazon SNS ou Kafka utilisée comme point de terminaison de destination.

- Si vous activez les notifications d'événements pour un compartiment contenant des objets, les notifications sont envoyées uniquement pour les actions effectuées après l'enregistrement de la configuration de notification.

Étapes

1. Activer les notifications pour votre bucket source :

- Utilisez un éditeur de texte pour créer le XML de configuration de notification requis pour activer les notifications d'événements, comme spécifié dans l'API de notification S3.
- Lors de la configuration du XML, utilisez l'URN d'un point de terminaison de notifications d'événements comme rubrique 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 **STOCKAGE (S3) > Buckets**.

3. Sélectionnez le nom du bucket source.

La page des détails du bucket apparaît.

4. Sélectionnez **Services de plateforme > Notifications d'événements**.

5. Cochez la case **Activer les notifications d'événements**.

6. Collez le XML de configuration de notification 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 Grid Management. Contactez votre administrateur StorageGRID si une erreur se produit lorsque vous enregistrez le XML de configuration.

7. Vérifiez que les notifications d'événements sont correctement configurées :

- a. Exécutez une action sur un objet dans le bucket source qui répond aux exigences de déclenchement d'une notification telle que configurée dans le 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 Amazon SNS ou Kafka de destination.

Par exemple, si votre rubrique de destination est hébergée sur Amazon SNS, vous pouvez configurer le service pour qu'il vous envoie un e-mail lorsque la notification est envoyée.

```
{
  "Records": [
    {
      "eventVersion": "2.0",
      "eventSource": "sgws:s3",
      "eventTime": "2017-08-08T23:52:38Z",
      "eventName": "ObjectCreated:Put",
      "userIdentity": {
        "principalId": "11111111111111111111"
      },
      "requestParameters": {
        "sourceIPAddress": "193.51.100.20"
      },
      "responseElements": {
        "x-amz-request-id": "122047343"
      },
      "s3": {
        "s3SchemaVersion": "1.0",
        "configurationId": "Image-created",
        "bucket": {
          "name": "test1",
          "ownerIdentity": {
            "principalId": "11111111111111111111"
          },
          "arn": "arn:sgws:s3:::test1"
        },
        "object": {
          "key": "images/cat.jpg",
          "size": 0,
          "eTag": "d41d8cd98f00b204e9800998ecf8427e",
          "sequencer": "14D90402421461C7"
        }
      }
    }
  ]
}
```

+

Si la notification est reçue sur la rubrique de destination, vous avez correctement configuré votre bucket

source pour les notifications StorageGRID .

Informations connexes

["Comprendre les notifications pour les buckets"](#)

["Utiliser l'API REST S3"](#)

["Créer un point de terminaison des services de plateforme"](#)

Configurer le service d'intégration de recherche

Vous activez l'intégration de recherche pour un bucket en créant un XML d'intégration de recherche et en utilisant le gestionnaire de locataires pour appliquer le XML au bucket.

Avant de commencer

- Les services de plateforme ont été activés pour votre compte locataire par un administrateur StorageGRID .
- Vous avez déjà créé un bucket S3 dont vous souhaitez indexer le contenu.
- Le point de terminaison que vous souhaitez utiliser comme destination pour le service d'intégration de recherche existe déjà et vous disposez de son URN.
- Vous appartenez à un groupe d'utilisateurs qui possède le ["Gérer tous les buckets ou l'autorisation d'accès root"](#) . Ces autorisations remplacent les paramètres d'autorisation dans les stratégies de groupe ou de compartiment lors de la configuration du compartiment à l'aide du gestionnaire de locataires.

À propos de cette tâche

Une fois que vous avez configuré le service d'intégration de recherche pour un bucket source, la création d'un objet ou la mise à jour des métadonnées ou des balises d'un objet déclenche l'envoi des métadonnées de l'objet au point de terminaison de destination.

Si vous activez le service d'intégration de recherche pour un bucket qui contient déjà des objets, les notifications de métadonnées ne sont pas automatiquement envoyées pour les objets existants. Mettez à jour ces objets existants pour garantir que leurs métadonnées sont ajoutées à l'index de recherche de destination.

Étapes

1. Activer l'intégration de la recherche pour un bucket :

- Utilisez un éditeur de texte pour créer le XML de notification de métadonnées requis pour activer l'intégration de la recherche.
- Lors de la configuration du XML, utilisez l'URN d'un point de terminaison d'intégration de recherche comme destination.

Les objets peuvent être filtrés sur le préfixe du nom de l'objet. Par exemple, vous pouvez envoyer des métadonnées pour des objets avec le préfixe `images` vers une destination et des métadonnées pour les objets avec le préfixe `videos` à un autre. Les configurations dont les préfixes 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 deuxième règle pour les objets avec le préfixe `test2` n'est pas autorisé.

Au besoin, reportez-vous à [laexemples pour la configuration des métadonnées XML](#) .

```

<MetadataNotificationConfiguration>
  <Rule>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
      <Urn>/Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>

```

Éléments dans le XML de configuration des notifications de métadonnées :

Nom	Description	Obligatoire
Configuration des notifications de métadonnées	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 pour 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 MetadataNotificationConfiguration.	Oui
ID	Identifiant unique de la règle. Inclus dans l'élément Règle.	Non
Statut	Le statut peut être « Activé » ou « Désactivé ». Aucune action n'est entreprise 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

Nom	Description	Obligatoire
Urne	URN de la destination où les métadonnées de l'objet sont envoyées. Doit être l'URN d'un point de terminaison 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 <code>domain-name/myindex/mytype</code>. Les points de terminaison sont configurés à l'aide de l'API Tenant Manager ou Tenant Management. Ils prennent la forme suivante : • <code>arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype</code> • <code>urn:mystore:es:::mydomain/myindex/mytype</code> Le point de terminaison doit être configuré avant que le XML de configuration ne soit soumis, sinon la configuration échouera avec une erreur 404. L'URN est incluse dans l'élément Destination.	Oui

2. Dans le gestionnaire de locataires, sélectionnez **STOCKAGE (S3) > Compartiments**.

3. Sélectionnez le nom du bucket source.

La page des détails du bucket apparaît.

4. Sélectionnez **Services de plateforme > Intégration de recherche**

5. Cochez la case **Activer l'intégration de la recherche**.

6. Collez la configuration de notification des métadonnées 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. Contactez votre administrateur StorageGRID si une erreur se produit lorsque vous enregistrez le XML de configuration.

7. Vérifiez que le service d'intégration de recherche est correctement configuré :

- Ajoutez un objet au bucket source qui répond aux exigences de déclenchement d'une notification de métadonnées comme spécifié dans le XML de configuration.

Dans l'exemple présenté précédemment, tous les objets ajoutés au bucket déclenchent une notification de métadonnées.

- Confirmez qu'un document JSON contenant les métadonnées et les balises de l'objet a été ajouté à l'index de recherche spécifié dans le point de terminaison.

Après avoir terminé

Si nécessaire, vous pouvez désactiver l'intégration de la recherche pour un bucket en utilisant l'une des méthodes suivantes :

- Sélectionnez **STOCKAGE (S3) > Compartiments** et décochez la case **Activer l'intégration de la recherche**.
- Si vous utilisez directement l'API S3, utilisez une demande de notification de métadonnées DELETE Bucket. Consultez les instructions pour implémenter les applications clientes S3.

Exemple : Configuration de notification de métadonnées qui s'applique à tous les objets

Dans cet exemple, les métadonnées d'objet pour 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>
```

Exemple : Configuration de notification de métadonnées avec deux règles

Dans cet exemple, les métadonnées d'objet pour les objets qui correspondent au préfixe `/images` est envoyé à une destination, tandis que les métadonnées d'objet pour les objets qui correspondent au préfixe `/videos` est envoyé vers une deuxième 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-1:2222222:domain/es-
domain/graphics/videotype</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>

```

Format de notification des métadonnées

Lorsque vous activez le service d'intégration de recherche pour un bucket, un document JSON est généré et envoyé au point de terminaison de destination chaque fois que des métadonnées ou des balises d'objet sont ajoutées, mises à jour ou supprimées.

Cet exemple montre un exemple de JSON qui pourrait être généré lorsqu'un objet avec la clé SGWS/Tagging.txt est créé dans un bucket nommé test . Le test le bucket n'est pas versionné, donc le versionId la balise 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"
  }
}
```

Champs inclus dans le document JSON

Le nom du document inclut le nom du bucket, le nom de l'objet et l'ID de version s'il est présent.

Informations sur le bucket et l'objet

bucket: Nom du bucket

key: Nom de la clé de l'objet

versionID: Version de l'objet, pour les objets dans les buckets versionnés

region: Région de bucket, par exemple us-east-1

Métadonnées du système

size: Taille de l'objet (en octets) telle que visible par un client HTTP

md5: Hachage d'objet

Métadonnées de l'utilisateur

metadata: Toutes les métadonnées utilisateur pour l'objet, sous forme de paires clé-valeur

key: valeur

Mots-clés

tags: Toutes les balises d'objet définies pour l'objet, sous forme de paires clé-valeur

key: valeur

Comment afficher les résultats dans Elasticsearch

Pour les balises et les métadonnées utilisateur, StorageGRID transmet des dates et des nombres à Elasticsearch sous forme de chaînes ou de notifications d'événements S3. Pour configurer Elasticsearch afin

d'interpréter ces chaînes comme des dates ou des nombres, suivez les instructions Elasticsearch pour le mappage de champs dynamiques et pour le mappage des formats de date. Activez les mappages de champs dynamiques sur l'index avant de configurer le service d'intégration de recherche. Une fois qu'un document est indexé, vous ne pouvez pas modifier les types de champs du document dans l'index.

Utiliser 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 sous la forme d'un ensemble de services Web Representational State Transfer (REST).

La prise en charge de l'API REST S3 vous permet de connecter des applications orientées services développées pour les services Web S3 avec un stockage d'objets sur site qui utilise le système StorageGRID . Des modifications minimales sont requises dans l'utilisation actuelle des appels d'API REST S3 par une application cliente.

Versions prises en charge

StorageGRID prend en charge les versions spécifiques suivantes de S3 et HTTP.

Article	Version
Spécification de l'API S3	"Documentation Amazon Web Services (AWS) : Référence de l'API Amazon Simple Storage Service"
HTTP	1,1 Pour plus d'informations sur HTTP, consultez HTTP/1.1 (RFC 7230-35). "IETF RFC 2616 : Protocole de transfert hypertexte (HTTP/1.1)" Remarque : StorageGRID ne prend pas en charge le pipeline HTTP/1.1.

Mises à jour de la prise en charge de l'API REST S3

Libérer	Commentaires
11,9	• Ajout de la prise en charge des valeurs de somme de contrôle SHA-256 précalculées pour les requêtes suivantes et les en-têtes pris en charge. Vous pouvez utiliser cette fonctionnalité pour vérifier l'intégrité des objets téléchargés : ◦ Téléchargement complet en plusieurs parties : <code>x-amz-checksum-sha256</code> ◦ Créer un téléchargement multi-parties : <code>x-amz-checksum-algorithm</code> ◦ Obtenir l'objet : <code>x-amz-checksum-mode</code> ◦ HeadObject : <code>x-amz-checksum-mode</code> ◦ Liste des pièces ◦ PutObject : <code>x-amz-checksum-sha256</code> ◦ TéléchargerPartie : <code>x-amz-checksum-sha256</code> • Ajout de la possibilité pour l'administrateur de la grille de contrôler les paramètres de conservation et de conformité au niveau du locataire. Ces paramètres affectent les paramètres de verrouillage d'objet S3. ◦ Mode de conservation par défaut du bucket et mode de conservation des objets : Gouvernance ou Conformité, si autorisé par l'administrateur de la grille. ◦ Période de conservation par défaut du bucket et date de conservation de l'objet : doit être inférieure ou égale à ce qui est autorisé par la période de conservation maximale définie par l'administrateur de la grille. • Prise en charge améliorée pour <code>aws-chunked</code> encodage et streaming de contenu <code>x-amz-content-sha256</code> valeurs. Limites: ◦ Si présent, <code>chunk-signature</code> est facultatif et non validé ◦ Si présent, <code>x-amz-trailer</code> le contenu est ignoré
11,8	Mise à jour des noms des opérations S3 pour correspondre aux noms utilisés dans le "Documentation Amazon Web Services (AWS) : Référence de l'API Amazon Simple Storage Service" .
11,7	• Ajouté "Référence rapide : requêtes API S3 prises en charge" . • Ajout de la prise en charge de l'utilisation du mode GOUVERNANCE avec S3 Object Lock. • Ajout de la prise en charge spécifique à StorageGRID <code>x-ntap-sg-cgr-replication-status</code> en-tête de réponse pour les requêtes GET Object et HEAD Object. Cet en-tête fournit l'état de réplification d'un objet pour la réplification inter-grille. • Les requêtes SelectObjectContent prennent désormais en charge les objets Parquet.

Libérer	Commentaires
11,6	• Ajout de la prise en charge de l'utilisation du <code>partNumber</code> paramètre de requête dans les requêtes d'objet GET et d'objet HEAD. • Ajout de la prise en charge d'un mode de conservation par défaut et d'une période de conservation par défaut au niveau du bucket pour S3 Object Lock. • Ajout du support pour le <code>s3:object-lock-remaining-retention-days</code> clé de condition de politique pour définir la plage de périodes de conservation autorisées pour vos objets. • La taille maximale <i>recommandée</i> pour une seule opération d'objet PUT a été modifiée à 5 Gio (5 368 709 120 octets). Si vous avez des objets dont la taille est supérieure à 5 Gio, utilisez plutôt le téléchargement en plusieurs parties.
11,5	• Prise en charge ajoutée pour la gestion du chiffrement du bucket. • Ajout de la prise en charge du verrouillage d'objet S3 et des demandes de conformité héritées obsolètes. • Ajout de la prise en charge de l'utilisation de DELETE Multiple Objects sur des buckets versionnés. • Le <code>Content-MD5</code> l'en-tête de requête est désormais correctement pris en charge.
11,4	• Prise en charge ajoutée pour le balisage des buckets DELETE, GET et PUT. Les balises d'allocation des coûts ne sont pas prises en charge. • Pour les buckets créés dans StorageGRID 11.4, la restriction des noms de clés d'objet pour respecter les meilleures pratiques en matière de performances n'est plus nécessaire. • Ajout de la prise en charge des notifications de bucket sur le <code>s3:ObjectRestore:Post</code> type d'événement. • Les limites de taille AWS pour les pièces en plusieurs parties sont désormais appliquées. Chaque partie d'un téléchargement en plusieurs parties doit être comprise entre 5 Mio et 5 Gio. La dernière partie peut être inférieure à 5 Mio. • Ajout de la prise en charge de TLS 1.3
11,3	• Ajout de la prise en charge du chiffrement côté serveur des données d'objet avec des clés fournies par le client (SSE-C). • Prise en charge ajoutée pour les opérations de cycle de vie du bucket DELETE, GET et PUT (action d'expiration uniquement) et pour le <code>x-amz-expiration</code> en-tête de réponse. • Objet PUT mis à jour, Objet PUT - Copie et Téléchargement en plusieurs parties pour décrire l'impact des règles ILM qui utilisent le placement synchrone lors de l'ingestion. • Les chiffrements TLS 1.1 ne sont plus pris en charge.

Libérer	Commentaires
11,2	Prise en charge ajoutée pour la restauration d'objets POST à utiliser avec les pools de stockage cloud. Ajout de la prise en charge de l'utilisation de la syntaxe AWS pour l'ARN, les clés de condition de stratégie et les variables de stratégie dans les stratégies de groupe et de compartiment. Les stratégies de groupe et de compartiment existantes qui utilisent la syntaxe StorageGRID continueront d'être prises en charge. Remarque : les utilisations d'ARN/URN dans d'autres configurations JSON/XML, y compris celles utilisées dans les fonctionnalités StorageGRID personnalisées, n'ont pas changé.
11,1	Ajout de la prise en charge du partage de ressources inter-origines (CORS), du HTTP pour les connexions client S3 aux nœuds de grille et des paramètres de conformité sur les buckets.
11,0	Prise en charge ajoutée pour la configuration des services de plateforme (réplication CloudMirror, notifications et intégration de recherche Elasticsearch) pour les buckets. La prise en charge des contraintes d'emplacement de balisage d'objets pour les buckets et la cohérence disponible ont également été ajoutées.
10,4	Ajout de la prise en charge des modifications d'analyse ILM apportées au contrôle de version, aux mises à jour de la page Noms de domaine de point de terminaison, aux conditions et variables dans les politiques, aux exemples de politiques et à l'autorisation PutOverwriteObject.
10,3	Prise en charge ajoutée pour le contrôle de version.
10,2	Ajout de la prise en charge des stratégies d'accès aux groupes et aux buckets, ainsi que de la copie en plusieurs parties (Télécharger une partie - Copier).
10,1	Prise en charge ajoutée pour le téléchargement en plusieurs parties, les demandes de type hébergé virtuellement et 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 la <i>Référence API du service de stockage simple</i> est le 01/03/2006.

Référence rapide : requêtes API S3 prises en charge

Cette page résume la manière dont StorageGRID prend en charge les API Amazon Simple Storage Service (S3).

Cette page inclut uniquement les opérations S3 prises en charge par StorageGRID.



Pour voir la documentation AWS pour chaque opération, sélectionnez le lien dans l'en-tête.

Paramètres de requête URI courants et en-têtes de requête

Sauf indication contraire, les paramètres de requête URI courants suivants sont pris en charge :

- `versionId`(comme requis pour les opérations sur les objets)

Sauf indication 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 connexes

- ["Détails d'implémentation de l'API REST S3"](#)
- ["Référence de l'API Amazon Simple Storage Service : en-têtes de requête courants"](#)

"Abandonner le téléchargement en plusieurs parties"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette requête, plus ce paramètre de requête URI supplémentaire :

- `uploadId`

Corps de la requête

Aucune

Documentation de StorageGRID

["Opérations pour les téléchargements en plusieurs parties"](#)

"Téléchargement complet en plusieurs parties"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette requête, plus ce paramètre de requête URI supplémentaire :

- `uploadId`
- `x-amz-checksum-sha256`

Balises XML du corps de la requête

StorageGRID prend en charge ces balises XML de corps de requête :

- ChecksumSHA256
- CompleteMultipartUpload
- ETag
- Part
- PartNumber

Documentation de StorageGRID

["Téléchargement complet en plusieurs parties"](#)

"Copier l'objet"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette demande, plus ces en-têtes 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-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 requête

Aucune

Documentation de StorageGRID

["Copier l'objet"](#)

"Créer un bucket"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette demande, plus ces en-têtes supplémentaires :

- `x-amz-bucket-object-lock-enabled`

Corps de la requête

StorageGRID prend en charge tous les paramètres du corps de la requête définis par l'API REST Amazon S3 au moment de l'implémentation.

Documentation de StorageGRID

["Opérations sur les godets"](#)

"Créer un téléchargement multi-parties"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette demande, plus ces en-têtes supplémentaires :

- `Cache-Control`
- `Content-Disposition`
- `Content-Encoding`
- `Content-Language`
- `Expires`
- `x-amz-checksum-algorithm`
- `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 requête

Aucune

Documentation de StorageGRID

["Créer un téléchargement multi-parties"](#)

"Supprimer le bucket"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette demande.

Documentation de StorageGRID

["Opérations sur les godets"](#)

"SupprimerBucketCors"

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 requête

Aucune

Documentation de StorageGRID

["Opérations sur les godets"](#)

"Supprimer le chiffrement du bucket"

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 requête

Aucune

Documentation de StorageGRID

["Opérations sur les godets"](#)

"Supprimer le cycle de vie du bucket"

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 requête

Aucune

Documentation de StorageGRID

- ["Opérations sur les godets"](#)
- ["Créer une configuration du cycle de vie S3"](#)

"Supprimer la politique de bucket"

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 requête

Aucune

Documentation de StorageGRID

["Opérations sur les godets"](#)

"SupprimerBucketReplication"

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 requête

Aucune

Documentation de StorageGRID

["Opérations sur les godets"](#)

"Supprimer le balisage du bucket"

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 requête

Aucune

Documentation de StorageGRID

["Opérations sur les godets"](#)

"Supprimer l'objet"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette requête, plus cet en-tête de requête supplémentaire :

- `x-amz-bypass-governance-retention`

Corps de la requête

Aucune

Documentation de StorageGRID

["Opérations sur les objets"](#)

"Supprimer les objets"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette requête, plus cet en-tête de requête supplémentaire :

- `x-amz-bypass-governance-retention`

Corps de la requête

StorageGRID prend en charge tous les paramètres du corps de la requête définis par l'API REST Amazon S3 au moment de l'implémentation.

Documentation de StorageGRID

["Opérations sur les objets"](#)

"Supprimer l'étiquetage des objets"

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette demande.

Corps de la requête

Aucune

Documentation de StorageGRID

["Opérations sur les objets"](#)

"ObtenirBucketAcl"

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 requête

Aucune

Documentation de StorageGRID

["Opérations sur les godets"](#)

"ObtenirBucketCors"

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 requête

Aucune

Documentation de StorageGRID

["Opérations sur les godets"](#)

"Obtenir le chiffrement du bucket"

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 requête

Aucune

Documentation de StorageGRID

["Opérations sur les godets"](#)

"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 requête

Aucune

Documentation de StorageGRID

- ["Opérations sur les godets"](#)
- ["Créer une configuration du cycle de vie S3"](#)

"Obtenir l'emplacement du bucket"

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 requête

Aucune

Documentation de StorageGRID

["Opérations sur les godets"](#)

"Configuration de GetBucketNotification"

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 requête

Aucune

Documentation de StorageGRID

["Opérations sur les godets"](#)

"Obtenir la politique de Bucket"

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 requête

Aucune

Documentation de StorageGRID

["Opérations sur les godets"](#)

"Réplication GetBucket"

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 requête

Aucune

Documentation de StorageGRID

["Opérations sur les godets"](#)

"Obtenir le balisage du bucket"

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 requête

Aucune

Documentation de StorageGRID

["Opérations sur les godets"](#)

"Obtenir la gestion des versions du bucket"

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 requête

Aucune

Documentation de StorageGRID

["Opérations sur les godets"](#)

"Obtenir l'objet"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette requête, plus ces paramètres de requête URI supplémentaires :

- x-amz-checksum-mode
- partNumber
- response-cache-control
- response-content-disposition
- response-content-encoding
- response-content-language
- response-content-type
- response-expires

Et ces en-têtes de requête 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 requête

Aucune

Documentation de StorageGRID

["Obtenir l'objet"](#)

"ObtenirObjectAcl"

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 requête

Aucune

Documentation de StorageGRID

["Opérations sur les objets"](#)

"Obtenir la conservation légale de l'objet"

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 requête

Aucune

Documentation de StorageGRID

["Utiliser l'API REST S3 pour configurer le verrouillage d'objet S3"](#)

"Obtenir la configuration du verrouillage de l'objet"

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 requête

Aucune

Documentation de StorageGRID

["Utiliser l'API REST S3 pour configurer le verrouillage d'objet S3"](#)

"Obtenir la rétention d'objet"

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 requête

Aucune

Documentation de StorageGRID

"Utiliser l'API REST S3 pour configurer le verrouillage d'objet S3"

"Obtenir l'étiquetage des objets"

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 requête

Aucune

Documentation de StorageGRID

["Opérations sur les objets"](#)

"Tête de godet"

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 requête

Aucune

Documentation de StorageGRID

["Opérations sur les godets"](#)

"HeadObject"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette demande, plus ces en-têtes supplémentaires :

- x-amz-checksum-mode
- 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 requête

Aucune

Documentation de StorageGRID

["HeadObject"](#)

"Listes de seaux"

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 requête

Aucune

Documentation de StorageGRID

[Opérations sur le service](#) › [ListBuckets](#)

"ListeMultipartUploads"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette requête, plus ces paramètres supplémentaires :

- `encoding-type`
- `key-marker`
- `max-uploads`
- `prefix`
- `upload-id-marker`

Corps de la requête

Aucune

Documentation de StorageGRID

["ListeMultipartUploads"](#)

"Liste d'objets"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette requête, plus ces paramètres supplémentaires :

- `delimiter`
- `encoding-type`
- `marker`
- `max-keys`
- `prefix`

Corps de la requête

Aucune

Documentation de StorageGRID

["Opérations sur les godets"](#)

"ListObjectsV2"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette requête, plus ces paramètres supplémentaires :

- continuation-token
- delimiter
- encoding-type
- fetch-owner
- max-keys
- prefix
- start-after

Corps de la requête

Aucune

Documentation de StorageGRID

["Opérations sur les godets"](#)

"ListObjectVersions"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette requête, plus ces paramètres supplémentaires :

- delimiter
- encoding-type
- key-marker
- max-keys
- prefix
- version-id-marker

Corps de la requête

Aucune

Documentation de StorageGRID

["Opérations sur les godets"](#)

"Liste des pièces"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette requête, plus ces paramètres supplémentaires :

- max-parts

- part-number-marker
- uploadId

Corps de la requête

Aucune

Documentation de StorageGRID

["ListeMultipartUploads"](#)

"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 requête

StorageGRID prend en charge tous les paramètres du corps de la requête définis par l'API REST Amazon S3 au moment de l'implémentation.

Documentation de StorageGRID

["Opérations sur les godets"](#)

"Cryptage PutBucket"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette demande.

Balises XML du corps de la requête

StorageGRID prend en charge ces balises XML de corps de requête :

- ApplyServerSideEncryptionByDefault
- Rule
- ServerSideEncryptionConfiguration
- SSEAlgorithm

Documentation de StorageGRID

["Opérations sur les godets"](#)

"Configuration du cycle de vie de PutBucket"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette demande.

Balises XML du corps de la requête

StorageGRID prend en charge ces balises XML de corps de requête :

- And
- Days
- Expiration

- ExpiredObjectDeleteMarker
- Filter
- ID
- Key
- LifecycleConfiguration
- NewerNoncurrentVersions
- NoncurrentDays
- NoncurrentVersionExpiration
- Prefix
- Rule
- Status
- Tag
- Value

Documentation de StorageGRID

- ["Opérations sur les godets"](#)
- ["Créer une configuration du cycle de vie S3"](#)

"Configuration de PutBucketNotification"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette demande.

Balises XML du corps de la requête

StorageGRID prend en charge ces balises XML de corps de requête :

- Event
- Filter
- FilterRule
- Id
- Name
- NotificationConfiguration
- Prefix
- S3Key
- Suffix
- Topic
- TopicConfiguration
- Value

Documentation de StorageGRID

["Opérations sur les godets"](#)

"Politique de PutBucket"

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 requête

Pour plus de détails sur les champs de corps JSON pris en charge, voir ["Utiliser des politiques d'accès aux buckets et aux groupes"](#).

"Réplication de PutBucket"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette demande.

Balises XML du corps de la requête

- Bucket
- Destination
- Prefix
- ReplicationConfiguration
- Rule
- Status
- StorageClass

Documentation de StorageGRID

["Opérations sur les godets"](#)

"Balisage de PutBucket"

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 requête

StorageGRID prend en charge tous les paramètres du corps de la requête définis par l'API REST Amazon S3 au moment de l'implémentation.

Documentation de StorageGRID

["Opérations sur les godets"](#)

"Gestion des versions de PutBucket"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette demande.

Paramètres du corps de la requête

StorageGRID prend en charge ces paramètres de corps de requête :

- VersioningConfiguration
- Status

Documentation de StorageGRID

"Opérations sur les godets"

"Mettre l'objet"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette demande, plus ces en-têtes supplémentaires :

- Cache-Control
- Content-Disposition
- Content-Encoding
- Content-Language
- Expires
- x-amz-checksum-sha256
- 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 requête

- Données binaires de l'objet

Documentation de StorageGRID

"Mettre l'objet"

"MettreObjetLegalHold"

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 requête

StorageGRID prend en charge tous les paramètres du corps de la requête définis par l'API REST Amazon S3 au moment de l'implémentation.

Documentation de StorageGRID

["Utiliser l'API REST S3 pour configurer le verrouillage d'objet S3"](#)

"Configuration de PutObjectLock"

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 requête

StorageGRID prend en charge tous les paramètres du corps de la requête définis par l'API REST Amazon S3 au moment de l'implémentation.

Documentation de StorageGRID

["Utiliser l'API REST S3 pour configurer le verrouillage d'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 requête

StorageGRID prend en charge tous les paramètres du corps de la requête définis par l'API REST Amazon S3 au moment de l'implémentation.

Documentation de StorageGRID

["Utiliser l'API REST S3 pour configurer le verrouillage d'objet S3"](#)

"Balisage d'objets"

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 requête

StorageGRID prend en charge tous les paramètres du corps de la requête définis par l'API REST Amazon S3 au moment de l'implémentation.

Documentation de StorageGRID

["Opérations sur les objets"](#)

"Restaurer l'objet"

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 requête

Pour plus de détails sur les champs de corps pris en charge, voir ["Restaurer l'objet"](#) .

"Sélectionner le contenu de l'objet"

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 requête

Pour plus de détails sur les champs de corps pris en charge, consultez les éléments suivants :

- ["Utiliser S3 Select"](#)
- ["Sélectionner le contenu de l'objet"](#)

"Télécharger une partie"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette requête, plus ces paramètres de requête URI supplémentaires :

- `partNumber`
- `uploadId`

Et ces en-têtes de requête supplémentaires :

- `x-amz-checksum-sha256`
- `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 requête

- Données binaires de la pièce

Documentation de StorageGRID

["Télécharger une partie"](#)

"TéléchargerPartCopy"

Paramètres de requête URI et en-têtes de requête

StorageGRID prend en charge tous les [paramètres et en-têtes communs](#) pour cette requête, plus ces paramètres de requête URI supplémentaires :

- `partNumber`
- `uploadId`

Et ces en-têtes de requête 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 requête

Aucune

Documentation de StorageGRID

["TéléchargerPartCopy"](#)

Tester la configuration de l'API REST S3

Vous pouvez utiliser l'interface de ligne de commande Amazon Web Services (AWS CLI) pour tester votre connexion au système et vérifier que vous pouvez lire et écrire des objets.

Avant de commencer

- Vous avez téléchargé et installé l'AWS CLI depuis ["aws.amazon.com/cli"](https://aws.amazon.com/cli) .
- En option, vous avez ["créé un point de terminaison d'équilibrage de charge"](#) . Sinon, vous connaissez l'adresse IP du nœud de stockage auquel vous souhaitez vous connecter et le numéro de port à utiliser. Voir ["Adresses IP et ports pour les connexions client"](#) .
- Tu as ["créé un compte locataire S3"](#) .
- Vous vous êtes connecté au locataire et ["créé une clé d'accès"](#) .

Pour plus de détails sur ces étapes, voir ["Configurer les connexions client"](#) .

Étapes

1. Configurez les paramètres AWS CLI pour utiliser le compte que vous avez créé dans le système StorageGRID :
 - a. Entrer en mode configuration : `aws configure`
 - b. Saisissez l'ID de clé d'accès pour le compte que vous avez créé.
 - c. Saisissez la clé d'accès secrète du compte que vous avez créé.
 - d. Entrez la région par défaut à utiliser. Par exemple : `us-east-1` .
 - e. Saisissez le format de sortie par défaut à utiliser ou appuyez sur **Entrée** pour sélectionner JSON.
2. Créer un bucket.

Cet exemple suppose que vous avez configuré un point de terminaison d'équilibrage 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 bucket est créé avec succès, l'emplacement du bucket est renvoyé, comme indiqué 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. Répertoirez le contenu du bucket 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. Supprimer 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 bucket.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
delete-bucket --bucket testbucket
```

Comment StorageGRID implémente l'API REST S3

Demandes clients conflictuelles

Les demandes client conflictuelles, telles que deux clients écrivant sur la même clé, sont résolues sur la base des « derniers gagnants ».

Le moment de l'évaluation des « dernières victoires » est basé sur le moment où le système StorageGRID termine une demande donnée, et non sur le moment où les clients S3 commencent une opération.

Valeurs de cohérence

La cohérence fournit un équilibre entre la disponibilité des objets et la cohérence de ces objets sur différents nœuds de stockage et sites. Vous pouvez modifier la cohérence selon les besoins de votre application.

Par défaut, StorageGRID garantit la cohérence de lecture après écriture pour les objets nouvellement créés. Tout GET suivant un PUT terminé avec succès pourra lire les données nouvellement écrites. Les écrasements d'objets existants, les mises à jour de métadonnées et les suppressions sont finalement cohérents. Les écrasements prennent généralement quelques secondes ou minutes pour se propager, mais peuvent prendre jusqu'à 15 jours.

Si vous souhaitez effectuer des opérations sur les objets avec une cohérence différente, vous pouvez :

- Spécifier une consistance pour [chaque seau](#) .
- Spécifier une consistance pour [chaque opération API](#) .
- Modifiez la cohérence par défaut de l'ensemble de la grille en effectuant l'une des tâches suivantes :
 - Dans le gestionnaire de grille, accédez à **CONFIGURATION > Système > Paramètres de stockage > Cohérence par défaut**.
 - .



Une modification de la cohérence à l'échelle de la grille s'applique uniquement aux compartiments créés après la modification du paramètre. Pour déterminer les détails d'une modification, consultez le journal d'audit situé à l'adresse `/var/local/log` (rechercher **consistencyLevel**).

Valeurs de cohérence

La cohérence affecte la manière dont les métadonnées utilisées par StorageGRID pour suivre les objets sont distribuées entre les nœuds et, par conséquent, la disponibilité des objets pour les demandes des clients.

Vous pouvez définir la cohérence d'un bucket ou d'une opération API sur l'une des valeurs suivantes :

- **Tous** : Tous les nœuds reçoivent les données immédiatement, sinon la demande échouera.
- **Strong-global** : garantit la cohérence de lecture après écriture pour toutes les demandes client sur tous les sites.
- **Strong-site** : garantit la cohérence de lecture après écriture pour toutes les requêtes client au sein d'un site.
- **Lecture après nouvelle écriture** : (par défaut) Fournit une cohérence de lecture après écriture pour les nouveaux objets et une cohérence éventuelle pour les mises à jour d'objets. Offre des garanties de haute disponibilité et de protection des données. Recommandé dans la plupart des cas.
- **Disponible** : Fournit une cohérence éventuelle pour les nouveaux objets et les mises à jour d'objets. Pour les buckets S3, utilisez-les uniquement si nécessaire (par exemple, pour un bucket contenant des valeurs de journal rarement lues ou pour des opérations HEAD ou GET sur des clés qui n'existent pas). Non pris en charge pour les buckets S3 FabricPool .

Utiliser la cohérence « Lecture après nouvelle écriture » et « Disponible »

Lorsqu'une opération HEAD ou GET utilise la cohérence « Lecture après nouvelle écriture », StorageGRID effectue la recherche en plusieurs étapes, comme suit :

- Il recherche d'abord l'objet en utilisant une faible cohérence.
- Si cette recherche échoue, elle répète la recherche à la valeur de cohérence suivante jusqu'à ce qu'elle atteigne une cohérence équivalente au comportement de strong-global.

Si une opération HEAD ou GET utilise la cohérence « Lecture après nouvelle écriture » mais que l'objet n'existe pas, la recherche d'objet atteindra toujours une cohérence équivalente au comportement de strong-global. Étant donné que cette cohérence nécessite que plusieurs copies des métadonnées de l'objet soient disponibles sur chaque site, vous pouvez recevoir un nombre élevé d'erreurs de serveur interne 500 si deux ou plusieurs nœuds de stockage sur le même site ne sont pas disponibles.

À moins que vous n'ayez besoin de garanties de cohérence similaires à celles d'Amazon S3, vous pouvez éviter ces erreurs pour les opérations HEAD et GET en définissant la cohérence sur « Disponible ».

Lorsqu'une opération HEAD ou GET utilise la cohérence « Disponible », StorageGRID fournit uniquement la cohérence éventuelle. Il ne réessaye pas une opération ayant échoué en augmentant la cohérence, il ne nécessite donc pas que plusieurs copies des métadonnées de l'objet soient disponibles.

Spécifier la cohérence pour le fonctionnement de l'API

Pour définir la cohérence d'une opération API individuelle, les valeurs de cohérence doivent être prises en charge pour l'opération et vous devez spécifier la cohérence dans l'en-tête de la demande. Cet exemple définit la cohérence sur « Strong-site » pour une opération GetObject.

```
GET /bucket/object HTTP/1.1
Date: date
Authorization: authorization name
Host: host
Consistency-Control: strong-site
```



Vous devez utiliser la même cohérence pour les opérations PutObject et GetObject.

Spécifier la cohérence du bucket

Pour définir la cohérence du bucket, vous pouvez utiliser le StorageGRID ["Cohérence du seau PUT"](#) demande. Ou vous pouvez ["changer la consistance d'un seau"](#) du gestionnaire locataire.

Lorsque vous définissez la cohérence d'un bucket, tenez compte des éléments suivants :

- La définition de la cohérence d'un bucket détermine la cohérence utilisée pour les opérations S3 effectuées sur les objets du bucket ou sur la configuration du bucket. Cela n'affecte pas les opérations sur le bucket lui-même.
- La cohérence d'une opération API individuelle remplace la cohérence du bucket.
- En général, les buckets doivent utiliser la cohérence par défaut, « Lecture après nouvelle écriture ». Si les requêtes ne fonctionnent pas correctement, modifiez le comportement du client de l'application si possible. Ou configurez le client pour spécifier la cohérence de chaque demande d'API. Définissez la consistance au niveau du seau uniquement en dernier recours.

Comment les règles de cohérence et de gestion des informations interagissent pour affecter la protection des données

Votre choix de cohérence et votre règle ILM affectent la manière dont les objets sont protégés. Ces paramètres peuvent interagir.

Par exemple, la cohérence utilisée lors du stockage d'un objet affecte le placement initial des métadonnées de l'objet, tandis que le comportement d'ingestion sélectionné pour la règle ILM affecte le placement initial des copies de l'objet. Étant donné que StorageGRID nécessite l'accès aux métadonnées d'un objet et à ses données pour répondre aux demandes des clients, la sélection de niveaux de protection correspondants pour la cohérence et le comportement d'ingestion peut fournir une meilleure protection initiale des données et des réponses système plus prévisibles.

Ce qui suit "options d'ingestion" sont disponibles pour les règles ILM :

Double engagement

StorageGRID effectue immédiatement des copies intermédiaires de l'objet et renvoie le succès au client. Les copies spécifiées dans la règle ILM sont réalisées 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 réaliser toutes les copies spécifiées dans la règle ILM lors de l'ingestion ; si cela n'est pas possible, des copies intermédiaires sont réalisées et le succès est renvoyé au client. Les copies spécifiées dans la règle ILM sont réalisées lorsque cela est possible.

Exemple de la manière dont la règle de cohérence et la règle ILM peuvent interagir

Supposons que vous ayez une grille à deux sites avec la règle ILM suivante et la cohérence suivante :

- **Règle ILM** : Créez deux copies d'objet, une sur le site local et une sur un site distant. Adoptez un comportement d'ingestion strict.
- **cohérence** : Global fort (les métadonnées de l'objet sont immédiatement distribuées à tous les sites).

Lorsqu'un client stocke un objet dans la grille, StorageGRID effectue les deux copies de l'objet et distribue les métadonnées aux deux sites avant de renvoyer le succès au client.

L'objet est entièrement protégé contre la perte au moment de l'ingestion réussie du message. Par exemple, si le site local est perdu peu de temps après l'ingestion, des copies des données d'objet et des métadonnées d'objet existent toujours sur le site distant. L'objet est entièrement récupérable.

Si vous avez utilisé la même règle ILM et la cohérence de site forte, le client peut recevoir un message de réussite après la répllication des données d'objet sur le site distant, mais avant que les métadonnées d'objet y soient distribuées. Dans ce cas, le niveau de protection des métadonnées de l'objet ne correspond pas au niveau de protection des données de l'objet. Si le site local est perdu peu de temps après l'ingestion, les métadonnées de l'objet sont perdues. L'objet ne peut pas être récupéré.

L'interrelation entre la cohérence et les règles ILM peut être complexe. Contactez NetApp si vous avez besoin d'aide.

Versionnage d'objet

Vous pouvez définir l'état de version d'un bucket si vous souhaitez conserver plusieurs versions de chaque objet. L'activation du contrôle de version pour un bucket peut aider à protéger contre la suppression accidentelle d'objets et vous permet de récupérer et de restaurer des versions antérieures d'un objet.

Le système StorageGRID implémente le contrôle de version avec prise en charge de la plupart des fonctionnalités et avec certaines limitations. StorageGRID prend en charge jusqu'à 10 000 versions de chaque objet.

Le contrôle de version des objets peut être combiné avec la gestion du cycle de vie des informations StorageGRID (ILM) ou avec la configuration du cycle de vie du bucket S3. Vous devez activer explicitement le contrôle de version pour chaque bucket. Lorsque le contrôle de version est activé pour un bucket, chaque objet ajouté au bucket se voit attribuer un ID de version, généré par le système StorageGRID .

L'utilisation de l'authentification multifacteur (MFA) n'est pas prise en charge.



Le contrôle de version ne peut être activé que sur les buckets créés avec StorageGRID version 10.3 ou ultérieure.

ILM et gestion des versions

Les politiques ILM sont appliquées à chaque version d'un objet. Un processus d'analyse ILM analyse en continu tous les objets et les réévalue par rapport à la politique ILM actuelle. Toutes les modifications que vous apportez aux stratégies ILM sont appliquées à tous les objets précédemment ingérés. Cela inclut les versions précédemment ingérées si le contrôle de version est activé. L'analyse ILM applique de nouvelles modifications ILM aux objets précédemment ingérés.

Pour les objets S3 dans les compartiments activés pour le contrôle de version, la prise en charge du contrôle de version vous permet de créer des règles ILM qui utilisent « Heure non actuelle » comme heure de référence (sélectionnez **Oui** pour la question « Appliquer cette règle uniquement aux anciennes versions d'objet ? » dans "[Étape 1 de l'assistant Créer une règle ILM](#)"). Lorsqu'un objet est mis à jour, ses versions précédentes deviennent obsolètes. L'utilisation d'un filtre « Heure non actuelle » vous permet de créer des politiques qui réduisent l'impact sur le stockage des versions précédentes des objets.



Lorsque vous téléchargez une nouvelle version d'un objet à l'aide d'une opération de téléchargement en plusieurs parties, l'heure non actuelle de la version d'origine de l'objet reflète le moment où le téléchargement en plusieurs parties a été créé pour la nouvelle version, et non le moment où le téléchargement en plusieurs parties a été terminé. Dans des cas limités, l'heure non actuelle de la version originale peut être antérieure de plusieurs heures ou jours à l'heure de la version actuelle.

Informations connexes

- "[Comment les objets versionnés S3 sont supprimés](#)"
- "[Règles et politiques ILM pour les objets versionnés S3 \(exemple 4\)](#)".

Utiliser l'API REST S3 pour configurer le verrouillage d'objet S3

Si le paramètre global de verrouillage d'objet S3 est activé pour votre système StorageGRID , vous pouvez créer des buckets avec le verrouillage d'objet S3 activé. Vous pouvez spécifier la rétention par défaut pour chaque compartiment ou les paramètres de rétention pour chaque version d'objet.

Comment activer le verrouillage d'objet S3 pour un bucket

Si le paramètre global de verrouillage d'objet S3 est activé pour votre système StorageGRID , vous pouvez éventuellement activer le verrouillage d'objet S3 lorsque vous créez chaque bucket.

Le verrouillage d'objet S3 est un paramètre permanent qui ne peut être activé que lorsque vous créez un bucket. Vous ne pouvez pas ajouter ou désactiver le verrouillage d'objet S3 après la création d'un bucket.

Pour activer le verrouillage d'objet S3 pour un bucket, utilisez l'une de ces méthodes :

- Créez le bucket à l'aide du gestionnaire de locataires. Voir ["Créer un bucket S3"](#) .
- Créez le bucket à l'aide d'une requête CreateBucket avec le `x-amz-bucket-object-lock-enabled` en-tête de requête. Voir ["Opérations sur les godets"](#) .

S3 Object Lock nécessite le contrôle de version du bucket, qui est activé automatiquement lors de la création du bucket. Vous ne pouvez pas suspendre le contrôle de version du bucket. Voir ["Versionnage d'objet"](#) .

Paramètres de conservation par défaut pour un bucket

Lorsque le verrouillage d'objet S3 est activé pour un compartiment, vous pouvez éventuellement activer la rétention par défaut pour le compartiment et spécifier un mode de rétention par défaut et une période de rétention par défaut.

Mode de rétention par défaut

- En mode CONFORMITÉ :
 - L'objet ne peut pas être supprimé tant que sa date de conservation n'est pas atteinte.
 - La date de conservation de l'objet peut être augmentée, mais elle ne peut pas être diminuée.
 - La date de conservation de l'objet ne peut pas être supprimée tant que cette date n'est pas atteinte.
- En mode GOUVERNANCE :
 - Les utilisateurs avec le `s3:BypassGovernanceRetention` l'autorisation peut utiliser le `x-amz-bypass-governance-retention: true` en-tête de demande pour contourner les paramètres de conservation.
 - Ces utilisateurs peuvent supprimer une version d'objet avant que sa date de conservation ne soit atteinte.
 - Ces utilisateurs peuvent augmenter, diminuer ou supprimer la date de conservation d'un objet.

Période de conservation par défaut

Chaque bucket peut avoir une période de conservation par défaut spécifiée en années ou en jours.

Comment définir la rétention par défaut pour un bucket

Pour définir la rétention par défaut d'un bucket, utilisez l'une de ces méthodes :

- Gérez les paramètres du bucket à partir du gestionnaire de locataires. Voir ["Créer un bucket S3"](#) et ["Mettre à jour la conservation par défaut du verrouillage des objets S3"](#) .
- Émettez une demande PutObjectLockConfiguration pour le bucket afin de spécifier le mode par défaut et le nombre de jours ou d'années par défaut.

Configuration de PutObjectLock

La demande PutObjectLockConfiguration vous permet de définir et de modifier le mode de conservation par défaut et la période de conservation par défaut pour un bucket sur lequel le verrouillage d'objet S3 est activé. Vous pouvez également supprimer les paramètres de conservation par défaut précédemment configurés.

Lorsque de nouvelles versions d'objet sont ingérées dans le bucket, le mode de rétention 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 conservation 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 date de conservation de la version d'objet reste la même et n'est pas recalculée à l'aide de la nouvelle période de conservation par défaut.

Vous devez avoir le `s3:PutBucketObjectLockConfiguration` autorisation, ou être un compte root, pour terminer cette opération.

Le `Content-MD5` l'en-tête de la requête doit être spécifié dans la requête PUT.

Exemple de demande

Cet exemple active le verrouillage d'objet S3 pour un bucket 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 rétention par défaut d'un bucket

Pour déterminer si le verrouillage d'objet S3 est activé pour un bucket et pour voir le mode de conservation par défaut et la période de conservation, utilisez l'une de ces méthodes :

- Afficher le bucket dans le gestionnaire de locataires. Voir "[Afficher les buckets S3](#)".
- Émettez une demande `GetObjectLockConfiguration`.

Obtenir la configuration du verrouillage de l'objet

La demande `GetObjectLockConfiguration` vous permet de déterminer si le verrouillage d'objet S3 est activé pour un compartiment et, s'il est activé, de voir s'il existe un mode de conservation par défaut et une période de conservation configurés pour le compartiment.

Lorsque de nouvelles versions d'objet sont ingérées dans le bucket, le mode de rétention par défaut est appliqué si `x-amz-object-lock-mode` n'est pas spécifié. La période de conservation 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 un compte root, 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 bucket avec S3 Object Lock activé peut contenir une combinaison d'objets avec et sans paramètres de conservation S3 Object Lock.

Les paramètres de conservation au niveau de l'objet sont spécifiés à l'aide de l'API REST S3. Les paramètres de rétention d'un objet remplacent tous les paramètres de rétention par défaut du compartiment.

Vous pouvez spécifier les paramètres suivants pour chaque objet :

- **Mode de conservation** : Soit CONFORMITÉ, soit GOUVERNANCE.
- **Retain-until-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 est dans le futur, l'objet peut être récupéré, mais il ne peut pas être modifié ou supprimé. La date de conservation peut être augmentée, mais cette date ne peut pas être diminuée ou supprimée.
 - En mode GOUVERNANCE, les utilisateurs disposant d'une autorisation spéciale peuvent contourner le paramètre de conservation jusqu'à la date. Ils peuvent supprimer une version d'objet avant l'expiration de sa période de conservation. Ils peuvent également augmenter, diminuer ou même supprimer la date de conservation.
- **Conservation légale** : L'application d'une conservation légale à une version d'objet verrouille immédiatement cet objet. Par exemple, vous pourriez avoir besoin de suspendre légalement un objet lié à une enquête ou à un litige juridique. Une conservation 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. Si une version d'objet est soumise à une suspension 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 bucket, émettez un "[Mettre l'objet](#)", "[Copier l'objet](#)", ou "[Créer un téléchargement multi-parties](#)" demande.

Vous pouvez utiliser les éléments suivants :

- `x-amz-object-lock-mode`, qui peut être CONFORMITÉ ou GOUVERNANCE (sensible à la casse).



Si vous précisez `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 de conservation jusqu'à la date doit être au format `2020-08-10T21:46:00Z`. Les fractions de secondes sont autorisées, mais seuls 3 chiffres décimaux sont conservés (précision en millisecondes). Les autres formats ISO 8601 ne sont pas autorisés.
 - La date de conservation doit être dans le futur.
- `x-amz-object-lock-legal-hold`

Si la conservation légale est activée (sensible à la casse), l'objet est placé sous conservation légale. Si la retenue légale est désactivée, aucune retenue légale n'est placée. Toute autre valeur entraîne une erreur 400 Bad Request (InvalidArgument).

Si vous utilisez l'un de ces en-têtes de requête, tenez compte de ces restrictions :

- Le `Content-MD5` l'en-tête de la demande est requis le cas échéant `x-amz-object-lock-*` l'en-tête de requête est présent dans la requête `PutObject`. `Content-MD5` n'est pas requis pour `CopyObject` ou `CreateMultipartUpload`.
- Si le compartiment n'a pas de verrouillage d'objet S3 activé et qu'un `x-amz-object-lock-*` l'en-tête de requête est présent, une erreur 400 Bad Request (InvalidRequest) est renvoyée.
- La requête `PutObject` prend en charge l'utilisation de `x-amz-storage-class: REDUCED_REDUNDANCY` pour correspondre au comportement d'AWS. Cependant, lorsqu'un objet est ingéré dans un bucket avec S3 Object Lock activé, StorageGRID effectuera toujours une ingestion à double validation.
- Une réponse de version `GET` ou `HeadObject` ultérieure 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 requête a le bon `s3:Get*` autorisations.

Vous pouvez utiliser le `s3:object-lock-remaining-retention-days` clé de condition de politique pour limiter les périodes de conservation minimales et maximales autorisées 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 rétention d'une version d'objet existante, vous pouvez effectuer les opérations de sous-ressources d'objet suivantes :

- `PutObjectLegalHold`

Si la nouvelle valeur de conservation légale est activée, l'objet est placé sous une conservation légale. Si la valeur de maintien légal est OFF, le maintien légal est levé.

- `PutObjectRetention`
 - La valeur du mode peut être COMPLIANCE ou GOVERNANCE (sensible à la casse).
 - La valeur de conservation jusqu'à la date doit être au format `2020-08-10T21:46:00Z`. Les fractions de secondes sont autorisées, mais seuls 3 chiffres décimaux sont conservés (précision en millisecondes). Les autres formats ISO 8601 ne sont pas autorisés.
 - Si une version d'objet possède une date de conservation existante, vous ne pouvez que l'augmenter. La nouvelle valeur doit être dans le futur.

Comment utiliser le mode GOUVERNANCE

Les utilisateurs qui ont le `s3:BypassGovernanceRetention` l'autorisation peut contourner les paramètres de conservation actifs d'un objet qui utilise le mode GOUVERNANCE. Toutes les opérations `DELETE` ou `PutObjectRetention` doivent inclure le `x-amz-bypass-governance-retention:true` en-tête de requête. Ces utilisateurs peuvent effectuer ces opérations supplémentaires :

- Exécutez les opérations `DeleteObject` ou `DeleteObjects` pour supprimer une version d'objet avant l'expiration de sa période de conservation.

Les objets faisant l'objet d'une suspension légale ne peuvent pas être supprimés. La retenue légale doit être désactivée.

- Exécutez des opérations `PutObjectRetention` qui modifient le mode de version d'un objet de GOUVERNANCE à CONFORMITÉ avant l'expiration de la période de conservation de l'objet.

Le passage du mode CONFORMITÉ au mode GOUVERNANCE n'est jamais autorisé.

- Exécutez des opérations PutObjectRetention pour augmenter, diminuer ou supprimer la période de conservation d'une version d'objet.

Informations connexes

- ["Gérer les objets avec S3 Object Lock"](#)
- ["Utilisez S3 Object Lock pour conserver les objets"](#)
- ["Guide de l'utilisateur d'Amazon Simple Storage Service : Verrouillage d'objets"](#)

Créer une configuration du cycle de vie S3

Vous pouvez créer une configuration de cycle de vie S3 pour contrôler le moment où des objets spécifiques sont supprimés du système StorageGRID .

L'exemple simple de cette section illustre comment une configuration de cycle de vie S3 peut contrôler le moment où certains objets sont supprimés (expirés) de compartiments S3 spécifiques. L'exemple dans cette section est fourni à titre d'illustration uniquement. Pour plus de détails sur la création de configurations de cycle de vie S3, consultez ["Guide de l'utilisateur d'Amazon Simple Storage Service : Gestion du cycle de vie des objets"](#) . Notez que StorageGRID prend uniquement en charge les actions d'expiration ; il ne prend pas en charge les actions de transition.

Quelle est la configuration du cycle de vie

Une configuration de cycle de vie est un ensemble de règles appliquées aux objets dans des compartiments S3 spécifiques. Chaque règle spécifie quels objets sont concernés et quand ces objets expireront (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 de 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 compter du moment où l'objet a été ingéré.
- NoncurrentVersionExpiration : supprimez un objet lorsqu'un nombre de jours spécifié est atteint, à compter du moment où l'objet est devenu non actuel.
- Filtre (préfixe, balise)
- Statut
- ID

Chaque objet suit les paramètres de conservation d'un cycle de vie de compartiment S3 ou d'une politique ILM. Lorsqu'un cycle de vie de compartiment S3 est configuré, les actions d'expiration du cycle de vie remplacent la stratégie ILM pour les objets correspondant au filtre de cycle de vie du compartiment. Les objets qui ne correspondent pas au filtre de cycle de vie du bucket utilisent les paramètres de conservation de la stratégie ILM. Si un objet correspond à un filtre de cycle de vie de compartiment et qu'aucune action d'expiration n'est explicitement spécifiée, les paramètres de conservation de la stratégie ILM ne sont pas utilisés et il est implicite que les versions d'objet sont conservées pour toujours. Voir ["Exemples de priorités pour le cycle de vie du bucket S3 et la politique ILM"](#) .

Par conséquent, un objet peut être supprimé de la grille même si les instructions de placement d'une règle ILM s'appliquent toujours à l'objet. Ou bien, un objet peut être conservé sur la grille même après l'expiration des instructions de placement ILM pour l'objet. Pour plus de détails, consultez la section ["Comment ILM fonctionne tout au long de la vie d'un objet"](#) .



La configuration du cycle de vie du bucket peut être utilisée avec les buckets pour lesquels le verrouillage d'objet S3 est activé, mais la configuration du cycle de vie du bucket n'est pas prise en charge pour les buckets conformes hérités.

StorageGRID prend en charge l'utilisation des opérations de bucket suivantes pour gérer les configurations du cycle de vie :

- Supprimer le cycle de vie du bucket
- GetBucketLifecycleConfiguration
- Configuration du cycle de vie de PutBucket

Créer une configuration du cycle de vie

Comme première étape de la création d'une configuration de cycle de vie, vous créez un fichier JSON qui inclut une ou plusieurs règles. Par exemple, ce fichier JSON comprend 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 spécifie que les objets correspondant au filtre expireront 100 jours après leur ingestion.



Les règles qui spécifient un nombre de jours sont relatives au moment où l'objet a été ingéré. Si la date actuelle dépasse la date d'ingestion plus le nombre de jours, certains objets peuvent être supprimés du bucket dès que la configuration du cycle de vie est appliquée.

3. La règle 3 s'applique uniquement aux objets qui correspondent au préfixe `category3 /`. Le `Expiration` le paramètre spécifie que toutes les versions non actuelles des objets correspondants expireront 50 jours après être devenues non actuelles.

```

{
  "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"
    }
  ]
}

```

Appliquer la configuration du cycle de vie au bucket

Après avoir créé le fichier de configuration du cycle de vie, vous l'appliquez à un bucket en émettant une requête `PutBucketLifecycleConfiguration`.

Cette requête applique la configuration du cycle de vie dans le fichier d'exemple aux objets d'un bucket nommé `testbucket`.

```
aws s3api --endpoint-url <StorageGRID endpoint> put-bucket-lifecycle-configuration
--bucket testbucket --lifecycle-configuration file://bktjson.json
```

Pour valider qu'une configuration de cycle de vie a été correctement appliquée au bucket, émettez une demande `GetBucketLifecycleConfiguration`. Par exemple:

```
aws s3api --endpoint-url <StorageGRID endpoint> get-bucket-lifecycle-configuration
--bucket testbucket
```

Une réponse réussie répertorie la configuration du cycle de vie que vous venez d'appliquer.

Valider que l'expiration du cycle de vie du bucket s'applique à l'objet

Vous pouvez déterminer si une règle d'expiration dans la configuration du cycle de vie s'applique à un objet spécifique lors de l'émission d'une demande `PutObject`, `HeadObject` ou `GetObject`. Si une règle s'applique, la réponse comprend une `Expiration` paramètre qui indique quand l'objet expire et quelle règle d'expiration a été respectée.



Étant donné que le cycle de vie du bucket remplace ILM, le `expiry-date` la date réelle à laquelle l'objet sera supprimé est indiquée. Pour plus de détails, consultez la section ["Comment la rétention d'objet est déterminée"](#).

Par exemple, cette requête `PutObject` a été émise le 22 juin 2020 et place un objet dans le `testbucket` `seau`.

```
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 (1er octobre 2020) et qu'il correspond à la règle 2 de la configuration du cycle de vie.

```
{
  "Expiration": "expiry-date=\"Thu, 01 Oct 2020 09:07:49 GMT\", rule-id=\"rule2\"",
  "ETag": "\"9762f8a803bc34f5340579d4446076f7\""
}
```

Par exemple, cette requête HeadObject a été utilisée pour obtenir des métadonnées pour le même objet dans le bucket testbucket.

```
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": {}
}
```



Pour les buckets avec contrôle de version activé, le x-amz-expiration l'en-tête de réponse s'applique uniquement aux versions actuelles des objets.

Recommandations pour la mise en œuvre de l'API REST S3

Vous devez suivre ces recommandations lors de l'implémentation de l'API REST S3 à utiliser avec StorageGRID.

Recommandations pour les HEADs vers 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 l'option « Disponible » ["cohérence"](#) . Par exemple, vous devez utiliser la cohérence « Disponible » si votre application HEAD un emplacement avant d'y effectuer un PUT.

Dans le cas contraire, si l'opération HEAD ne trouve pas l'objet, vous risquez de recevoir un nombre élevé d'erreurs de serveur interne 500 si deux ou plusieurs nœuds de stockage sur le même site ne sont pas disponibles ou si un site distant est inaccessible.

Vous pouvez définir la cohérence « Disponible » pour chaque bucket à l'aide de l'["Cohérence du seau PUT"](#) demande, ou vous pouvez spécifier la 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 initiale du bucket.

Buckets créés dans StorageGRID 11.4 ou version antérieure

- N'utilisez pas de valeurs aléatoires comme quatre premiers caractères des clés d'objet. Ceci est en contraste avec l'ancienne recommandation AWS pour les préfixes de clé. Utilisez plutôt des préfixes non aléatoires et non uniques, tels que `image`.
- Si vous suivez l'ancienne recommandation AWS d'utiliser des caractères aléatoires et uniques dans les préfixes de clé, préfixez les clés d'objet avec un nom de répertoire. C'est-à-dire, utilisez ce format :

```
mybucket/mydir/f8e3-image3132.jpg
```

Au lieu de ce format :

```
mybucket/f8e3-image3132.jpg
```

Buckets créés dans StorageGRID 11.4 ou version ultérieure

Il n'est pas nécessaire de restreindre les noms de clés d'objet pour respecter les meilleures pratiques en matière de performances. Dans la plupart des cas, vous pouvez utiliser des valeurs aléatoires pour les quatre premiers caractères des noms de clés d'objet.



Une exception à cette règle est une charge de travail 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, faites varier une partie initiale du nom de la clé tous les plusieurs milliers d'objets avec quelque chose comme la date. Par exemple, supposons qu'un client S3 écrit généralement 2 000 objets/seconde et que la politique de cycle de vie ILM ou bucket supprime tous les objets après trois jours. Pour minimiser l'impact sur les performances, vous pouvez nommer les clés en utilisant un modèle comme celui-ci :

```
/mybucket/mydir/yyyymmddhhmmss-random_UUID.jpg
```

Recommandations pour les « lectures de plage »

Si le "option globale pour compresser les objets stockés" est activé, les applications clientes S3 doivent éviter d'effectuer des opérations `GetObject` qui spécifient une plage d'octets à renvoyer. Ces opérations de « lecture de plage » sont inefficaces car StorageGRID doit décompresser efficacement les objets pour accéder aux octets demandés. Les opérations `GetObject` qui demandent une petite plage d'octets à partir d'un très grand objet sont particulièrement inefficaces ; par exemple, il est 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 des clients peuvent expirer.



Si vous devez compresser des objets et que votre application cliente doit utiliser des lectures de plage, augmentez le délai d'expiration de lecture pour l'application.

Prise en charge de l'API REST Amazon S3

Détails d'implémentation de l'API REST S3

Le système StorageGRID implémente l'API Simple Storage Service (version API 2006-03-01) avec prise en charge de la plupart des opérations et avec certaines limitations. Vous devez comprendre les détails d'implémentation lorsque vous intégrez des applications clientes S3 REST API.

Le système StorageGRID prend en charge à la fois les demandes de type hébergé virtuel et les demandes de type chemin.

Gestion des dates

L'implémentation StorageGRID de l'API REST S3 prend uniquement en charge 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 horaire de la date peut être spécifiée au format Greenwich Mean Time (GMT) ou au format Universal Coordinated Time (UTC) sans décalage de fuseau horaire (+0000 doit être spécifié). Si vous incluez le `x-amz-date` en-tête de votre demande, il remplace toute valeur spécifiée dans l'en-tête de la demande Date. Lors de l'utilisation d'AWS Signature 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 requête courants

Le système StorageGRID prend en charge les en-têtes de requête courants définis par "[Référence de l'API Amazon Simple Storage Service : en-têtes de requête courants](#)", à une exception près.

En-tête de la requête	Mise en œuvre
Autorisation	Prise en charge complète d'AWS Signature Version 2 Prise en charge d'AWS Signature version 4, avec les exceptions suivantes : • Lorsque vous fournissez la valeur réelle de la somme de contrôle de la charge utile dans <code>x-amz-content-sha256</code>, la valeur est acceptée sans validation, comme si la valeur <code>UNSIGNED-PAYLOAD</code> avait été prévu pour l'en-tête. Lorsque vous fournissez un <code>x-amz-content-sha256</code> valeur d'en-tête qui implique <code>aws-chunked</code> en streaming (par exemple, <code>STREAMING-AWS4-HMAC-SHA256-PAYLOAD</code>), les signatures de bloc ne sont pas vérifiées par rapport aux données de bloc.
jeton de sécurité x-amz	Non implémenté. Retours <code>XNotImplemented</code> .

En-têtes de réponse courants

Le système StorageGRID prend en charge tous les en-têtes de réponse courants définis par la *Référence API du service de stockage simple*, à une exception près.

En-tête de réponse	Mise en œuvre
<code>x-amz-id-2</code>	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 les versions Signature 2 et Signature 4 pour l'authentification des requêtes API S3.

Les demandes authentifiées doivent être signées à l'aide de votre identifiant de clé d'accès et de votre clé

d'accès secrète.

Le système StorageGRID prend en charge deux méthodes d'authentification : HTTP Authorization en-tête et utilisation des paramètres de requête.

Utiliser l'en-tête d'autorisation HTTP

Le HTTP Authorization L'en-tête est utilisé par toutes les opérations API S3, à l'exception des demandes anonymes lorsque la politique de compartiment le permet. Le Authorization L'en-tête contient toutes les informations de signature requises pour authentifier une demande.

Utiliser les paramètres de requête

Vous pouvez utiliser des paramètres de requête pour ajouter des informations d'authentification à une URL. Ceci est connu sous le nom de présignature de l'URL, qui peut être utilisée pour accorder un accès temporaire à des ressources spécifiques. Les utilisateurs disposant de 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 restreint à un tiers à une ressource.

Opérations sur le service

Le système StorageGRID prend en charge les opérations suivantes sur le service.

Opération	Mise en œuvre
Listes de seaux (anciennement nommé service GET)	Implémenté avec tous les comportements de l'API REST Amazon S3. Sous réserve de modifications sans préavis.
Utilisation du stockage GET	Le StorageGRID" Utilisation du stockage GET " La demande 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 clientes peuvent émettre OPTIONS / demandes adressées au port S3 sur un nœud de stockage, sans fournir les informations d'identification d'authentification S3, pour déterminer si le nœud de stockage est disponible. Vous pouvez utiliser cette demande pour la surveillance ou pour permettre aux équilibres de charge externes d'identifier quand un nœud de stockage est en panne.

Opérations sur les godets

Le système StorageGRID prend en charge un maximum de 5 000 buckets pour chaque compte de locataire S3.

Chaque grille peut contenir un maximum de 100 000 buckets.

Pour prendre en charge 5 000 buckets, chaque nœud de stockage de la grille doit disposer d'un minimum de 64 Go de RAM.

Les restrictions de nom de bucket suivent les restrictions régionales standard AWS US, mais vous devez les restreindre davantage aux conventions de dénomination DNS pour prendre en charge les demandes de style hébergé virtuel S3.

Pour plus d'informations, voir les éléments suivants :

- ["Guide de l'utilisateur d'Amazon Simple Storage Service : quotas, restrictions et limitations des buckets"](#)
- ["Configurer les noms de domaine des points de terminaison S3"](#)

Les opérations ListObjects (GET Bucket) et ListObjectVersions (versions d'objet GET Bucket) prennent en charge StorageGRID ["valeurs de cohérence"](#) .

Vous pouvez vérifier si les mises à jour de l'heure du dernier accès sont activées ou désactivées pour des compartiments individuels. Voir ["Heure du dernier accès au bucket GET"](#) .

Le tableau suivant décrit comment StorageGRID implémente les opérations de bucket S3 REST API. Pour effectuer l'une de ces opérations, les informations d'accès nécessaires doivent être fournies pour le compte.

Opération	Mise en œuvre
Créer un bucket	Crée un nouveau bucket. En créant le bucket, vous devenez le propriétaire du bucket. - Les noms de bucket doivent respecter les règles suivantes : - Doit être unique sur chaque système StorageGRID (pas seulement unique au sein du compte locataire). - Doit être conforme au DNS. - Doit contenir au moins 3 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 minuscule ou un chiffre et ne peut utiliser que des lettres minuscules, des chiffres et des traits d'union. - Ne doit pas ressembler à une adresse IP au format texte. - Ne doit pas utiliser de points dans les requêtes de style hébergé virtuellement. Les points entraîneront des problèmes avec la vérification du certificat générique du serveur. - Par défaut, les buckets sont créés dans le <code>us-east-1</code> région; cependant, vous pouvez utiliser le <code>LocationConstraint</code> élément de demande dans le corps de la demande pour spécifier une région différente. Lors de l'utilisation du <code>LocationConstraint</code> élément, 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 la région à utiliser. Remarque : une erreur se produira si votre demande <code>CreateBucket</code> utilise une région qui n'a pas été définie dans StorageGRID. - Vous pouvez inclure le <code>x-amz-bucket-object-lock-enabled</code> en-tête de demande pour créer un bucket avec S3 Object Lock activé. Voir "Utiliser l'API REST S3 pour configurer le verrouillage d'objet S3" . Vous devez activer le verrouillage d'objet S3 lorsque vous créez le bucket. Vous ne pouvez pas ajouter ou désactiver le verrouillage d'objet S3 après la création d'un bucket. S3 Object Lock nécessite le contrôle de version du bucket, qui est activé automatiquement lorsque vous créez le bucket.
Supprimer le bucket	Supprime le bucket.
SupprimerBucketCors	Supprime la configuration CORS pour le bucket.
Supprimer le chiffrement du bucket	Supprime le cryptage par défaut du bucket. Les objets chiffrés existants restent chiffrés, mais tous les nouveaux objets ajoutés au bucket ne sont pas chiffrés.
Supprimer le cycle de vie du bucket	Supprime la configuration du cycle de vie du bucket. Voir "Créer une configuration du cycle de vie S3" .

Opération	Mise en œuvre
Supprimer la politique de bucket	Supprime la politique attachée au bucket.
SupprimerBucketReplication	Supprime la configuration de réplication attachée au bucket.
Supprimer le balisage du bucket	Utilise le <code>tagging</code> sous-ressource pour supprimer toutes les balises d'un bucket. Attention : Si une balise de politique ILM non par défaut est définie pour ce compartiment, il y aura un <code>NTAP-SG-ILM-BUCKET-TAG</code> balise de bucket avec une valeur qui lui est attribuée. N'émettez pas de demande <code>DeleteBucketTagging</code> s'il y a un <code>NTAP-SG-ILM-BUCKET-TAG</code> étiquette de seau. Au lieu de cela, émettez une requête <code>PutBucketTagging</code> avec uniquement le <code>NTAP-SG-ILM-BUCKET-TAG</code> balise et sa valeur attribuée pour supprimer toutes les autres balises du bucket. Ne pas modifier ni supprimer le <code>NTAP-SG-ILM-BUCKET-TAG</code> étiquette de seau.
ObtenirBucketAcl	Renvoie une réponse positive et l'ID, le nom d'affichage et l'autorisation du propriétaire du bucket, indiquant que le propriétaire a un accès complet au bucket.
ObtenirBucketCors	Renvoie le <code>cors</code> configuration pour le bucket.
Obtenir le chiffrement du bucket	Renvoie la configuration de chiffrement par défaut pour le bucket.
GetBucketLifecycleConfiguration (anciennement appelé cycle de vie du bucket GET)	Renvoie la configuration du cycle de vie du bucket. Voir "Créer une configuration du cycle de vie S3" .
Obtenir l'emplacement du bucket	Renvoie la région qui a été définie à l'aide de <code>LocationConstraint</code> élément dans la requête <code>CreateBucket</code> . Si la région du bucket est <code>us-east-1</code> , une chaîne vide est renvoyée pour la région.
Configuration de GetBucketNotification (anciennement appelée notification GET Bucket)	Renvoie la configuration de notification attachée au bucket.
Obtenir la politique de Bucket	Renvoie la politique attachée au bucket.
Réplication GetBucket	Renvoie la configuration de réplication attachée au bucket.

Opération	Mise en œuvre
Obtenir le balisage du bucket	Utilise le <code>tagging</code> sous-ressource pour renvoyer toutes les balises d'un bucket. Attention : Si une balise de politique ILM non par défaut est définie pour ce compartiment, il y aura un <code>NTAP-SG-ILM-BUCKET-TAG</code> balise de bucket avec une valeur qui lui est attribuée. Ne pas modifier ni supprimer cette balise.
Obtenir la gestion des versions du bucket	Cette implémentation utilise le <code>versioning</code> sous-ressource pour renvoyer l'état de version d'un bucket. • <i>blank</i> : le contrôle de version n'a jamais été activé (le bucket est « Non versionné ») • <i>Activé</i> : le contrôle de version est activé • <i>Suspendu</i> : le contrôle de version était précédemment activé et est suspendu
Obtenir la configuration du verrouillage de l'objet	Renvoie le mode de conservation par défaut du bucket et la période de conservation par défaut, si configurés. Voir "Utiliser l'API REST S3 pour configurer le verrouillage d'objet S3" .
Tête de godet	Détermine si un bucket existe et si vous avez l'autorisation d'y accéder. Cette opération renvoie : • <code>x-ntap-sg-bucket-id</code>: L'UUID du bucket au format UUID. • <code>x-ntap-sg-trace-id</code>: L'ID de trace unique de la demande associée.
ListObjects et ListObjectsV2 (anciennement nommé GET Bucket)	Renvoie tout ou partie (jusqu'à 1 000) des objets d'un bucket. La classe de stockage des objets peut avoir l'une des deux valeurs, même si l'objet a été ingéré avec le <code>REDUCED_REDUNDANCY</code> option de classe de stockage : • <code>STANDARD</code>, ce qui indique que l'objet est stocké dans un pool de stockage composé de nœuds de stockage. • <code>GLACIER</code>, ce qui indique que l'objet a été déplacé vers le bucket 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 certaines <code>CommonPrefixes</code> qui ne contiennent pas de clés.
ListObjectVersions (anciennement appelées versions d'objets GET Bucket)	Avec un accès en <code>LECTURE</code> sur un bucket, en utilisant cette opération avec le <code>versions</code> la sous-ressource répertorie les métadonnées de toutes les versions des objets dans le bucket.

Opération	Mise en œuvre
PutBucketCors	Définit la configuration CORS pour un bucket afin que celui-ci puisse traiter les demandes inter-origines. Le partage de ressources inter-origines (CORS) est un mécanisme de sécurité qui permet aux applications Web clientes d'un domaine d'accéder aux ressources d'un domaine différent. Par exemple, supposons que vous utilisiez un bucket S3 nommé <code>images</code> pour stocker des graphiques. En définissant la configuration CORS pour le <code>images</code> bucket, vous pouvez autoriser l'affichage des images de ce bucket sur le site Web <code>http://www.example.com</code> .
Cryptage PutBucket	Définit l'état de cryptage par défaut d'un bucket existant. Lorsque le chiffrement au niveau du bucket est activé, tout nouvel objet ajouté au bucket est chiffré. StorageGRID prend en charge le chiffrement côté serveur avec des clés gérées par StorageGRID. Lors de la spécification de la règle de configuration de chiffrement côté serveur, définissez le <code>SSEAlgorithm</code> paramètre à <code>AES256</code>, et n'utilisez pas le <code>KMSMasterKeyID</code> paramètre. La configuration de chiffrement par défaut du bucket est ignorée si la demande de téléchargement d'objet spécifie déjà le chiffrement (c'est-à-dire si la demande inclut le <code>x-amz-server-side-encryption-*</code> en-tête de requête).
Configuration du cycle de vie de PutBucket (anciennement appelé cycle de vie du bucket PUT)	Crée une nouvelle configuration de cycle de vie pour le bucket 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 de cycle de vie. Chaque règle peut inclure les éléments XML suivants : • Expiration (jours, date, ExpiredObjectDeleteMarker) • NoncurrentVersionExpiration (NewerNoncurrentVersions, NoncurrentDays) • Filtre (préfixe, balise) • Statut • ID StorageGRID ne prend pas en charge ces actions : • AbandonnerTéléchargement multi-parties incomplet • Transition Voir "Créer une configuration du cycle de vie S3". Pour comprendre comment l'action Expiration dans un cycle de vie de bucket interagit avec les instructions de placement ILM, voir "Comment ILM fonctionne tout au long de la vie d'un objet". Remarque : la configuration du cycle de vie du bucket peut être utilisée avec les buckets pour lesquels le verrouillage d'objet S3 est activé, mais la configuration du cycle de vie du bucket n'est pas prise en charge pour les buckets conformes hérités.

Opération	Mise en œuvre
Configuration de PutBucketNotification (anciennement appelée notification PUT Bucket)	Configure les notifications pour le bucket à l'aide du XML de configuration de notification inclus dans le corps de la demande. Vous devez être conscient des détails de mise en œuvre suivants : • StorageGRID prend en charge les rubriques Amazon Simple Notification Service (Amazon SNS) ou Kafka comme destinations. Les points de terminaison Simple Queue Service (SQS) ou Amazon Lambda ne sont pas pris en charge. • La destination des notifications doit être spécifiée comme l'URN d'un point de terminaison StorageGRID . Les points de terminaison peuvent être créés à l'aide du gestionnaire de locataires ou de l'API de gestion des locataires. Le point de terminaison doit exister pour que la configuration des notifications réussisse. Si le point de terminaison 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 ne sont pas pris en charge. ◦ <code>s3:ReducedRedundancyLostObject</code> ◦ <code>s3:ObjectRestore:Completed</code> • Les notifications d'événements envoyées depuis StorageGRID utilisent le format JSON standard, sauf qu'elles n'incluent pas certaines clés et utilisent des valeurs spécifiques pour d'autres, comme indiqué dans la liste suivante : ◦ Source de l'événement <code>sgws:s3</code> ◦ awsRegion non inclus ◦ x-amz-id-2 non inclus ◦ arn <code>urn:sgws:s3:::bucket_name</code>
Politique de PutBucket	Définit la politique attachée au bucket. Voir "Utiliser des politiques d'accès aux buckets et aux groupes" .

Opération	Mise en œuvre
Réplication de PutBucket	Configure "Réplication StorageGRID CloudMirror" pour le bucket utilisant la configuration de réplication XML fournie dans le corps de la demande. Pour la réplication CloudMirror, vous devez connaître les détails d'implémentation suivants : • StorageGRID prend uniquement en charge la version V1 de la configuration de réplication. Cela signifie que StorageGRID ne prend pas en charge l'utilisation du <code>Filter</code> élément pour les règles et suit les conventions V1 pour la suppression des versions d'objet. Pour plus de détails, voir "Guide de l'utilisateur d'Amazon Simple Storage Service : Configuration de la réplication" . • La réplication de bucket peut être configurée sur des buckets versionnés ou non versionnés. • Vous pouvez spécifier un bucket de destination différent dans chaque règle du XML de configuration de réplication. Un bucket source peut être répliqué vers plusieurs buckets de destination. • Les buckets de destination doivent être spécifiés comme URN des points de terminaison StorageGRID comme spécifié dans le gestionnaire de locataires ou l'API de gestion des locataires. Voir "Configurer la réplication CloudMirror" . Le point de terminaison doit exister pour que la configuration de la réplication réussisse. Si le point de terminaison n'existe pas, la demande échoue en tant que 400 Bad Request . Le message d'erreur indique : <code>Unable to save the replication policy. The specified endpoint URN does not exist: URN.</code> • Vous n'avez pas besoin de spécifier un <code>Role</code> dans la configuration XML. Cette valeur n'est pas utilisée par StorageGRID et sera ignorée si elle est soumise. • Si vous omettez la classe de stockage du XML de configuration, StorageGRID utilise le <code>STANDARD</code> classe de stockage par défaut. • Si vous supprimez un objet du bucket source ou si vous supprimez le bucket source lui-même, le comportement de la réplication inter-région est le suivant : ◦ Si vous supprimez l'objet ou le bucket avant qu'il ne soit répliqué, l'objet/bucket n'est pas répliqué et vous n'en êtes pas averti. ◦ Si vous supprimez l'objet ou le compartiment après sa réplication, StorageGRID suit le comportement de suppression standard d'Amazon S3 pour la V1 de la réplication inter-régions.

Opération	Mise en œuvre
Balisage de PutBucket	Utilise le <code>tagging</code> sous-ressource pour ajouter ou mettre à jour un ensemble de balises pour un bucket. Lorsque vous ajoutez des balises de bucket, tenez compte des limitations suivantes : • StorageGRID et Amazon S3 prennent en charge jusqu'à 50 balises pour chaque compartiment. • Les balises associées à un bucket doivent avoir des clés de balise uniques. Une clé de balise peut comporter jusqu'à 128 caractères Unicode. • Les valeurs des balises peuvent contenir jusqu'à 256 caractères Unicode. • La clé et les valeurs sont sensibles à la casse. Attention : Si une balise de politique ILM non par défaut est définie pour ce compartiment, il y aura un <code>NTAP-SG-ILM-BUCKET-TAG</code> balise de bucket avec une valeur qui lui est attribuée. Assurez-vous que le <code>NTAP-SG-ILM-BUCKET-TAG</code> la balise de bucket est incluse avec la valeur attribuée dans toutes les requêtes <code>PutBucketTagging</code>. Ne pas modifier ni supprimer cette balise. Remarque : cette opération écrasera toutes les balises actuelles que le bucket possède déjà. Si des balises existantes sont omises de l'ensemble, ces balises seront supprimées pour le bucket.
Gestion des versions de PutBucket	Utilise le <code>versioning</code> sous-ressource pour définir l'état de version d'un bucket existant. Vous pouvez définir l'état de versionnage avec l'une des valeurs suivantes : • Activé : active le contrôle de version pour les objets du bucket. Tous les objets ajoutés au bucket reçoivent un ID de version unique. • Suspendu : désactive le contrôle de version pour les objets du bucket. Tous les objets ajoutés au bucket reçoivent l'ID de version <code>null</code>.
Configuration de PutObjectLock	Configure ou supprime le mode de conservation par défaut du bucket et la période de conservation par défaut. Si la période de conservation par défaut est modifiée, la date de conservation des versions d'objet existantes reste la même et n'est pas recalculée à l'aide de la nouvelle période de conservation par défaut. Voir "Utiliser l'API REST S3 pour configurer le verrouillage d'objet S3" pour des informations détaillées.

Opérations sur les objets

Opérations sur les objets

Cette section décrit comment le système StorageGRID implémente les opérations API REST S3 pour les objets.

Les conditions suivantes s'appliquent à toutes les opérations sur les objets :

- StorageGRID "**valeurs de cohérence**" sont pris en charge par toutes les opérations sur les objets, à l'exception des suivantes :
 - ObtenirObjectAcl
 - OPTIONS /
 - MettreObjetLegalHold
 - PutObjectRetention
 - Sélectionner le contenu de l'objet
- Les demandes client conflictuelles, telles que deux clients écrivant sur la même clé, sont résolues sur la base des « derniers gagnants ». Le moment de l'évaluation des « dernières victoires » est basé sur le moment où le système StorageGRID termine une demande donnée, et non sur le moment où les clients S3 commencent une opération.
- Tous les objets d'un bucket StorageGRID appartiennent au propriétaire du bucket, 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 suivant décrit comment StorageGRID implémente les opérations d'objet S3 REST API.

Opération	Mise en œuvre
Supprimer l'objet	Authentification multifacteur (MFA) et en-tête de réponse <code>x-amz-mfa</code> ne sont pas pris en charge. Lors du traitement d'une demande <code>DeleteObject</code>, StorageGRID tente de supprimer immédiatement toutes les copies de l'objet de tous les 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, puis indique la réussite au client. Gestion des versions Pour supprimer une version spécifique, le demandeur doit être le propriétaire du bucket et utiliser le <code>versionId</code> sous-ressource. L'utilisation de cette sous-ressource supprime définitivement la version. Si le <code>versionId</code> correspond à un marqueur de suppression, l'en-tête de réponse <code>x-amz-delete-marker</code> est renvoyé défini sur <code>true</code>. • Si un objet est supprimé sans le <code>versionId</code> sous-ressource sur un bucket avec le contrôle de version activé, cela entraîne la génération d'un marqueur de suppression. Le <code>versionId</code> pour le marqueur de suppression est renvoyé en utilisant le <code>x-amz-version-id</code> en-tête de réponse et le <code>x-amz-delete-marker</code> l'en-tête de réponse est renvoyé défini sur <code>true</code>. • Si un objet est supprimé sans le <code>versionId</code> sous-ressource sur un bucket avec contrôle de version suspendu, cela entraîne une suppression permanente d'une version « null » déjà existante ou d'un marqueur de suppression « null », et la génération d'un nouveau marqueur de suppression « null ». Le <code>x-amz-delete-marker</code> l'en-tête de réponse est renvoyé défini sur <code>true</code>. Remarque : Dans certains cas, plusieurs marqueurs de suppression peuvent exister pour un objet. Voir "Utiliser l'API REST S3 pour configurer le verrouillage d'objet S3" pour savoir comment supprimer des versions d'objets en mode GOUVERNANCE.
Supprimer les objets (précédemment nommé SUPPRIMER plusieurs objets)	Authentification multifacteur (MFA) et en-tête de réponse <code>x-amz-mfa</code> ne sont pas pris en charge. Plusieurs objets peuvent être supprimés dans le même message de demande. Voir "Utiliser l'API REST S3 pour configurer le verrouillage d'objet S3" pour savoir comment supprimer des versions d'objets en mode GOUVERNANCE.

Opération	Mise en œuvre
Supprimer l'étiquetage des objets	Utilise le <code>tagging</code> sous-ressource pour supprimer toutes les balises d'un objet. Gestion des versions Si le <code>versionId</code> si le paramètre de requête n'est pas spécifié dans la requête, l'opération supprime toutes les balises de la version la plus récente de l'objet dans un bucket versionné. Si la version actuelle de l'objet est un marqueur de suppression, un statut « <code>MethodNotAllowed</code> » est renvoyé avec le <code>x-amz-delete-marker</code> en-tête de réponse défini sur <code>true</code>.
Obtenir l'objet	"Obtenir l'objet"
ObtenirObjectAcl	Si les informations d'identification d'accès nécessaires sont fournies pour le compte, l'opération renvoie une réponse positive et l'ID, le nom d'affichage et l'autorisation du propriétaire de l'objet, indiquant que le propriétaire dispose d'un accès complet à l'objet.
Obtenir la conservation légale de l'objet	"Utiliser l'API REST S3 pour configurer le verrouillage d'objet S3"
Obtenir la rétention d'objet	"Utiliser l'API REST S3 pour configurer le verrouillage d'objet S3"
Obtenir l'étiquetage des objets	Utilise le <code>tagging</code> sous-ressource pour renvoyer toutes les balises d'un objet. Gestion des versions Si le <code>versionId</code> si le paramètre de requête n'est pas spécifié dans la requête, l'opération renvoie toutes les balises de la version la plus récente de l'objet dans un bucket versionné. Si la version actuelle de l'objet est un marqueur de suppression, un statut « <code>MethodNotAllowed</code> » est renvoyé avec le <code>x-amz-delete-marker</code> en-tête de réponse défini sur <code>true</code>.
HeadObject	"HeadObject"
Restaurer l'objet	"Restaurer l'objet"
Mettre l'objet	"Mettre l'objet"
Copier l'objet (précédemment nommé PUT Object - Copy)	"Copier l'objet"
MettreObjetLegalHold	"Utiliser l'API REST S3 pour configurer le verrouillage d'objet S3"

Opération	Mise en œuvre
PutObjectRetention	"Utiliser l'API REST S3 pour configurer le verrouillage d'objet S3"
Balimage d'objets	Utilise le <code>tagging</code> sous-ressource pour ajouter un ensemble de balises à un objet existant. Limites des balises d'objet Vous pouvez ajouter des balises aux nouveaux objets lorsque vous les téléchargez, ou vous pouvez les ajouter aux 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 contenir jusqu'à 128 caractères Unicode et les valeurs de balise peuvent contenir jusqu'à 256 caractères Unicode. La clé et les valeurs sont sensibles à la casse. Mises à jour des balises et comportement d'ingestion Lorsque vous utilisez PutObjectTagging pour mettre à jour les balises d'un objet, StorageGRID ne réingère pas l'objet. Cela signifie que l'option pour le comportement d'ingestion spécifiée dans la règle ILM correspondante n'est pas utilisée. Toutes les modifications apportées au placement des objets déclenchées par la mise à jour sont effectuées lorsque ILM est réévalué par les processus ILM d'arrière-plan normaux. Cela signifie que si la règle ILM utilise l'option Strict pour le comportement d'ingestion, aucune action n'est entreprise si les placements d'objets requis ne peuvent pas être effectués (par exemple, parce qu'un emplacement nouvellement requis n'est pas disponible). L'objet mis à jour conserve son emplacement actuel jusqu'à ce que le placement requis soit possible. Résoudre les conflits Les demandes client conflictuelles, telles que deux clients écrivant sur la même clé, sont résolues sur la base des « derniers gagnants ». Le moment de l'évaluation des « dernières victoires » est basé sur le moment où le système StorageGRID termine une demande donnée, et non sur le moment où les clients S3 commencent une opération. Gestion des versions Si le <code>versionId</code> 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 bucket versionné. Si la version actuelle de l'objet est un marqueur de suppression, un statut « MethodNotAllowed » est renvoyé avec le <code>x-amz-delete-marker</code> en-tête de réponse défini sur <code>true</code>.
Sélectionner le contenu de l'objet	"Sélectionner le contenu de l'objet"

Utiliser S3 Select

StorageGRID prend en charge les clauses, types de données et opérateurs Amazon S3 Select suivants pour le ["Commande SelectObjectContent"](#) .



Tous les éléments non répertoriés ne sont pas pris en charge.

Pour la syntaxe, voir ["Sélectionner le contenu de l'objet"](#) . Pour plus d'informations sur S3 Select, consultez le ["Documentation AWS pour S3 Select"](#) .

Seuls les comptes locataires pour lesquels S3 Select est activé peuvent émettre des requêtes SelectObjectContent. Voir le ["considérations et exigences pour l'utilisation de S3 Select"](#) .

Clauses

- Liste SELECT
- Clause FROM
- Clause WHERE
- Clause LIMIT

Types de données

- booléen
- entier
- chaîne
- flotter
- décimal, numérique
- horodatage

Opérateurs

Opérateurs logiques

- ET
- PAS
- OU

Opérateurs de comparaison

- <
- >
- <=
- >=
- =
- =
- <>

- !=
- ENTRE
- DANS

Opérateurs de recherche de motifs

- COMME
- _
- %

opérateurs unitaires

- EST NUL
- N'EST PAS NUL

opérateurs mathématiques

- +
- -
- *
- /
- %

StorageGRID suit la priorité de l'opérateur Amazon S3 Select.

Fonctions d'agrégation

- MOYENNE()
- COMPTE(*)
- MAX()
- MIN()
- SOMME()

Fonctions conditionnelles

- CAS
- SE FONDRE
- NULLIF

Fonctions de conversion

- CAST (pour le type de données pris en charge)

Fonctions de date

- DATE_ADD
- DATE_DIFF

- EXTRAIT
- TO_STRING
- À_HORODATAGE
- UTCNOW

Fonctions de chaîne

- LONGUEUR_CARACTÈRE, LONGUEUR_CARACTÈRE
- INFÉRIEUR
- SOUS-CHAÎNE
- GARNITURE
- SUPÉRIEUR

Utiliser le cryptage côté serveur

Le chiffrement côté serveur vous permet de protéger vos données d'objet au repos. StorageGRID crypte les données lorsqu'il écrit l'objet 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 manière dont les clés de chiffrement sont gérées :

- **SSE (chiffrement côté serveur avec clés gérées par StorageGRID)** : lorsque vous émettez une demande S3 pour stocker un objet, StorageGRID chiffre l'objet avec une clé unique. Lorsque vous émettez une demande S3 pour récupérer l'objet, StorageGRID utilise la clé stockée pour déchiffrer 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 déchiffré et vos données d'objet sont renvoyées.

Bien que StorageGRID gère toutes les opérations de chiffrement et de déchiffrement d'objets, vous devez gérer les clés de chiffrement 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 bucket ou de la grille sont ignorés.

Utiliser SSE

Pour chiffrer un objet avec une clé unique gérée par StorageGRID, vous utilisez l'en-tête de requête suivant :

```
x-amz-server-side-encryption
```

L'en-tête de requête SSE est pris en charge par les opérations d'objet suivantes :

- ["Mettre l'objet"](#)

- ["Copier l'objet"](#)
- ["Créer un téléchargement multi-parties"](#)

Utiliser SSE-C

Pour crypter un objet avec une clé unique que vous gérez, vous utilisez trois en-têtes de requête :

En-tête de la requête	Description
x-amz-server-side-encryption-customer-algorithm	Spécifiez l'algorithme de cryptage. La valeur de l'en-tête doit être AES256 .
x-amz-server-side-encryption-customer-key	Spécifiez la clé de chiffrement qui sera utilisée pour chiffrer ou déchiffrer l'objet. La valeur de la clé doit être de 256 bits, codée en base64.
x-amz-server-side-encryption-customer-key-MD5	Spécifiez le condensé MD5 de la clé de chiffrement conformément à la RFC 1321, qui est utilisé pour garantir que la clé de chiffrement a été transmise sans erreur. La valeur du condensé MD5 doit être codée en base64 sur 128 bits.

Les en-têtes de requête SSE-C sont pris en charge par les opérations d'objet suivantes :

- ["Obtenir l'objet"](#)
- ["HeadObject"](#)
- ["Mettre l'objet"](#)
- ["Copier l'objet"](#)
- ["Créer un téléchargement multi-parties"](#)
- ["Télécharger une partie"](#)
- ["TéléchargerPartCopy"](#)

Considérations relatives à l'utilisation du chiffrement côté serveur avec des clés fournies par le client (SSE-C)

Avant d'utiliser SSE-C, tenez compte des considérations suivantes :

- Vous devez utiliser https.



StorageGRID rejette toute requête effectuée via http lors de l'utilisation de SSE-C. Pour des raisons de sécurité, il est important de considérer que toute clé envoyée accidentellement via http est compromise. Jetez la clé et faites-la tourner comme il convient.

- L'ETag dans la réponse n'est pas le MD5 des données de l'objet.
- Vous devez gérer le mappage des clés de chiffrement aux objets. StorageGRID ne stocke pas les clés de chiffrement. Vous êtes responsable du suivi de la clé de cryptage que vous fournissez pour chaque objet.
- Si votre bucket est compatible avec le contrôle de version, chaque version d'objet doit avoir sa propre clé de chiffrement. Vous êtes responsable du suivi de la clé de chiffrement utilisée pour chaque version d'objet.

- Étant donné que vous gérez les clés de chiffrement côté client, vous devez également gérer toutes les mesures de protection supplémentaires, telles 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-grille ou la réplication CloudMirror est configurée pour le bucket, vous ne pouvez pas ingérer d'objets SSE-C. L'opération d'ingestion échouera.

Informations connexes

["Guide de l'utilisateur Amazon S3 : Utilisation du chiffrement côté serveur avec les clés fournies par le client \(SSE-C\)"](#)

Copier l'objet

Vous pouvez utiliser la requête S3 CopyObject pour créer une copie d'un objet déjà stocké dans S3. Une opération CopyObject revient à exécuter GetObject suivi de PutObject.

Résoudre les conflits

Les demandes client conflictuelles, telles que deux clients écrivant sur la même clé, sont résolues sur la base des « derniers gagnants ». Le moment de l'évaluation des « dernières victoires » est basé sur le moment où le système StorageGRID termine une demande donnée, et non sur le moment où les clients S3 commencent une opération.

Taille de l'objet

La taille maximale *recommandée* pour une seule opération PutObject est de 5 Gio (5 368 709 120 octets). Si vous avez des objets dont la taille est supérieure à 5 Gio, utilisez ["téléchargement en plusieurs parties"](#) plutôt.

La taille maximale *prise en charge* pour une seule opération PutObject est de 5 Tio (5 497 558 138 880 octets).



Si vous avez effectué une mise à niveau à partir de StorageGRID 11.6 ou d'une version antérieure, l'alerte S3 PUT La taille de l'objet est trop grande sera déclenchée si vous tentez de télécharger un objet dépassant 5 Gio. Si vous disposez d'une nouvelle installation de StorageGRID 11.7 ou 11.8, l'alerte ne sera pas déclenchée dans ce cas. Cependant, pour s'aligner sur la norme AWS S3, les futures versions de StorageGRID ne prendront pas en charge les téléchargements d'objets supérieurs à 5 Gio.

Caractères UTF-8 dans les métadonnées utilisateur

Si une demande inclut des valeurs UTF-8 (non échappées) dans le nom de clé ou la valeur des métadonnées définies par l'utilisateur, le comportement de StorageGRID n'est pas défini.

StorageGRID n'analyse ni n'interprète les caractères UTF-8 échappés inclus 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 inclut des caractères non imprimables.

En-têtes de requête 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 vous permet de copier l'objet et les métadonnées associées.

Vous pouvez spécifier `REPLACE` pour écraser les métadonnées existantes lors de la copie de l'objet, ou pour mettre à jour les 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 écraser 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 conservation par défaut du bucket sont utilisés pour calculer le mode de version de l'objet et la date de conservation. Voir ["Utiliser l'API REST S3 pour configurer le verrouillage d'objet S3"](#) .

- En-têtes de requête 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 [En-têtes de requête pour le chiffrement côté serveur](#)

En-têtes de requête non pris en charge

Les en-têtes de requête suivants ne sont pas pris en charge :

- `Cache-Control`
- `Content-Disposition`
- `Content-Encoding`
- `Content-Language`
- `Expires`
- `x-amz-checksum-algorithm`

Lorsque vous copiez un objet, si l'objet source possède une somme de contrôle, StorageGRID ne copie pas cette valeur de somme de contrôle dans le nouvel objet. Ce comportement s'applique que vous essayiez ou non d'utiliser `x-amz-checksum-algorithm` dans la demande d'objet.

- `x-amz-website-redirect-location`

Options de classe de stockage

Le `x-amz-storage-class` L'en-tête de requête est pris en charge et affecte le nombre de copies d'objets créées par StorageGRID si la règle ILM correspondante utilise la validation double ou équilibrée ["option d'ingestion"](#) .

- `STANDARD`

(Par défaut) Spécifie une opération d'ingestion à double validation lorsque la règle ILM utilise l'option Double validation ou lorsque l'option Équilibré revient à la création de copies intermédiaires.

- `REDUCED_REDUNDANCY`

Spécifie une opération d'ingestion à validation unique lorsque la règle ILM utilise l'option de validation double ou lorsque l'option Équilibré revient à la création de copies intermédiaires.



Si vous ingérez un objet dans un bucket avec le verrouillage d'objet S3 activé, le `REDUCED_REDUNDANCY` l'option est ignorée. Si vous ingérez un objet dans un bucket conforme hérité, le `REDUCED_REDUNDANCY` l'option renvoie une erreur. StorageGRID effectuera toujours une ingestion à double validation pour garantir que les exigences de conformité sont satisfaites.

Utilisation de `x-amz-copy-source` dans `CopyObject`

Si le bucket source et la clé, spécifiés dans le `x-amz-copy-source` en-tête, sont différents du bucket et de la clé de destination, une copie des données de l'objet source est écrite dans la destination.

Si la source et la destination correspondent, et que 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. Cela a deux conséquences importantes :

- Vous ne pouvez pas utiliser `CopyObject` pour crypter un objet existant sur place ou pour modifier le cryptage d'un objet existant sur place. 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 `XNotImplemented`.
- L'option pour le comportement d'ingestion spécifiée dans la règle ILM correspondante n'est pas utilisée. Toutes les modifications apportées au placement des objets déclenchées par la mise à jour sont effectuées lorsque ILM est réévalué par les processus ILM d'arrière-plan normaux.

Cela signifie que si la règle ILM utilise l'option `Strict` pour le comportement d'ingestion, aucune action n'est entreprise si les placements d'objets requis ne peuvent pas être effectués (par exemple, parce qu'un emplacement nouvellement requis n'est pas disponible). L'objet mis à jour conserve son emplacement actuel jusqu'à ce que le placement requis soit possible.

En-têtes de requête pour le chiffrement côté serveur

Si tu [utilises le cryptage côté serveur](#), les en-têtes de requête que vous fournissez dépendent du fait que l'objet source est chiffré ou non et du fait que vous prévoyez 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 `CopyObject`, afin que l'objet puisse être déchiffré puis copié :
 - `x-amz-copy-source-server-side-encryption-customer-algorithm`: Préciser `AES256`.
 - `x-amz-copy-source-server-side-encryption-customer-key`: Spécifiez la clé de chiffrement que vous avez fournie lors de la création de l'objet source.
 - `x-amz-copy-source-server-side-encryption-customer-key-MD5`: Spécifiez le condensé MD5 que vous avez fourni lors de la création de l'objet source.
- Si vous souhaitez crypter 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`: Préciser `AES256`.
 - `x-amz-server-side-encryption-customer-key`: Spécifiez une nouvelle clé de chiffrement pour l'objet cible.
 - `x-amz-server-side-encryption-customer-key-MD5`: Spécifiez le condensé 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 les clés fournies par le client pour sécuriser les données d'objet, examinez les considérations relatives ["en utilisant le cryptage côté serveur"](#).

- Si vous souhaitez crypter l'objet cible (la copie) avec une clé unique gérée par StorageGRID (SSE), incluez cet en-tête dans la requête `CopyObject` :
 - `x-amz-server-side-encryption`



Le `server-side-encryption` la valeur de l'objet ne peut pas être mise à jour. Au lieu de cela, faites une copie avec un nouveau `server-side-encryption` valeur en utilisant `x-amz-metadata-directive: REPLACE`.

Gestion des versions

Si le bucket source est versionné, 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 la commande `versionId` sous-ressource. Si le bucket de destination est versionné, la version générée est renvoyée dans le `x-amz-version-id` en-tête de réponse. Si le contrôle de version est suspendu pour le bucket cible, alors `x-amz-version-id` renvoie une valeur « null ».

Obtenir l'objet

Vous pouvez utiliser la requête S3 `GetObject` pour récupérer un objet d'un bucket S3.

GetObject et objets multipartites

Vous pouvez utiliser le `partNumber` paramètre de requête pour récupérer une partie spécifique d'un objet en plusieurs parties ou segmenté. Le `x-amz-mp-parts-count` L'élément de réponse indique le nombre de parties que contient l'objet.

Vous pouvez définir `partNumber` à 1 pour les objets segmentés/multipartites et les objets non segmentés/non multipartites ; cependant, le `x-amz-mp-parts-count` L'élément de réponse n'est renvoyé que pour les objets segmentés ou en plusieurs parties.

Caractères UTF-8 dans les métadonnées utilisateur

StorageGRID n'analyse ni n'interprète les caractères UTF-8 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 inclut des caractères non imprimables.

En-tête de requête pris en charge

L'en-tête de requête suivant est pris en charge :

- `x-amz-checksum-mode`: Préciser `ENABLED`

Le Range l'en-tête n'est pas pris en charge avec `x-amz-checksum-mode` pour `GetObject`. Lorsque vous incluez Range dans la demande avec `x-amz-checksum-mode` activé, StorageGRID ne renvoie pas de valeur de somme de contrôle dans la réponse.

En-tête de requête non pris en charge

L'en-tête de requête 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 récupère la version la plus récente de l'objet dans un bucket versionné. Si la version actuelle de l'objet est un marqueur de suppression, un statut « Non trouvé » est renvoyé avec le `x-amz-delete-marker` en-tête de réponse défini sur `true`.

En-têtes de requête pour le chiffrement côté serveur avec les 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: Préciser AES256 .
- x-amz-server-side-encryption-customer-key:Spécifiez votre clé de chiffrement pour l'objet.
- x-amz-server-side-encryption-customer-key-MD5: Spécifiez le condensé 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 les clés fournies par le client pour sécuriser les données d'objet, examinez les considérations dans"[Utiliser le cryptage côté serveur](#)" .

Comportement de GetObject pour les objets Cloud Storage Pool

Si un objet a été stocké dans un"[Pool de stockage cloud](#)" , le comportement d'une requête GetObject dépend de l'état de l'objet. Voir"[HeadObject](#)" pour plus de détails.



Si un objet est stocké dans un pool de stockage cloud et qu'une ou plusieurs copies de l'objet existent également sur la grille, les requêtes GetObject tenteront de récupérer les données de la grille, avant de les récupérer du pool de stockage cloud.

État de l'objet	Comportement de GetObject
Objet ingéré dans StorageGRID mais pas encore évalué par ILM, ou objet stocké dans un pool de stockage traditionnel ou utilisant un codage d'effacement	200 OK Une copie de l'objet est récupérée.
Objet dans le pool de stockage cloud, mais pas encore passé à un état non récupérable	200 OK Une copie de l'objet est récupérée.
Objet passé à un état non récupérable	403 Forbidden , InvalidObjectState Utiliser un" Restaurer l'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 RestoreObject soit terminée.
Objet entièrement restauré dans le pool de stockage cloud	200 OK Une copie de l'objet est récupérée.

Objets multipartites ou segmentés dans un pool de stockage cloud

Si vous avez téléchargé un objet en plusieurs parties ou si StorageGRID a divisé un objet volumineux en segments, StorageGRID détermine si l'objet est disponible dans le pool de stockage cloud en échantillonnant un sous-ensemble des parties ou des segments de l'objet. Dans certains cas, une requête `GetObject` peut renvoyer de manière incorrecte `200 OK` lorsque certaines parties de l'objet ont déjà été transférées vers un état non récupérable ou lorsque certaines parties de l'objet n'ont pas encore été restaurées.

Dans ces cas :

- La requête `GetObject` peut renvoyer des données mais s'arrêter à mi-chemin du transfert.
- Une requête `GetObject` ultérieure peut renvoyer `403 Forbidden`.

GetObject et réplication inter-grille

Si vous utilisez "fédération de réseau" et "réplication inter-réseaux" est activé pour un bucket, le client S3 peut vérifier l'état de réplication d'un objet en émettant une requête `GetObject`. La réponse inclut le StorageGRID spécifique `x-ntap-sg-cgr-replication-status` en-tête de réponse, qui aura l'une des valeurs suivantes :

Grille	État de réplication
Source	• TERMINÉ : La réplication a réussi. • EN ATTENTE : L'objet n'a pas encore été répliqué. • ÉCHEC : La réplication a échoué avec un échec permanent. Un 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.

HeadObject

Vous pouvez utiliser la requête S3 `HeadObject` pour récupérer les métadonnées d'un objet sans renvoyer l'objet lui-même. Si l'objet est stocké dans un pool de stockage cloud, vous pouvez utiliser `HeadObject` pour déterminer l'état de transition de l'objet.

HeadObject et objets multipartites

Vous pouvez utiliser le `partNumber` paramètre de demande pour récupérer les métadonnées d'une partie spécifique d'un objet en plusieurs parties ou segmenté. Le `x-amz-mp-parts-count` L'élément de réponse indique le nombre de parties que contient l'objet.

Vous pouvez définir `partNumber` à 1 pour les objets segmentés/multipartites et les objets non segmentés/non multipartites ; cependant, le `x-amz-mp-parts-count` L'élément de réponse n'est renvoyé que pour les objets segmentés ou en plusieurs parties.

Caractères UTF-8 dans les métadonnées utilisateur

StorageGRID n'analyse ni n'interprète les caractères UTF-8 échappés dans les métadonnées définies par

l'utilisateur. Les requêtes 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 inclut des caractères non imprimables.

En-tête de requête pris en charge

L'en-tête de requête suivant est pris en charge :

- `x-amz-checksum-mode`

Le `partNumber` paramètre et `Range` les en-têtes ne sont pas pris en charge avec `x-amz-checksum-mode` pour `HeadObject`. Lorsque vous les incluez dans la demande avec `x-amz-checksum-mode` activé, `StorageGRID` ne renvoie pas de valeur de somme de contrôle dans la réponse.

En-tête de requête non pris en charge

L'en-tête de requête 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 récupère la version la plus récente de l'objet dans un bucket versionné. Si la version actuelle de l'objet est un marqueur de suppression, un statut « Non trouvé » est renvoyé avec le `x-amz-delete-marker` en-tête de réponse défini sur `true`.

En-têtes de requête pour le chiffrement côté serveur avec les clés de chiffrement fournies par le client (SSE-C)

Utilisez ces trois en-têtes si l'objet est chiffré avec une clé unique que vous avez fournie.

- `x-amz-server-side-encryption-customer-algorithm`: Préciser AES256.
- `x-amz-server-side-encryption-customer-key`: Spécifiez votre clé de chiffrement pour l'objet.
- `x-amz-server-side-encryption-customer-key-MD5`: Spécifiez le condensé 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 les clés fournies par le client pour sécuriser les données d'objet, examinez les considérations dans ["Utiliser le cryptage côté serveur"](#).

Réponses `HeadObject` pour les objets `Cloud Storage Pool`

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 lorsqu'il est déplacé vers un pool de stockage cloud, éventuellement transféré vers un état non récupérable et restauré.

État de l'objet	Réponse à HeadObject
Objet ingéré dans StorageGRID mais pas encore évalué par ILM, ou objet stocké dans un pool de stockage traditionnel ou utilisant un codage d'effacement	200 OK(Aucun en-tête de réponse spécial n'est renvoyé.)
Objet dans le pool de stockage cloud, mais pas encore passé à 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 vers un état non récupérable, la valeur de expiry-date se déroule à une époque lointaine dans le futur. L'heure exacte de la transition n'est pas contrôlée par le système StorageGRID .
L'objet est passé à un état non récupérable, mais au moins une copie existe également 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 se déroule à une époque lointaine 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 " Restaurer l'objet " demandez à restaurer la copie à partir du pool de stockage cloud avant de pouvoir récupérer l'objet avec succès.
L'objet est passé 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 HeadObject
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 2018 00:00:00 GMT" Le expiry-date indique quand l'objet dans le pool de stockage cloud sera renvoyé à un état non récupérable.

Objets multipartites ou segmentés dans le pool de stockage cloud

Si vous avez téléchargé un objet en plusieurs parties ou si StorageGRID a divisé un objet volumineux en segments, StorageGRID détermine si l'objet est disponible dans le pool de stockage cloud en échantillonnant un sous-ensemble des parties ou des segments de l'objet. Dans certains cas, une requête HeadObject peut renvoyer de manière incorrecte `x-amz-restore: ongoing-request="false"` lorsque certaines parties de l'objet ont déjà été transférées vers un état non récupérable ou lorsque certaines parties de l'objet n'ont pas encore été restaurées.

Réplication HeadObject et inter-grille

Si vous utilisez ["fédération de réseau"](#) et ["réplication inter-réseaux"](#) est activé pour un bucket, le client S3 peut vérifier l'état de réplication d'un objet en émettant une demande HeadObject. La réponse inclut le StorageGRID spécifique `x-ntap-sg-cgr-replication-status` en-tête de réponse, qui aura l'une des valeurs suivantes :

Grille	État de réplication
Source	• TERMINÉ : La réplication a réussi. • EN ATTENTE : L'objet n'a pas encore été répliqué. • ÉCHEC : La réplication a échoué avec un échec permanent. Un 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.

Mettre l'objet

Vous pouvez utiliser la requête S3 PutObject pour ajouter un objet à un bucket.

Résoudre les conflits

Les demandes client conflictuelles, telles que deux clients écrivant sur la même clé, sont résolues sur la base des « derniers gagnants ». Le moment de l'évaluation des « dernières victoires » est basé sur le moment où le système StorageGRID termine une demande donnée, et non sur le moment où les clients S3 commencent une

opération.

Taille de l'objet

La taille maximale *recommandée* pour une seule opération PutObject est de 5 Gio (5 368 709 120 octets). Si vous avez des objets dont la taille est supérieure à 5 Gio, utilisez ["téléchargement en plusieurs parties"](#) plutôt.

La taille maximale *prise en charge* pour une seule opération PutObject est de 5 Tio (5 497 558 138 880 octets).



Si vous avez effectué une mise à niveau à partir de StorageGRID 11.6 ou d'une version antérieure, l'alerte S3 PUT La taille de l'objet est trop grande sera déclenchée si vous tentez de télécharger un objet dépassant 5 Gio. Si vous disposez d'une nouvelle installation de StorageGRID 11.7 ou 11.8, l'alerte ne sera pas déclenchée dans ce cas. Cependant, pour s'aligner sur la norme AWS S3, les futures versions de StorageGRID ne prendront pas en charge les téléchargements d'objets supérieurs à 5 Gio.

Taille des métadonnées utilisateur

Amazon S3 limite la taille des métadonnées définies par l'utilisateur dans chaque en-tête de requête PUT à 2 Ko. StorageGRID limite les métadonnées utilisateur à 24 Ko. La taille des métadonnées définies par l'utilisateur est mesurée en prenant la somme du nombre d'octets dans l'encodage UTF-8 de chaque clé et valeur.

Caractères UTF-8 dans les métadonnées utilisateur

Si une demande inclut des valeurs UTF-8 (non échappées) dans le nom de clé ou la valeur des métadonnées définies par l'utilisateur, le comportement de StorageGRID n'est pas défini.

StorageGRID n'analyse ni n'interprète les caractères UTF-8 échappés inclus 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 PutObject, CopyObject, GetObject et HeadObject 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 inclut des caractères non imprimables.

Limites des balises d'objet

Vous pouvez ajouter des balises aux nouveaux objets lorsque vous les téléchargez, ou vous pouvez les ajouter aux 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 contenir jusqu'à 128 caractères Unicode et les valeurs de balise peuvent contenir jusqu'à 256 caractères Unicode. La clé et les valeurs sont sensibles à la casse.

Propriété de l'objet

Dans StorageGRID, tous les objets appartiennent au compte propriétaire du bucket, y compris les objets créés par un compte non propriétaire ou un utilisateur anonyme.

En-têtes de requête 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 du 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

L'encodage de transfert fragmenté est pris en charge si `aws-chunked` la signature de la charge utile est également utilisée.

- `x-amz-checksum-sha256`
- `x-amz-meta-`, suivi d'une paire nom-valeur contenant des métadonnées définies par l'utilisateur.

Lors de la spécification de la paire nom-valeur pour les métadonnées définies par l'utilisateur, utilisez ce format général :

```
x-amz-meta-name: value
```

Si vous souhaitez utiliser l'option **Heure de création définie par l'utilisateur** comme heure de référence pour une règle ILM, vous devez utiliser `creation-time` comme le nom des métadonnées qui enregistrent quand l'objet a été créé. Par exemple:

```
x-amz-meta-creation-time: 1443399726
```

La valeur pour `creation-time` est évalué 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 l'option d'ingestion équilibrée ou stricte. Une erreur est renvoyée lors de la création de la règle ILM.

- `x-amz-tagging`
- 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 conservation par défaut du bucket sont utilisés pour calculer le mode de version de l'objet et la date de conservation. Voir ["Utiliser l'API REST S3 pour configurer le verrouillage d'objet S3"](#) .

- En-têtes de requête 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 [En-têtes de requête pour le chiffrement côté serveur](#)

En-têtes de requête non pris en charge

Les en-têtes de requête suivants ne sont pas pris en charge :

- `x-amz-acl`
- `x-amz-sdk-checksum-algorithm`
- `x-amz-trailer`
- `x-amz-website-redirect-location`

Le `x-amz-website-redirect-location` retourne d'en-tête `XNotImplemented` .

Options de classe de stockage

Le `x-amz-storage-class` l'en-tête de requête est pris en charge. La valeur soumise pour `x-amz-storage-class` affecte la manière dont StorageGRID protège les données de l'objet pendant l'ingestion et non le nombre de copies persistantes de l'objet stockées dans le système StorageGRID (qui est déterminé par ILM).

Si la règle ILM correspondant à un objet ingéré utilise l'option d'ingestion stricte, le `x-amz-storage-class` l'en-tête n'a aucun effet.

Les valeurs suivantes peuvent être utilisées pour `x-amz-storage-class` :

- STANDARD(Défaut)
 - **Double validation** : si la règle ILM spécifie l'option Double validation pour le comportement d'ingestion, dès qu'un objet est ingéré, une deuxième copie de cet objet est créée et distribuée à un autre nœud de stockage (double validation). Lorsque l'ILM est évalué, StorageGRID détermine si ces copies intermédiaires initiales satisfont aux instructions de placement de la règle. Si ce n'est pas le

cas, de nouvelles copies d'objets devront peut-être être réalisées à des emplacements différents et les copies intermédiaires initiales devront peut-être être supprimées.

- **Équilibré** : si la règle ILM spécifie l'option Équilibré et que StorageGRID ne peut pas effectuer immédiatement toutes les copies spécifiées dans la règle, StorageGRID effectue deux copies intermédiaires sur différents nœuds de stockage.

Si StorageGRID peut créer immédiatement toutes les copies d'objets spécifiées dans la règle ILM (placement synchrone), le `x-amz-storage-class` l'en-tête n'a aucun effet.

- **REDUCED_REDUNDANCY**

- *** Double validation *** : si la règle ILM spécifie l'option Double validation pour le comportement d'ingestion, StorageGRID crée une copie intermédiaire unique lorsque l'objet est ingéré (validation unique).
- **Équilibré** : si la règle ILM spécifie l'option Équilibré, StorageGRID effectue une seule copie intermédiaire uniquement si le système ne peut pas effectuer immédiatement 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 mieux utilisée lorsque la règle ILM qui correspond à l'objet crée une seule copie répliquée. Dans ce cas, en utilisant **REDUCED_REDUNDANCY** élimine la création et la suppression inutiles d'une copie d'objet supplémentaire pour chaque opération d'ingestion.

En utilisant le **REDUCED_REDUNDANCY** Cette option n'est pas recommandée dans d'autres circonstances. **REDUCED_REDUNDANCY** augmente le risque de perte de données d'objet lors de l'ingestion. Par exemple, vous risquez de perdre des données si la copie unique est initialement stockée sur un nœud de stockage qui échoue avant que l'évaluation ILM puisse avoir lieu.



Le fait de n'avoir qu'une seule copie répliquée pendant une période donnée expose les données à un risque de perte permanente. Si une seule copie répliquée d'un objet existe, cet objet est perdu si un nœud de stockage échoue ou présente une erreur importante. Vous perdez également temporairement l'accès à l'objet pendant les procédures de maintenance telles que les mises à niveau.

Spécification **REDUCED_REDUNDANCY** affecte uniquement le nombre de copies créées lorsqu'un objet est ingéré pour la première fois. Cela n'affecte pas le nombre de copies de l'objet effectuées lorsque l'objet est évalué par les stratégies ILM actives et n'entraîne pas le stockage des données à des niveaux de redondance inférieurs dans le système StorageGRID .



Si vous ingérez un objet dans un bucket avec le verrouillage d'objet S3 activé, le **REDUCED_REDUNDANCY** l'option est ignorée. Si vous ingérez un objet dans un bucket conforme hérité, le **REDUCED_REDUNDANCY** l'option renvoie une erreur. StorageGRID effectuera toujours une ingestion à double validation pour garantir que les exigences de conformité sont satisfaites.

En-têtes de requête pour le chiffrement côté serveur

Vous pouvez utiliser les en-têtes de requête suivants pour crypter un objet avec un cryptage côté serveur. Les options SSE et SSE-C s'excluent mutuellement.

- **SSE** : utilisez l'en-tête suivant si vous souhaitez chiffrer l'objet avec une clé unique gérée par StorageGRID.
 - `x-amz-server-side-encryption`

Quand le `x-amz-server-side-encryption` l'en-tête n'est pas inclus dans la requête `PutObject`, la grille entière "[paramètre de cryptage des objets stockés](#)" est omis de la réponse `PutObject`.

- **SSE-C** : utilisez ces trois en-têtes si vous souhaitez chiffrer l'objet avec une clé unique que vous fournissez et gérez.
 - `x-amz-server-side-encryption-customer-algorithm`: Préciser AES256 .
 - `x-amz-server-side-encryption-customer-key`: Spécifiez votre clé de chiffrement pour le nouvel objet.
 - `x-amz-server-side-encryption-customer-key-MD5`: Spécifiez le condensé 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 les clés fournies par le client pour sécuriser les données d'objet, examinez les considérations relatives "[en utilisant le cryptage côté serveur](#)".



Si un objet est chiffré avec SSE ou SSE-C, tous les paramètres de chiffrement au niveau du bucket ou de la grille sont ignorés.

Gestion des versions

Si le contrôle de version est activé pour un bucket, un `versionId` est généré automatiquement pour la version de l'objet stocké. Ce `versionId` est également renvoyé dans la réponse en utilisant le `x-amz-version-id` en-tête de réponse.

Si le contrôle de version est suspendu, la version de l'objet est stockée avec une valeur nulle `versionId` et si une version nulle existe déjà, elle sera écrasée.

Calculs de signature pour l'en-tête d'autorisation

Lors de l'utilisation du `Authorization` en-tête pour authentifier les requêtes, StorageGRID diffère d'AWS des manières suivantes :

- StorageGRID ne nécessite pas `host` en-têtes à inclure dans `CanonicalHeaders` .
- StorageGRID ne nécessite pas `Content-Type` à inclure dans `CanonicalHeaders` .
- StorageGRID ne nécessite pas `x-amz-*` en-têtes à inclure dans `CanonicalHeaders` .



En règle générale, incluez toujours ces en-têtes dans `CanonicalHeaders` pour garantir 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 en un seul bloc \(AWS Signature Version 4\)](#)".

Informations connexes

- "[Gérer les objets avec ILM](#)"
- "[Référence de l'API Amazon Simple Storage Service : PutObject](#)"

Restaurer l'objet

Vous pouvez utiliser la demande S3 RestoreObject pour restaurer un objet stocké dans un pool de stockage cloud.

Type de demande pris en charge

StorageGRID prend uniquement en charge les requêtes RestoreObject pour restaurer un objet. Il ne prend pas en charge le SELECT type de restauration. Sélectionnez les demandes de retour XNotImplemented .

Gestion des versions

En option, précisez versionId pour restaurer une version spécifique d'un objet dans un bucket versionné. Si vous ne précisez pas versionId , la version la plus récente de l'objet est restaurée

Comportement de RestoreObject sur les objets du pool de stockage cloud

Si un objet a été stocké dans un "Pool de stockage cloud" , une demande RestoreObject a le comportement suivant, en fonction de l'état de l'objet. Voir "HeadObject" pour plus de détails.



Si un objet est stocké dans un pool de stockage cloud et qu'une ou plusieurs copies de l'objet existent également sur la grille, il n'est pas nécessaire de restaurer l'objet en émettant une demande RestoreObject. Au lieu de cela, la copie locale peut être récupérée directement, à l'aide d'une requête GetObject.

État de l'objet	Comportement de RestoreObject
Objet 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 le pool de stockage cloud, mais pas encore passé à un état non récupérable	`200 OK`Aucune modification n'est apportée. Remarque : Avant qu'un objet ne soit passé à un état non récupérable, vous ne pouvez pas modifier son expiry-date .

État de l'objet	Comportement de RestoreObject
Objet passé à un état non récupérable	`202 Accepted` Restaure une copie récupérable de l'objet dans 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 remis dans un état non récupérable. En option, utilisez le <code>Tier</code> élément de demande pour déterminer combien de temps la tâche de restauration prendra pour se terminer(<code>Expedited</code>, <code>Standard</code>, ou <code>Bulk</code>). Si vous ne précisez pas <code>Tier</code>, le <code>Standard</code> 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 de <code>Expedited</code> étage. L'erreur suivante est renvoyée <code>403 Forbidden, InvalidTier: Retrieval option is not supported by this storage class.</code>
Objet en cours de restauration à partir d'un état non récupérable	<code>409 Conflict, RestoreAlreadyInProgress</code>
Objet entièrement restauré dans le pool de stockage cloud	<code>200 OK</code> Remarque : si un objet a été restauré dans un état récupérable, vous pouvez modifier son <code>expiry-date</code> en réémettant la requête <code>RestoreObject</code> avec une nouvelle valeur pour <code>Days</code>. La date de restauration est mise à jour par rapport à l'heure de la demande.

Sélectionner le contenu de l'objet

Vous pouvez utiliser la requête `S3 SelectObjectContent` pour filtrer le contenu d'un objet S3 en fonction d'une simple instruction SQL.

Pour plus d'informations, voir ["Référence de l'API Amazon Simple Storage Service : SelectObjectContent"](#).

Avant de commencer

- Le compte locataire dispose de l'autorisation `S3 Select`.
- Tu as `s3:GetObject` autorisation pour l'objet que vous souhaitez interroger.
- L'objet que vous souhaitez interroger doit être dans l'un des formats suivants :
 - **CSV.** Peut être utilisé tel quel ou compressé dans des archives GZIP ou BZIP2.
 - **Parquet.** Exigences supplémentaires pour les objets Parquet :
 - S3 Select prend uniquement en charge la compression en colonnes à l'aide de GZIP ou 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 compressé est de 512 Mo.
 - Vous devez utiliser les types de données spécifiés dans le schéma de l'objet.

- Vous ne pouvez pas utiliser les types logiques INTERVAL, JSON, LIST, TIME ou 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 Mio.

Exemple de syntaxe de requête 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, les populations de 2010, les populations estimées de 2015 et le pourcentage de changement à partir des données du recensement américain. 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 , ressemble à 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, ressemble 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
```

Exemple d'utilisation d'AWS-CLI (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, changes.csv, 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 en plusieurs parties

Opérations pour les téléchargements en plusieurs parties

Cette section décrit comment StorageGRID prend en charge les opérations de téléchargement en plusieurs parties.

Les conditions et notes suivantes s'appliquent à toutes les opérations de téléchargement en plusieurs parties :

- Vous ne devez pas dépasser 1 000 téléchargements multipartites simultanés vers un seul bucket, car les résultats des requêtes ListMultipartUploads pour ce bucket peuvent renvoyer des résultats incomplets.
- StorageGRID applique les limites de taille AWS pour les parties en plusieurs parties. Les clients S3 doivent suivre ces directives :
 - Chaque partie d'un téléchargement en plusieurs parties 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, les tailles des pièces doivent être aussi grandes que possible. Par exemple, utilisez des tailles de partie de 5 Gio pour un objet de 100 Gio. Étant donné que chaque partie est considérée comme un objet unique, l'utilisation de grandes tailles de partie réduit la surcharge des métadonnées StorageGRID .
 - Pour les objets inférieurs à 5 Gio, envisagez plutôt d'utiliser un téléchargement non multipartite.
- L'ILM est évalué pour chaque partie d'un objet multipartite au fur et à mesure de son ingestion et pour l'objet dans son ensemble lorsque le téléchargement multipartite est terminé, si la règle ILM utilise l'option Équilibré ou Strict ["option d'ingestion"](#) . Vous devez être conscient de la manière dont cela affecte le placement des objets et des pièces :
 - Si l'ILM change pendant qu'un téléchargement multipartite S3 est en cours, certaines parties de l'objet

peuvent ne pas répondre aux exigences ILM actuelles une fois le téléchargement multipartie terminé. Toute pièce qui n'est pas placée correctement est mise en file d'attente pour une réévaluation ILM et déplacée vers l'emplacement correct ultérieurement.

- Lors de l'évaluation de l'ILM pour une pièce, StorageGRID filtre sur la taille de la pièce, et non sur la taille de l'objet. Cela signifie que des parties d'un objet peuvent être stockées dans des emplacements qui ne répondent pas aux exigences ILM pour l'objet dans son ensemble. Par exemple, si une règle spécifie que tous les objets de 10 Go ou plus sont stockés sur DC1 tandis que tous les objets plus petits sont stockés sur DC2, chaque partie de 1 Go d'un téléchargement multipartie en 10 parties est stockée sur DC2 lors de l'ingestion. Cependant, lorsque l'ILM est évalué pour l'objet dans son ensemble, toutes les parties de l'objet sont déplacées vers DC1.
- Toutes les opérations de téléchargement en plusieurs parties prennent en charge StorageGRID ["valeurs de cohérence"](#) .
- Lorsqu'un objet est ingéré à l'aide d'un téléchargement en plusieurs parties, le ["seuil de segmentation des objets \(1 Gio\)"](#) n'est pas appliqué.
- Selon vos besoins, vous pouvez utiliser ["chiffrement côté serveur"](#) avec des téléchargements en plusieurs parties. Pour utiliser SSE (chiffrement côté serveur avec clés gérées par StorageGRID), vous incluez le `x-amz-server-side-encryption` en-tête de demande dans la demande CreateMultipartUpload uniquement. Pour utiliser SSE-C (chiffrement côté serveur avec clés fournies par le client), vous spécifiez les trois mêmes en-têtes de demande de clé de chiffrement dans la demande CreateMultipartUpload et dans chaque demande UploadPart ultérieure.

Opération	Mise en œuvre
Abandonner le téléchargement en plusieurs parties	Implémenté avec tous les comportements de l'API REST Amazon S3. Sous réserve de modifications sans préavis.
Téléchargement complet en plusieurs parties	Voir "Téléchargement complet en plusieurs parties"
Créer un téléchargement multi-parties (anciennement appelé Initiate Multipart Upload)	Voir "Créer un téléchargement multi-parties"
ListeMultipartUploads	Voir "ListeMultipartUploads"
Liste des pièces	Implémenté avec tous les comportements de l'API REST Amazon S3. Sous réserve de modifications sans préavis.
Télécharger une partie	Voir "Télécharger une partie"
TéléchargerPartCopy	Voir "TéléchargerPartCopy"

Téléchargement complet en plusieurs parties

L'opération CompleteMultipartUpload termine un téléchargement en plusieurs parties d'un objet en assemblant les parties précédemment téléchargées.



StorageGRID prend en charge les valeurs non consécutives dans l'ordre croissant pour le `partNumber` paramètre de demande avec `CompleteMultipartUpload`. Le paramètre peut commencer par n'importe quelle valeur.

Résoudre les conflits

Les demandes client conflictuelles, telles que deux clients écrivant sur la même clé, sont résolues sur la base des « derniers gagnants ». Le moment de l'évaluation des « dernières victoires » est basé sur le moment où le système StorageGRID termine une demande donnée, et non sur le moment où les clients S3 commencent une opération.

En-têtes de requête pris en charge

Les en-têtes de requête suivants sont pris en charge :

- `x-amz-checksum-sha256`
- `x-amz-storage-class`

Le `x-amz-storage-class` l'en-tête affecte le nombre de copies d'objets créées par StorageGRID si la règle ILM correspondante spécifie le ["Option de double validation ou d'ingestion équilibrée"](#) .

- STANDARD

(Par défaut) Spécifie une opération d'ingestion à double validation lorsque la règle ILM utilise l'option Double validation ou lorsque l'option Équilibré revient à la création de copies intermédiaires.

- REDUCED_REDUNDANCY

Spécifie une opération d'ingestion à validation unique lorsque la règle ILM utilise l'option de validation double ou lorsque l'option Équilibré revient à la création de copies intermédiaires.



Si vous ingérez un objet dans un bucket avec le verrouillage d'objet S3 activé, le REDUCED_REDUNDANCY l'option est ignorée. Si vous ingérez un objet dans un bucket conforme hérité, le REDUCED_REDUNDANCY l'option renvoie une erreur. StorageGRID effectuera toujours une ingestion à double validation pour garantir que les exigences de conformité sont satisfaites.



Si un téléchargement en plusieurs parties 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 de la ETag valeur pour les objets en plusieurs parties.

En-têtes de requête non pris en charge

Les en-têtes de requête suivants ne sont pas pris en charge :

- `x-amz-sdk-checksum-algorithm`
- `x-amz-trailer`

Gestion des versions

Cette opération termine un téléchargement en plusieurs parties. Si le contrôle de version est activé pour un bucket, la version de l'objet est créée une fois le téléchargement en plusieurs parties terminé.

Si le contrôle de version est activé pour un bucket, un `versionId` est généré automatiquement pour la version de l'objet stocké. Ce `versionId` est également renvoyé dans la réponse en utilisant le `x-amz-version-id` en-tête de réponse.

Si le contrôle de version est suspendu, la version de l'objet est stockée avec une valeur nulle `versionId` et si une version nulle existe déjà, elle sera écrasée.



Lorsque le contrôle de version est activé pour un bucket, l'exécution d'un téléchargement en plusieurs parties crée toujours une nouvelle version, même s'il existe des téléchargements en plusieurs parties simultanés effectués sur la même clé d'objet. Lorsque le contrôle de version n'est pas activé pour un bucket, il est possible de lancer un téléchargement en plusieurs parties, puis de lancer et de terminer un autre téléchargement en plusieurs parties sur la même clé d'objet. Sur les buckets non versionnés, le téléchargement en plusieurs parties qui se termine en dernier est prioritaire.

Échec de la réplication, de la notification ou de la notification des métadonnées

Si le bucket dans lequel le téléchargement en plusieurs parties se produit est configuré pour un service de plateforme, le téléchargement en plusieurs parties réussit même si l'action de réplication ou de notification associée échoue.

Un locataire peut déclencher la réplication ou la notification ayant échoué en mettant à jour les métadonnées ou les balises de l'objet. Un locataire peut soumettre à nouveau les valeurs existantes pour éviter d'apporter des modifications indésirables.

["Dépanner les services de la plateforme"](#) .

Créer un téléchargement multi-parties

L'opération `CreateMultipartUpload` (précédemment nommée `Initiate Multipart Upload`) lance un téléchargement en plusieurs parties pour un objet et renvoie un ID de téléchargement.

Le `x-amz-storage-class` l'en-tête de requête est pris en charge. La valeur soumise pour `x-amz-storage-class` affecte la manière dont `StorageGRID` protège les données de l'objet pendant l'ingestion et non le nombre de copies persistantes de l'objet stockées dans le système `StorageGRID` (qui est déterminé par ILM).

Si la règle ILM correspondant à un objet ingéré utilise le Strict "[option d'ingestion](#)", le `x-amz-storage-class` l'en-tête n'a aucun effet.

Les valeurs suivantes peuvent être utilisées pour `x-amz-storage-class` :

- **STANDARD**(Défaut)
 - **Double validation** : si la règle ILM spécifie l'option d'ingestion `Double validation`, dès qu'un objet est ingéré, une deuxième copie de cet objet est créée et distribuée à un autre nœud de stockage (double validation). Lorsque l'ILM est évalué, `StorageGRID` détermine si ces copies intermédiaires initiales satisfont aux instructions de placement de la règle. Si ce n'est pas le cas, de nouvelles copies d'objets

devront peut-être être réalisées à des emplacements différents et les copies intermédiaires initiales devront peut-être être supprimées.

- **Équilibré** : si la règle ILM spécifie l'option Équilibré et que StorageGRID ne peut pas effectuer immédiatement toutes les copies spécifiées dans la règle, StorageGRID effectue deux copies intermédiaires sur différents nœuds de stockage.

Si StorageGRID peut créer immédiatement toutes les copies d'objets spécifiées dans la règle ILM (placement synchrone), le `x-amz-storage-class` l'en-tête n'a aucun effet.

- **REDUCED_REDUNDANCY**

- **Double validation** : si la règle ILM spécifie l'option Double validation, StorageGRID crée une seule copie intermédiaire lorsque l'objet est ingéré (validation unique).
- **Équilibré** : si la règle ILM spécifie l'option Équilibré, StorageGRID effectue une seule copie intermédiaire uniquement si le système ne peut pas effectuer immédiatement 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 mieux utilisée lorsque la règle ILM qui correspond à l'objet crée une seule copie répliquée. Dans ce cas, en utilisant `REDUCED_REDUNDANCY` élimine la création et la suppression inutiles d'une copie d'objet supplémentaire pour chaque opération d'ingestion.

En utilisant le `REDUCED_REDUNDANCY` Cette option n'est pas recommandée dans d'autres circonstances. `REDUCED_REDUNDANCY` augmente le risque de perte de données d'objet lors de l'ingestion. Par exemple, vous risquez de perdre des données si la copie unique est initialement stockée sur un nœud de stockage qui échoue avant que l'évaluation ILM puisse avoir lieu.



Le fait de n'avoir qu'une seule copie répliquée pendant une période donnée expose les données à un risque de perte permanente. Si une seule copie répliquée d'un objet existe, cet objet est perdu si un nœud de stockage échoue ou présente une erreur importante. Vous perdez également temporairement l'accès à l'objet pendant les procédures de maintenance telles que les mises à niveau.

Spécification `REDUCED_REDUNDANCY` affecte uniquement le nombre de copies créées lorsqu'un objet est ingéré pour la première fois. Cela n'affecte pas le nombre de copies de l'objet effectuées lorsque l'objet est évalué par les stratégies ILM actives et n'entraîne pas le stockage des données à des niveaux de redondance inférieurs dans le système StorageGRID .



Si vous ingérez un objet dans un bucket avec le verrouillage d'objet S3 activé, le `REDUCED_REDUNDANCY` l'option est ignorée. Si vous ingérez un objet dans un bucket conforme hérité, le `REDUCED_REDUNDANCY` l'option renvoie une erreur. StorageGRID effectuera toujours une ingestion à double validation pour garantir que les exigences de conformité sont satisfaites.

En-têtes de requête pris en charge

Les en-têtes de requête suivants sont pris en charge :

- `Content-Type`
- `x-amz-checksum-algorithm`

Actuellement, seule la valeur `SHA256` pour `x-amz-checksum-algorithm` est pris en charge.

- `x-amz-meta-`, suivi d'une paire nom-valeur contenant des métadonnées définies par l'utilisateur

Lors de la spécification de la paire nom-valeur pour les métadonnées définies par l'utilisateur, utilisez ce format général :

```
x-amz-meta-_name_: `value`
```

Si vous souhaitez utiliser l'option **Heure de création définie par l'utilisateur** comme heure de référence pour une règle ILM, vous devez utiliser `creation-time` comme le nom des métadonnées qui enregistrent quand l'objet a été créé. Par exemple:

```
x-amz-meta-creation-time: 1443399726
```

La valeur pour `creation-time` est évalué en secondes depuis le 1er janvier 1970.



Ajout `creation-time` car les métadonnées définies par l'utilisateur ne sont pas autorisées si vous ajoutez un objet à un bucket 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 conservation par défaut du bucket sont utilisés pour calculer la date de conservation de la version de l'objet.

["Utiliser l'API REST S3 pour configurer le verrouillage d'objet S3"](#)

- En-têtes de requête 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`

[En-têtes de requête pour le chiffrement côté serveur](#)



Pour plus d'informations sur la façon dont StorageGRID gère les caractères UTF-8, consultez ["Mettre l'objet"](#) .

En-têtes de requête pour le chiffrement côté serveur

Vous pouvez utiliser les en-têtes de requête suivants pour chiffrer un objet en plusieurs parties avec un chiffrement côté serveur. Les options SSE et SSE-C s'excluent mutuellement.

- **SSE** : utilisez l'en-tête suivant dans la demande `CreateMultipartUpload` si vous souhaitez chiffrer l'objet avec une clé unique gérée par `StorageGRID`. Ne spécifiez pas cet en-tête dans aucune des requêtes `UploadPart`.
 - `x-amz-server-side-encryption`
- **SSE-C** : utilisez ces trois en-têtes dans la demande `CreateMultipartUpload` (et dans chaque demande `UploadPart` ultérieure) si vous souhaitez crypter l'objet avec une clé unique que vous fournissez et gérez.
 - `x-amz-server-side-encryption-customer-algorithm`: Préciser `AES256` .
 - `x-amz-server-side-encryption-customer-key`: Spécifiez votre clé de chiffrement pour le nouvel objet.
 - `x-amz-server-side-encryption-customer-key-MD5`: Spécifiez le condensé 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 les clés fournies par le client pour sécuriser les données d'objet, examinez les considérations relatives ["en utilisant le cryptage côté serveur"](#) .

En-têtes de requête non pris en charge

L'en-tête de requête suivant n'est pas pris en charge :

- `x-amz-website-redirect-location`

Le `x-amz-website-redirect-location` retourne d'en-tête `XNotImplemented` .

Gestion des versions

Le téléchargement en plusieurs parties consiste en des opérations distinctes pour lancer le téléchargement, répertorier les téléchargements, télécharger des parties, assembler les parties téléchargées et terminer le téléchargement. Les objets sont créés (et versionnés si applicable) lorsque l'opération `CompleteMultipartUpload` est effectuée.

ListeMultipartUploads

L'opération `ListMultipartUploads` répertorie les téléchargements multipartites en cours pour un bucket.

Les paramètres de requête suivants sont pris en charge :

- `encoding-type`
- `key-marker`
- `max-uploads`
- `prefix`
- `upload-id-marker`
- `Host`
- `Date`

- Authorization

Gestion des versions

Le téléchargement en plusieurs parties consiste en des opérations distinctes pour lancer le téléchargement, répertorier les téléchargements, télécharger des parties, assembler les parties téléchargées et terminer le téléchargement. Les objets sont créés (et versionnés si applicable) lorsque l'opération CompleteMultipartUpload est effectuée.

Télécharger une partie

L'opération UploadPart télécharge une partie dans un téléchargement en plusieurs parties pour un objet.

En-têtes de requête pris en charge

Les en-têtes de requête suivants sont pris en charge :

- x-amz-checksum-sha256
- Content-Length
- Content-MD5

En-têtes de requête pour le chiffrement côté serveur

Si vous avez spécifié le chiffrement SSE-C pour la demande CreateMultipartUpload, vous devez également inclure les en-têtes de demande suivants dans chaque demande UploadPart :

- x-amz-server-side-encryption-customer-algorithm: Préciser AES256 .
- x-amz-server-side-encryption-customer-key: Spécifiez la même clé de chiffrement que celle que vous avez fournie dans la demande CreateMultipartUpload.
- x-amz-server-side-encryption-customer-key-MD5: Spécifiez le même condensé MD5 que celui que vous avez fourni dans la demande CreateMultipartUpload.



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, examinez les considérations dans ["Utiliser le cryptage côté serveur"](#) .

Si vous avez spécifié une somme de contrôle SHA-256 lors de la demande CreateMultipartUpload, vous devez également inclure l'en-tête de demande suivant dans chaque demande UploadPart :

- x-amz-checksum-sha256: Spécifiez la somme de contrôle SHA-256 pour cette partie.

En-têtes de requête non pris en charge

Les en-têtes de requête suivants ne sont pas pris en charge :

- x-amz-sdk-checksum-algorithm
- x-amz-trailer

Gestion des versions

Le téléchargement en plusieurs parties consiste en des opérations distinctes pour lancer le téléchargement, répertorier les téléchargements, télécharger des parties, assembler les parties téléchargées et terminer le téléchargement. Les objets sont créés (et versionnés si applicable) lorsque l'opération `CompleteMultipartUpload` est effectuée.

TéléchargerPartCopy

L'opération `UploadPartCopy` télécharge une partie d'un objet en copiant les données d'un objet existant comme source de données.

L'opération `UploadPartCopy` est implémentée avec tout le comportement de l'API REST Amazon S3. Sous réserve de modifications sans préavis.

Cette requête lit et écrit les données d'objet spécifiées dans `x-amz-copy-source-range` au sein du 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`

En-têtes de requête pour le chiffrement côté serveur

Si vous avez spécifié le chiffrement SSE-C pour la demande `CreateMultipartUpload`, vous devez également inclure les en-têtes de demande suivants dans chaque demande `UploadPartCopy` :

- `x-amz-server-side-encryption-customer-algorithm`: Préciser AES256.
- `x-amz-server-side-encryption-customer-key`: Spécifiez la même clé de chiffrement que celle que vous avez fournie dans la demande `CreateMultipartUpload`.
- `x-amz-server-side-encryption-customer-key-MD5`: Spécifiez le même condensé MD5 que celui que vous avez fourni dans la demande `CreateMultipartUpload`.

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 `UploadPartCopy`, afin que l'objet puisse être déchiffré puis copié :

- `x-amz-copy-source-server-side-encryption-customer-algorithm`: Préciser AES256.
- `x-amz-copy-source-server-side-encryption-customer-key`: Spécifiez la clé de chiffrement que vous avez fournie lors de la création de l'objet source.
- `x-amz-copy-source-server-side-encryption-customer-key-MD5`: Spécifiez le condensé 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, examinez les considérations dans ["Utiliser le cryptage côté serveur"](#).

Gestion des versions

Le téléchargement en plusieurs parties consiste en des opérations distinctes pour lancer le téléchargement, répertorier les téléchargements, télécharger des parties, assembler les parties téléchargées et terminer le téléchargement. Les objets sont créés (et versionnés si applicable) lorsque l'opération CompleteMultipartUpload est effectuée.

Réponses d'erreur

Le système StorageGRID prend en charge toutes les réponses d'erreur standard de l'API REST S3 qui s'appliquent. De plus, l'implémentation StorageGRID ajoute plusieurs réponses personnalisées.

Codes d'erreur de l'API S3 pris en charge

Nom	Statut HTTP
Accès refusé	403 Interdit
BadDigest	400 Mauvaise requête
BucketExisteDéjà	409 Conflit
Seau non vide	409 Conflit
Corps incomplet	400 Mauvaise requête
Erreur interne	Erreur interne du serveur 500
ID de clé d'accès non valide	403 Interdit
Argument invalide	400 Mauvaise requête
Nom de bucket invalide	400 Mauvaise requête
État du bucket invalide	409 Conflit
InvalidDigest	400 Mauvaise requête
Erreur d'algorithme de chiffrement invalide	400 Mauvaise requête
Partie invalide	400 Mauvaise requête
Commande de pièces invalide	400 Mauvaise requête
Plage invalide	416 Plage demandée non satisfaisante

Nom	Statut HTTP
Demande invalide	400 Mauvaise requête
Classe de stockage invalide	400 Mauvaise requête
Balise invalide	400 Mauvaise requête
URI invalide	400 Mauvaise requête
Clé trop longue	400 Mauvaise requête
XML malformé	400 Mauvaise requête
Métadonnées trop volumineuses	400 Mauvaise requête
Méthode non autorisée	Méthode 405 non autorisée
Longueur du contenu manquant	411 Longueur requise
Erreur de corps de demande manquante	400 Mauvaise requête
En-tête de sécurité manquant	400 Mauvaise requête
Aucun seau de ce type	404 non trouvé
Aucune clé de ce type	404 non trouvé
Aucun téléchargement de ce type	404 non trouvé
Non implémenté	501 non implémenté
Politique NoSuchBucket	404 non trouvé
Erreur de configuration de verrouillage d'objet non trouvée	404 non trouvé
Précondition échouée	412 Échec de la condition préalable
RequestTimeTooSkewed	403 Interdit
Service non disponible	Service 503 indisponible
La signature ne correspond pas	403 Interdit

Nom	Statut HTTP
Trop de seaux	400 Mauvaise requête
La clé utilisateur doit être spécifiée	400 Mauvaise requête

Codes d'erreur personnalisés StorageGRID

Nom	Description	Statut HTTP
XBucketLifecycleNon autorisé	La configuration du cycle de vie du bucket n'est pas autorisée dans un bucket conforme hérité	400 Mauvaise requête
Exception d'analyse de politique XBucket	Échec de l'analyse de la politique de bucket JSON reçue.	400 Mauvaise requête
Conflit de conformité X	Opération refusée en raison de paramètres de conformité hérités.	403 Interdit
XComplianceRéduitRedondanceInterdit	La redondance réduite n'est pas autorisée dans le bucket conforme hérité	400 Mauvaise requête
XMaxBucketPolicyLengthDépassé	Votre politique dépasse la durée maximale autorisée pour la politique de compartiment.	400 Mauvaise requête
En-tête de demande interne XMissing	Il manque un en-tête d'une requête interne.	400 Mauvaise requête
XNoSuchBucketCompliance	La conformité héritée n'est pas activée pour le bucket spécifié.	404 non trouvé
XNonAcceptable	La demande contient un ou plusieurs en-têtes d'acceptation qui n'ont pas pu être satisfaits.	406 Non acceptable
XNonImplémenté	La demande que vous avez fournie implique une fonctionnalité qui n'est pas implémentée.	501 non implémenté

Opérations personnalisées StorageGRID

Opérations personnalisées StorageGRID

Le système StorageGRID prend en charge les opérations personnalisées qui sont ajoutées à l'API REST S3.

Le tableau suivant répertorie les opérations personnalisées prises en charge par StorageGRID.

Opération	Description
"Cohérence du bucket GET"	Renvoie la cohérence appliquée à un bucket particulier.
"Cohérence du seau PUT"	Définit la cohérence appliquée à un bucket particulier.
"Heure du dernier accès au bucket GET"	Renvoie si les dernières mises à jour de l'heure d'accès sont activées ou désactivées pour un bucket particulier.
"Heure du dernier accès au bucket PUT"	Vous permet d'activer ou de désactiver les mises à jour de l'heure du dernier accès pour un bucket particulier.
"SUPPRIMER la configuration de notification des métadonnées du bucket"	Supprime la configuration XML de notification de métadonnées associée à un bucket particulier.
"Configuration de la notification des métadonnées du bucket GET"	Renvoie la configuration XML de notification de métadonnées associée à un bucket particulier.
"Configuration des notifications de métadonnées du compartiment PUT"	Configure le service de notification de métadonnées pour un bucket.
"Utilisation du stockage GET"	Vous indique la quantité totale de stockage utilisée par un compte et pour chaque bucket associé au compte.
"Obsolète : CreateBucket avec paramètres de conformité"	Obsolète et non pris en charge : vous ne pouvez plus créer de nouveaux buckets avec la conformité activée.
"Obsolète : conformité du bucket GET"	Obsolète mais pris en charge : renvoie les paramètres de conformité actuellement en vigueur pour un bucket conforme hérité existant.
"Obsolète : conformité du compartiment PUT"	Obsolète mais pris en charge : vous permet de modifier les paramètres de conformité d'un bucket conforme hérité existant.

Cohérence du bucket GET

La demande de cohérence GET Bucket vous permet de déterminer la cohérence appliquée à un bucket particulier.

La cohérence par défaut est définie pour garantir la lecture après écriture des objets nouvellement créés.

Vous devez disposer de l'autorisation `s3:GetBucketConsistency` ou être root du compte pour terminer cette opération.

Exemple de demande

```
GET /bucket?x-ntap-sg-consistency HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Réponse

Dans la réponse XML, <Consistency> renverra l'une des valeurs suivantes :

Cohérence	Description
tous	Tous les nœuds reçoivent les données immédiatement, sinon la demande échouera.
fort-mondial	Garantit la 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 au sein d'un site.
lecture après nouvelle écriture	(Par défaut) Fournit une cohérence de lecture après écriture pour les nouveaux objets et une cohérence éventuelle pour les mises à jour d'objets. Offre des garanties de haute disponibilité et de protection des données. Recommandé dans la plupart des cas.
disponible	Assure une cohérence éventuelle pour les nouveaux objets et les mises à jour d'objets. Pour les buckets S3, utilisez-les uniquement si nécessaire (par exemple, pour un bucket contenant des valeurs de journal rarement lues ou pour des opérations HEAD ou GET sur des clés qui n'existent pas). Non pris en charge pour les buckets S3 FabricPool .

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 connexes

["Valeurs de cohérence"](#)

Cohérence du seau PUT

La demande de cohérence PUT Bucket vous permet de spécifier la cohérence à appliquer aux opérations effectuées sur un bucket.

La cohérence par défaut est définie pour garantir la lecture après écriture des objets nouvellement créés.

Avant de commencer

Vous devez disposer de l'autorisation `s3:PutBucketConsistency` ou être root du compte pour terminer cette opération.

Demande

Le `x-ntap-sg-consistency` le paramètre doit contenir l'une des valeurs suivantes :

Cohérence	Description
tous	Tous les nœuds reçoivent les données immédiatement, sinon la demande échouera.
fort-mondial	Garantit la 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 au sein d'un site.
lecture après nouvelle écriture	(Par défaut) Fournit une cohérence de lecture après écriture pour les nouveaux objets et une cohérence éventuelle pour les mises à jour d'objets. Offre des garanties de haute disponibilité et de protection des données. Recommandé dans la plupart des cas.

Cohérence	Description
disponible	Assure une cohérence éventuelle pour les nouveaux objets et les mises à jour d'objets. Pour les buckets S3, utilisez-les uniquement si nécessaire (par exemple, pour un bucket contenant des valeurs de journal rarement lues ou pour des opérations HEAD ou GET sur des clés qui n'existent pas). Non pris en charge pour les buckets S3 FabricPool .

Remarque : En général, vous devez utiliser la cohérence « Lecture après nouvelle écriture ». Si les requêtes ne fonctionnent pas correctement, modifiez le comportement du client de l'application si possible. Ou configurez le client pour spécifier la cohérence de chaque demande d'API. Définissez la consistance au niveau du seau 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 connexes

["Valeurs de cohérence"](#)

Heure du dernier accès au bucket GET

La demande d'heure du dernier accès au bucket GET vous permet de déterminer si les mises à jour de l'heure du dernier accès sont activées ou désactivées pour les buckets individuels.

Vous devez disposer de l'autorisation `s3:GetBucketLastAccessTime` ou être root du compte pour terminer 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 de l'heure du dernier accès sont activées pour le bucket.

```
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>
```

Heure du dernier accès au bucket PUT

La demande d'heure du dernier accès au bucket PUT vous permet d'activer ou de désactiver les mises à jour de l'heure du dernier accès pour des buckets individuels. La désactivation des mises à jour de l'heure du dernier accès améliore les performances et constitue le paramètre par défaut pour tous les buckets créés avec la version 10.3.0 ou ultérieure.

Vous devez disposer de l'autorisation `s3:PutBucketLastAccessTime` pour un bucket ou être root du compte pour terminer cette opération.



À partir de la version 10.3 de StorageGRID, les mises à jour de l'heure du dernier accès sont désactivées par défaut pour tous les nouveaux buckets. Si vous disposez de buckets créés à l'aide d'une version antérieure de StorageGRID et que vous souhaitez appliquer le nouveau comportement par défaut, vous devez désactiver explicitement les mises à jour de l'heure du dernier accès pour chacun de ces buckets antérieurs. Vous pouvez activer ou désactiver les mises à jour de l'heure du dernier accès à l'aide de la demande d'heure du dernier accès au bucket PUT ou à partir de la page de détails d'un bucket dans le gestionnaire de locataires. Voir ["Activer ou désactiver les mises à jour de l'heure du dernier accès"](#).

Si les mises à jour de l'heure du dernier accès sont désactivées pour un bucket, le comportement suivant est appliqué aux opérations sur le bucket :

- Les requêtes `GetObject`, `GetObjectAcl`, `GetObjectTagging` et `HeadObject` 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).
- Les requêtes `CopyObject` et `PutObjectTagging` 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 bucket source, les demandes `CopyObject` ne mettent pas à jour l'heure du dernier accès pour le bucket source. L'objet qui a été copié n'est pas ajouté aux files d'attente pour l'évaluation ILM pour le bucket source. Cependant, pour la destination, les demandes `CopyObject` mettent toujours à jour l'heure du dernier accès. La copie de l'objet est ajoutée aux files d'attente pour l'évaluation ILM.
- Les demandes `CompleteMultipartUpload` mettent à jour l'heure du dernier accès. L'objet terminé est ajouté aux files d'attente pour l'évaluation ILM.

Exemples de demandes

Cet exemple active l'heure du dernier accès à un bucket.

```
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 à un bucket.

```
PUT /bucket?x-ntap-sg-lastaccesstime=disabled HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

SUPPRIMER la configuration de notification des métadonnées du bucket

La demande de configuration de notification des métadonnées DELETE Bucket vous permet de désactiver le service d'intégration de recherche pour des buckets individuels en supprimant le XML de configuration.

Vous devez disposer de l'autorisation `s3:DeleteBucketMetadataNotification` pour un bucket ou être root du compte pour terminer cette opération.

Exemple de demande

Cet exemple montre la désactivation du service d'intégration de recherche pour un bucket.

```
DELETE /test1?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Configuration de la notification des métadonnées du bucket GET

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 des buckets individuels.

Vous devez disposer de l'autorisation `s3:GetBucketMetadataNotification` ou être root du compte pour terminer cette opération.

Exemple de demande

Cette requête récupère la configuration de notification des métadonnées pour le bucket nommé `bucket`.


```
GET /bucket?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Réponse

Le corps de la réponse inclut la configuration de notification de métadonnées pour le bucket. La configuration de notification des métadonnées vous permet de déterminer comment le bucket est configuré pour l'intégration de la recherche. Autrement dit, il vous permet de déterminer quels objets sont indexés et à quels points de terminaison 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 spécifie les objets auxquels elle s'applique et la destination vers laquelle StorageGRID doit envoyer les métadonnées de l'objet. Les destinations doivent être spécifiées à l'aide de l'URN d'un point de terminaison StorageGRID .

Nom	Description	Obligatoire
Configuration des notifications de métadonnées	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

Nom	Description	Obligatoire
Règle	Balise de conteneur pour 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 <code>MetadataNotificationConfiguration</code>.	Oui
ID	Identifiant unique de la règle. Inclus dans l'élément Règle.	Non
Statut	Le statut peut être « Activé » ou « Désactivé ». Aucune action n'est entreprise 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

Nom	Description	Obligatoire
Urne	URN de la destination où les métadonnées de l'objet sont envoyées. Doit être l'URN d'un point de terminaison 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 <code>domain-name/myindex/mytype</code> . Les points de terminaison sont configurés à l'aide de l'API Tenant Manager ou Tenant Management. Ils prennent la forme suivante : • <code>arn:aws:es:_region:account-ID_:domain/mydomain/myindex/mytype</code> • <code>urn:mysite:es:::mydomain/myindex/mytype</code> Le point de terminaison doit être configuré avant que le XML de configuration ne soit soumis, sinon la configuration échouera avec une erreur 404. L'urne est incluse dans l'élément Destination.	Oui

Exemple de réponse

Le XML inclus entre le

`<MetadataNotificationConfiguration></MetadataNotificationConfiguration>` Les balises montrent comment l'intégration avec un point de terminaison d'intégration de recherche est configurée pour le bucket. Dans cet exemple, les métadonnées de l'objet sont envoyées à un index Elasticsearch nommé `current` et le type nommé `2017` qui est 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 connexes

["Utiliser un compte locataire"](#)

Configuration des notifications de métadonnées du compartiment PUT

La demande de configuration de notification des métadonnées PUT Bucket vous permet d'activer le service d'intégration de recherche pour des buckets individuels. La configuration XML de notification de métadonnées que vous fournissez dans le corps de la demande spécifie les objets dont les métadonnées sont envoyées à l'index de recherche de destination.

Vous devez disposer de l'autorisation `s3:PutBucketMetadataNotification` pour un bucket ou être root du compte pour terminer cette opération.

Demande

La demande doit inclure la configuration de notification des métadonnées dans le corps de la demande. Chaque configuration de notification de métadonnées comprend une ou plusieurs règles. Chaque règle spécifie les objets auxquels elle s'applique et la destination vers laquelle StorageGRID doit envoyer les métadonnées de l'objet.

Les objets peuvent être filtrés sur le préfixe du nom de l'objet. Par exemple, vous pouvez envoyer des métadonnées pour des objets avec le préfixe `/images` vers une destination et les objets avec le préfixe `/videos` à un autre.

Les configurations dont les préfixes se chevauchent ne sont pas valides et sont rejetées lorsqu'elles sont soumises. Par exemple, une configuration qui incluait une règle pour les objets avec le préfixe `test` et une deuxième 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 point de terminaison StorageGRID . Le point de terminaison doit exister lorsque la configuration de notification des métadonnées est soumise, sinon 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 de métadonnées.

Nom	Description	Obligatoire
Configuration des notifications de métadonnées	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 pour 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 MetadataNotificationConfiguration.	Oui
ID	Identifiant unique de la règle. Inclus dans l'élément Règle.	Non

Nom	Description	Obligatoire
Statut	Le statut peut être « Activé » ou « Désactivé ». Aucune action n'est entreprise 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 de l'objet sont envoyées. Doit être l'URN d'un point de terminaison 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 <code>domain-name/myindex/mytype</code>. Les points de terminaison sont configurés à l'aide de l'API Tenant Manager ou Tenant Management. Ils prennent la forme suivante : • <code>arn:aws:es:region:account-ID:domain/mydomain/myindex/mytype</code> • <code>urn:mysite:es:::mydomain/myindex/mytype</code> Le point de terminaison doit être configuré avant que le XML de configuration ne soit soumis, sinon 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 bucket. Dans cet exemple, les métadonnées d'objet pour 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 envoyé à une destination, tandis que les métadonnées d'objet pour les objets qui correspondent au préfixe `/videos` est envoyé vers une deuxième 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-1:33333333: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 recherche

Lorsque vous activez le service d'intégration de recherche pour un bucket, un document JSON est généré et envoyé au point de terminaison de destination chaque fois que des métadonnées ou des balises d'objet sont ajoutées, mises à jour ou supprimées.

Cet exemple montre un exemple de JSON qui pourrait être généré lorsqu'un objet avec la clé `SGWS/Tagging.txt` est créé dans un bucket nommé `test`. Le `test` le bucket n'est pas versionné, donc le `versionId` la balise 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 envoyé au point de terminaison de destination lorsque l'intégration de la recherche est activée.

Le nom du document inclut le nom du bucket, le nom de l'objet et l'ID de version s'il est présent.

Type	Nom de l'article	Description
Informations sur le bucket et l'objet	seau	Nom du seau
Informations sur le bucket et l'objet	clé	Nom de la clé de l'objet
Informations sur le bucket et l'objet	ID de version	Version de l'objet, pour les objets dans les buckets versionnés
Informations sur le bucket et l'objet	région	Région de bucket, par exemple <code>us-east-1</code>
Métadonnées du système	taille	Taille de l'objet (en octets) telle que visible par un client HTTP
Métadonnées du système	md5	Hachage d'objet
Métadonnées de l'utilisateur	métadonnées <i>key:value</i>	Toutes les métadonnées utilisateur pour l'objet, sous forme de paires clé-valeur

Type	Nom de l'article	Description
Mots-clés	balises <i>key:value</i>	Toutes les balises d'objet définies pour l'objet, sous forme de paires clé-valeur



Pour les balises et les métadonnées utilisateur, StorageGRID transmet des dates et des nombres à Elasticsearch sous forme de chaînes ou de notifications d'événements S3. Pour configurer Elasticsearch afin d'interpréter ces chaînes comme des dates ou des nombres, suivez les instructions Elasticsearch pour le mappage de champs dynamiques et pour le mappage des formats de date. Vous devez activer les mappages de champs dynamiques sur l'index avant de configurer le service d'intégration de recherche. Une fois qu'un document est indexé, vous ne pouvez pas modifier les types de champs du document dans l'index.

Informations connexes

["Utiliser un compte locataire"](#)

Demande d'utilisation du stockage GET

La demande GET Storage Usage vous indique la quantité totale de stockage utilisée par un compte et pour chaque bucket associé au compte.

La quantité de stockage utilisée par un compte et ses buckets peut être obtenue par une requête ListBuckets modifiée avec le `x-ntap-sg-usage` paramètre de requête. L'utilisation du stockage du bucket est suivie séparément des requêtes 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. Si une cohérence globale forte ne peut pas être obtenue, StorageGRID tente de récupérer les informations d'utilisation avec une cohérence de site forte.

Vous devez disposer de l'autorisation `s3:ListAllMyBuckets` ou être root du compte pour terminer 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 comporte 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 connexes

["Valeurs de cohérence"](#)

Demandes de bucket obsolètes pour la conformité héritée

Demandes de bucket obsolètes pour la conformité héritée

Vous devrez peut-être utiliser l'API REST StorageGRID S3 pour gérer les buckets créés à l'aide de la fonctionnalité de conformité héritée.

Fonctionnalité de conformité obsolète

La fonctionnalité de conformité StorageGRID disponible dans les versions précédentes de StorageGRID est obsolète et a été remplacée par S3 Object Lock.

Si vous avez précédemment activé le paramètre de conformité global, le paramètre de verrouillage d'objet S3 global est activé dans StorageGRID 11.6. Vous ne pouvez plus créer de nouveaux buckets avec la conformité activée ; toutefois, si nécessaire, vous pouvez utiliser l'API REST StorageGRID S3 pour gérer tous les buckets conformes existants.

- ["Utiliser l'API REST S3 pour configurer le verrouillage d'objet S3"](#)
- ["Gérer les objets avec ILM"](#)
- ["Base de connaissances NetApp : Gestion des buckets compatibles hérités dans StorageGRID 11.5"](#)

Demandes de conformité obsolètes :

- ["Obsolète - Modifications de la demande PUT Bucket pour la conformité"](#)

L'élément XML SGCompliance est obsolète. Auparavant, vous pouviez inclure cet élément personnalisé StorageGRID dans le corps de la requête XML facultatif des requêtes PUT Bucket pour créer un bucket conforme.

- ["Obsolète - Conformité du bucket GET"](#)

La demande de conformité GET Bucket est obsolète. Toutefois, vous pouvez continuer à utiliser cette demande pour déterminer les paramètres de conformité actuellement en vigueur pour un bucket conforme hérité existant.

- ["Obsolète - Conformité du compartiment PUT"](#)

La demande de conformité PUT Bucket est obsolète. Toutefois, vous pouvez continuer à utiliser cette demande pour modifier les paramètres de conformité d'un bucket conforme hérité existant. Par exemple, vous pouvez placer un bucket existant en attente légale ou augmenter sa période de conservation.

Obsolète : CreateBucket demande des modifications pour la conformité

L'élément XML SGCompliance est obsolète. Auparavant, vous pouviez inclure cet élément personnalisé StorageGRID dans le corps de la requête XML facultatif des requêtes CreateBucket pour créer un bucket conforme.



La fonctionnalité de conformité StorageGRID disponible dans les versions précédentes de StorageGRID est obsolète et a été remplacée par S3 Object Lock. Voir ce qui suit pour plus de détails :

- ["Utiliser l'API REST S3 pour configurer le verrouillage d'objet S3"](#)
- ["Base de connaissances NetApp : Gestion des buckets compatibles hérités dans StorageGRID 11.5"](#)

Vous ne pouvez plus créer de nouveaux buckets avec la conformité activée. Le message d'erreur suivant est renvoyé si vous tentez d'utiliser les modifications de demande CreateBucket pour la conformité afin de créer un nouveau bucket conforme :

```
The Compliance feature is deprecated.
Contact your StorageGRID administrator if you need to create new Compliant
buckets.
```

Obsolète : demande de conformité GET Bucket

La demande de conformité GET Bucket est obsolète. Toutefois, vous pouvez continuer à utiliser cette demande pour déterminer les paramètres de conformité actuellement en vigueur pour un bucket conforme hérité existant.



La fonctionnalité de conformité StorageGRID disponible dans les versions précédentes de StorageGRID est obsolète et a été remplacée par S3 Object Lock. Voir ce qui suit pour plus de détails :

- ["Utiliser l'API REST S3 pour configurer le verrouillage d'objet S3"](#)
- ["Base de connaissances NetApp : Gestion des buckets compatibles hérités dans StorageGRID 11.5"](#)

Vous devez disposer de l'autorisation `s3:GetBucketCompliance` ou être root du compte pour terminer cette opération.

Exemple de demande

Cet exemple de requête vous permet de déterminer les paramètres de conformité pour le bucket nommé `mybucket`.

```
GET /mybucket/?x-ntap-sg-compliance HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Exemple de réponse

Dans la réponse XML, `<SGCompliance>` répertorie les paramètres de conformité en vigueur pour le bucket. Cet exemple de réponse montre les paramètres de conformité d'un bucket dans lequel chaque objet sera conservé pendant un an (525 600 minutes), à compter du moment où l'objet est ingéré dans la grille. Il n'y a actuellement aucune retenue légale sur ce bucket. 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
Durée de conservation (minutes)	Durée de la période de conservation des objets ajoutés à ce bucket, en minutes. La période de conservation commence lorsque l'objet est ingéré dans la grille.
Conservation légale	• Vrai : ce bucket est actuellement sous une suspension 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 bucket n'est actuellement pas soumis à une suspension légale. Les objets de ce compartiment peuvent être supprimés lorsque leur période de conservation expire.
Suppression automatique	• Vrai : les objets de ce compartiment seront supprimés automatiquement à l'expiration de leur période de conservation, sauf si le compartiment est soumis à une suspension légale. • Faux : les objets de ce bucket ne seront pas supprimés automatiquement à l'expiration de la période de conservation. Vous devez supprimer ces objets manuellement si vous devez les supprimer.

Réponses d'erreur

Si le bucket 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 : demande de conformité du compartiment PUT

La demande de conformité PUT Bucket est obsolète. Toutefois, vous pouvez continuer à utiliser cette demande pour modifier les paramètres de conformité d'un bucket conforme hérité existant. Par exemple, vous pouvez placer un bucket existant en attente légale ou augmenter sa période de conservation.



La fonctionnalité de conformité StorageGRID disponible dans les versions précédentes de StorageGRID est obsolète et a été remplacée par S3 Object Lock. Voir ce qui suit pour plus de détails :

- ["Utiliser l'API REST S3 pour configurer le verrouillage d'objet S3"](#)
- ["Base de connaissances NetApp : Gestion des buckets compatibles hérités dans StorageGRID 11.5"](#)

Vous devez disposer de l'autorisation s3:PutBucketCompliance ou être root du compte pour terminer 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 requête modifie les paramètres de conformité pour le bucket nommé `mybucket`. Dans cet exemple, les objets dans `mybucket` seront désormais conservés pendant deux ans (1 051 200 minutes) au lieu d'un an, à compter de la date d'ingestion de l'objet dans la grille. Il n'y a aucune retenue légale sur ce seau. 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
Durée de conservation (minutes)	Durée de la période de conservation des objets ajoutés à ce bucket, en minutes. La période de conservation commence lorsque l'objet est ingéré dans la grille. Important Lorsque vous spécifiez une nouvelle valeur pour <code>RetentionPeriodMinutes</code>, vous devez spécifier une valeur égale ou supérieure à la période de rétention actuelle du bucket. Une fois la période de conservation du bucket définie, vous ne pouvez pas diminuer cette valeur ; vous pouvez uniquement l'augmenter.
Conservation légale	• Vrai : ce bucket est actuellement sous une suspension 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 bucket n'est actuellement pas soumis à une suspension légale. Les objets de ce compartiment peuvent être supprimés lorsque leur période de conservation expire.
Suppression automatique	• Vrai : les objets de ce compartiment seront supprimés automatiquement à l'expiration de leur période de conservation, sauf si le compartiment est soumis à une suspension légale. • Faux : les objets de ce bucket ne seront pas supprimés automatiquement à l'expiration de la période de conservation. Vous devez supprimer ces objets manuellement si vous devez les supprimer.

Cohérence des paramètres de conformité

Lorsque vous mettez à jour les paramètres de conformité d'un bucket S3 avec une demande de conformité PUT Bucket, StorageGRID tente de mettre à jour les métadonnées du bucket sur la grille. Par défaut, StorageGRID utilise la cohérence **Strong-global** pour garantir que tous les sites de centre de données et tous les nœuds de stockage contenant des métadonnées de bucket ont une cohérence de lecture après écriture pour les paramètres de conformité modifiés.

Si StorageGRID ne peut pas atteindre la cohérence **Strong-global** parce qu'un site de centre de données ou plusieurs nœuds de stockage sur un site ne sont pas disponibles, le code d'état HTTP de la réponse est 503 Service Unavailable.

Si vous recevez cette réponse, vous devez contacter l'administrateur du réseau pour vous assurer que les services de stockage requis sont mis à disposition dès que possible. Si l'administrateur du réseau ne parvient pas à rendre disponibles suffisamment de nœuds de stockage sur chaque site, le support technique peut vous demander de réessayer la demande ayant échoué en forçant la cohérence **Strong-site**.



Ne forcez jamais la cohérence **Strong-site** pour la conformité du bucket PUT, sauf si le support technique vous l'a demandé et si vous comprenez les conséquences potentielles de l'utilisation de ce niveau.

Lorsque la cohérence est réduite à **Strong-site**, StorageGRID garantit que les paramètres de conformité mis à jour auront une cohérence de lecture après écriture uniquement pour les demandes client au sein d'un site. Cela signifie que le système StorageGRID peut temporairement avoir plusieurs paramètres incohérents pour ce bucket 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 bucket sous une suspension légale et que vous forcez une cohérence inférieure, les paramètres de conformité précédents du bucket (c'est-à-dire la suspension légale) peuvent continuer à être en vigueur sur certains sites de centres de données. Par conséquent, les objets que vous pensez être en attente légale peuvent être supprimés à l'expiration de leur période de conservation, soit par l'utilisateur, soit par la suppression automatique, si cette option est activée.

Pour forcer l'utilisation de la cohérence **Strong-site**, réémettez la demande de conformité PUT Bucket 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 bucket n'a pas été créé pour être conforme, le code d'état HTTP de la réponse est 404 Not Found .
- Si RetentionPeriodMinutes si la demande est inférieure à la période de conservation actuelle du bucket, le code d'état HTTP est 400 Bad Request .

Informations connexes

["Obsolète : Modifications de la demande PUT Bucket pour la conformité"](#)

Politiques d'accès aux buckets et aux groupes

Utiliser des politiques d'accès aux buckets et aux groupes

StorageGRID utilise le langage de stratégie Amazon Web Services (AWS) pour permettre aux locataires S3 de contrôler l'accès aux buckets et aux objets au sein de ces buckets. Le système StorageGRID implémente un sous-ensemble du langage de politique de l'API REST S3. Les politiques d'accès pour l'API S3 sont écrites en JSON.

Aperçu de la politique d'accès

Il existe deux types de politiques d'accès prises en charge par StorageGRID.

- **Stratégies de bucket**, qui sont gérées à l'aide des opérations API S3 GetBucketPolicy, PutBucketPolicy et DeleteBucketPolicy ou de l'API Tenant Manager ou Tenant Management. Les stratégies de bucket sont attachées aux buckets, elles sont donc configurées pour contrôler l'accès des utilisateurs du compte propriétaire du bucket ou d'autres comptes au bucket et aux objets qu'il contient. Une politique de bucket s'applique à un seul bucket et éventuellement à plusieurs groupes.
- **Stratégies de groupe**, qui sont configurées à l'aide de Tenant Manager ou de l'API Tenant Management. Les stratégies de groupe sont attachées à un groupe dans le compte, elles sont donc configurées pour 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 éventuellement à plusieurs compartiments.



Il n'y a aucune différence de priorité entre les politiques de groupe et de compartiment.

Les stratégies de bucket et de groupe StorageGRID suivent une grammaire spécifique définie par Amazon. À l'intérieur de chaque politique se trouve un ensemble d'énoncés de politique, et chaque énoncé contient les éléments suivants :

- ID de relevé (Sid) (facultatif)
- Effet
- Principal/Non principal
- Ressource/PasRessource
- Action/Pas d'action
- Condition (facultatif)

Les instructions de politique sont construites à l'aide de cette structure pour spécifier les autorisations : Accorder <Effet> pour autoriser/refuser à <Principal> d'effectuer <Action> sur <Ressource> lorsque <Condition> s'applique.

Chaque élément de politique est utilisé pour une fonction spécifique :

Élément	Description
Sid	L'élément Sid est facultatif. Le Sid est uniquement destiné à servir de description pour l'utilisateur. Il est stocké mais non interprété par le système StorageGRID .

Élément	Description
Effet	Utilisez l'élément Effet pour déterminer si les opérations spécifiées sont autorisées ou refusées. Vous devez identifier les opérations que vous autorisez (ou refusez) sur les buckets ou les objets à l'aide des mots-clés d'élément Action pris en charge.
Principal/Non principal	Vous pouvez autoriser les utilisateurs, les groupes et les 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 a accès aux ressources appartenant au compte. Il vous suffit de spécifier l'élément Principal dans une stratégie de bucket. Pour les stratégies de groupe, le groupe auquel la stratégie est attachée est l'élément principal implicite.
Ressource/PasRessource	L'élément Ressource identifie les buckets et les objets. Vous pouvez autoriser ou refuser des autorisations sur des buckets et des objets à l'aide du nom de ressource Amazon (ARN) pour identifier la ressource.
Action/Pas d'action	Les éléments Action et Effet sont les deux composants des autorisations. Lorsqu'un groupe demande une ressource, l'accès à cette ressource lui est accordé ou refusé. L'accès est refusé à moins que vous n'attribuiez spécifiquement des autorisations, mais vous pouvez utiliser un refus explicite pour remplacer une autorisation accordée par une autre politique.
Condition	L'élément Condition est facultatif. Les conditions vous permettent de créer des expressions pour déterminer quand une politique 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 aux 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 ou plusieurs caractères, le point d'interrogation (?) correspond à n'importe quel caractère unique.

Dans l'élément Principal, les caractères génériques ne sont pas pris en charge, sauf pour définir un accès anonyme, qui accorde une autorisation à tout le monde. Par exemple, vous définissez le caractère générique (*) comme valeur principale.

```
"Principal": "*"

```

```
"Principal":{"AWS":"*"}
```

Dans l'exemple suivant, l'instruction utilise les éléments Effet, Principal, Action et Ressource. Cet exemple montre une déclaration de politique de compartiment complète qui utilise l'effet « Autoriser » pour donner aux principaux, le groupe d'administrateurs `federated-group/admin` et le groupe financier `federated-group/finance`, autorisations pour effectuer l'action `s3:ListBucket` sur le seau nommé `mybucket` et l'action `s3:GetObject` sur tous les objets à l'intérieur de ce seau.

```
{
  "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:s3::mybucket",
        "arn:aws:s3::mybucket/*"
      ]
    }
  ]
}
```

La politique de compartiment a une limite de taille de 20 480 octets et la politique de groupe a une limite de taille de 5 120 octets.

Cohérence des politiques

Par défaut, toutes les mises à jour que vous apportez aux stratégies de groupe sont finalement cohérentes. Lorsqu'une stratégie de groupe devient cohérente, les modifications peuvent prendre 15 minutes supplémentaires pour prendre effet, en raison de la mise en cache des stratégies. Par défaut, toutes les mises à jour que vous apportez aux stratégies de compartiment sont fortement cohérentes.

Si nécessaire, vous pouvez modifier les garanties de cohérence pour les mises à jour de la stratégie de compartiment. Par exemple, vous souhaitez peut-être qu'une modification apportée à une stratégie de compartiment soit disponible en cas de panne du site.

Dans ce cas, vous pouvez soit définir le `Consistency-Control` en-tête dans la demande `PutBucketPolicy`, ou vous pouvez utiliser la demande de cohérence `PUT Bucket`. Lorsqu'une stratégie de compartiment devient cohérente, les modifications peuvent prendre 8 secondes supplémentaires pour prendre effet, en raison de la

mise en cache de la stratégie.



Si vous définissez la cohérence sur une valeur différente pour contourner une situation temporaire, assurez-vous de redéfinir le paramètre au niveau du bucket sur sa valeur d'origine lorsque vous avez terminé. Dans le cas contraire, toutes les futures demandes de bucket utiliseront le paramètre modifié.

Utiliser l'ARN dans les déclarations de politique

Dans les déclarations de politique, l'ARN est utilisé dans les éléments Principal et Ressource.

- Utilisez cette syntaxe pour spécifier l'ARN de la ressource S3 :

```
arn:aws:s3:::bucket-name
arn:aws:s3:::bucket-name/object_key
```

- Utilisez cette syntaxe pour spécifier l'ARN de la ressource d'identité (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 faire correspondre zéro ou plusieurs caractères à l'intérieur de 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 à l'aide de séquences d'échappement JSON \u. Le codage en pourcentage n'est pas pris en charge.

"Syntaxe URN RFC 2141"

Le corps de la requête HTTP pour l'opération PutBucketPolicy doit être codé avec charset=UTF-8.

Spécifier les ressources dans une politique

Dans les instructions de politique, vous pouvez utiliser l'élément Ressource pour spécifier le compartiment ou l'objet pour lequel les autorisations sont accordées ou refusées.

- Chaque déclaration de politique nécessite un élément Ressource. Dans une politique, les ressources sont désignées par l'élément `Resource`, ou alternativement, `NotResource` pour l'exclusion.
- Vous spécifiez les ressources avec un ARN de ressource S3. Par exemple:

```
"Resource": "arn:aws:s3:::mybucket/*"
```

- Vous pouvez également utiliser des variables de politique à l'intérieur de la clé d'objet. Par exemple:

```
"Resource": "arn:aws:s3:::mybucket/home/${aws:username}/*"
```

- La valeur de la ressource peut spécifier un compartiment qui n'existe pas encore lors de la création d'une stratégie de groupe.

Spécifier les principaux dans une politique

Utilisez l'élément Principal pour identifier le compte d'utilisateur, de groupe ou de locataire auquel l'accès à la ressource est autorisé/refusé par l'instruction de stratégie.

- Chaque déclaration de politique dans une politique de compartiment doit inclure un élément Principal. Les instructions de politique dans une politique de groupe n'ont pas besoin de l'élément Principal car le groupe est considéré comme le principal.
- Dans une politique, les mandants sont désignés par l'élément « Principal » ou « NotPrincipal » pour l'exclusion.
- Les identités basées sur un compte doivent être spécifiées à l'aide d'un ID ou d'un ARN :

```
"Principal": { "AWS": "account_id"}  
"Principal": { "AWS": "identity_arn" }
```

- Cet exemple utilise l'ID de compte locataire 27233906934684427525, qui inclut la racine du compte 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 (« Managers ») :

```
"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 qu'Alex quitte l'organisation et le nom d'utilisateur `Alex` est supprimé. Si un nouvel Alex rejoint l'organisation et se voit attribuer le même `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.

Spécifier les autorisations dans une politique

Dans une politique, 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 politique, qui sont indiquées par l'élément « Action » ou, alternativement, « NotAction » pour l'exclusion. Chacun de ces éléments correspond à des opérations spécifiques de l'API REST S3.

Les tableaux répertorient les autorisations qui s'appliquent aux buckets et les autorisations qui s'appliquent aux objets.



Amazon S3 utilise désormais l'autorisation `s3:PutReplicationConfiguration` pour les actions `PutBucketReplication` et `DeleteBucketReplication`. StorageGRID utilise des autorisations distinctes pour chaque action, ce qui correspond à la spécification Amazon S3 d'origine.



Une suppression est effectuée lorsqu'un put est utilisé pour écraser une valeur existante.

Autorisations qui s'appliquent aux buckets

Autorisations	Opérations de l'API REST S3	Personnalisé pour StorageGRID
s3:Créer un bucket	Créer un bucket	Oui. Remarque : À utiliser uniquement dans la stratégie de groupe.
s3 : Supprimer le bucket	Supprimer le bucket	
s3 : Supprimer la notification des métadonnées du bucket	SUPPRIMER la configuration de notification des métadonnées du bucket	Oui

Autorisations	Opérations de l'API REST S3	Personnalisé pour StorageGRID
s3 : Supprimer la politique de bucket	Supprimer la politique de bucket	
s3 : Supprimer la configuration de réplication	SupprimerBucketReplication	Oui, des autorisations distinctes pour PUT et DELETE
s3 : Obtenir l'Acl du bucket	ObtenirBucketAcl	
s3 : Obtenir la conformité du bucket	Conformité du bucket GET (obsolète)	Oui
s3 : GetBucketConsistency	Cohérence du bucket GET	Oui
s3:Obtenir le bucket CORS	ObtenirBucketCors	
s3 : Obtenir la configuration du chiffrement	Obtenir le chiffrement du bucket	
s3 : Obtenir l'heure du dernier accès au bucket	Heure du dernier accès au bucket GET	Oui
s3 : Obtenir l'emplacement du bucket	Obtenir l'emplacement du bucket	
s3 : GetBucketMetadataNotification	Configuration de la notification des métadonnées du bucket GET	Oui
s3 : Obtenir une notification de bucket	Configuration de GetBucketNotification	
s3 : GetBucketObjectLockConfiguration	Obtenir la configuration du verrouillage de l'objet	
s3 : Obtenir la politique du bucket	Obtenir la politique de Bucket	
s3 : Obtenir le balisage du bucket	Obtenir le balisage du bucket	
s3 : Obtenir la gestion des versions du bucket	Obtenir la gestion des versions du bucket	
s3 : Obtenir la configuration du cycle de vie	GetBucketLifecycleConfiguration	
s3 : Obtenir la configuration de réplication	Réplication GetBucket	

Autorisations	Opérations de l'API REST S3	Personnalisé pour StorageGRID
s3 : ListeTousMesSeaux	- Listes de seaux - Utilisation du stockage GET	Oui, pour l'utilisation du stockage GET. Remarque : À utiliser uniquement dans la stratégie de groupe.
s3:ListBucket	- Liste d'objets - Tête de godet - Restaurer l'objet	
s3 : ListBucketMultipartUploads	- ListeMultipartUploads - Restaurer l'objet	
s3 : ListBucketVersions	Versions du bucket GET	
s3 : PutBucketCompliance	Conformité du compartiment PUT (obsolète)	Oui
s3 : PutBucketConsistency	Cohérence du seau PUT	Oui
s3:PutBucketCORS	- SupprimerBucketCors† - PutBucketCors	
s3 : PutEncryptionConfiguration	- Supprimer le chiffrement du bucket - Cryptage PutBucket	
s3 : PutBucketLastAccessTime	Heure du dernier accès au bucket PUT	Oui
s3 : PutBucketMetadataNotification	Configuration des notifications de métadonnées du compartiment PUT	Oui
s3 : PutBucketNotification	Configuration de PutBucketNotification	
s3 : PutBucketObjectLockConfiguration	- CreateBucket avec le x-amz-bucket-object-lock-enabled: true en-tête de requête (nécessite également l'autorisation s3:CreateBucket) - Configuration de PutObjectLock	
s3 : PutBucketPolicy	Politique de PutBucket	

Autorisations	Opérations de l'API REST S3	Personnalisé pour StorageGRID
s3 : Mettre en place le balisage du bucket	- Supprimer le balisage du bucket† - Balisage de PutBucket	
s3 : PutBucketVersioning	Gestion des versions de PutBucket	
s3 : PutLifecycleConfiguration	- Supprimer le cycle de vie du bucket† - Configuration du cycle de vie de PutBucket	
s3 : PutReplicationConfiguration	Réplication de PutBucket	Oui, des autorisations distinctes pour PUT et DELETE

Autorisations qui s'appliquent aux objets

Autorisations	Opérations de l'API REST S3	Personnalisé pour StorageGRID
s3 : Abandonner le téléchargement en plusieurs parties	- Abandonner le téléchargement en plusieurs parties - Restaurer l'objet	
s3 : Contournement de la gouvernance et de la rétention	- Supprimer l'objet - Supprimer les objets - PutObjectRetention	
s3:Supprimer l'objet	- Supprimer l'objet - Supprimer les objets - Restaurer l'objet	
s3 : Supprimer le balisage d'objet	Supprimer l'étiquetage des objets	
s3 : Supprimer le balisage de version d'objet	DeleteObjectTagging (une version spécifique de l'objet)	
s3 : Supprimer la version de l'objet	DeleteObject (une version spécifique de l'objet)	

Autorisations	Opérations de l'API REST S3	Personnalisé pour StorageGRID
s3:Obtenir l'objet	• Obtenir l'objet • HeadObject • Restaurer l'objet • Sélectionner le contenu de l'objet	
s3:GetObjectAcl	ObtenirObjectAcl	
s3 : GetObjectLegalHold	Obtenir la conservation légale de l'objet	
s3 : Obtenir la rétention d'objet	Obtenir la rétention d'objet	
s3 : Obtenir le balisage des objets	Obtenir l'étiquetage des objets	
s3 : Obtenir le balisage de la version de l'objet	GetObjectTagging (une version spécifique de l'objet)	
s3 : Obtenir la version de l'objet	GetObject (une version spécifique de l'objet)	
s3 : ListeMultipartUploadParts	ListParts, RestoreObject	
s3:PutObject	• Mettre l'objet • Copier l'objet • Restaurer l'objet • Créer un téléchargement multi-parties • Téléchargement complet en plusieurs parties • Télécharger une partie • TéléchargerPartCopy	
s3 : PutObjectLegalHold	MettreObjetLegalHold	
s3 : PutObjectRetention	PutObjectRetention	
s3 : Mettre en place un balisage d'objet	Balisage d'objets	
s3 : Mettre en place la version de l'objet	PutObjectTagging (une version spécifique de l'objet)	

Autorisations	Opérations de l'API REST S3	Personnalisé pour StorageGRID
s3 : PutOverwriteObject	• Mettre l'objet • Copier l'objet • Balisage d'objets • Supprimer l'étiquetage des objets • Téléchargement complet en plusieurs parties	Oui
s3:RestoreObject	Restaurer l'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 écraser les données d'un objet, les métadonnées définies par l'utilisateur ou le balisage d'un objet S3.

Les paramètres possibles pour cette autorisation incluent :

- **Autoriser**: Le client peut écraser un objet. Il s'agit du paramètre par défaut.
- **Refuser** : Le client ne peut pas écraser un objet. Lorsqu'elle est définie sur Refuser, l'autorisation PutOverwriteObject fonctionne comme suit :
 - Si un objet existant est trouvé sur le même chemin :
 - Les données de l'objet, les métadonnées définies par l'utilisateur ou le balisage de l'objet S3 ne peuvent pas être écrasés.
 - Toutes les opérations d'ingestion en cours sont annulées et une erreur est renvoyée.
 - Si le contrôle de version S3 est activé, le paramètre Refuser empêche les opérations PutObjectTagging ou DeleteObjectTagging 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 Autoriser était défini.



Si la stratégie 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'un objet. De plus, si la case à cocher **Empêcher la modification du client** est sélectionnée (**CONFIGURATION > Paramètres de sécurité > Réseau et objets**), ce paramètre remplace le paramètre de l'autorisation PutOverwriteObject.

Spécifier les conditions dans une politique

Les conditions définissent quand une politique sera en vigueur. Les conditions sont constituées d'opérateurs et de paires clé-valeur.

Les conditions utilisent des paires clé-valeur pour l'évaluation. Un élément Condition peut contenir plusieurs conditions, et chaque condition peut contenir plusieurs paires clé-valeur. Le bloc de condition utilise le format suivant :

```
Condition: {
  condition_type: {
    condition_key: condition_values
```

Dans l'exemple suivant, la condition `IpAddress` utilise la clé de 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
- Numérique
- Booléen
- adresse IP
- Vérification nulle

Opérateurs de condition	Description
Chaîne égale	Compare une clé à une valeur de chaîne en fonction d'une correspondance exacte (sensible à la casse).
Chaîne non égale	Compare une clé à une valeur de chaîne en fonction d'une correspondance négative (sensible à la casse).
Chaîne égale à Ignorer la casse	Compare une clé à une valeur de chaîne en fonction d'une correspondance exacte (ignore la casse).
Chaîne non égale à ignorer la casse	Compare une clé à une valeur de chaîne en fonction d'une correspondance négative (ignore la casse).
Comme une chaîne	Compare une clé à une valeur de chaîne en fonction d'une correspondance exacte (sensible à la casse). Peut inclure les caractères génériques * et ?.
ChaînePasComme	Compare une clé à une valeur de chaîne en fonction d'une correspondance négative (sensible à la casse). Peut inclure les caractères génériques * et ?.

Opérateurs de condition	Description
NumériqueÉgal	Compare une clé à une valeur numérique en fonction d'une correspondance exacte.
NumériqueNonÉgal	Compare une clé à une valeur numérique en fonction d'une correspondance négative.
Numérique supérieur à	Compare une clé à une valeur numérique en fonction d'une correspondance « supérieure à ».
Numérique supérieur à égal	Compare une clé à une valeur numérique en fonction d'une correspondance « supérieure ou égale ».
NumériqueInférieurÀ	Compare une clé à une valeur numérique en fonction d'une correspondance « inférieure à ».
NumériqueInférieurÀÉgal	Compare une clé à une valeur numérique en fonction d'une correspondance « inférieure ou égale ».
Booléen	Compare une clé à une valeur booléenne en fonction d'une correspondance « vrai ou faux ».
Adresse IP	Compare une clé à une adresse IP ou à une plage d'adresses IP.
Pas d'adresse IP	Compare une clé à une adresse IP ou à une plage d'adresses IP en fonction d'une correspondance négative.
Nul	Vérifie si une clé de condition est présente dans le contexte de la demande actuelle.

Clés de condition prises en charge

Clés de condition	Actions	Description
aws:SourceIP	opérateurs IP	Sera comparé à l'adresse IP à partir de laquelle la demande a été envoyée. Peut être utilisé pour les opérations de bucket ou d'objet. Remarque : si la requête S3 a été envoyée via le service d'équilibrage de charge sur les nœuds d'administration et les nœuds de passerelle, elle sera comparée à l'adresse IP en amont du service d'équilibrage de charge. Remarque : si un équilibreur de charge tiers non transparent est utilisé, cela sera comparé à l'adresse IP de cet équilibreur de charge. N'importe lequel <code>X-Forwarded-For</code> l'en-tête sera ignoré car sa validité ne peut pas être vérifiée.
aws:nom d'utilisateur	Ressource/Identité	Sera comparé au nom d'utilisateur de l'expéditeur à partir duquel la demande a été envoyée. Peut être utilisé pour les opérations de bucket ou d'objet.
s3:délimiteur	s3:ListBucket et s3:Authorisations ListBucketVersions	Sera comparé au paramètre délimiteur spécifié dans une demande ListObjects ou ListObjectVersions.

Clés de condition	Actions	Description
s3:ExistingObjectTag/<clé-balise>	s3 : Supprimer le balisage d'objet s3 : Supprimer le balisage de version d'objet s3:Obtenir l'objet s3:GetObjectAcl 3 : Obtenir le balisage des objets s3 : Obtenir la version de l'objet s3 : ObtenirObjectVersionAcl s3 : Obtenir le balisage de la version de l'objet s3:PutObjectAcl s3 : Mettre en place un balisage d'objet s3:PutObjectVersionAcl s3 : Mettre en place la version de l'objet	Nécessitera que l'objet existant possède la clé et la valeur de balise spécifiques.
s3:max-clés	s3:ListBucket et s3:Autorisations ListBucketVersions	Sera comparé au paramètre max-keys spécifié dans une requête ListObjects ou ListObjectVersions.
s3 : jours de conservation restants pour le verrouillage d'objet	s3:PutObject	Comparable à la date de conservation spécifiée dans le x-amz-object-lock-retain-until-date en-tête de demande ou période de conservation par défaut calculée à partir du compartiment pour garantir que ces valeurs se situent dans la plage autorisée pour les demandes suivantes : • Mettre l'objet • Copier l'objet • Créer un téléchargement multi-parties

Clés de condition	Actions	Description
s3 : jours de conservation restants pour le verrouillage d'objet	s3 : PutObjectRetention	Compare la date de conservation spécifiée dans la demande PutObjectRetention pour garantir qu'elle se situe dans la plage autorisée.
s3:préfixe	s3:ListBucket et s3:Autorisations ListBucketVersions	Sera comparé au paramètre de préfixe spécifié dans une demande ListObjects ou ListObjectVersions.
s3:RequestObjectTag/<clé-balise>	s3:PutObject s3 : Mettre en place un balisage d'objet s3 : Mettre en place la version de l'objet	Nécessitera une clé et une valeur de balise spécifiques lorsque la demande d'objet inclut le balisage.

Spécifier les variables dans une politique

Vous pouvez utiliser des variables dans les politiques pour renseigner les informations de politique lorsqu'elles sont disponibles. Vous pouvez utiliser des variables de politique dans le `Resource` élément et dans les comparaisons de chaînes dans le `Condition` élément.

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 de condition :

```
"Condition": {
  "StringLike": {
    "s3:prefix": "${aws:username}/*"
    ...
  },
  ...
}
```

Variable	Description
<code>\${aws:SourceIp}</code>	Utilise la clé <code>SourceIp</code> comme variable fournie.
<code>\${aws:username}</code>	Utilise la clé du nom d'utilisateur comme variable fournie.
<code>\${s3:prefix}</code>	Utilise la clé de préfixe spécifique au service comme variable fournie.

Variable	Description
<code>\$ { s3 : max - keys }</code>	Utilise la clé max-keys spécifique au service comme variable fournie.
<code>\$ { * }</code>	Caractère spécial. Utilise le caractère comme un caractère * littéral.
<code>\$ { ? }</code>	Caractère spécial. Utilise le caractère comme un caractère ? littéral.
<code>\$ { \$ }</code>	Caractère spécial. Utilise le caractère comme un caractère \$ littéral.

Créer des politiques nécessitant un traitement spécial

Parfois, une politique peut accorder des autorisations dangereuses pour la sécurité ou pour la poursuite des opérations, comme le verrouillage de l'utilisateur root du compte. L'implémentation de l'API REST StorageGRID S3 est moins restrictive lors de la validation des politiques qu'Amazon, mais tout aussi stricte lors de l'évaluation des politiques.

Description de la politique	Type de politique	Comportement d'Amazon	Comportement de StorageGRID
Refuser toute autorisation sur le compte root	Seau	Valide et appliqué, mais le compte utilisateur root conserve l'autorisation pour toutes les opérations de stratégie de compartiment S3	Même
Se refuser toute autorisation d'utilisateur/groupe	Groupe	Valide et appliqué	Même
Autoriser un groupe de comptes étrangers à accorder n'importe quelle autorisation	Seau	Principal invalide	Valide, mais les autorisations pour toutes les opérations de stratégie de compartiment S3 renvoient une erreur 405 Méthode non autorisée lorsqu'elles sont autorisées par une stratégie
Autoriser un compte root ou un utilisateur étranger à accéder à n'importe quelle autorisation	Seau	Valide, mais les autorisations pour toutes les opérations de stratégie de compartiment S3 renvoient une erreur 405 Méthode non autorisée lorsqu'elles sont autorisées par une stratégie	Même

Description de la politique	Type de politique	Comportement d'Amazon	Comportement de StorageGRID
Accorder à tout le monde des autorisations pour toutes les actions	Seau	Valide, mais les autorisations pour toutes les opérations de stratégie de compartiment S3 renvoient une erreur 405 Méthode non autorisée pour la racine du compte étranger et les utilisateurs	Même
Refuser à tout le monde les autorisations pour toutes les actions	Seau	Valide et appliqué, mais le compte utilisateur root conserve l'autorisation pour toutes les opérations de stratégie de compartiment S3	Même
Le principal est un utilisateur ou un groupe inexistant	Seau	Principal invalide	Valide
La ressource est un bucket S3 inexistant	Groupe	Valide	Même
Principal est un groupe local	Seau	Principal invalide	Valide
La politique accorde à un compte non propriétaire (y compris les comptes anonymes) des autorisations pour placer des objets.	Seau	Valide. Les objets appartiennent au compte créateur et la politique 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 (ACL) d'objet.	Valide. Les objets appartiennent au compte propriétaire du bucket. La politique des seaux s'applique.

Protection WORM (écriture unique, lecture multiple)

Vous pouvez créer des buckets WORM (Write-Once-Read-Many) pour protéger les données, les métadonnées d'objet définies par l'utilisateur et le balisage d'objet S3. Vous configurez les buckets WORM pour permettre la création de nouveaux objets et pour empêcher l'écrasement ou la suppression du contenu existant. Utilisez l'une des approches décrites ici.

Pour garantir que les écrasements sont toujours refusés, vous pouvez :

- Depuis 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 et politiques S3 suivantes :
 - Ajoutez une opération PutOverwriteObject DENY à la stratégie S3.
 - Ajoutez une opération DeleteObject DENY à la stratégie S3.
 - Ajoutez une opération PutObject ALLOW à la stratégie S3.



La définition de DeleteObject sur DENY dans une stratégie 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)

```
/mybucket/important.doc  
PUT#1 ---> OK  
PUT#2 -----> OK
```

Situation B : Écrasements séquentiels terminés (protégés contre)

```
/mybucket/important.doc  
PUT#1 -----> PUT#2 ---X (denied)
```

Informations connexes

- ["Comment les règles ILM de StorageGRID gèrent les objets"](#)
- ["Exemples de politiques de compartiment"](#)
- ["Exemples de stratégies de groupe"](#)
- ["Gérer les objets avec ILM"](#)
- ["Utiliser un compte locataire"](#)

Exemples de politiques de compartiment

Utilisez les exemples de cette section pour créer des politiques d'accès StorageGRID pour les buckets.

Les stratégies de compartiment spécifient les autorisations d'accès pour le compartiment auquel la stratégie est attachée. Vous configurez une stratégie de bucket en utilisant l'API S3 PutBucketPolicy via l'un de ces outils :

- ["Gestionnaire de locataires"](#) .
- AWS CLI utilisant cette commande (reportez-vous à ["Opérations sur les godets"](#)) :

```
> aws s3api put-bucket-policy --bucket examplebucket --policy  
file://policy.json
```

Exemple : autoriser tout le monde à accéder en lecture seule à un bucket

Dans cet exemple, tout le monde, y compris les personnes anonymes, est autorisé à répertorier les objets du bucket et à effectuer des opérations GetObject sur tous les objets du bucket. 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, n'a l'autorisation d'écrire dans le bucket.

```
{
  "Statement": [
    {
      "Sid": "AllowEveryoneReadOnlyAccess",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [ "s3:GetObject", "s3:ListBucket" ],
      "Resource":
[ "arn:aws:s3:::examplebucket", "arn:aws:s3:::examplebucket/*" ]
    }
  ]
}
```

Exemple : autoriser tous les utilisateurs d'un compte à accéder pleinement à un bucket et tous les utilisateurs d'un autre compte à accéder en lecture seule à un bucket.

Dans cet exemple, toutes les personnes d'un compte spécifié sont autorisées à accéder pleinement à un compartiment, tandis que toutes les personnes d'un autre compte spécifié sont uniquement autorisées à répertorier le compartiment et à effectuer des opérations GetObject sur les objets du compartiment commençant par le `shared/` préfixe de clé d'objet.



Dans StorageGRID, les objets créés par un compte non propriétaire (y compris les comptes anonymes) appartiennent au compte propriétaire du bucket. La politique de bucket 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 accorder un accès complet au groupe spécifié

Dans cet exemple, tout le monde, y compris les anonymes, est autorisé à répertorier le bucket et à effectuer des opérations GetObject sur tous les objets du bucket, tandis que seuls les utilisateurs appartenant au groupe Marketing dans le compte spécifié, un accès complet est autorisé.

```

{
  "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 accéder en lecture et en écriture à un bucket si le client se trouve dans la plage d'adresses IP

Dans cet exemple, tout le monde, y compris les personnes anonymes, est autorisé à répertorier le bucket et à effectuer toutes les opérations d'objet sur tous les objets du bucket, à condition que les demandes proviennent d'une plage d'adresses 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 l'accès complet à un bucket exclusivement par un utilisateur fédéré spécifié

Dans cet exemple, l'utilisateur fédéré Alex est autorisé à accéder pleinement au `examplebucket` seau et ses objets. Tous les autres utilisateurs, y compris « root », se voient explicitement refuser toutes les opérations. Notez cependant que « root » ne se voit jamais refuser les autorisations pour `Put/Get/DeleteBucketPolicy`.

```

{
  "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` L'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 de l'objet 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 politiques d'accès StorageGRID pour les groupes.

Les stratégies de groupe spécifient les autorisations d'accès pour le groupe auquel la stratégie est attachée. Il n'y a pas de `Principal` élément de la politique car il est implicite. Les stratégies de groupe sont configurées à l'aide du gestionnaire de locataires ou de l'API.

Exemple : définir une stratégie de groupe à l'aide de Tenant Manager

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 disposeront les membres de ce groupe. Voir ["Créer 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 stratégie de compartiment. Si vous sélectionnez cette option, seul l'utilisateur root aura accès aux ressources S3 par défaut.
- **Accès en lecture seule** : les utilisateurs de ce groupe ont un accès en lecture seule aux ressources S3. Par exemple, les utilisateurs de ce groupe peuvent répertorier les objets et lire les données, les métadonnées et les balises des objets. Lorsque vous sélectionnez cette option, la chaîne JSON d'une stratégie de groupe en lecture seule apparaît dans la zone de texte. Vous ne pouvez pas modifier cette chaîne.
- **Accès complet** : les utilisateurs de ce groupe ont un accès complet aux ressources S3, y compris aux buckets. Lorsque vous sélectionnez cette option, la chaîne JSON d'une stratégie de groupe à accès complet apparaît dans la zone de texte. Vous ne pouvez pas modifier cette chaîne.
- **Atténuation des ransomwares** : cet exemple de politique s'applique à tous les compartiments de ce locataire. Les utilisateurs de ce groupe peuvent effectuer des actions courantes, mais ne peuvent pas supprimer définitivement les objets des buckets pour lesquels le contrôle de version des objets est activé.

Les utilisateurs de Tenant Manager qui disposent 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 multifactor (MFA) lorsqu'elle est disponible.

- **Personnalisé** : les utilisateurs du groupe bénéficient des autorisations que vous spécifiez dans la zone de texte.

Exemple : autoriser le groupe à accéder à tous les compartiments

Dans cet exemple, tous les membres du groupe sont autorisés à accéder pleinement à tous les compartiments appartenant au compte locataire, sauf si cela est explicitement refusé 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, sauf si cela est explicitement refusé par la politique de bucket. Par exemple, les utilisateurs de ce groupe peuvent répertorier les 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 : autoriser les membres du groupe à accéder pleinement à leur « dossier » dans un compartiment

Dans cet exemple, les membres du groupe sont uniquement autorisés à répertorier et à accéder à leur dossier spécifique (préfixe de clé) dans le compartiment spécifié. Notez que les autorisations d'accès provenant d'autres stratégies de groupe et de la stratégie 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}/*"
    }
  ]
}
```

Opérations S3 suivies dans les journaux d'audit

Les messages d'audit sont générés par les services StorageGRID et stockés dans des fichiers journaux texte. Vous pouvez consulter les messages d'audit spécifiques à S3 dans le journal d'audit pour obtenir des détails sur les opérations de bucket et d'objet.

Opérations de bucket suivies dans les journaux d'audit

- Créer un bucket
- Supprimer le bucket
- Supprimer le balisage du bucket
- Supprimer les objets
- Obtenir le balisage du bucket
- Tête de godet
- Liste d'objets
- ListObjectVersions
- Conformité du compartiment PUT
- Balisage de PutBucket
- Gestion des versions de PutBucket

Opérations sur les objets suivies dans les journaux d'audit

- Téléchargement complet en plusieurs parties
- Copier l'objet
- Supprimer l'objet
- Obtenir l'objet
- HeadObject
- Mettre l'objet
- Restaurer l'objet
- Sélectionner un objet
- UploadPart (lorsqu'une règle ILM utilise une ingestion équilibrée ou stricte)
- UploadPartCopy (lorsqu'une règle ILM utilise une ingestion équilibrée ou stricte)

Informations connexes

- ["Accéder au fichier journal d'audit"](#)
- ["Le client écrit des messages d'audit"](#)
- ["Le client lit les messages d'audit"](#)

Utiliser l'API REST Swift (fin de vie)

Utiliser l'API REST Swift

La prise en charge de l'API Swift a atteint sa fin de vie et sera supprimée dans une prochaine version.



Les détails Swift ont été supprimés de cette version du site de documentation. Voir ["StorageGRID 11.8 : utiliser l'API REST Swift"](#).

Surveiller et dépanner un système StorageGRID

Surveiller le système StorageGRID

Surveiller un système StorageGRID

Surveillez régulièrement votre système StorageGRID pour vous assurer qu'il fonctionne comme prévu.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un [navigateur Web pris en charge](#) .
- Tu as [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**.

À propos de cette tâche

Ces instructions décrivent comment :

- ["Afficher et gérer le tableau de bord"](#)
- ["Afficher la page Nœuds"](#)
- ["Surveillez régulièrement ces aspects du système :"](#)
 - ["Santé du système"](#)
 - ["Capacité de stockage"](#)
 - ["Gestion du cycle de vie de l'information"](#)
 - ["Ressources réseau et système"](#)
 - ["Activité des locataires"](#)
 - ["Opérations d'équilibrage de charge"](#)
 - ["Connexions de la fédération de réseau"](#)
- ["Gérer les alertes"](#)
- ["Afficher les fichiers journaux"](#)
- ["Configurer les messages d'audit et les destinations des journaux"](#)
- ["Utiliser un serveur syslog externe"](#) pour collecter des informations d'audit
- ["Utiliser SNMP pour la surveillance"](#)
- ["Obtenir des données StorageGRID supplémentaires"](#), y compris les mesures et les diagnostics

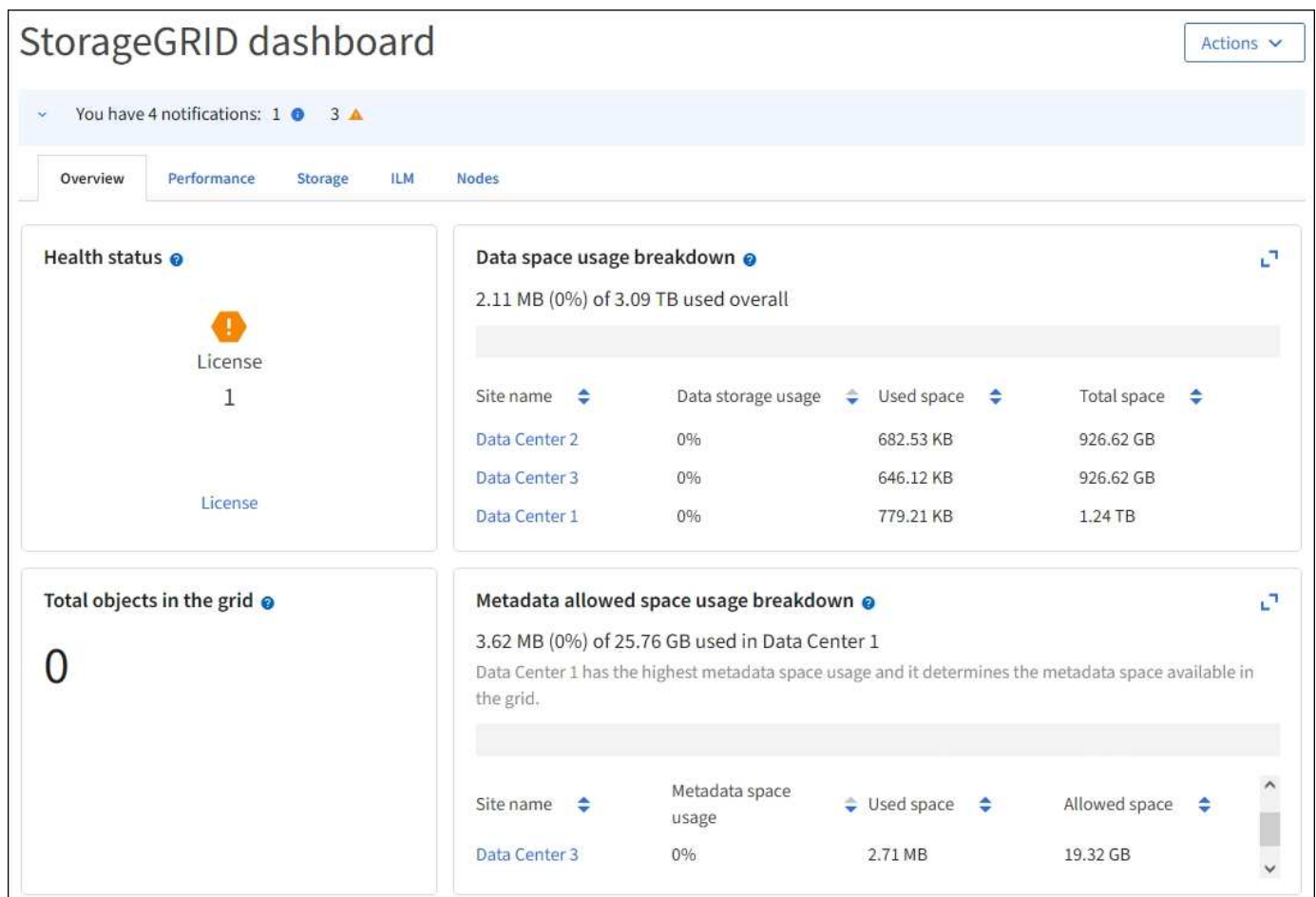
Afficher et gérer le tableau de bord

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 surveiller 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**.

Votre tableau de bord peut être différent en fonction de la configuration du système.



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 quel. De plus, vous pouvez créer des tableaux de bord personnalisés qui contiennent uniquement les onglets et les cartes pertinents pour la surveillance de votre implémentation de StorageGRID.

Les onglets du tableau de bord fournis par le système contiennent des cartes avec les types d'informations suivants :

Onglet sur le tableau de bord fourni par le système	Contient
Aperçu	Informations générales sur la grille, telles que les alertes actives, l'utilisation de l'espace et le nombre total d'objets dans la grille.

Onglet sur le tableau de bord fourni par le système	Contient
Performances	Utilisation de l'espace, stockage utilisé au fil du temps, opérations S3, durée de la requête, taux d'erreur.
Stockage	Utilisation des quotas des locataires et utilisation logique de l'espace. Prévisions d'utilisation de l'espace pour les données et métadonnées des utilisateurs.
ILM	File d'attente de gestion du cycle de vie des informations et taux d'évaluation.
Nœuds	Utilisation du processeur, des données et de la mémoire par nœud. Opérations S3 par nœud. Distribution du nœud au site.

Certaines cartes peuvent être agrandies pour une visualisation plus facile. Sélectionnez l'icône de maximisation  dans le coin supérieur droit de la carte. Pour fermer une carte agrandie, sélectionnez l'icône de réduction  ou sélectionnez **Fermer**.

Gérer les tableaux de bord

Si vous avez un accès root (voir "[Autorisations du groupe d'administrateurs](#)"), 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 les informations StorageGRID affichées et la manière dont ces informations sont organisées.
- Clonez 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 le tableau de bord fourni par le système ou un tableau de bord personnalisé.
- Définissez un tableau de bord par défaut, qui est ce que tous les utilisateurs voient, à moins qu'ils n'activent leur propre tableau de bord.
- Modifier 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.
- Supprimer un tableau de bord.



Si vous disposez d'une autre autorisation en plus de l'accès root, 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
- Renommer les onglets et donner aux nouveaux onglets des noms uniques
- Ajouter, supprimer ou réorganiser (faire glisser) des cartes pour chaque onglet
- Sélectionnez la taille des cartes individuelles en sélectionnant **S**, **M**, **L** ou **XL** en haut de la carte

Site name	Data storage usage	Used space	Total space
Data Center 1	0%	1.79 MB	1.24 TB
Data Center 2	0%	921.11 KB	926.62 GB
Data Center 3	0%	790.21 KB	926.62 GB

Afficher la page Nœuds

Afficher la page Nœuds

Lorsque vous avez besoin d'informations plus détaillées sur votre système StorageGRID que celles fournies par le tableau de bord, vous pouvez utiliser la page Nœuds pour afficher les métriques de l'ensemble de la grille, 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 apparaît à côté du nom du nœud. Si le nœud est connecté et n'a aucune alerte active, aucune icône n'est affichée.



Lorsqu'un nœud n'est pas connecté au réseau, par exemple lors d'une mise à niveau ou d'un état déconnecté, certaines mesures peuvent être indisponibles ou exclues des totaux du site et du réseau. Une fois qu'un nœud se reconnecte au réseau, attendez quelques 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**.



Les captures d'écran présentées sont des exemples. Vos résultats peuvent varier en fonction de votre version de StorageGRID .

Nodes

View the list and status of sites and grid nodes.

Search...					Total node count: 12
Name	Type	Object data used	Object metadata used	CPU usage	
StorageGRID Webscale Deployment	Grid	0%	0%	—	
^ DC1	Site	0%	0%	—	
 DC1-ADM1	Primary Admin Node	—	—	6%	
 DC1-ARC1	Archive Node	—	—	1%	
 DC1-G1	Gateway Node	—	—	3%	
DC1-S1	Storage Node	0%	0%	6%	
DC1-S2	Storage Node	0%	0%	8%	
DC1-S3	Storage Node	0%	0%	4%	

Icônes d'état de connexion

Si un nœud est déconnecté du réseau, l'une des icônes suivantes apparaît à côté du nom du nœud.

Icône	Description	Action requise
	Non connecté - Inconnu Pour une raison inconnue, un nœud est déconnecté ou les services sur le nœud sont interrompus de manière inattendue. Par exemple, un service sur le nœud peut être arrêté ou le nœud peut avoir perdu sa connexion réseau en raison d'une panne de courant ou d'une panne inattendue. L'alerte Impossible de communiquer avec le nœud peut également être déclenchée. D'autres alertes peuvent également être actives.	Nécessite une attention immédiate. "Sélectionnez chaque alerte" et suivez les actions recommandées. Par exemple, vous devrez peut-être redémarrer un service qui s'est arrêté ou redémarrer l'hôte du nœud. Remarque : un nœud peut apparaître comme inconnu lors des opérations d'arrêt géré. Vous pouvez ignorer l'état Inconnu dans ces cas.
	Non connecté - Administrativement en panne Pour une raison attendue, le nœud n'est pas connecté au réseau. Par exemple, le nœud ou les services sur le nœud ont été arrêtés correctement, le nœud redémarre ou le logiciel est en cours de mise à niveau. Une ou plusieurs alertes peuvent également être actives. En fonction du problème sous-jacent, ces nœuds reviennent souvent en ligne sans intervention.	Déterminez si des alertes affectent ce nœud. Si une ou plusieurs alertes sont actives, "Sélectionnez chaque alerte" et suivez les actions recommandées.

Si un nœud est déconnecté du réseau, il peut y avoir une alerte sous-jacente, mais seule l'icône « Non connecté » apparaît. Pour voir les alertes actives pour un nœud, sélectionnez le nœud.

Icônes d'alerte

S'il existe une alerte active pour un nœud, l'une des icônes suivantes apparaît à côté du nom du nœud :

 **Critique** : une condition anormale existe qui a arrêté les opérations normales d'un nœud ou d'un service StorageGRID . Vous devez résoudre le problème sous-jacent immédiatement. Une interruption de service et une perte de données peuvent survenir si le problème n'est pas résolu.

 **Majeur** : Une condition anormale existe qui affecte les opérations en cours ou approche le seuil d'une alerte critique. Vous devez enquêter sur les alertes majeures et résoudre tous les problèmes sous-jacents pour garantir que la condition anormale n'arrête pas le fonctionnement normal d'un nœud ou d'un service StorageGRID .

 **Mineur** : Le système fonctionne normalement, mais une condition anormale existe qui pourrait affecter la capacité du système à fonctionner si elle persiste. Vous devez surveiller et résoudre les alertes mineures qui ne disparaissent pas d'elles-mêmes pour vous assurer qu'elles n'entraînent pas un problème plus grave.

Afficher les détails d'un système, d'un site ou d'un nœud

Pour filtrer les informations affichées dans le tableau Nœuds, saisissez une chaîne de recherche dans le champ **Rechercher**. Vous pouvez effectuer une recherche par nom de système, nom d'affichage ou type (par exemple, saisissez **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 voir un résumé global des statistiques de l'ensemble de votre système StorageGRID .
- Sélectionnez un site de centre de données spécifique pour voir un résumé global des statistiques de tous les nœuds de ce site.
- Sélectionnez un nœud spécifique pour afficher des informations détaillées sur ce nœud.

Afficher l'onglet Aperçu

L'onglet Présentation fournit des informations de base sur chaque nœud. Il affiche également toutes les alertes affectant actuellement le nœud.

L'onglet Présentation s'affiche pour tous les nœuds.

Informations sur le nœud

La section Informations sur le nœud de l'onglet Présentation répertorie les informations de base sur le nœud.

NYC-ADM1 (Primary Admin Node) [🔗](#)

Overview Hardware Network Storage Load balancer Tasks

Node information [?](#)

Display name:	NYC-ADM1
System name:	DC1-ADM1
Type:	Primary Admin Node
ID:	3adb1aa8-9c7a-4901-8074-47054aa06ae6
Connection state:	✔ Connected
Software version:	11.7.0
IP addresses:	10.96.105.85 - eth0 (Grid Network)

[Show additional IP addresses](#) [▼](#)

Les informations générales d'un nœud incluent les éléments suivants :

- **Nom d’affichage** (affiché uniquement si le nœud a été renommé) : le nom d’affichage actuel du nœud. Utilisez le "[Renommer la grille, les sites et les nœuds](#)" procédure pour mettre à jour 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** : le type de nœud : nœud d’administration, nœud d’administration principal, nœud de stockage ou nœud de passerelle.
- **ID** : l’identifiant unique du nœud, également appelé UUID.
- **État 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 au réseau ou un ou plusieurs services sont inopinément hors service. Par exemple, la connexion réseau entre les nœuds a été perdue, l’alimentation est coupée ou un service est en panne. L’alerte ***Impossible de communiquer avec le nœud** peut également être déclenchée. D’autres alertes peuvent également être actives. Cette situation nécessite une attention immédiate.



Un nœud peut apparaître comme inconnu lors des opérations d’arrêt gérées. Vous pouvez ignorer l’état Inconnu dans ces cas.

- ***Administrativement en panne***  : Le nœud n’est pas connecté au réseau pour une raison attendue. Par exemple, le nœud ou les services sur le nœud ont été arrêtés correctement, le nœud redémarre ou le logiciel est en cours de mise à niveau. Une ou plusieurs alertes peuvent également être actives.

- ***Connecté***  : Le nœud est connecté au réseau.

- **Stockage utilisé** : Pour les nœuds de stockage uniquement.
 - **Données d’objet** : le pourcentage de l’espace total utilisable pour les données d’objet qui a été utilisé sur le nœud de stockage.
 - **Métadonnées d’objet** : le 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.
- **Groupe HA** : pour les nœuds d’administration et les nœuds de passerelle uniquement. Indique si une interface réseau sur le nœud est incluse dans un groupe de haute disponibilité et si cette interface est l’interface principale.
- **Adresses IP** : Les adresses IP du nœud. Cliquez sur **Afficher les adresses IP supplémentaires** pour afficher les adresses IPv4 et IPv6 du nœud et les mappages d’interface.

Alertes

La section Alertes de l’onglet Aperçu répertorie toutes les "[alertes affectant actuellement ce nœud qui n’ont pas été désactivées](#)". Sélectionnez le nom de l’alerte pour afficher des détails supplémentaires et les actions recommandées.

Alerts			
Alert name	Severity	Time triggered	Current values
Low installed node memory The amount of installed memory on a node is low.	✖ Critical	11 hours ago	Total RAM size: 8.37 GB

Des alertes sont également incluses pour "[états de connexion des nœuds](#)".

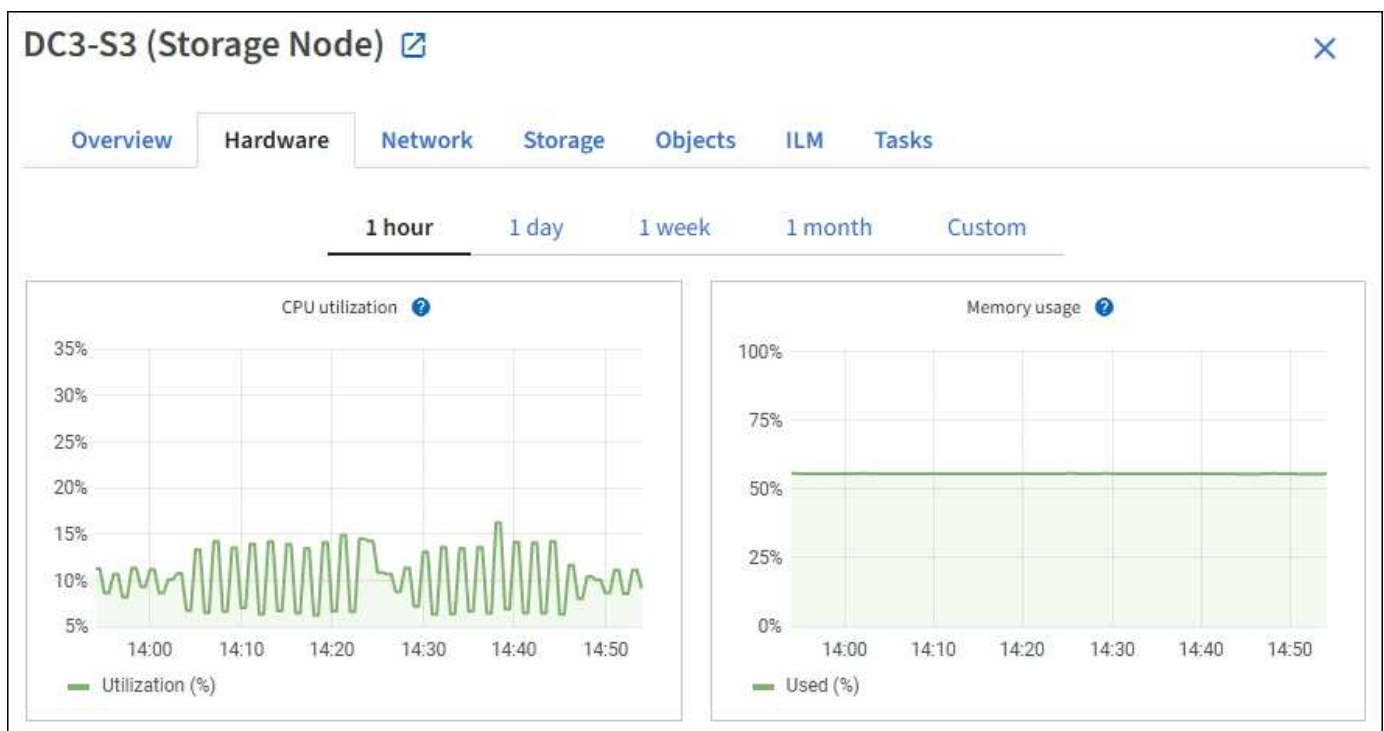
Afficher l'onglet Matériel

L'onglet Matériel affiche l'utilisation du processeur et de la mémoire pour chaque nœud, ainsi que des informations matérielles supplémentaires sur les appareils.



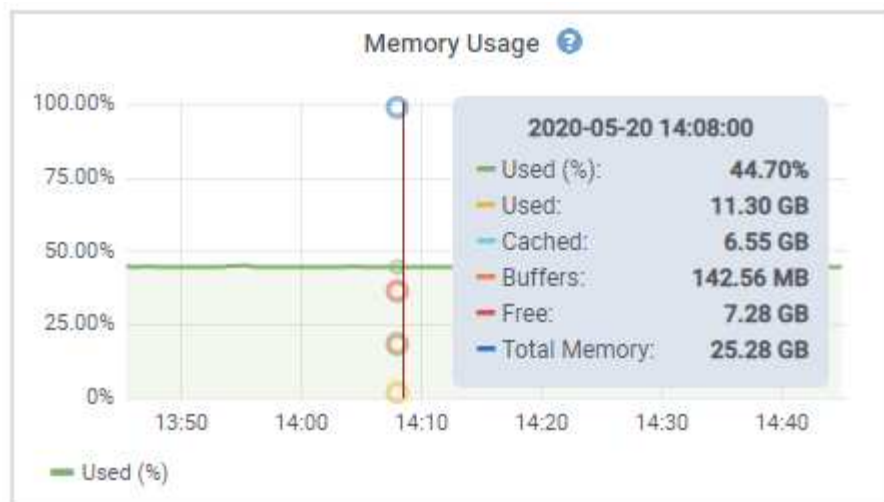
Le gestionnaire de grille est mis à jour à chaque version et peut ne pas correspondre aux exemples de captures d'écran sur cette page.

L'onglet Matériel est affiché pour tous les nœuds.



Pour afficher un intervalle de temps différent, sélectionnez l'un des contrôles au-dessus du graphique ou du diagramme. Vous pouvez afficher les informations disponibles pour des 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 dates et d'heures.

Pour voir les détails de l'utilisation du processeur 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 plus d'informations sur le matériel de l'appliance.

Afficher les informations sur les nœuds de stockage de l'appliance

La page Nœuds répertorie les informations sur l'état du service et toutes les ressources de calcul, de disque et de réseau pour chaque nœud de stockage de l'appliance. Vous pouvez également voir la mémoire, le matériel de stockage, la version du micrologiciel du contrôleur, les ressources réseau, les interfaces réseau, les adresses réseau et recevoir et transmettre des données.

Étapes

1. Depuis la page Nœuds, sélectionnez un nœud de stockage d'appliance.
2. Sélectionnez **Aperçu**.

La section Informations sur le nœud de l'onglet Présentation affiche des informations récapitulatives sur le nœud, telles que le nom, le type, l'ID et l'état de connexion du nœud. La liste des adresses IP comprend le nom de l'interface pour chaque adresse, comme suit :

- **eth** : Le réseau Grid, le réseau administrateur ou le réseau client.
- **hic** : L'un des ports physiques 10, 25 ou 100 GbE de l'appareil. Ces ports peuvent être liés ensemble et connectés au réseau de grille StorageGRID (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.

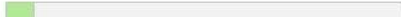
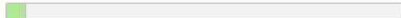
[Overview](#) [Hardware](#) [Network](#) [Storage](#) [Objects](#) [ILM](#) [Tasks](#)Node information [?](#)

Name: DC2-SGA-010-096-106-021

Type: Storage Node

ID: f0890e03-4c72-401f-ae92-245511a38e51

Connection state:  Connected

Storage used:
Object data  7% [?](#)
Object metadata  5% [?](#)

Software version: 11.6.0 (build 20210915.1941.afce2d9)

IP addresses: 10.96.106.21 - eth0 (Grid Network)

[Hide additional IP addresses](#) [^](#)

Interface ↕	IP address ↕
eth0 (Grid Network)	10.96.106.21
eth0 (Grid Network)	fe80::2a0:98ff:fe64:6582
hic2	10.96.106.21
hic4	10.96.106.21
mtc2	169.254.0.1

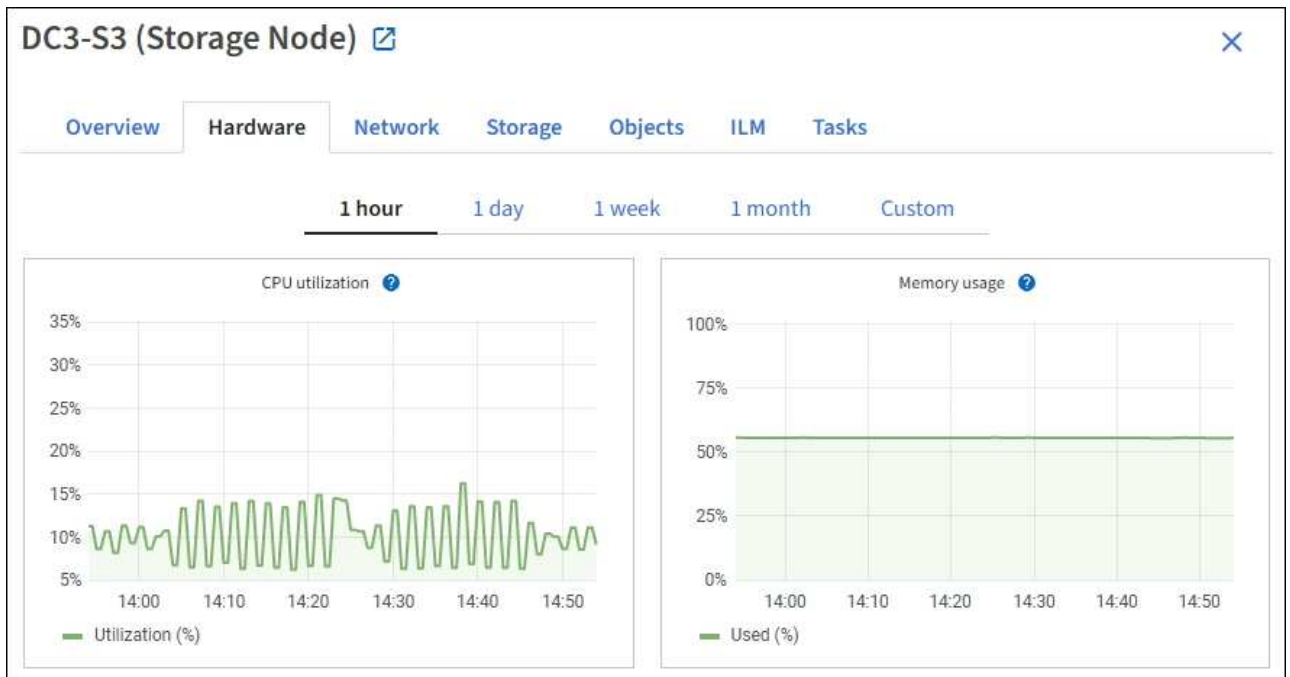
Alerts

Alert name ↕	Severity ? ↕	Time triggered ↕	Current values
ILM placement unachievable ↗	 Major	2 hours ago ?	
A placement instruction in an ILM rule cannot be achieved for certain objects.			

La section Alertes de l'onglet Présentation affiche toutes les alertes actives pour le nœud.

3. Sélectionnez **Matériel** pour voir plus d'informations sur l'appareil.

- Affichez les graphiques d'utilisation du processeur et de la mémoire pour déterminer les pourcentages d'utilisation du processeur et de la mémoire au fil du temps. Pour afficher un intervalle de temps différent, sélectionnez l'un des contrôles au-dessus du graphique ou du diagramme. Vous pouvez afficher les informations disponibles pour des 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 dates et d'heures.



- 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'appareil, les noms des contrôleurs, les numéros de série et les adresses IP, ainsi que l'état de chaque composant.



Certains champs, tels que l'adresse IP du contrôleur de calcul BMC et le matériel de calcul, n'apparaissent que pour les appliances dotées de cette fonctionnalité.

Les composants des étagères de stockage et des étagères d'extension si elles font partie de l'installation apparaissent dans un tableau séparé sous le tableau des appareils.

StorageGRID Appliance

Appliance model: ?	SG6060	
Storage controller name: ?	StorageGRID-Lab79-SG6060-7-134	
Storage controller A management IP: ?	10.2	
Storage controller B management IP: ?	10.2	
Storage controller WWID: ?	6d039ea0000173e50000000065b7b761	
Storage appliance chassis serial number: ?	721924500068	
Storage controller firmware version: ?	08.53.00.09	
Storage controller SANtricity OS version: ?	11.50.3R2	
Storage controller NVSRAM version: ?	N280X-853834-DG1	
Storage hardware: ?	Nominal	
Storage controller failed drive count: ?	0	
Storage controller A: ?	Nominal	
Storage controller B: ?	Nominal	
Storage controller power supply A: ?	Nominal	
Storage controller power supply B: ?	Nominal	
Storage data drive type: ?	NL-SAS HDD	
Storage data drive size: ?	4.00 TB	
Storage RAID mode: ?	DDP16	
Storage connectivity: ?	Nominal	
Overall power supply: ?	Degraded	
Compute controller BMC IP: ?	10.2	
Compute controller serial number: ?	721917500060	
Compute hardware: ?	Needs Attention	
Compute controller CPU temperature: ?	Nominal	
Compute controller chassis temperature: ?	Nominal	
Compute controller power supply A: ?	Failed	
Compute controller power supply B: ?	Nominal	

Storage shelves

Shelf chassis serial number ?	Shelf ID ?	Shelf status ?	IOM status ?	Power supply status ?	Drawer status ?	Fan status
721924500068	99	Nominal	N/A	Nominal	Nominal	Nominal

Champ dans la table Appliance	Description
Modèle d'appareil	Le numéro de modèle de cet appareil StorageGRID affiché dans SANtricity OS.
Nom du contrôleur de stockage	Le nom de cet appareil StorageGRID affiché dans SANtricity OS.
Contrôleur de stockage Une adresse IP de gestion	Adresse IP pour le port de gestion 1 sur le contrôleur de stockage A. Vous utilisez cette adresse IP pour accéder à SANtricity OS afin de résoudre les problèmes de stockage.
IP de gestion du contrôleur de stockage B	Adresse IP pour le port de gestion 1 sur le contrôleur de stockage B. Vous utilisez cette adresse IP pour accéder à SANtricity OS afin de résoudre les problèmes de stockage. Certains modèles d'appareils ne disposent pas de contrôleur de stockage B.

Champ dans la table Appliance	Description
WWID du contrôleur de stockage	L'identifiant mondial du contrôleur de stockage affiché dans SANtricity OS.
Numéro de série du châssis de l'appareil de stockage	Le numéro de série du châssis de l'appareil.
Version du micrologiciel du contrôleur de stockage	La version du micrologiciel sur le contrôleur de stockage de cet appareil.
Version du système d'exploitation SANtricity du contrôleur de stockage	La version du système d'exploitation SANtricity du contrôleur de stockage A.
Contrôleur de stockage version NVSRAM	Version NVSRAM du contrôleur de stockage telle que rapportée par SANtricity System Manager. Pour les SG6060 et SG6160, s'il existe une incompatibilité de version NVSRAM entre les deux contrôleurs, la version du contrôleur A s'affiche. Si le contrôleur A n'est pas installé ou opérationnel, la version du contrôleur B s'affiche.
Matériel de stockage	L'état général du matériel du contrôleur de stockage. Si SANtricity System Manager signale un état « Nécessite une attention particulière » pour le matériel de stockage, le système StorageGRID signale également cette valeur. Si le statut est « nécessite une attention particulière », vérifiez d'abord le contrôleur de stockage à l'aide de SANtricity OS. Ensuite, assurez-vous qu'aucune autre alerte n'existe qui s'applique au contrôleur de calcul.
Nombre de disques défaillants du contrôleur de stockage	Le nombre de lecteurs 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'appareils ne disposent pas de contrôleur de stockage B.
Alimentation du contrôleur de stockage A	L'état de l'alimentation A pour le contrôleur de stockage.
Alimentation du contrôleur de stockage B	L'état de l'alimentation B du contrôleur de stockage.
Type de lecteur de données de stockage	Le type de lecteurs de l'appareil, tels que HDD (disque dur) ou SSD (disque SSD).

Champ dans la table Appliance	Description
Taille du lecteur de données de stockage	La taille effective d'un lecteur de données. Pour le SG6160, la taille du lecteur de cache s'affiche également. Remarque : Pour les nœuds avec des étagères d'extension, utilisez le Taille du lecteur de données pour chaque étagère plutôt. La taille effective du lecteur peut varier selon l'étagère.
Mode RAID de stockage	Le mode RAID configuré pour l'appareil.
Connectivité de stockage	L'état de connectivité du stockage.
Alimentation électrique globale	L'état de toutes les alimentations électriques de l'appareil.
Contrôleur de calcul BMC IP	L'adresse IP du port du contrôleur de gestion de la carte mère (BMC) dans le contrôleur de calcul. Vous utilisez cette IP pour vous connecter à l'interface BMC afin de surveiller et de diagnostiquer le matériel de l'appliance. Ce champ n'est pas affiché pour les modèles d'appareils qui ne contiennent pas de BMC.
Numéro de série du contrôleur de calcul	Le numéro de série du contrôleur de calcul.
Matériel informatique	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 distincts.
Température du processeur du contrôleur de calcul	L'état de température du processeur du contrôleur de calcul.
Température du châssis du contrôleur de calcul	L'état de température du contrôleur de calcul.

+

Colonne dans le tableau des étagères de rangement	Description
Numéro de série du châssis d'étagère	Le numéro de série du châssis de l'étagère de stockage.

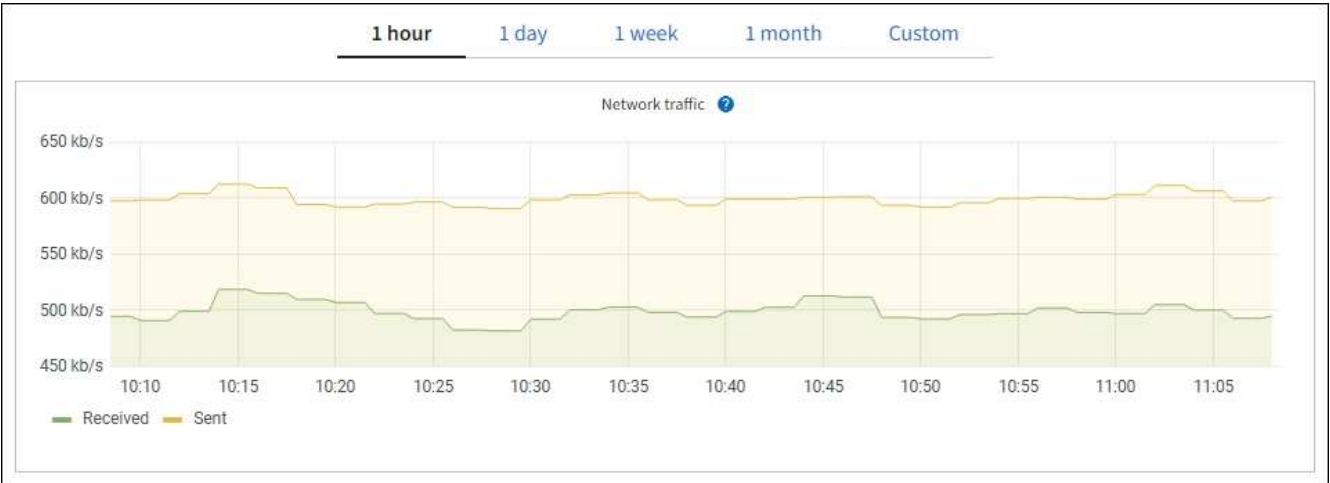
Colonne dans le tableau des étagères de rangement	Description
ID d'étagère	L'identifiant numérique de l'étagère de stockage. • 99 : Étagère de contrôleur de stockage • 0 : Première étagère d'extension • 1 : Deuxième étagère d'extension Remarque : les étagères d'extension s'appliquent uniquement aux modèles SG6060 et SG6160.
État des étagères	L'état général de l'étagère de stockage.
Statut de l'OIM	L'état des modules d'entrée/sortie (IOM) dans toutes les étagères d'extension. N/A s'il ne s'agit pas d'une étagère d'extension.
État de l'alimentation électrique	L'état général des alimentations électriques de l'étagère de stockage.
État du tiroir	L'état des tiroirs de l'étagère de rangement. N/A si l'étagère ne contient pas de tiroirs.
Statut du ventilateur	L'état général des ventilateurs de refroidissement dans l'étagère de stockage.
Emplacements de lecteur	Le nombre total d'emplacements de lecteur dans l'étagère de stockage.
Lecteurs de données	Le nombre de lecteurs dans l'étagère de stockage qui sont utilisés pour le stockage des données.
Taille du lecteur de données	La taille effective d'un lecteur de données dans l'étagère de stockage.
Lecteurs de cache	Le nombre de lecteurs dans l'étagère de stockage qui sont utilisés comme cache.
Taille du lecteur de cache	La taille du plus petit lecteur de cache dans l'étagère de stockage. Normalement, les lecteurs de cache ont tous la même taille.
État de la configuration	L'état de configuration de l'étagère de stockage.

a. Confirmez que tous les statuts sont « Nominaux ».

Si un statut n'est pas « Nominal », vérifiez toutes les alertes actuelles. Vous pouvez également utiliser SANtricity System Manager pour en savoir plus sur certaines de ces valeurs matérielles. Consultez les instructions d'installation et d'entretien de votre appareil.

4. Sélectionnez **Réseau** pour afficher les informations de chaque réseau.

Le graphique du trafic réseau fournit un résumé 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 **Vitesse** du tableau Interfaces réseau pour déterminer si les ports réseau 10/25-GbE de l’appliance ont été configurés pour utiliser le mode actif/de secours ou le mode LACP.

 Les valeurs indiquées dans le tableau supposent que les quatre liens sont utilisés.

Mode de liaison	Mode liaison	Vitesse de liaison HIC individuelle (hic1, hic2, hic3, hic4)	Vitesse attendue du réseau grille/client (eth0, eth2)
Agrégat	LACP	25	100
Fixé	LACP	25	50
Fixé	Actif/Sauvegarde	25	25
Agrégat	LACP	10	40
Fixé	LACP	10	20
Fixé	Actif/Sauvegarde	10	10

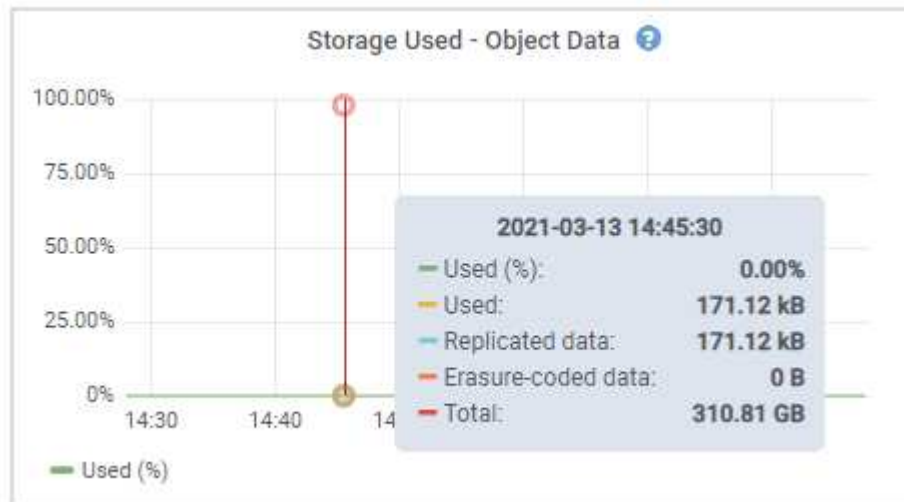
Voir "[Configurer les liens réseau](#)" pour plus d’informations sur la configuration des ports 10/25-GbE.

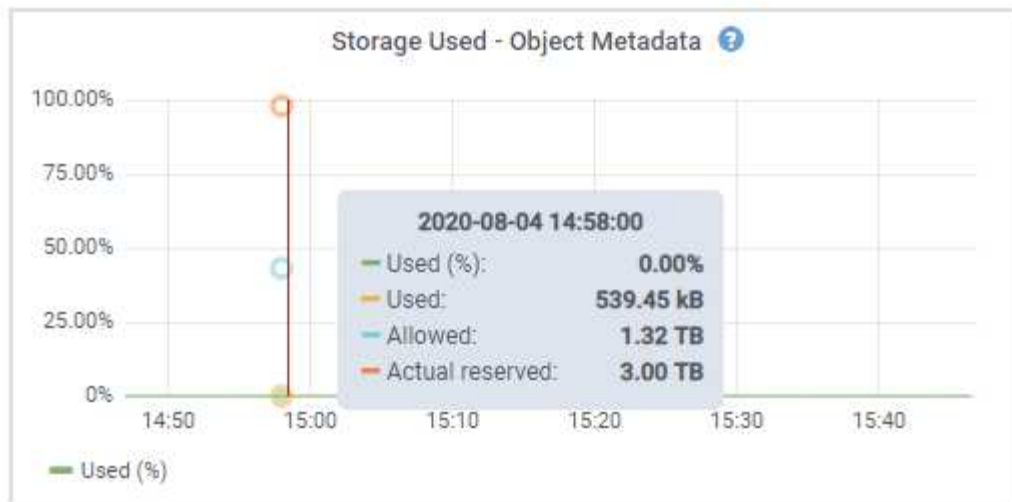
b. Consultez la section Communication réseau.

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.

Network communication						
Receive						
Interface ?	Data ?	Packets ?	Errors ?	Dropped ?	Frame overruns ?	Frames ?
eth0	2.89 GB	19,421,503	0	24,032	0	0
Transmit						
Interface ?	Data ?	Packets ?	Errors ?	Dropped ?	Collisions ?	Carrier ?
eth0	3.64 GB	18,494,381	0	0	0	0

5. Sélectionnez **Stockage** pour afficher les graphiques qui montrent les pourcentages de stockage utilisés au fil du temps pour les données d'objet et les métadonnées d'objet, ainsi que des informations sur les périphériques de disque, les volumes et les magasins d'objets.





- 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 mondial du volume (WWID) qui apparaît lorsque vous affichez les propriétés du volume standard 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 sur disque liées aux points de montage de volume, la première partie du nom affichée dans la colonne **Nom** du tableau Périphériques de disque (c'est-à-dire *sdc*, *sdd*, *sde*, etc.) correspond à la valeur affichée dans la colonne **Périphérique** du tableau 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

Afficher les informations sur les nœuds d'administration et les nœuds de passerelle de l'appareil

La page Nœuds répertorie les informations sur l'état du service et toutes les ressources de calcul, de périphérique de disque et de réseau pour chaque dispositif de services utilisé comme nœud d'administration ou nœud de passerelle. Vous pouvez également voir la mémoire, le matériel de stockage, les ressources réseau, les interfaces réseau, les adresses réseau et recevoir et transmettre des données.

Étapes

1. À partir de la page Nœuds, sélectionnez un nœud d'administration d'appareil ou un nœud de passerelle d'appareil.
2. Sélectionnez **Aperçu**.

La section Informations sur le nœud de l'onglet Présentation affiche des informations récapitulatives sur le

nœud, telles que le nom, le type, l'ID et l'état de connexion du nœud. La liste des adresses IP comprend le nom de l'interface pour chaque adresse, comme suit :

- **adllb** et **adlli** : affichés si la liaison active/de secours est utilisée pour l'interface réseau d'administration
- **eth** : Le réseau Grid, le réseau administrateur ou le réseau client.
- **hic** : L'un des ports physiques 10, 25 ou 100 GbE de l'appareil. Ces ports peuvent être liés ensemble et connectés au réseau de grille StorageGRID (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 (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 Présentation affiche toutes les alertes actives pour le nœud.

3. Sélectionnez **Matériel** pour voir plus d'informations sur l'appareil.
 - a. Affichez les graphiques d'utilisation du processeur et de la mémoire pour déterminer les pourcentages d'utilisation du processeur et de la mémoire au fil du temps. Pour afficher un intervalle de temps différent, sélectionnez l'un des contrôles au-dessus du graphique ou du diagramme. Vous pouvez afficher les informations disponibles pour des 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 dates et d'heures.
 - 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.

StorageGRID Appliance		
Appliance model: ?	SG100	
Storage controller failed drive count: ?	0	
Storage data drive type: ?	SSD	
Storage data drive size: ?	960.20 GB	
Storage RAID mode: ?	RAID1 [healthy]	
Storage connectivity: ?	Nominal	
Overall power supply: ?	Nominal	
Compute controller BMC IP: ?	10.60.8.38	
Compute controller serial number: ?	372038000093	
Compute hardware: ?	Nominal	
Compute controller CPU temperature: ?	Nominal	
Compute controller chassis temperature: ?	Nominal	
Compute controller power supply A: ?	Nominal	
Compute controller power supply B: ?	Nominal	

Champ dans la table Appliance	Description
Modèle d'appareil	Le numéro de modèle de cet appareil StorageGRID .
Nombre de disques défaillants du contrôleur de stockage	Le nombre de lecteurs qui ne sont pas optimaux.
Type de lecteur de données de stockage	Le type de lecteurs de l'appareil, tels que HDD (disque dur) ou SSD (disque SSD).
Taille du lecteur de données de stockage	La taille effective d'un lecteur de données.
Mode RAID de stockage	Le mode RAID de l'appareil.
Alimentation électrique globale	L'état de toutes les alimentations de l'appareil.
Contrôleur de calcul BMC IP	L'adresse IP du port du contrôleur de gestion de la carte mère (BMC) dans le contrôleur de calcul. Vous pouvez utiliser cette IP pour vous connecter à l'interface BMC afin de surveiller et de diagnostiquer le matériel de l'appliance. Ce champ n'est pas affiché pour les modèles d'appareils qui ne contiennent pas de BMC.
Numéro de série du contrôleur de calcul	Le numéro de série du contrôleur de calcul.
Matériel informatique	L'état du matériel du contrôleur de calcul.
Température du processeur du contrôleur de calcul	L'état de température du processeur du contrôleur de calcul.
Température du châssis du contrôleur de calcul	L'état de température du contrôleur de calcul.

a. Confirmez que tous les statuts sont « Nominaux ».

Si un statut n'est pas « Nominal », vérifiez toutes les alertes actuelles.

4. Sélectionnez **Réseau** pour afficher les informations de chaque réseau.

Le graphique du trafic réseau fournit un résumé 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 **Vitesse** du tableau Interfaces réseau pour déterminer si les quatre ports réseau 40/100-GbE de l'apppliance ont été configurés pour utiliser le mode actif/de secours ou le mode LACP.



Les valeurs indiquées dans le tableau supposent que les quatre liens sont utilisés.

Mode de liaison	Mode liaison	Vitesse de liaison HIC individuelle (hic1, hic2, hic3, hic4)	Vitesse attendue du réseau grille/client (eth0, eth2)
Agrégat	LACP	100	400
Fixé	LACP	100	200
Fixé	Actif/Sauvegarde	100	100
Agrégat	LACP	40	160
Fixé	LACP	40	80
Fixé	Actif/Sauvegarde	40	40

b. Consultez 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.

Network communication						
Receive						
Interface ?	Data ?	Packets ?	Errors ?	Dropped ?	Frame overruns ?	Frames ?
eth0	2.89 GB	19,421,503	0	24,032	0	0
Transmit						
Interface ?	Data ?	Packets ?	Errors ?	Dropped ?	Collisions ?	Carrier ?
eth0	3.64 GB	18,494,381	0	0	0	0

5. Sélectionnez **Stockage** pour afficher des informations sur les périphériques de disque et les volumes sur le dispositif de services.

Disk devices

Name ? ↕	World Wide Name ? ↕	I/O load ? ↕	Read rate ? ↕	Write rate ? ↕
croot(8:1,sda1)	N/A	0.02%	0 bytes/s	3 KB/s
cvloc(8:2,sda2)	N/A	0.03%	0 bytes/s	6 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	84.63 GB 	Unknown

Afficher l'onglet Réseau

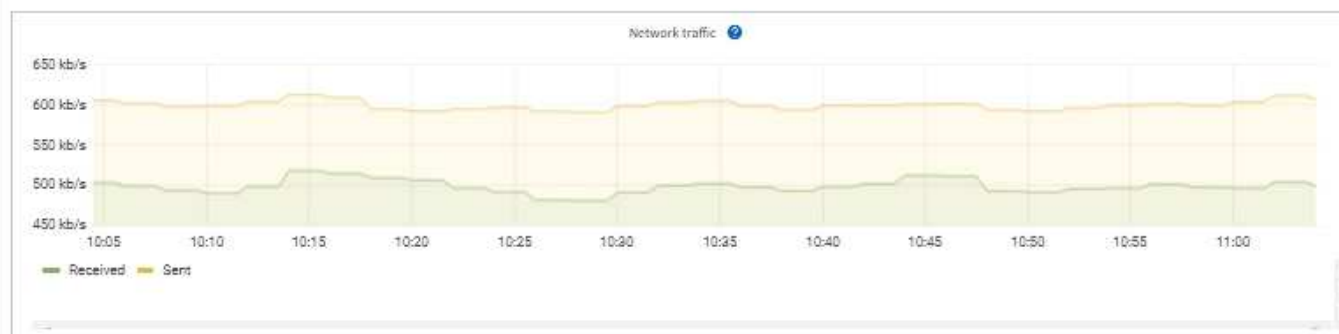
L'onglet Réseau affiche un graphique montrant le trafic réseau reçu et envoyé sur toutes les interfaces réseau du nœud, du site ou de la grille.

L'onglet Réseau s'affiche pour tous les nœuds, chaque site et l'ensemble de la grille.

Pour afficher un intervalle de temps différent, sélectionnez l'un des contrôles au-dessus du graphique ou du diagramme. Vous pouvez afficher les informations disponibles pour des 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 dates et d'heures.

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 les compteurs d'erreurs signalés par le pilote.

DC1-S2 (Storage Node)

[Overview](#)[Hardware](#)[Network](#)[Storage](#)[Objects](#)[ILM](#)[Tasks](#)[1 hour](#)[1 day](#)[1 week](#)[1 month](#)[Custom](#)

Network interfaces

Name	Hardware address	Speed	Duplex	Auto-negotiation	Link status
eth0	00:50:56:A7:E8:1D	10 Gigabit	Full	Off	Up

Network communication

Receive

Interface	Data	Packets	Errors	Dropped	Frame overruns	Frames
eth0	3.04 GB	20,403,428	0	24,899	0	0

Transmit

Interface	Data	Packets	Errors	Dropped	Collisions	Carrier
eth0	3.65 GB	19,061,947	0	0	0	0

Informations connexes

["Surveiller les connexions et les performances du réseau"](#)

Afficher l'onglet Stockage

L'onglet Stockage résume la disponibilité du stockage et d'autres mesures de stockage.

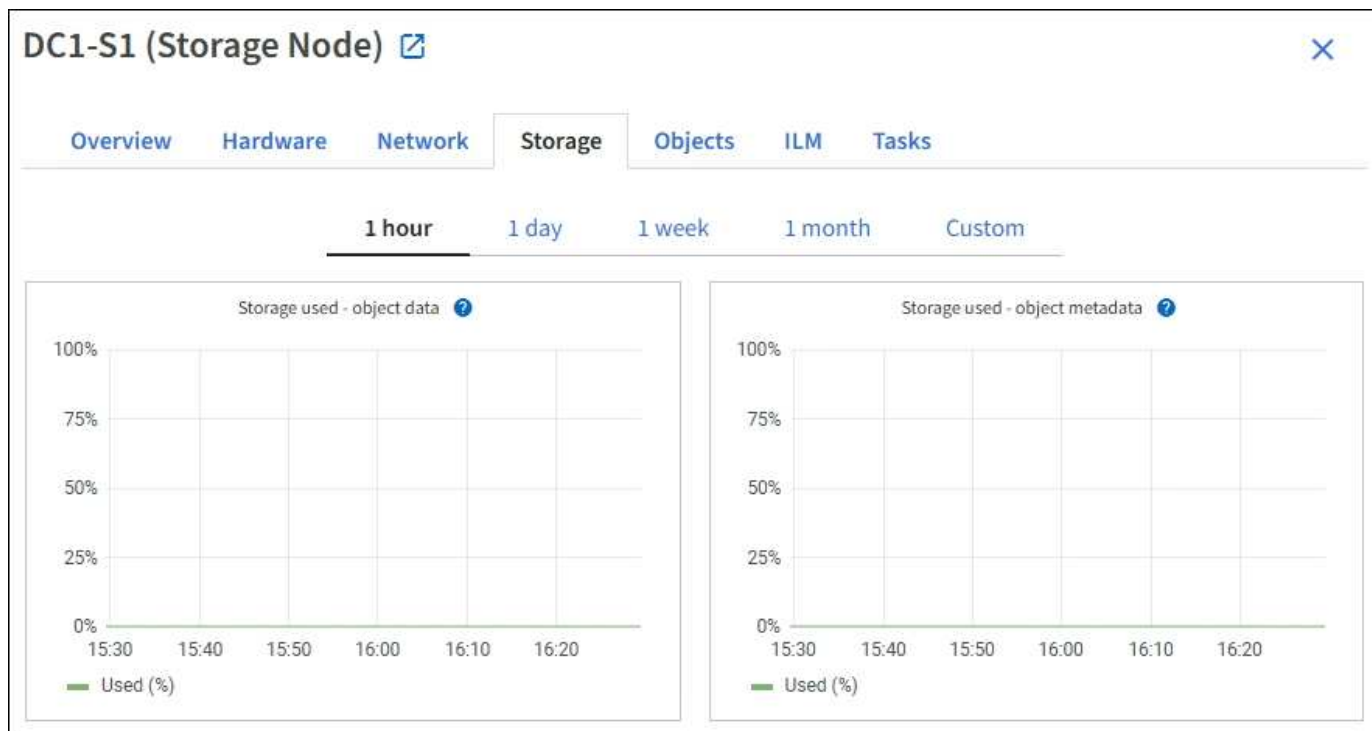
L'onglet Stockage s'affiche pour tous les nœuds, chaque site et l'ensemble de la grille.

Graphiques utilisés pour le stockage

Pour les nœuds de stockage, chaque site et l'ensemble de la grille, l'onglet Stockage inclut 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 au réseau, par exemple lors d'une mise à niveau ou d'un état déconnecté, certaines mesures peuvent être indisponibles ou exclues des totaux du site et du réseau. Une fois qu'un nœud se reconnecte au réseau, attendez quelques minutes que les valeurs se stabilisent.



Tableaux des périphériques de disque, des volumes et des magasins d'objets

Pour tous les nœuds, l'onglet Stockage contient des détails sur les périphériques de disque et les volumes sur le 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 connexes

["Surveiller la capacité de stockage"](#)

Afficher l'onglet Objets

L'onglet Objets fournit des informations sur ["Taux d'ingestion et de récupération S3"](#) .

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.

[Overview](#)[Hardware](#)[Network](#)[Storage](#)[Objects](#)[ILM](#)[Tasks](#)[1 hour](#)[1 day](#)[1 week](#)[1 month](#)[Custom](#)

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 des informations (ILM).

L'onglet ILM s'affiche pour chaque nœud de stockage, chaque site et la grille entière. Pour chaque site et la grille, l'onglet ILM affiche un graphique de la file d'attente ILM au fil du temps. Pour la grille, cet onglet fournit également le temps estimé pour effectuer une analyse ILM complète de tous les objets.

Pour les nœuds de stockage, l'onglet ILM fournit des détails sur l'évaluation ILM et la vérification en arrière-plan des objets à code d'effacement.

Informations connexes

- ["Surveiller la gestion du cycle de vie des informations"](#)
- ["Administrer StorageGRID"](#)

Utiliser l'onglet Tâches

L'onglet Tâches s'affiche pour tous les nœuds. Vous pouvez utiliser cet onglet pour renommer ou redémarrer un nœud ou pour mettre un nœud d'appliance en mode maintenance.

Pour connaître les exigences et les instructions complètes pour chaque option de cet onglet, consultez les éléments suivants :

- ["Renommer la grille, les sites et les nœuds"](#)
- ["Redémarrer le nœud de grille"](#)
- ["Mettre l'appareil en mode maintenance"](#)

Afficher l'onglet Équilibreur de charge

L'onglet Équilibreur de charge inclut des graphiques de performances et de diagnostic liés au fonctionnement du service Équilibreur de charge.

L'onglet Équilibreur de charge s'affiche pour les nœuds d'administration et les nœuds de passerelle, chaque site et l'ensemble de la grille. Pour chaque site, l'onglet Équilibreur de charge fournit un résumé global des statistiques de tous les nœuds de ce site. Pour l'ensemble de la grille, l'onglet Équilibreur de charge fournit un résumé global des statistiques pour tous les sites.

S'il n'y a aucune E/S exécutée via le service Load Balancer ou si aucun équilibreur de charge n'est configuré, les graphiques affichent « Aucune donnée ».



Demande de trafic

Ce graphique fournit une moyenne mobile sur 3 minutes du débit des données transmises entre les points de terminaison 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 requête. Par conséquent, cette valeur peut différer du débit en temps réel à des taux de requête faibles ou pour des requêtes de très longue durée. Vous pouvez consulter l'onglet Réseau pour obtenir une vue plus réaliste du comportement actuel du réseau.

Taux de demandes entrantes

Ce graphique fournit une moyenne mobile sur 3 minutes du nombre de nouvelles requêtes par seconde, réparties par type de requête (GET, PUT, HEAD et DELETE). Cette valeur est mise à jour lorsque les en-têtes d'une nouvelle requête ont été validés.

Durée moyenne de la requête (sans erreur)

Ce graphique fournit une moyenne mobile sur 3 minutes des durées de requête, réparties par type de requête (GET, PUT, HEAD et DELETE). La durée de chaque demande commence lorsqu'un en-tête de demande est analysé par le service Load Balancer et se termine lorsque le corps de la réponse complet est renvoyé au

client.

Taux de réponse aux erreurs

Ce graphique fournit une moyenne mobile sur 3 minutes du nombre de réponses d'erreur renvoyées aux clients par seconde, ventilées par code de réponse d'erreur.

Informations connexes

- ["Surveiller les opérations d'équilibrage de charge"](#)
- ["Administrer StorageGRID"](#)

Afficher l'onglet Services de la plateforme

L'onglet Services de plateforme fournit des informations sur toutes les opérations de service de plateforme S3 sur un site.

L'onglet Services de la plateforme est affiché pour chaque site. Cet onglet fournit des informations sur les services de la plateforme S3, tels que la réplication CloudMirror et le service d'intégration de recherche. Les graphiques de cet onglet affichent des mesures telles que le nombre de demandes en attente, le taux d'achèvement des demandes et le taux d'échec des demandes.

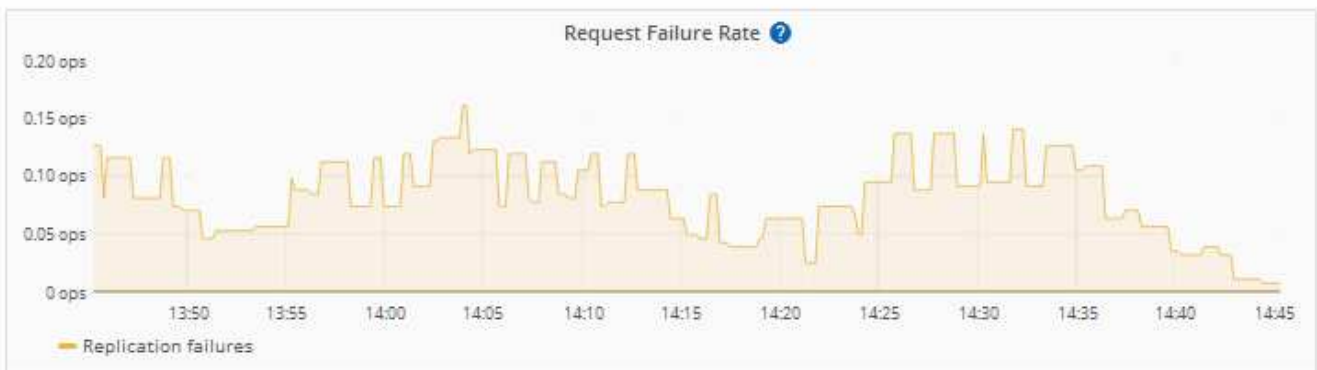
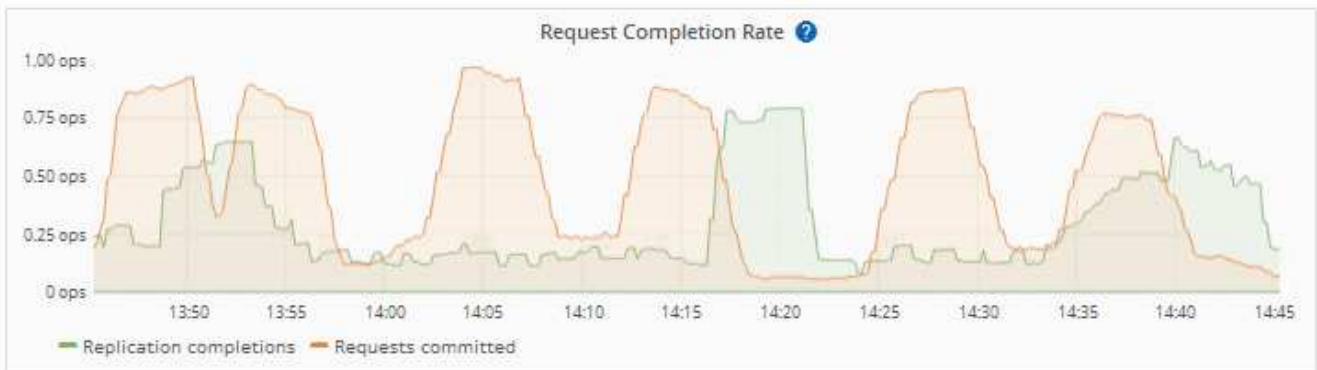
1 hour

1 day

1 week

1 month

Custom



Pour plus d'informations sur les services de la plateforme S3, y compris les détails de dépannage, consultez le ["instructions pour administrer StorageGRID"](#) .

Afficher l'onglet Gérer les lecteurs

L'onglet Gérer les lecteurs vous permet d'accéder aux détails et d'effectuer des tâches de dépannage et de maintenance sur les lecteurs des appareils qui prennent en charge cette fonctionnalité.

À l'aide de l'onglet Gérer les lecteurs, vous pouvez effectuer les opérations suivantes :

- Afficher la disposition des lecteurs de stockage de données dans l'appareil
- Afficher un tableau qui répertorie chaque emplacement de lecteur, type, état, version du micrologiciel et numéro de série
- Exécuter des fonctions de dépannage et de maintenance sur chaque lecteur

Pour accéder à l'onglet Gérer les lecteurs, vous devez disposer du ["Administrateur de l'appareil de stockage ou autorisation d'accès root"](#) .

Pour plus d'informations sur l'utilisation de l'onglet Gérer les lecteurs, consultez ["Utiliser l'onglet Gérer les lecteurs"](#) .

Afficher l'onglet Gestionnaire de système SANtricity (série E uniquement)

L'onglet SANtricity System Manager vous permet d'accéder à SANtricity System Manager sans avoir à configurer ou à connecter le port de gestion du dispositif de stockage. Vous pouvez utiliser cet onglet pour consulter les informations de diagnostic matériel et environnementales ainsi que les problèmes liés aux lecteurs.



L'accès à SANtricity System Manager à partir du Grid Manager est généralement destiné uniquement à surveiller le matériel de l'appareil et à configurer E-Series AutoSupport. De nombreuses fonctionnalités et opérations au sein de SANtricity System Manager, telles que la mise à niveau du micrologiciel, ne s'appliquent pas à la surveillance de votre appliance StorageGRID . Pour éviter les problèmes, suivez toujours les instructions de maintenance matérielle de votre appareil. Pour mettre à niveau le micrologiciel SANtricity , consultez le ["Procédures de configuration de maintenance"](#) pour votre appareil de stockage.



L'onglet Gestionnaire de système SANtricity s'affiche uniquement pour les nœuds d'appliance de stockage utilisant du matériel de la série E.

En utilisant SANtricity System Manager, vous pouvez effectuer les opérations suivantes :

- Affichez les données de performances telles que les performances au niveau de la baie de stockage, la latence d'E/S, l'utilisation du processeur du contrôleur de stockage et le débit.
- Vérifiez l'état des composants matériels.
- Exécutez des fonctions d'assistance, notamment l'affichage des données de diagnostic et la configuration d'E-Series AutoSupport.



Pour utiliser SANtricity System Manager pour configurer un proxy pour E-Series AutoSupport, voir ["Envoyer des packages AutoSupport de la série E via StorageGRID"](#) .

Pour accéder à SANtricity System Manager via Grid Manager, vous devez disposer du ["Administrateur de l'appareil de stockage ou autorisation d'accès root"](#) .



Vous devez disposer du micrologiciel SANtricity 8.70 ou supérieur pour accéder à SANtricity System Manager à l'aide de Grid Manager.

L'onglet affiche la page d'accueil de SANtricity System Manager.



Vous pouvez utiliser le lien SANtricity System Manager pour ouvrir SANtricity System Manager dans une nouvelle fenêtre de navigateur pour une visualisation plus facile.

Pour voir les détails des performances au niveau de la baie de stockage et de l'utilisation de la capacité, placez votre curseur sur chaque graphique.

Pour plus de détails sur l'affichage des informations accessibles depuis l'onglet SANtricity System Manager, voir "[Documentation NetApp E-Series et SANtricity](#)".

Informations à suivre 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 ne sont pas disponibles, 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](#)".
- Tu as "[autorisations d'accès spécifiques](#)".

À 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.

Que surveiller	Fréquence
" État de santé du système "	Tous les jours
Taux auquel " Capacité de l'objet et des métadonnées du nœud de stockage " est consommé	Hebdomadaire
" Opérations de gestion du cycle de vie de l'information "	Hebdomadaire
" Ressources réseau et système "	Hebdomadaire
" Activité des locataires "	Hebdomadaire
" Opérations client S3 "	Hebdomadaire
" Opérations d'équilibrage de charge "	Après la configuration initiale et après toute modification de configuration
" Connexions de la fédération de réseau "	Hebdomadaire

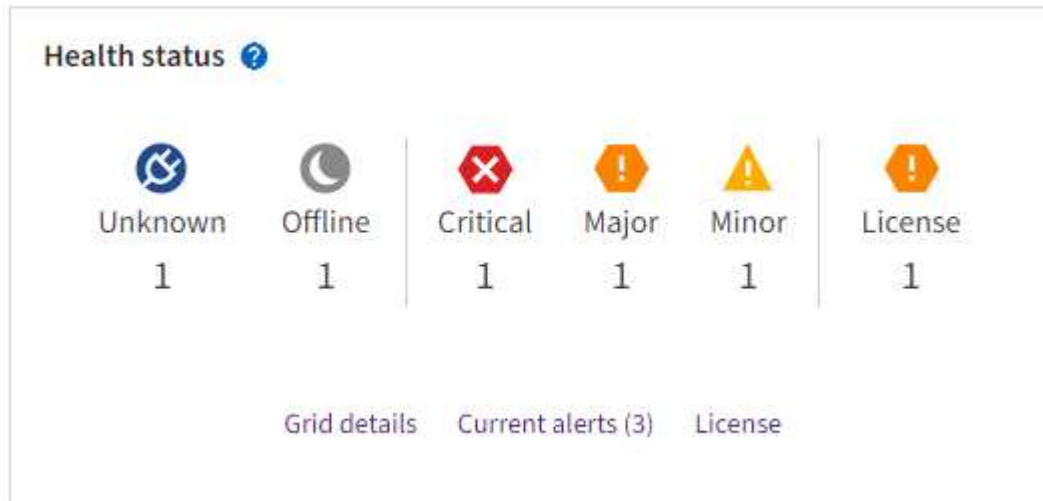
Surveiller la santé du système

Surveillez quotidiennement l'état de santé général de votre système StorageGRID .

À propos de cette tâche

Le système StorageGRID peut continuer à fonctionner lorsque certaines parties de la grille ne sont pas disponibles. Les problèmes potentiels indiqués par les alertes ne sont pas nécessairement des problèmes liés aux opérations du système. Enquêter sur les problèmes résumés sur la carte d'état de santé du tableau de bord du gestionnaire de grille.

Pour être averti des alertes dès qu'elles sont déclenchées, vous pouvez ["configurer des notifications par e-mail pour les alertes"](#) ou ["configurer les interruptions SNMP"](#) .



Lorsque des problèmes surviennent, des liens apparaissent qui vous permettent d'afficher des détails supplémentaires :

Lien	Apparaît lorsque...
Détails de la grille	Tous les nœuds sont déconnectés (état de connexion inconnu ou administrativement hors service).
Alertes actuelles (critiques, majeures, mineures)	Les alertes sont actuellement actif .
Alertes récemment résolues	Alertes déclenchées la semaine dernière sont maintenant résolus .
Licence	Il y a un problème avec la licence du logiciel pour ce système StorageGRID . Vous pouvez "mettre à jour les informations de licence selon les besoins" .

Surveiller les états de connexion des nœuds

Si un ou plusieurs nœuds sont déconnectés de la grille, les opérations critiques de StorageGRID peuvent être affectées. Surveillez les états de connexion des nœuds et résolvez rapidement tout problème.

Icône	Description	Action requise
	Non connecté - Inconnu Pour une raison inconnue, un nœud est déconnecté ou les services sur le nœud sont interrompus de manière inattendue. Par exemple, un service sur le nœud peut être arrêté ou le nœud peut avoir perdu sa connexion réseau en raison d'une panne de courant ou d'une panne inattendue. L'alerte Impossible de communiquer avec le nœud peut également être déclenchée. D'autres alertes peuvent également être actives.	Nécessite une attention immédiate. Sélectionnez chaque alerte et suivez les actions recommandées. Par exemple, vous devrez peut-être redémarrer un service qui s'est arrêté ou redémarrer l'hôte du nœud. Remarque : un nœud peut apparaître comme inconnu lors des opérations d'arrêt géré. Vous pouvez ignorer l'état Inconnu dans ces cas.
	Non connecté - Administrativement en panne Pour une raison attendue, le nœud n'est pas connecté au réseau. Par exemple, le nœud ou les services sur le nœud ont été arrêtés correctement, le nœud redémarre ou le logiciel est en cours de mise à niveau. Une ou plusieurs alertes peuvent également être actives. En fonction du problème sous-jacent, ces nœuds reviennent souvent en ligne sans intervention.	Déterminez si des alertes affectent ce nœud. Si une ou plusieurs alertes sont actives, sélectionnez chaque alerte et suivez les actions recommandées.
	Connecté Le nœud est connecté au réseau.	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 est également affichée 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 désactivée.

Alertes résolues : Vous pouvez rechercher et afficher un historique des alertes qui ont été résolues.

En option, vous avez regardé la vidéo : ["Vidéo : Aperçu des alertes"](#)



Le tableau suivant décrit les informations affichées dans le gestionnaire de grille pour les alertes actuelles et résolues.

En-tête de colonne	Description
Nom ou titre	Le nom de l'alerte et sa description.
Gravité	La 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 niveau de gravité.  Critique : une condition anormale existe qui a arrêté les opérations normales d'un nœud ou d'un service StorageGRID . Vous devez résoudre le problème sous-jacent immédiatement. Une interruption de service et une perte de données peuvent survenir si le problème n'est pas résolu.  Majeur : Une condition anormale existe qui affecte les opérations en cours ou approche le seuil d'une alerte critique. Vous devez enquêter sur les alertes majeures et résoudre tous les problèmes sous-jacents pour garantir que la condition anormale n'arrête pas le fonctionnement normal d'un nœud ou d'un service StorageGRID .  Mineur : Le système fonctionne normalement, mais une condition anormale existe qui pourrait affecter la capacité du système à fonctionner si elle persiste. Vous devez surveiller et résoudre les alertes mineures qui ne disparaissent pas d'elles-mêmes pour vous assurer qu'elles n'entraînent pas un problème plus grave.
Le temps déclenché	Alertes actuelles : La date et l'heure auxquelles l'alerte a été déclenchée dans votre 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 (<i>newest</i>) et de l'instance la plus ancienne de l'alerte (<i>oldest</i>). Alertes résolues : Il y a combien de temps l'alerte a été déclenchée.
Site/Nœud	Le nom du site et du nœud où l'alerte se produit ou s'est produite.

En-tête de colonne	Description
Statut	Que l'alerte soit active, silencieuse ou résolue. Si plusieurs alertes sont regroupées et que Toutes les alertes est sélectionné dans la liste déroulante, la ligne de titre indique combien d'instances de cette alerte sont actives et combien d'instances ont été désactivées.
Temps résolu (alertes résolues uniquement)	Il y a combien de temps l'alerte a été résolue.
Valeurs actuelles ou <i>valeurs de données</i>	La valeur de la métrique qui a provoqué le 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 Faible stockage de données d'objet incluent 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)	La valeur de la métrique qui a provoqué le 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 Faible stockage de données d'objet incluent 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 une liste des alertes dans ces catégories. Vous pouvez également afficher les détails d'une alerte en sélectionnant **Nœuds > node > Aperçu**, puis en sélectionnant l'alerte dans le tableau Alertes.

Par défaut, les alertes actuelles sont affichées comme suit :

- Les alertes déclenchées le plus récemment sont affichées en premier.
- Plusieurs alertes du même type sont affichées sous forme de groupe.
- Les alertes qui ont été désactivées ne sont pas affichées.
- Pour une alerte spécifique sur un nœud spécifique, si les seuils sont atteints pour plusieurs niveaux de gravité, seule l'alerte la plus grave est affichée. Autrement dit, si les seuils d'alerte sont atteints pour les niveaux de gravité mineur, majeur et critique, seule l'alerte critique est affichée.

La page Alertes actuelles est actualisée toutes les deux minutes.

2. Pour développer des groupes d'alertes, sélectionnez le curseur vers le bas ▼ . Pour réduire les alertes individuelles dans un groupe, sélectionnez le curseur vers le haut ▲ , 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 actuelles ou les groupes d'alertes, 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 au sein de chaque groupe sont triés. Par exemple, vous souhaitez peut-être trier les alertes d'un groupe par

Heure de déclenchement pour trouver l'instance la plus récente d'une alerte spécifique.

- Lorsque **Alertes de groupe** est effacé, la liste entière des alertes est triée. Par exemple, vous souhaitez peut-être trier toutes les alertes par **Nœud/Site** pour voir toutes les alertes affectant un nœud spécifique.

5. Pour filtrer les alertes actuelles par statut (**Toutes les alertes**, **Actif** ou **Silencieux**), utilisez le menu déroulant en haut du tableau.

Voir "[Notifications d'alerte silencieuses](#)".

6. Pour trier les alertes résolues :

- Sélectionnez une période dans le menu déroulant **Lors du déclenchement**.
- Sélectionnez une ou plusieurs gravités 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 liées à une règle d'alerte spécifique.
- Sélectionnez un ou plusieurs nœuds dans le menu déroulant **Nœud** 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 « Désactiver cette alerte » pour désactiver la règle d'alerte qui a provoqué le déclenchement de cette alerte.

Vous devez avoir le "[Gérer les alertes ou l'autorisation d'accès root](#)" pour faire taire une règle d'alerte.



Soyez prudent lorsque vous décidez de désactiver une règle d'alerte. Si une règle d'alerte est désactivée, vous risquez de ne pas détecter un problème sous-jacent jusqu'à ce qu'il empêche une opération critique de se terminer.

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 apparaît, 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 provoqué le déclenchement de cette alerte.

Vous devez avoir le "[Gérer les alertes ou l'autorisation d'accès root](#)" pour modifier une règle d'alerte.



Soyez prudent lorsque vous décidez de modifier une règle d'alerte. Si vous modifiez les valeurs de déclenchement, vous risquez de ne pas détecter un problème sous-jacent jusqu'à ce qu'il empêche une opération critique de se terminer.

11. Pour fermer les détails de l'alerte, sélectionnez **Fermer**.

Surveiller la capacité de stockage

Surveillez l'espace utilisable total disponible pour garantir que le système StorageGRID ne manque pas d'espace de stockage pour les objets ou pour les métadonnées des objets.

StorageGRID stocke les données d'objet et les métadonnées d'objet séparément et réserve une quantité spécifique d'espace pour une base de données Cassandra distribuée contenant des métadonnées d'objet. Surveillez la quantité totale d'espace consommée pour les objets et pour les métadonnées des objets, ainsi que les tendances de la quantité d'espace consommée pour chacun. Cela vous permettra de planifier à l'avance l'ajout de nœuds et d'éviter toute interruption de service.

Tu peux "[afficher les informations sur la capacité de stockage](#)" pour l'ensemble de la grille, pour chaque site et pour chaque nœud de stockage de votre système StorageGRID .

Surveiller la capacité de stockage de l'ensemble du réseau

Surveillez la capacité de stockage globale de votre grille pour garantir qu'il reste suffisamment d'espace libre pour les données d'objet et les métadonnées d'objet. Comprendre comment la capacité de stockage évolue au fil du temps peut vous aider à planifier l'ajout de nœuds de stockage ou de volumes de stockage avant que la capacité de stockage utilisable du réseau ne soit consommée.

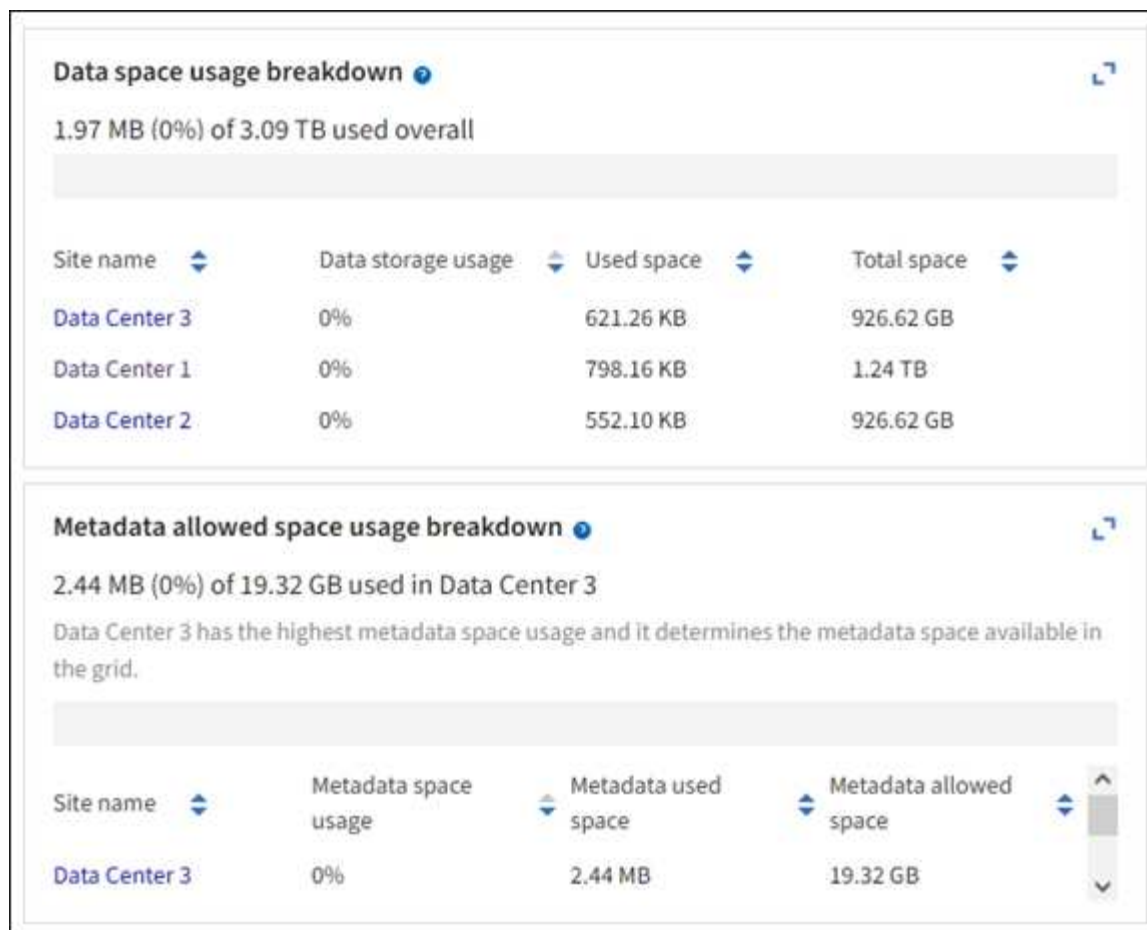
Le tableau de bord Grid Manager vous permet d'évaluer rapidement la quantité de stockage disponible pour l'ensemble du réseau et pour chaque centre de données. La page Nœuds fournit des valeurs plus détaillées pour les données d'objet et les métadonnées d'objet.

Étapes

1. Évaluez la quantité de stockage disponible pour l'ensemble du réseau et pour chaque centre de données.
 - a. Sélectionnez **Tableau de bord > Aperçu**.
 - b. Notez les valeurs sur les cartes de répartition de l'utilisation de l'espace de données et de répartition de l'utilisation de l'espace autorisé des métadonnées. Chaque carte répertorie un pourcentage d'utilisation du stockage, la capacité de l'espace utilisé et l'espace total disponible ou autorisé par le site.



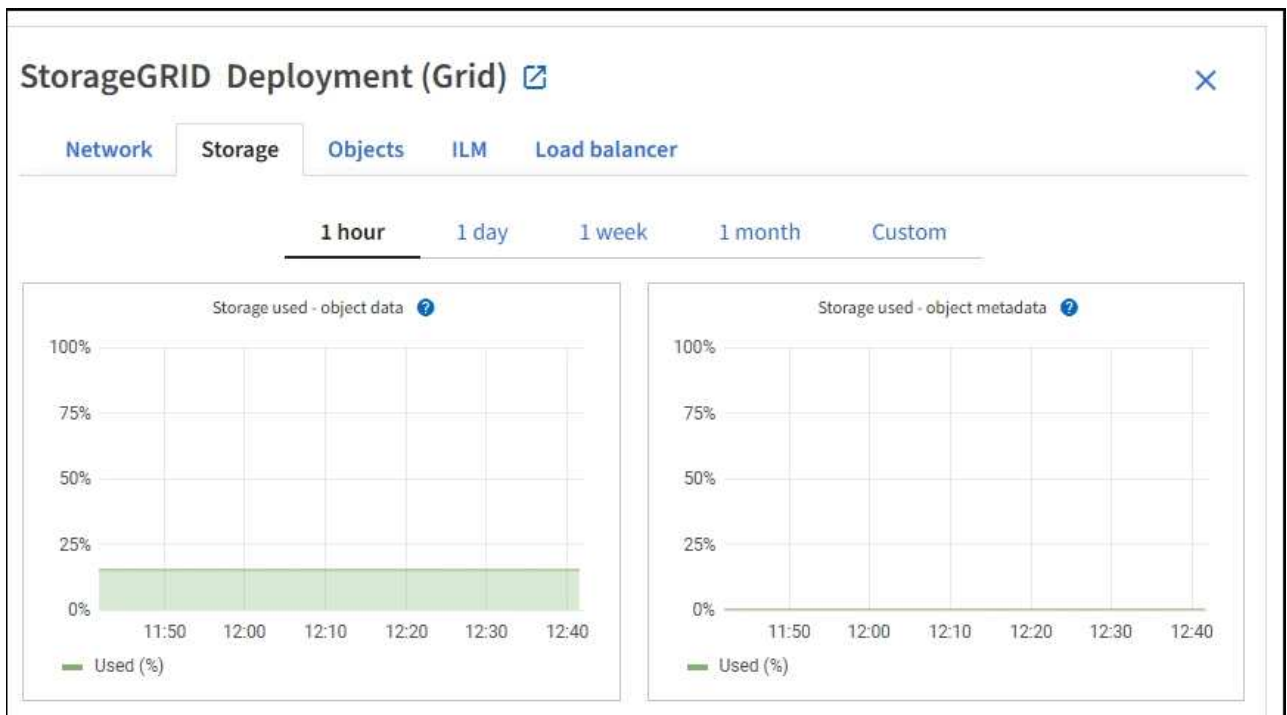
Le résumé n'inclut pas les supports d'archives.



- a. Notez le tableau sur la carte Stockage au fil du temps. Utilisez la liste déroulante de la période pour vous aider à déterminer la vitesse à laquelle le stockage est consommé.



2. Utilisez la page Nœuds pour obtenir des détails supplémentaires sur la quantité de stockage utilisée et la quantité de stockage restant disponible sur la grille pour les données d'objet et les métadonnées d'objet.
 - a. Sélectionnez **NODES**.
 - b. Sélectionnez **grid** > **Stockage**.



- c. Placez votre curseur sur les graphiques **Stockage utilisé - données d'objet** et **Stockage utilisé - métadonnées d'objet** pour voir la quantité de stockage d'objet et de stockage de métadonnées d'objet disponible pour l'ensemble de la grille, et 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, tels que les nœuds hors ligne.

3. Prévoyez d'effectuer une extension pour ajouter des nœuds de stockage ou des volumes de stockage avant que la capacité de stockage utilisable du réseau ne soit consommée.

Lorsque vous planifiez le calendrier d'une extension, tenez compte du temps qu'il faudra pour acquérir et installer un stockage supplémentaire.



Si votre stratégie ILM utilise le codage d'effacement, vous préférerez peut-être étendre lorsque les nœuds de stockage existants sont remplis à environ 70 % pour réduire le nombre de nœuds à ajouter.

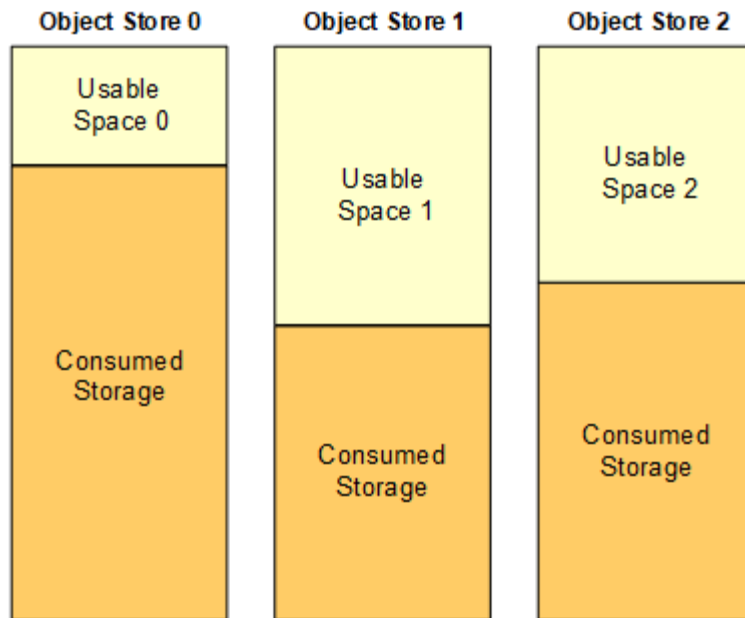
Pour plus d'informations sur la planification d'une extension de stockage, consultez le ["instructions pour étendre StorageGRID"](#).

Surveiller la capacité de stockage pour chaque nœud de stockage

Surveillez l'espace utilisable total pour chaque nœud de stockage pour vous assurer que le nœud dispose de suffisamment d'espace pour les nouvelles données d'objet.

À propos de cette tâche

L'espace utilisable est la quantité d'espace de stockage disponible pour stocker des objets. L'espace utilisable total pour un nœud de stockage est calculé en additionnant l'espace disponible sur tous les magasins d'objets au sein du nœud.



Total Usable Space = Usable Space 0 + Usable Space 1 + Usable Space 2

Étapes

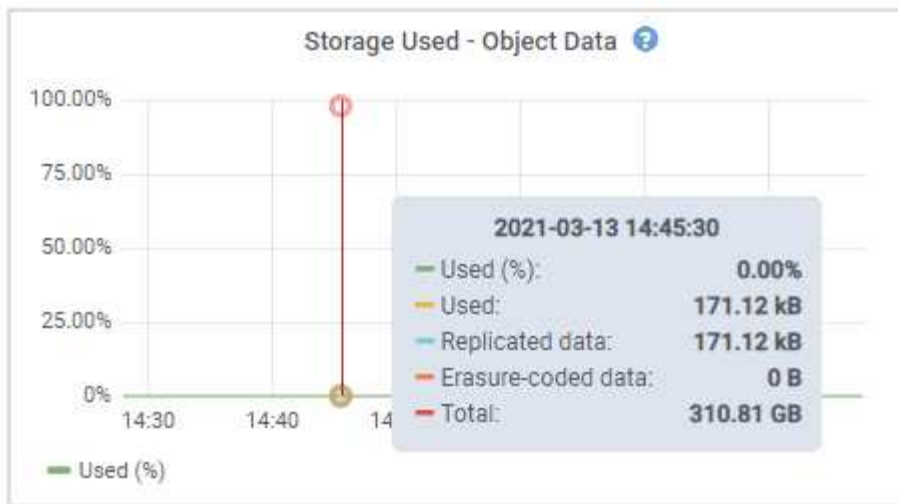
1. Sélectionnez **NODES > Storage Node > Storage**.

Les graphiques et les tableaux du nœud apparaissent.

2. Positionnez votre curseur sur le graphique Stockage utilisé - données de l'objet.

Les valeurs suivantes sont affichées :

- **Utilisé (%)** : Le pourcentage de l'espace total utilisable qui a été utilisé pour les données de l'objet.
- **Utilisé** : la quantité d'espace total utilisable qui a été utilisée pour les données de l'objet.
- **Données répliquées** : une estimation de la quantité de données d'objet répliquées sur ce nœud, ce site ou cette grille.
- **Données codées par effacement** : une estimation de la quantité de données d'objet codées par effacement sur ce nœud, ce site ou cette grille.
- **Total**: La quantité totale d'espace utilisable sur ce nœud, ce site ou cette grille. La valeur utilisée est la `storagegrid_storage_utilization_data_bytes` métrique.



3. Consultez 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 de 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

- Surveillez les valeurs au fil du temps pour estimer la vitesse à laquelle l'espace de stockage utilisable est consommé.
- Pour maintenir le fonctionnement normal du système, ajoutez des nœuds de stockage, ajoutez des volumes de stockage ou archivez les données d'objet avant que l'espace utilisable ne soit consommé.

Lorsque vous planifiez le calendrier d'une extension, tenez compte du temps qu'il faudra pour acquérir et installer un stockage supplémentaire.



Si votre stratégie ILM utilise le codage d'effacement, vous préférerez peut-être étendre 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, consultez le ["instructions pour](#)

[étendre StorageGRID](#) .

Le "[Faible stockage de données d'objets](#)" l'alerte est déclenchée lorsqu'il ne reste pas suffisamment d'espace pour stocker les données d'objet sur un nœud de stockage.

Surveiller la capacité des métadonnées des objets pour chaque nœud de stockage

Surveillez l'utilisation des métadonnées pour chaque nœud de stockage afin de garantir qu'un espace suffisant reste disponible pour les opérations de base de données essentielles. Vous devez ajouter de nouveaux nœuds de stockage sur chaque site avant que les métadonnées de l'objet ne dépassent 100 % de l'espace de métadonnées autorisé.

À propos de cette tâche

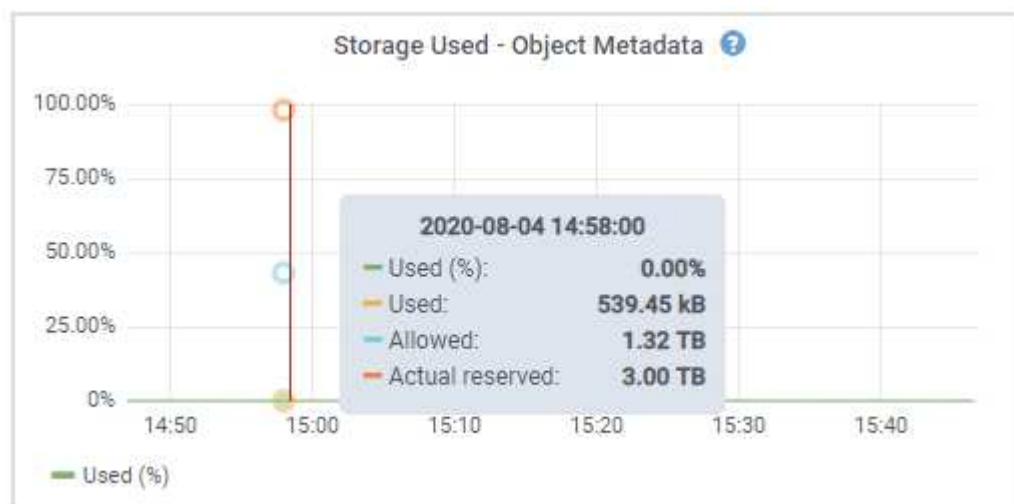
StorageGRID conserve trois copies des métadonnées d'objet sur chaque site pour assurer la redondance et protéger les métadonnées d'objet contre la perte. Les trois copies sont réparties uniformément sur tous les nœuds de stockage de chaque site à l'aide de l'espace réservé aux métadonnées sur le volume de stockage 0 de chaque nœud de stockage.

Dans certains cas, la capacité des métadonnées d'objet de la grille peut être consommée plus rapidement que sa capacité de stockage d'objet. Par exemple, si vous ingérez généralement un grand nombre de petits objets, vous devrez peut-être ajouter des nœuds de stockage pour augmenter la capacité des métadonnées, même si la capacité de stockage d'objets reste suffisante.

Certains des facteurs qui peuvent augmenter l'utilisation des métadonnées incluent la taille et la quantité de métadonnées et de balises utilisateur, le nombre total de parties dans un téléchargement en plusieurs parties et la fréquence des modifications des emplacements de stockage ILM.

Étapes

1. Sélectionnez **NODES > Storage Node > Storage**.
2. Placez votre curseur sur le graphique Stockage utilisé - métadonnées de l'objet pour voir les valeurs pour une période spécifique.



Utilisé (%)

Le pourcentage de l'espace de métadonnées autorisé qui a été utilisé sur ce nœud de stockage.

Métriques 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.

Métrique Prometheus : `storagegrid_storage_utilization_metadata_bytes`

Autorisé

L'espace autorisé pour les métadonnées d'objet sur ce nœud de stockage. Pour savoir comment cette valeur est déterminée pour chaque nœud de stockage, consultez le ["description complète de l'espace de métadonnées autorisé"](#).

Métrique Prometheus : `storagegrid_storage_utilization_metadata_allowed_bytes`

Réel réservé

L'espace réel réservé aux métadonnées sur ce nœud de stockage. Comprend l'espace autorisé et l'espace requis pour les opérations de métadonnées essentielles. Pour savoir comment cette valeur est calculée pour chaque nœud de stockage, consultez le ["description complète de l'espace réservé réel pour les métadonnées"](#).

La métrique Prometheus sera ajoutée 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, tels que les nœuds hors ligne.

3. Si la valeur **Utilisé (%)** est de 70 % ou plus, développez votre système StorageGRID en ajoutant des nœuds de stockage à chaque site.



L'alerte **Faible stockage de métadonnées** est déclenchée lorsque la valeur **Utilisé (%)** atteint certains seuils. Des résultats indésirables peuvent se produire si les métadonnées de l'objet utilisent plus de 100 % de l'espace autorisé.

Lorsque vous ajoutez les nouveaux nœuds, le système rééquilibre automatiquement les métadonnées des objets sur tous les nœuds de stockage du site. Voir le ["instructions pour étendre un système StorageGRID"](#).

Surveiller 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 quand vous en aurez besoin. ["étendre une grille"](#).

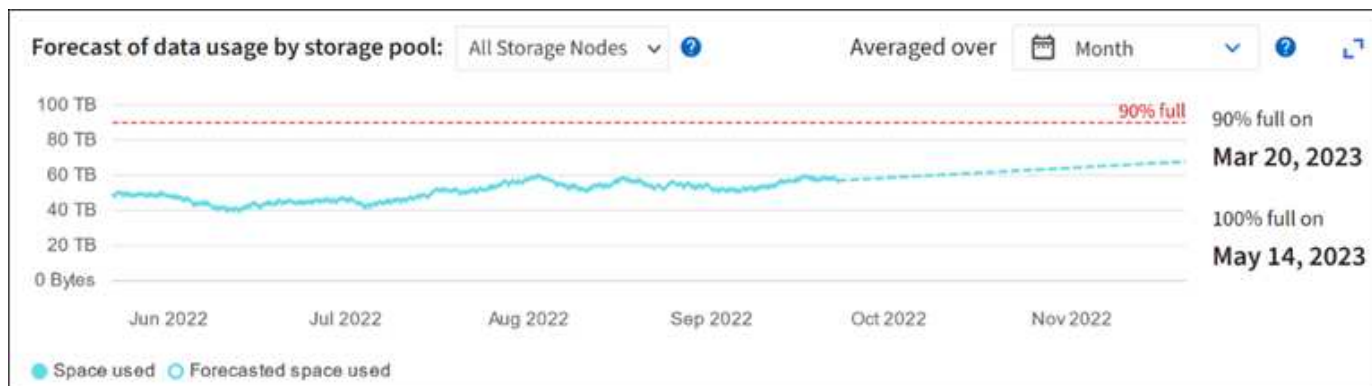
Si vous remarquez que le taux de consommation change au fil du temps, sélectionnez une plage plus courte dans le menu déroulant **Moyenne sur** pour refléter uniquement les modèles d'ingestion les plus récents. Si vous remarquez des tendances saisonnières, sélectionnez une plage plus longue.

Si vous disposez d'une nouvelle installation StorageGRID, laissez les données et les métadonnées s'accumuler avant d'évaluer les prévisions d'utilisation de l'espace.

Étapes

1. Sur le tableau de bord, sélectionnez **Stockage**.
2. Consultez les cartes du tableau de bord, les prévisions d'utilisation des données par pool de stockage et les prévisions d'utilisation des métadonnées par site.
3. Utilisez ces valeurs pour estimer quand vous devrez ajouter de nouveaux nœuds de stockage pour le

stockage des données et des métadonnées.



Surveiller la gestion du cycle de vie des informations

Le système de gestion du cycle de vie de l'information (ILM) fournit une gestion des données pour tous les objets stockés sur la grille. Vous devez surveiller les opérations ILM pour comprendre si le réseau peut gérer la charge actuelle ou si davantage de ressources sont nécessaires.

À propos de cette tâche

Le système StorageGRID gère les objets en appliquant les politiques ILM actives. Les politiques ILM et les règles ILM associées déterminent le nombre de copies effectuées, le type de copies créées, l'emplacement des copies et 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 ILM, ce qui oblige le système à mettre en file d'attente les objets dont les instructions de placement ILM ne peuvent pas être exécutées en temps quasi réel. Vous devez surveiller si StorageGRID suit les actions du client.

Utiliser l'onglet du tableau de bord Grid Manager

Étapes

Utilisez l'onglet ILM sur le tableau de bord du Grid Manager pour surveiller les opérations ILM :

1. Sign in au gestionnaire de grille.
2. Depuis le tableau de bord, sélectionnez l'onglet ILM et notez les valeurs sur la carte File d'attente ILM (Objets) et la carte de taux d'évaluation ILM.

Des pics temporaires dans la carte de file d'attente ILM (Objets) sur le tableau de bord sont à prévoir. Mais si la file d'attente continue d'augmenter et ne diminue jamais, la grille a besoin de plus de ressources pour fonctionner efficacement : soit plus de nœuds de stockage, soit, si la politique ILM place les objets dans des emplacements distants, plus de bande passante réseau.

Utiliser la page NODES

Étapes

De plus, examinez les files d'attente ILM à l'aide de la page **NODES** :



Les graphiques de la page **NODES** seront remplacés par les cartes de tableau de bord correspondantes dans une future version de StorageGRID .

1. Sélectionnez **NODES**.
2. Sélectionnez **nom de la grille > ILM**.
3. Placez votre 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 d'opérations client (par exemple, l'ingestion).
 - **Objets en file d'attente (de toutes les opérations)** : Le nombre total d'objets en attente d'évaluation ILM.
 - **Taux d'analyse (objets/s)** : Le taux auquel les objets de la grille sont analysés et mis en file d'attente pour ILM.
 - **Taux d'évaluation (objets/sec)** : Le taux actuel auquel les objets sont évalués par rapport à la politique ILM dans la grille.
4. Dans la section File d'attente ILM, examinez les attributs suivants.



La section de file d'attente ILM est incluse pour la grille uniquement. Ces informations ne sont pas affichées dans l'onglet ILM d'un site ou d'un nœud de stockage.

- **Période d'analyse - estimée** : Le temps estimé pour effectuer une analyse ILM complète de tous les objets.



Une analyse complète ne garantit pas que l'ILM a été appliqué à tous les objets.

- **Réparations tentées** : Nombre total d'opérations de réparation d'objets pour les données répliquées qui ont été tentées. Ce nombre augmente chaque fois qu'un nœud de stockage tente de réparer un objet à haut risque. Les réparations ILM à haut risque sont prioritaires si le réseau devient occupé.



La même réparation d'objet peut s'incrémenter à nouveau si la réplication échoue après la réparation.

Ces attributs peuvent être utiles lorsque vous surveillez la progression de la récupération du volume du nœud de stockage. Si le nombre de réparations tentées 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 grille individuels, sont essentielles à des opérations efficaces.

Surveiller les connexions et les performances du réseau

La connectivité réseau et la bande passante sont particulièrement importantes si votre politique de gestion du cycle de vie des informations (ILM) copie les objets répliqués entre les sites ou stocke les objets codés par effacement à l'aide d'un schéma offrant une protection contre la perte de site. Si le réseau entre les sites n'est pas disponible, la latence du réseau est trop élevée ou la bande passante du réseau est insuffisante, certaines règles ILM peuvent ne pas être en mesure de 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 des retards ILM.

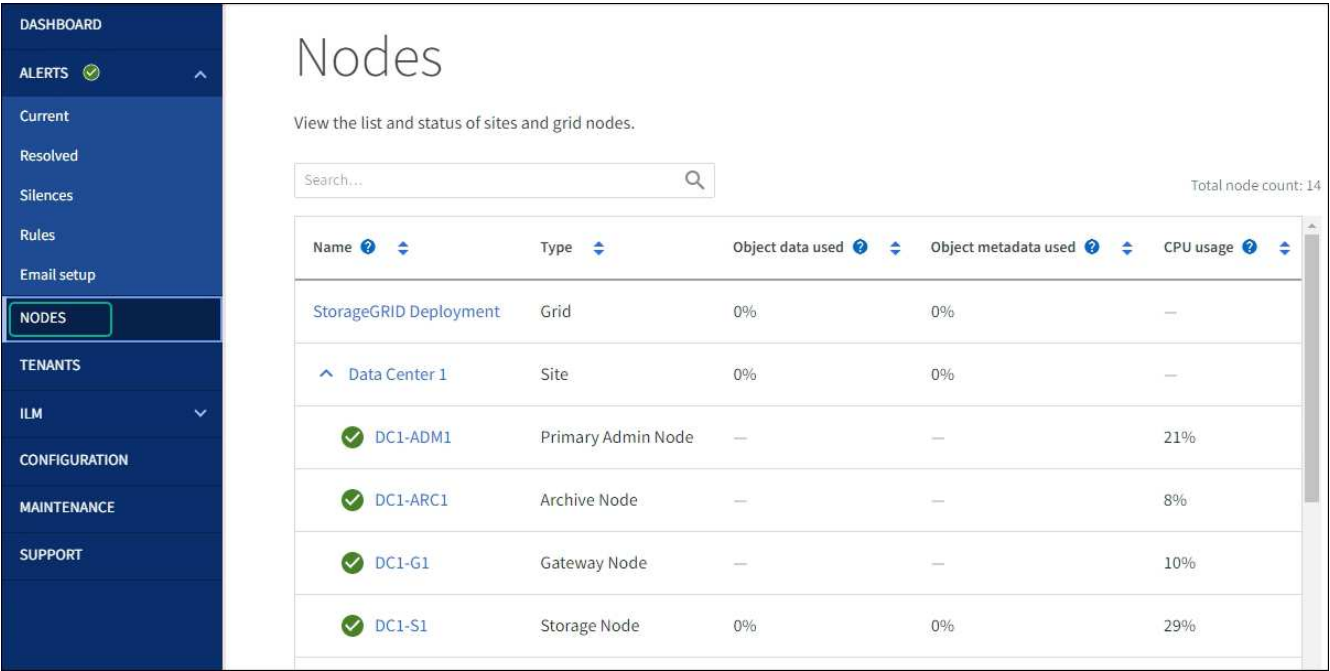
Utilisez Grid Manager pour surveiller la connectivité et les performances du réseau, afin de pouvoir résoudre rapidement tout problème.

En outre, considérez "création de politiques de classification du trafic réseau" afin que vous puissiez surveiller le trafic lié à des locataires, des buckets, des sous-réseaux ou des points de terminaison d'équilibrage de charge spécifiques. Vous pouvez définir des politiques de limitation du trafic selon vos besoins.

Étapes

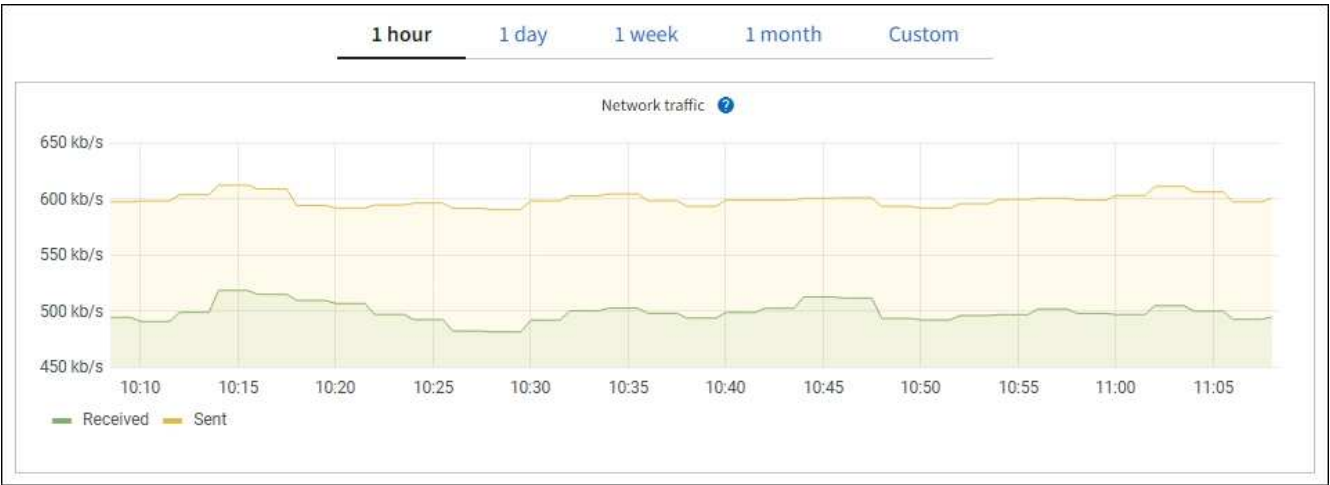
- 1. Sélectionnez **NODES**.

La page Nœuds apparaît. Chaque nœud de la grille est répertorié sous forme 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 du trafic réseau fournit un résumé du trafic réseau global pour la grille dans son ensemble, le site du centre de données ou pour 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.

Network interfaces					
Name ?	Hardware address ?	Speed ?	Duplex ?	Auto-negotiation ?	Link status ?
eth0	00:50:56:A7:66:75	10 Gigabit	Full	Off	Up

- 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.

Network communication						
Receive						
Interface ?	Data ?	Packets ?	Errors ?	Dropped ?	Frame overruns ?	Frames ?
eth0	2.89 GB	19,421,503	0	24,032	0	0
Transmit						
Interface ?	Data ?	Packets ?	Errors ?	Dropped ?	Collisions ?	Carrier ?
eth0	3.64 GB	18,494,381	0	0	0	0

3. Utilisez les mesures associées à vos stratégies de classification du trafic pour surveiller le trafic réseau.

- a. Sélectionnez **CONFIGURATION > Réseau > Classification du trafic**.

La page Stratégies de classification du trafic s'affiche et les stratégies existantes sont répertoriées dans le tableau.

Traffic Classification Policies

Traffic classification policies can be used to identify network traffic for metrics reporting and optional traffic limiting.

+ Create Edit ✕ Remove Metrics		
Name	Description	ID
☐ ERP Traffic Control	Manage ERP traffic into the grid	cd9afbc7-b85e-4208-b6f8-7e8a79e2c574
☒ Fabric Pools	Monitor Fabric Pools	223b0cbb-6968-4646-b32d-7665bdc894b
Displaying 2 traffic classification policies.		

- a. Pour afficher les graphiques qui montrent les mesures réseau associées à une stratégie, sélectionnez le bouton radio à gauche de la stratégie, puis cliquez sur **Mesures**.
- b. Consultez les graphiques pour comprendre le trafic réseau associé à la politique.

Si une politique de classification du trafic est conçue pour limiter le trafic réseau, analysez la fréquence

à laquelle le trafic est limité et décidez si la politique continue de répondre à vos besoins. De temps en temps, "[ajuster chaque politique de classification du trafic selon les besoins](#)".

Informations connexes

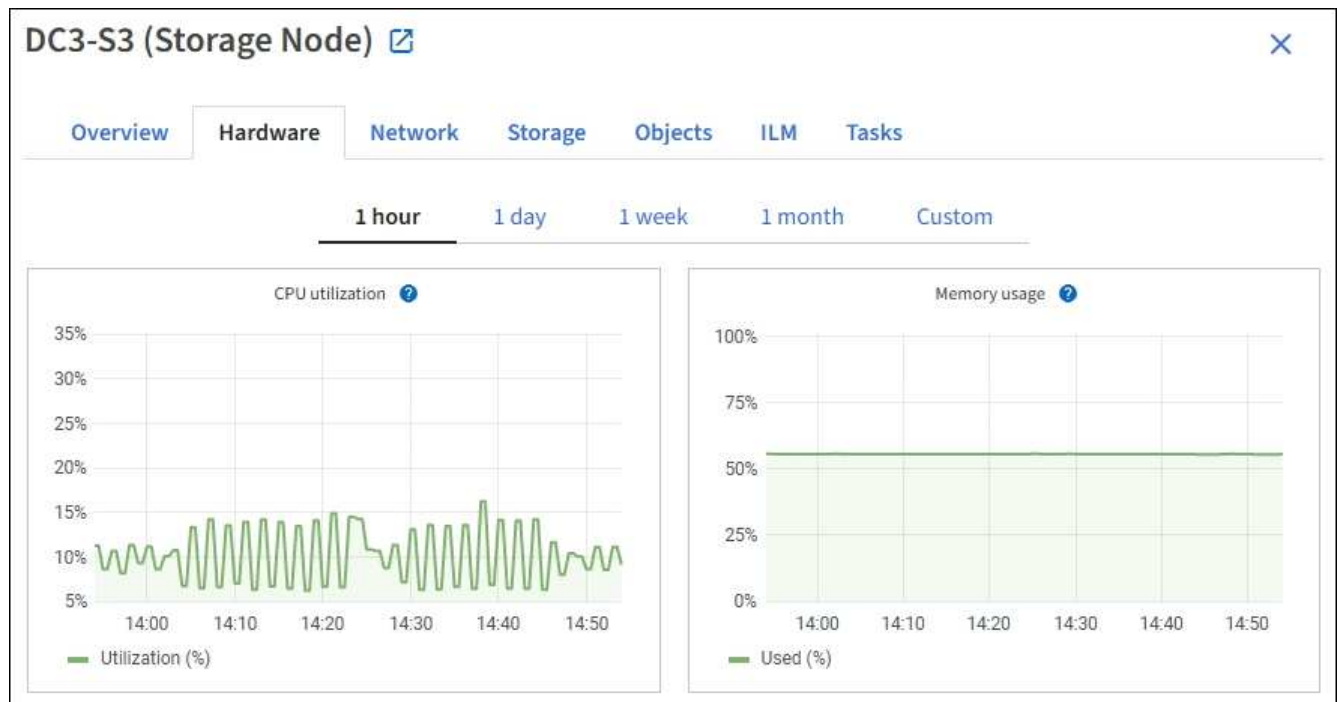
- "[Afficher l'onglet Réseau](#)"
- "[Surveiller les états de connexion des nœuds](#)"

Surveiller les ressources au niveau des nœuds

Surveillez les nœuds de grille individuels pour vérifier leurs niveaux d'utilisation des ressources. Si les nœuds sont constamment surchargés, davantage de nœuds peuvent être nécessaires pour des opérations efficaces.

Étapes

1. Depuis la page **NODES**, sélectionnez le nœud.
2. Sélectionnez l'onglet **Matériel** pour afficher les graphiques d'utilisation du processeur et de l'utilisation de la mémoire.



3. Pour afficher un intervalle de temps différent, sélectionnez l'un des contrôles au-dessus du graphique ou du diagramme. Vous pouvez afficher les informations disponibles pour des 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 dates et d'heures.
4. Si le nœud est hébergé sur un dispositif de stockage ou un dispositif de services, faites défiler vers le bas pour afficher les tableaux des composants. Le statut de tous les composants doit être « Nominal ». Examinez les composants qui ont un autre statut.

Informations connexes

- "[Afficher les informations sur les nœuds de stockage de l'appliance](#)"
- "[Afficher les informations sur les nœuds d'administration et les nœuds de passerelle de l'appareil](#)"

Surveiller l'activité des locataires

Toutes les activités des clients S3 sont associées aux comptes locataires StorageGRID . Vous pouvez utiliser Grid Manager pour surveiller l'utilisation du stockage ou le trafic réseau pour tous les locataires ou un locataire spécifique. Vous pouvez utiliser le journal d'audit ou les tableaux de bord Grafana pour collecter des informations plus détaillées sur la manière dont les locataires utilisent StorageGRID.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un ["navigateur Web pris en charge"](#) .
- Vous avez le ["Accès root ou autorisation des comptes locataires"](#) .

Voir tous les locataires

La page Locataires affiche les informations de base pour tous les comptes locataires actuels.

Étapes

1. Sélectionnez **LOCATAIRES**.
2. Consultez les informations affichées sur les pages Locataire.

L'espace logique utilisé, l'utilisation du quota, le quota et le nombre d'objets sont répertoriés pour chaque locataire. Si aucun quota n'est défini pour un locataire, les champs Utilisation du quota et Quota contiennent un tiret (—).



Les valeurs d'espace utilisées sont des estimations. Ces estimations sont affectées par le moment des ingestions, la connectivité réseau et l'état du nœud.

Tenants							
View information for each tenant account. Depending on the timing of ingests, network connectivity, and node status, the usage data shown might be out of date. To view more recent values, select the tenant name.							
Create	Export to CSV	Actions	Search tenants by name or ID		Displaying 5 results		
☐	Name	Logical space used	Quota utilization	Quota	Object count	Sign in/Copy URL	
☐	Tenant 01	2.00 GB	10%	20.00 GB	100	→	📄
☐	Tenant 02	85.00 GB	85%	100.00 GB	500	→	📄
☐	Tenant 03	500.00 TB	50%	1.00 PB	10,000	→	📄
☐	Tenant 04	475.00 TB	95%	500.00 TB	50,000	→	📄
☐	Tenant 05	5.00 GB	—	—	500	→	📄

3. Vous pouvez également vous connecter à un compte locataire en sélectionnant le lien de connexion. [→](#) dans la colonne * Sign in/ 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 * Sign in/ Copier l'URL*.

5. En option, sélectionnez **Exporter vers CSV** pour afficher et exporter un `.csv` fichier contenant les valeurs d'utilisation pour tous les locataires.

Vous êtes invité à ouvrir ou à enregistrer le `.csv` déposer.

Le contenu de la `.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` fichier dans une application de feuille de calcul ou utilisez-le dans l'automatisation.

6. Si aucun objet n'est répertorié, vous pouvez également sélectionner **Actions > Supprimer** pour supprimer un ou plusieurs locataires. Voir ["Supprimer le compte locataire"](#) .

Vous ne pouvez pas supprimer un compte locataire si le compte inclut des buckets ou des conteneurs.

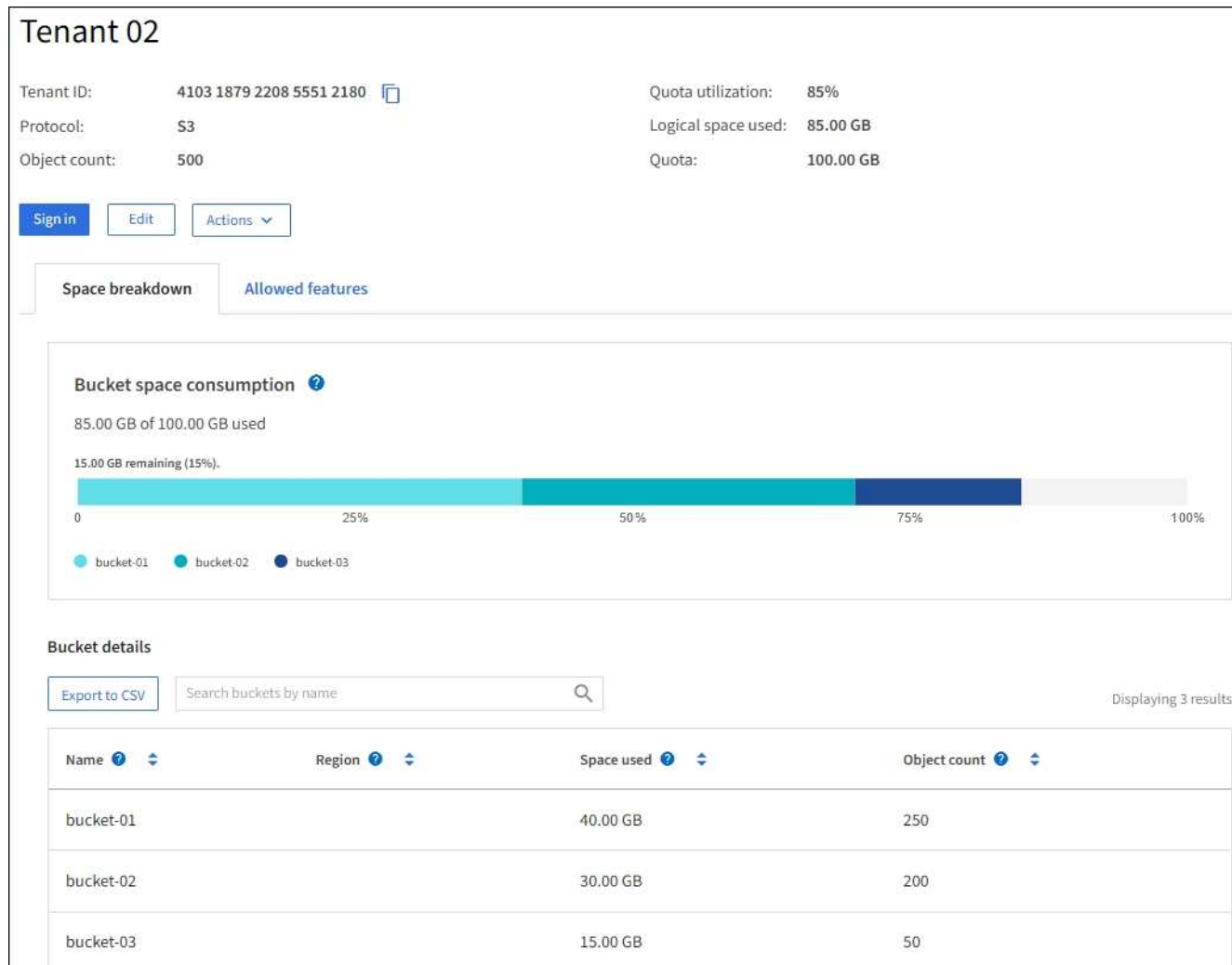
Afficher un locataire spécifique

Vous pouvez afficher les détails d'un locataire spécifique.

Étapes

1. Sélectionnez le nom du locataire sur la page Locataires.

La page des détails du locataire apparaît.



2. Consultez l'aperçu du locataire en haut de la page.

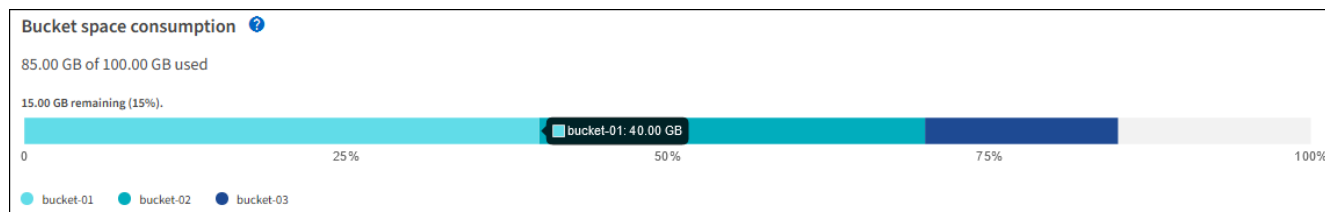
Cette section de la page de détails fournit des informations récapitulatives sur le locataire, notamment le nombre d'objets du locataire, l'utilisation du quota, l'espace logique utilisé et le paramètre de quota.

3. Dans l'onglet **Répartition de l'espace**, consultez le graphique **Consommation d'espace**.

Ce graphique montre la consommation totale d'espace pour tous les compartiments S3 du locataire.

Si un quota a été défini pour ce locataire, la quantité de quota utilisée et restante est affichée sous forme de texte (par exemple, 85.00 GB of 100 GB used). Si aucun quota n'a été défini, le locataire dispose d'un quota illimité et le texte n'inclut qu'une quantité d'espace utilisée (par exemple, 85.00 GB used). Le graphique à barres montre le pourcentage de quota dans chaque bucket ou conteneur. Si le locataire a dépassé le quota de stockage de plus de 1 % et d'au moins 1 Go, le graphique affiche le quota total et le montant excédentaire.

Vous pouvez placer votre curseur sur le graphique à barres pour voir le stockage utilisé par chaque bucket ou conteneur. Vous pouvez placer votre curseur sur le segment d'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 télécharger des objets et rejette les nouvelles acquisitions si le locataire a dépassé le quota. Cependant, StorageGRID ne prend pas en compte la taille du téléchargement actuel pour déterminer si le quota a été dépassé. Si des objets sont supprimés, un locataire peut être temporairement empêché de télécharger de nouveaux objets jusqu'à ce que l'utilisation du quota soit recalculée. Les calculs d'utilisation des quotas peuvent prendre 10 minutes ou plus.



L'utilisation du quota d'un locataire indique la quantité totale de données d'objet que le locataire a téléchargées sur StorageGRID (taille logique). L'utilisation du quota ne représente pas l'espace utilisé pour stocker des copies de ces objets et leurs métadonnées (taille physique).



Vous pouvez activer la règle d'alerte **Utilisation élevée du quota du locataire** pour déterminer si les locataires consomment leurs quotas. Si cette option est activée, cette alerte est déclenchée lorsqu'un locataire a utilisé 90 % de son quota. Pour les instructions, voir "[Modifier les règles d'alerte](#)".

4. Dans l'onglet **Répartition de l'espace**, examinez les **Détails du bucket**.

Ce tableau répertorie les compartiments S3 pour le locataire. L'espace utilisé correspond à la quantité totale de données d'objet dans le bucket 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 vers CSV** pour afficher et exporter un fichier .csv contenant les valeurs d'utilisation de chaque bucket ou conteneur.

Le contenu d'un locataire S3 individuel .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 fichier dans une application de feuille de calcul ou utilisez-le dans l'automatisation.

6. Vous pouvez également sélectionner l'onglet **Fonctionnalités autorisées** pour afficher la liste des autorisations et des fonctionnalités activées pour le locataire. Voir "[Modifier le compte locataire](#)" si vous devez modifier l'un de ces paramètres.

7. Si le locataire dispose de l'autorisation **Utiliser la connexion à la 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 réseau ?](#)" et "[Gérer les locataires autorisés pour la fédération de](#)

Afficher le trafic réseau

Si des stratégies de classification du trafic sont en place pour un locataire, examinez le trafic réseau pour ce locataire.

Étapes

1. Sélectionnez **CONFIGURATION > Réseau > Classification du trafic**.

La page Stratégies de classification du trafic s'affiche et les stratégies existantes sont répertoriées dans le tableau.

2. Passez en revue la liste des politiques pour identifier celles qui s'appliquent à un locataire spécifique.
3. Pour afficher les mesures associées à une politique, sélectionnez le bouton radio à gauche de la politique et sélectionnez **Mesures**.
4. Analysez les graphiques pour déterminer à quelle fréquence la politique limite le trafic et si vous devez ajuster la politique.

Voir "[Gérer les politiques de classification du trafic](#)" pour plus d'informations.

Utiliser le journal d'audit

En option, vous pouvez utiliser le journal d'audit pour une surveillance plus précise des activités d'un locataire.

Par exemple, vous pouvez surveiller les types d'informations suivants :

- Opérations client spécifiques, telles que PUT, GET ou DELETE
- Tailles des objets
- La règle ILM appliquée aux objets
- L'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 de journaux de votre choix. Cela vous permet de mieux comprendre les activités des clients ou de mettre en œuvre des modèles de rétrofacturation et de facturation sophistiqués.

Voir "[Examiner les journaux d'audit](#)" pour plus d'informations.

Utiliser les métriques Prometheus

Vous pouvez également utiliser les métriques Prometheus pour générer des rapports sur l'activité des locataires.

- Dans le gestionnaire de grille, sélectionnez **SUPPORT > Outils > Métriques**. Vous pouvez utiliser des tableaux de bord existants, tels que S3 Overview, pour examiner les activités des clients.



Les outils disponibles sur la page Métriques sont principalement destinés à être utilisés par le support technique. Certaines fonctionnalités et éléments de menu de ces outils sont intentionnellement non fonctionnels.

- En haut du gestionnaire de grille, sélectionnez l'icône d'aide et sélectionnez **Documentation API**. Vous pouvez utiliser les métriques de la section Métriques de l'API Grid Management pour créer des règles

d'alerte et des tableaux de bord personnalisés pour l'activité des locataires.

Voir "[Examiner les mesures de support](#)" pour plus d'informations.

Surveiller les opérations du client S3

Vous pouvez surveiller les taux d'ingestion et de récupération d'objets ainsi que les mesures relatives au nombre d'objets, aux requêtes et à la vérification. Vous pouvez afficher le nombre de tentatives réussies et infructueuses des applications clientes pour lire, écrire et modifier des objets dans le système StorageGRID .

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "[navigateur Web pris en charge](#)".

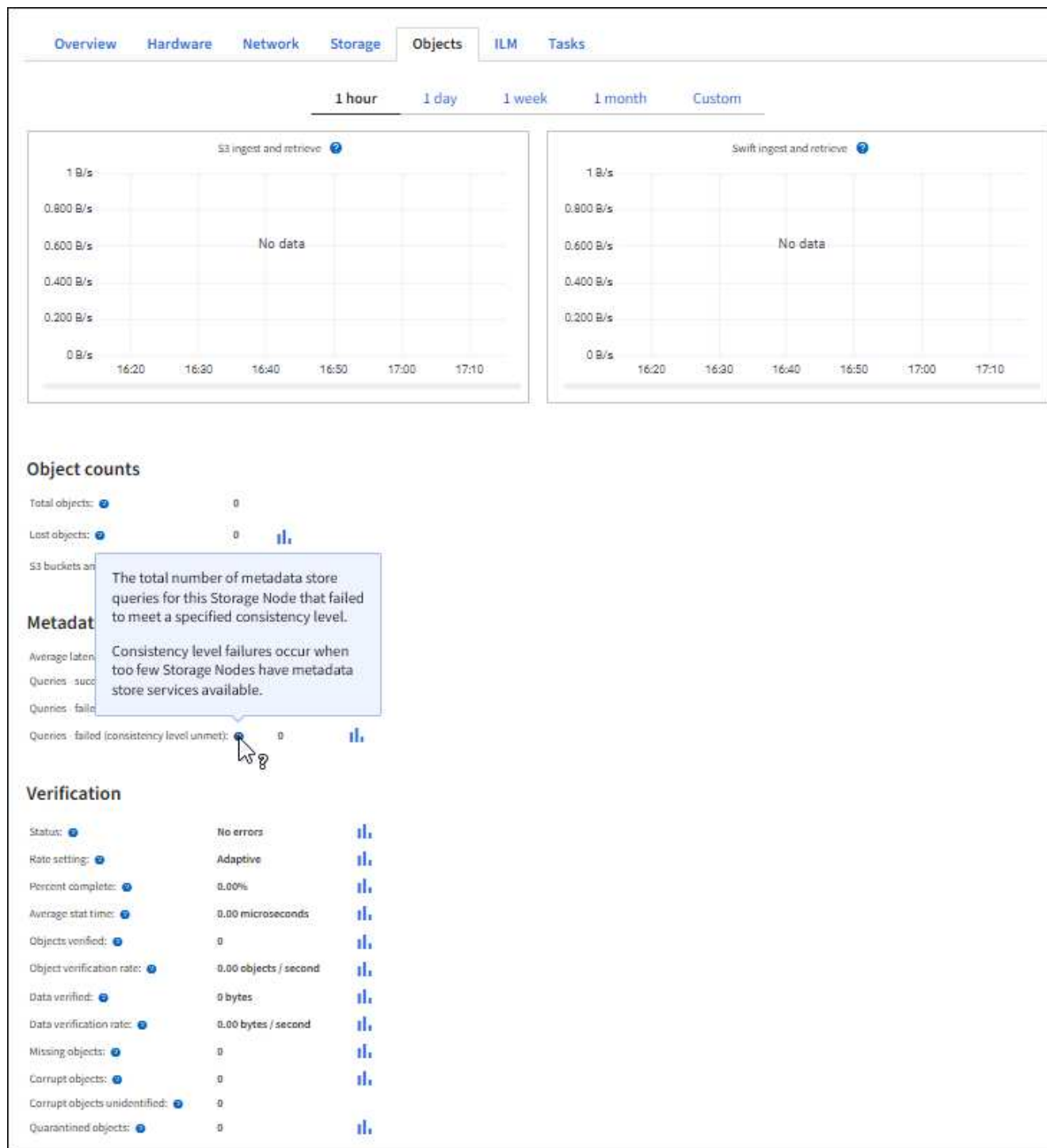
Étapes

1. Depuis le tableau de bord, sélectionnez l'onglet **Performance**.
2. Consultez les graphiques S3, qui résument le nombre d'opérations client effectuées par les nœuds de stockage et le nombre de requêtes API reçues par les nœuds de stockage pendant la période sélectionnée.
3. Sélectionnez **NODES** pour accéder à la page Nœuds.
4. Depuis la page d'accueil des nœuds (niveau de la grille), sélectionnez l'onglet **Objets**.

Le graphique montre les taux d'ingestion et de récupération S3 pour l'ensemble de votre système StorageGRID en octets par seconde et la quantité de données ingérées ou récupérées. Vous pouvez sélectionner un intervalle de temps ou appliquer un intervalle personnalisé.

5. Pour afficher les informations d'un nœud de stockage particulier, sélectionnez le nœud dans la liste de gauche, puis sélectionnez l'onglet **Objets**.

Le graphique montre les taux d'ingestion et de récupération du nœud. L'onglet inclut également des mesures pour le nombre d'objets, les requêtes de métadonnées et les opérations de vérification.



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 apporté des modifications de configuration ou effectué une extension.

À propos de cette 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 répartir les demandes des clients sur plusieurs nœuds de stockage.

Après avoir configuré l'équilibrage de charge, vous devez confirmer que les opérations d'ingestion et de récupération d'objets sont réparties uniformément sur les nœuds de stockage. Des demandes réparties uniformément garantissent que StorageGRID reste réactif aux demandes des clients sous charge et peut aider à maintenir les performances des clients.

Si vous avez configuré un groupe haute disponibilité (HA) de nœuds de passerelle ou de nœuds d'administration en mode de sauvegarde active, un seul nœud du groupe distribue activement les demandes des clients.

Pour plus d'informations, consultez la section "[Configurer les connexions client S3](#)".

Étapes

1. Si les clients S3 se connectent à l'aide du service Load Balancer, vérifiez que les nœuds d'administration ou les nœuds de passerelle distribuent activement le trafic comme prévu :
 - a. Sélectionnez **NODES**.
 - b. Sélectionnez un nœud de passerelle ou un nœud d'administration.
 - c. Dans l'onglet **Vue d'ensemble**, vérifiez si une interface de nœud se trouve dans un groupe HA et si l'interface de nœud a le rôle de Principal.

Les nœuds avec le rôle principal et les nœuds qui ne font pas partie d'un groupe HA doivent distribuer activement les demandes aux clients.

- d. Pour chaque nœud qui doit distribuer activement les demandes des clients, sélectionnez l'option "[Onglet Équilibreur de charge](#)".
 - e. Consultez le graphique du trafic des demandes d'équilibrage de charge de la semaine dernière pour vous assurer que le nœud a distribué activement les demandes.

Les nœuds d'un groupe HA de sauvegarde active peuvent assumer le rôle de sauvegarde de temps à autre. Pendant ce temps, les nœuds ne distribuent pas les requêtes des clients.

- f. Consultez le graphique du taux de demandes entrantes de l'équilibreur de charge de la semaine dernière pour évaluer le débit d'objet du nœud.
 - g. Répétez ces étapes pour chaque nœud d'administration ou nœud de passerelle dans le système StorageGRID.
 - h. Vous pouvez également utiliser des stratégies de classification du trafic pour afficher une analyse plus détaillée du trafic traité par le service Load Balancer.
2. Vérifiez que ces demandes sont réparties uniformément entre les nœuds de stockage.
 - a. Sélectionnez **Nœud de stockage > LDR > HTTP**.
 - b. Consultez le nombre de **sessions entrantes actuellement établies**.
 - c. Répétez l'opération pour chaque nœud de stockage dans la grille.

Le nombre de sessions doit être à peu près égal sur tous les nœuds de stockage.

Surveiller les connexions de la fédération de réseau

Vous pouvez surveiller les informations de base sur tous "[connexions de fédération de réseau](#)", des informations détaillées sur une connexion spécifique ou des mesures Prometheus sur les opérations de réplication inter-grille. 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 ou l'autre grille à l'aide d'un [navigateur Web pris en charge](#).
- Vous avez le ["Autorisation d'accès root"](#) pour la grille à laquelle vous êtes connecté.

Voir toutes les connexions

La page Fédération de grille 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

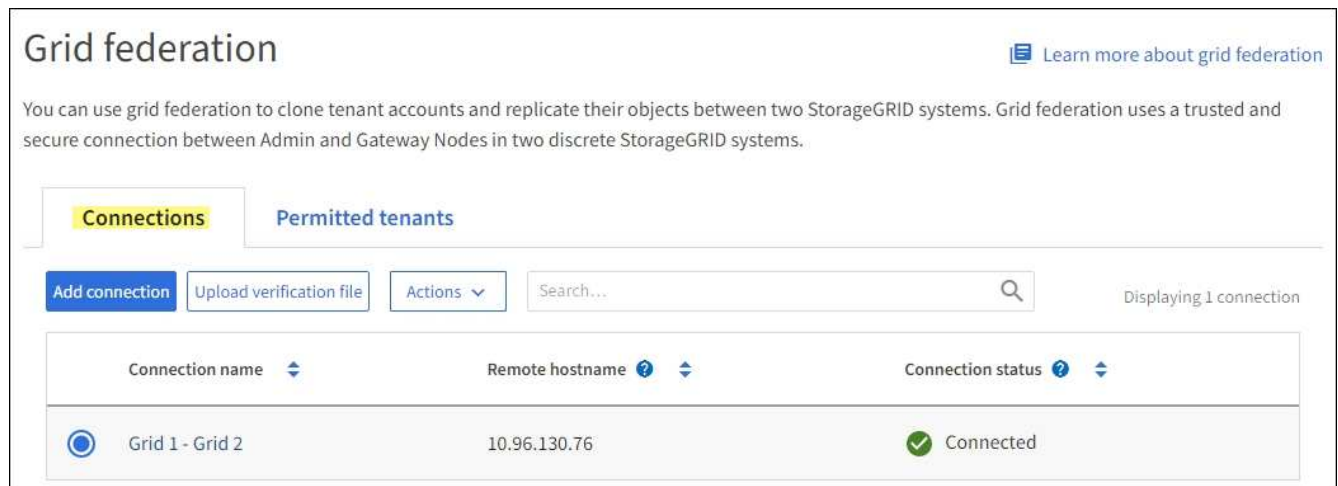
1. Sélectionnez **CONFIGURATION > Système > Fédération de grille**.

La page de la fédération Grid apparaît.

2. Pour voir les informations de base de toutes les connexions sur cette grille, sélectionnez l'onglet **Connexions**.

Depuis cet onglet, vous pouvez :

- ["Créer une nouvelle connexion"](#).
- Sélectionnez une connexion existante pour ["modifier ou tester"](#).



The screenshot shows the 'Grid federation' page. At the top, there's a header with the title 'Grid federation' and a link 'Learn more about grid federation'. Below the header, a descriptive paragraph explains that grid federation is used to clone tenant accounts and replicate objects between two StorageGRID systems. The main content area has two tabs: 'Connections' (active) and 'Permitted tenants'. Under the 'Connections' tab, there are buttons for 'Add connection', 'Upload verification file', and an 'Actions' dropdown. A search bar is also present. Below these controls is a table with columns for 'Connection name', 'Remote hostname', and 'Connection status'. The table displays one connection: 'Grid 1 - Grid 2' with remote hostname '10.96.130.76' and status 'Connected' (indicated by a green checkmark). A status indicator 'Displaying 1 connection' is shown on the right.

Connection name	Remote hostname	Connection status
Grid 1 - Grid 2	10.96.130.76	Connected

3. Pour afficher les informations de base de tous les comptes locataires de cette grille disposant de l'autorisation **Utiliser la connexion à la fédération de grille**, sélectionnez l'onglet **Locataires autorisés**.

Depuis cet onglet, vous pouvez :

- ["Consultez la page de détails pour chaque locataire autorisé"](#).
- Consultez la page de détails pour chaque connexion. Voir [Afficher une connexion spécifique](#).
- Sélectionnez un locataire autorisé et ["supprimer l'autorisation"](#).
- Vérifiez les erreurs de réplication inter-grille et effacez la dernière erreur, le cas échéant. Voir ["Résoudre les erreurs de fédération de grille"](#).

Grid federation [Learn more about grid federation](#)

You can use grid federation to clone tenant accounts and replicate their objects between two StorageGRID systems. Grid federation uses a trusted and secure connection between Admin and Gateway Nodes in two discrete StorageGRID systems.

[Connections](#)
[Permitted tenants](#)

[Remove permission](#)
[Clear error](#)

Displaying one result

Tenant name	Connection name	Connection status	Remote grid hostname	Last error
Tenant A	Grid 1 - Grid 2	Connected	10.96.130.76	Check for errors

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.

Depuis 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. Lorsque vous visualisez une connexion spécifique, sélectionnez l'onglet * Locataires autorisés * pour afficher les détails sur les locataires autorisés pour la connexion.

Depuis cet onglet, vous pouvez :

- "[Consultez la page de détails pour chaque locataire autorisé](#)".
- "[Supprimer l'autorisation d'un locataire](#)" pour utiliser la connexion.
- Vérifiez les erreurs de réplication inter-grille et effacez la dernière erreur. Voir "[Résoudre les erreurs de fédération de grille](#)".

Grid 1 - Grid 2

Local hostname (this grid):

10.96.130.64

Port:

23000

Remote hostname (other grid):

10.96.130.76

Connection status:

Connected

Edit

Download file

Test connection

Remove

Permitted tenants

Certificates

Remove permission

Clear error

Search...

Displaying one result

Tenant name	Last error
Tenant A	Check for errors

3. Lorsque vous affichez une connexion spécifique, sélectionnez l'onglet **Certificats** pour afficher les certificats serveur et client générés par le système pour cette connexion.

Depuis cet onglet, vous pouvez :

- "Faire tourner les certificats de connexion" .
- Sélectionnez **Serveur** ou **Client** pour afficher ou télécharger le certificat associé ou copier le certificat PEM.

Grid A-Grid B

Local hostname (this grid):10.96.106.230

Port:23000

Remote hostname (other grid):10.96.104.230

Connection status:

Connected

Edit

Download file

Test connection

Remove

Permitted tenants

Certificates

Rotate certificates

Server

Client

Download certificate

Copy certificate PEM

Metadata

Subject DN:/C=US/ST=California/L=Sunnyvale/O=NetApp Inc./OU=NetApp StorageGRID/CN=10.96.106.230

Serial number:30:81:B8:DD:AE:B2:86:0A

Issuer DN:/C=US/ST=California/L=Sunnyvale/O=NetApp Inc./OU=NetApp StorageGRID/CN=GPT

Issued on:2022-10-04T02:21:18.000Z

Expires on:2024-10-03T19:05:13.000Z

SHA-1 fingerprint:92:7A:03:AF:6D:1C:94:8C:33:24:08:84:F9:2B:01:23:7D:BE:F2:DF

SHA-256 fingerprint:54:97:3E:77:EB:D3:6A:0F:8F:EE:72:83:D0:39:86:02:32:A5:60:9D:6F:C0:A2:3C:76:DA:3F:4D:FF:64:5D:60

Alternative names:IP Address:10.96.106.230

Certificate PEM

-----BEGIN CERTIFICATE-----

MIIGdTCCBF2gAwIBAgIIHIG43a6yhgowDQYJKoZIhvcNAQENBQAwdzELMAkGA1UE

BhMCMVVM/EzARBgNVBAGlMCKNhbg1mb3JuaWExEjAQBgNVBAClMCVN1bm55dmFsZTEU

ABTGA1UECmVud1R2MTUwDzYyMTAwMDQwMjI1MTg0MDZGA1UEAwwtMTA5LjEwNi4yMzA0

-----END CERTIFICATE-----

Examiner les mesures de réplication inter-grille

Vous pouvez utiliser le tableau de bord de réplication inter-grille dans Grafana pour afficher les métriques Prometheus sur les opérations de réplication inter-grille sur votre grille.

Étapes

1. Depuis le gestionnaire de grille, sélectionnez **SUPPORT > Outils > Métriques**.



Les outils disponibles sur la page Métriques sont destinés à être utilisés par le support technique. Certaines fonctionnalités et éléments de menu de ces outils sont intentionnellement non fonctionnels et sont susceptibles d'être modifiés. Voir la liste des "[métriques Prometheus couramment utilisées](#)".

2. Dans la section Grafana de la page, sélectionnez **Réplication inter-grille**.

Pour des instructions détaillées, voir ["Examiner les mesures de support"](#).

3. Pour réessayer la réplication des objets dont la réplication a échoué, voir ["Identifier et réessayer les opérations de réplication ayant échoué"](#) .

Gérer les alertes

Gérer les alertes

Le système d'alerte fournit une interface facile à utiliser pour détecter, évaluer et résoudre les problèmes pouvant survenir pendant le fonctionnement de StorageGRID .

Les alertes sont déclenchées à des niveaux de gravité spécifiques lorsque les conditions de règle d'alerte sont évaluées comme vraies. 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 > Aperçu**.
- Une notification par e-mail est envoyée, en supposant que vous ayez 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 ayez configuré l'agent SNMP StorageGRID .

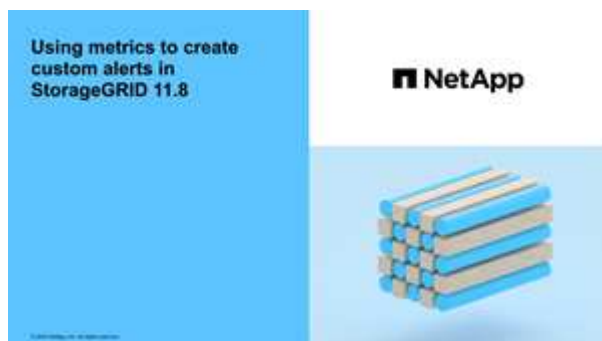
Vous pouvez créer des alertes personnalisées, modifier ou désactiver des alertes et gérer les notifications d'alerte.

Pour en savoir plus :

- Revoir la vidéo : ["Vidéo : Aperçu des alertes"](#)



- Revoir la vidéo : ["Vidéo : Alertes personnalisées"](#)



- Voir le ["Référence des alertes"](#) .

Afficher les règles d’alerte

Les règles d’alerte définissent les conditions qui déclenchent"alertes spécifiques" . StorageGRID inclut un ensemble de règles d’alerte par défaut, que vous pouvez utiliser telles quelles ou 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 déclencheront chaque alerte et pour voir si des alertes sont désactivées.

Avant de commencer

- Vous êtes connecté au Grid Manager à l’aide d’un"navigateur Web pris en charge" .
- Vous avez le"Gérer les alertes ou l’autorisation d’accès root" .
- En option, vous avez regardé la vidéo : "Vidéo : Aperçu des alertes"



Étapes

1. Sélectionnez **ALERTES > Règles.**

La page Règles d’alerte s’affiche.

Alert Rules [Learn more](#)

Alert rules define which conditions trigger specific alerts.

You can edit the conditions for default alert rules to better suit your environment, or create custom alert rules that use your own conditions for triggering alerts.

[+ Create custom rule](#) [Edit rule](#) [Remove custom rule](#)

Name	Conditions	Type	Status
☐ Appliance battery expired The battery in the appliance's storage controller has expired.	storagegrid_appliance_component_failure(type="REC_EXPIRED_BATTERY") Major > 0	Default	Enabled
☐ Appliance battery failed The battery in the appliance's storage controller has failed.	storagegrid_appliance_component_failure(type="REC_FAILED_BATTERY") Major > 0	Default	Enabled
☐ Appliance battery has insufficient learned capacity The battery in the appliance's storage controller has insufficient learned capacity.	storagegrid_appliance_component_failure(type="REC_BATTERY_WARN") Major > 0	Default	Enabled
☐ Appliance battery near expiration The battery in the appliance's storage controller is nearing expiration.	storagegrid_appliance_component_failure(type="REC_BATTERY_NEAR_EXPIRATION") Major > 0	Default	Enabled
☐ Appliance battery removed The battery in the appliance's storage controller is missing.	storagegrid_appliance_component_failure(type="REC_REMOVED_BATTERY") Major > 0	Default	Enabled
☐ Appliance battery too hot The battery in the appliance's storage controller is overheated.	storagegrid_appliance_component_failure(type="REC_BATTERY_OVERTEMP") Major > 0	Default	Enabled
☐ Appliance cache backup device failed A persistent cache backup device has failed.	storagegrid_appliance_component_failure(type="REC_CACHE_BACKUP_DEVICE_FAILED") Major > 0	Default	Enabled
☐ Appliance cache backup device insufficient capacity There is insufficient cache backup device capacity.	storagegrid_appliance_component_failure(type="REC_CACHE_BACKUP_DEVICE_INSUFFICIENT_CAPACITY") Major > 0	Default	Enabled
☐ Appliance cache backup device write-protected A cache backup device is write-protected.	storagegrid_appliance_component_failure(type="REC_CACHE_BACKUP_DEVICE_WRITE_PROTECTED") Major > 0	Default	Enabled
☐ Appliance cache memory size mismatch The two controllers in the appliance have different cache sizes.	storagegrid_appliance_component_failure(type="REC_CACHE_MEM_SIZE_MISMATCH") Major > 0	Default	Enabled

Displaying 62 alert rules.

2. Consultez les informations dans le tableau des règles d'alerte :

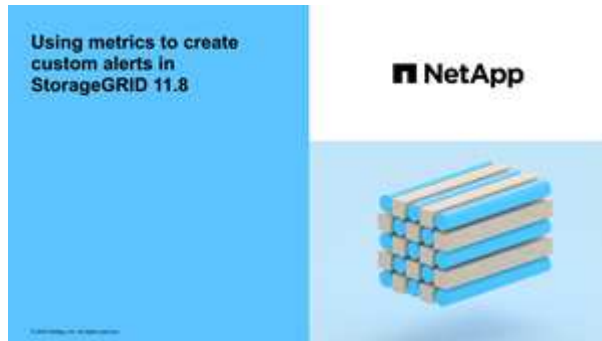
En-tête de colonne	Description
Nom	Le nom unique et la description de la règle d'alerte. Les règles d'alerte personnalisées sont répertoriées en premier, suivies des règles d'alerte par défaut. Le nom de la règle d'alerte est l'objet des notifications par e-mail.
Conditions	Les expressions Prometheus qui déterminent quand cette alerte est déclenchée. Une alerte peut être déclenchée à un ou plusieurs des niveaux de gravité suivants, mais une condition pour chaque gravité n'est pas requise. • *Critique*  : Une condition anormale existe qui a arrêté les opérations normales d'un nœud ou d'un service StorageGRID . Vous devez résoudre le problème sous-jacent immédiatement. Une interruption de service et une perte de données peuvent survenir si le problème n'est pas résolu. • *Majeur*  : Une condition anormale existe qui affecte les opérations en cours ou approche le seuil d'une alerte critique. Vous devez enquêter sur les alertes majeures et résoudre tous les problèmes sous-jacents pour garantir que la condition anormale n'arrête pas le fonctionnement normal d'un nœud ou d'un service StorageGRID . • *Mineure*  : Le système fonctionne normalement, mais une condition anormale existe qui pourrait affecter la capacité du système à fonctionner si elle persiste. Vous devez surveiller et résoudre les alertes mineures qui ne disparaissent pas d'elles-mêmes pour vous assurer qu'elles n'entraînent pas un problème plus grave.
Type	Le type de règle d'alerte : • Par défaut : une 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* : une règle d'alerte par défaut qui inclut une condition ou une durée modifiée. Si nécessaire, vous pouvez facilement rétablir une condition modifiée à la valeur par défaut d'origine. • Personnalisé : une règle d'alerte que vous avez créée. Vous pouvez désactiver, modifier et supprimer des règles d'alerte personnalisées.
Statut	Si cette règle d'alerte est actuellement activée ou désactivée. Les conditions des règles d'alerte désactivées ne sont pas évaluées, donc aucune alerte n'est déclenchée.

Créer des règles d'alerte personnalisées

Vous pouvez créer des règles d'alerte personnalisées pour définir vos propres conditions de déclenchement d'alertes.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un [navigateur Web pris en charge](#) .
- Vous avez le ["Gérer les alertes ou l'autorisation d'accès root"](#) .
- Vous connaissez le ["métriques Prometheus couramment utilisées"](#) .
- Vous comprenez le ["syntaxe des requêtes Prometheus"](#) .
- En option, vous avez regardé la vidéo : ["Vidéo : Alertes personnalisées"](#) .



À propos de cette tâche

StorageGRID ne valide pas les alertes personnalisées. Si vous décidez de créer des règles d'alerte personnalisées, suivez ces directives générales :

- 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. Ensuite, modifiez la valeur seuil pour chaque condition.
- Vérifiez soigneusement chaque condition pour détecter les fautes de frappe et les erreurs de logique.
- Utilisez uniquement les métriques répertoriées dans l'API Grid Management.
- Lorsque vous testez une expression à l'aide de l'API Grid Management, sachez qu'une réponse « réussie » peut être un corps de réponse vide (aucune alerte déclenchée). Pour voir si l'alerte est réellement déclenchée, vous pouvez définir temporairement un seuil sur une valeur que vous pensez être vraie actuellement.

Par exemple, pour tester l'expression `node_memory_MemTotal_bytes < 24000000000` , exécuter d'abord `node_memory_MemTotal_bytes >= 0` et assurez-vous d'obtenir les résultats attendus (tous les nœuds renvoient une valeur). Ensuite, modifiez l'opérateur et le seuil aux valeurs prévues et exécutez à nouveau. Aucun résultat n'indique qu'il n'y a aucune alerte actuelle pour cette expression.

- Ne présumez pas qu'une alerte personnalisée fonctionne à moins d'avoir validé que l'alerte est déclenchée au moment prévu.

Étapes

1. Sélectionnez **ALERTES > Règles**.

La page Règles d'alerte s'affiche.

2. Sélectionnez **Créer une règle personnalisée**.

La boîte de dialogue Créer une règle personnalisée s'affiche.

Create Custom Rule

Enabled ☒

Unique Name

Description

Recommended Actions
(optional)

Conditions

Minor

Major

Critical

Enter the amount of time a condition must continuously remain in effect before an alert is triggered.

Duration

minutes

Cancel

Save

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 est affiché sur la page Alertes et constitue également l'objet des notifications par e-mail. Les noms des règles d'alerte peuvent comporter entre 1 et 64 caractères.

Champ	Description
Description	Une description du problème qui se produit. 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	Facultativement, les actions recommandées à entreprendre lorsque cette alerte est déclenchée. Saisissez les actions recommandées sous forme de texte brut (sans codes de formatage). Les actions recommandées pour les règles d'alerte peuvent être comprises entre 0 et 1 024 caractères.

5. Dans la section Conditions, saisissez 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 avoir n'importe quelle longueur, mais apparaissent sur une seule ligne dans l'interface utilisateur. Au moins une expression est requise.

Cette expression provoque le déclenchement d'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 voir les métriques disponibles et tester les expressions Prometheus, sélectionnez l'icône d'aide  et suivez le lien vers la section Métriques de l'API de gestion de grille.

6. Dans le champ **Durée**, saisissez la durée pendant laquelle une condition doit rester en vigueur en continu avant que l'alerte ne soit déclenchée, puis sélectionnez une unité de temps.

Pour déclencher une alerte immédiatement lorsqu'une condition devient vraie, entrez **0**. Augmentez cette valeur pour empêcher des conditions temporaires de déclencher des alertes.

La valeur par défaut est de 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.

Modifier les règles d'alerte

Vous pouvez modifier une règle d'alerte pour changer les conditions de déclenchement. Pour une règle d'alerte personnalisée, vous pouvez également mettre à jour le nom de la règle, la 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 avez le ["Gérer les alertes ou l'autorisation d'accès root"](#) .

À propos de cette tâche

Lorsque vous modifiez une règle d'alerte par défaut, vous pouvez modifier les conditions des 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, vous risquez de ne pas détecter un problème sous-jacent jusqu'à ce qu'il empêche une opération critique de se terminer.

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.

Edit Rule - Low installed node memory

Enabled ☒

Unique Name Low installed node memory

Description The amount of installed memory on a node is low.

Recommended Actions (optional)

Increase the amount of RAM available to the virtual machine or Linux host. Check the threshold value for the major alert to determine the default minimum requirement for a StorageGRID node.

See the instructions for your platform:

- [VMware installation](#)
- [Red Hat Enterprise Linux or CentOS installation](#)
- [Ubuntu or Debian installation](#)

Conditions

Minor

Major

Critical

node_memory_MemTotal_bytes < 24000000000

node_memory_MemTotal_bytes <= 12000000000

Enter the amount of time a condition must continuously remain in effect before an alert is triggered.

Duration

2

minutes

Cancel

Save

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 pour que l'alerte n'apparaisse plus comme une alerte active.



En général, il n'est pas recommandé de désactiver une règle d'alerte par défaut. Si une règle d'alerte est désactivée, vous risquez de ne pas détecter un problème sous-jacent jusqu'à ce qu'il empêche une opération critique de se terminer.

5. Pour les règles d'alerte personnalisées, mettez à jour les informations suivantes selon vos besoins.



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 est affiché sur la page Alertes et constitue également l'objet des notifications par e-mail. Les noms des règles d'alerte peuvent comporter entre 1 et 64 caractères.
Description	Une description du problème qui se produit. 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	Facultativement, les actions recommandées à entreprendre lorsque cette alerte est déclenchée. Saisissez les actions recommandées sous forme de texte brut (sans codes de formatage). Les actions recommandées pour les règles d'alerte peuvent être comprises entre 0 et 1 024 caractères.

6. Dans la section Conditions, saisissez ou mettez à jour l'expression Prometheus pour un ou plusieurs niveaux de gravité d'alerte.



Si vous souhaitez restaurer une condition d'une règle d'alerte par défaut modifiée à sa valeur d'origine, sélectionnez les trois points à droite de la condition modifiée.

Conditions ?

Minor	
Major	node_memory_MemTotal_bytes < 24000000000
Critical	node_memory_MemTotal_bytes <= 14000000000



Si vous mettez à jour les conditions d'une alerte actuelle, 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 reflétera les valeurs mises à jour.

Une expression de base est généralement de la forme :

```
[metric] [operator] [value]
```

Les expressions peuvent avoir n'importe quelle longueur, mais apparaissent sur une seule ligne dans l'interface utilisateur. Au moins une expression est requise.

Cette expression provoque le déclenchement d'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**, saisissez la durée pendant laquelle une condition doit rester en vigueur en continu avant que l'alerte ne soit déclenchée, puis sélectionnez l'unité de temps.

Pour déclencher une alerte immédiatement lorsqu'une condition devient vraie, entrez **0**. Augmentez cette valeur pour empêcher des conditions temporaires de déclencher des alertes.

La valeur par défaut est de 5 minutes.

8. Sélectionnez **Enregistrer**.

Si vous avez modifié une règle d'alerte par défaut, **Par défaut*** apparaît dans la colonne Type. Si vous avez désactivé une règle d'alerte par défaut ou personnalisée, **Désactivé** apparaît dans la colonne **Statut**.

Désactiver les règles d'alerte

Vous pouvez modifier l'état activé/désactivé d'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 avez le ["Gérer les alertes ou l'autorisation d'accès root"](#).

À propos de cette tâche

Lorsqu'une règle d'alerte est désactivée, ses expressions ne sont pas évaluées et aucune alerte n'est déclenchée.



En général, il n'est pas recommandé de désactiver une règle d'alerte par défaut. Si une règle d'alerte est désactivée, vous risquez de ne pas détecter un problème sous-jacent jusqu'à ce qu'il empêche une opération critique de se terminer.

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 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 pour que l'alerte ne s'affiche plus comme une alerte active.

5. Sélectionnez **Enregistrer**.

Désactivé apparaît dans la colonne **Statut**.

Supprimer 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 avez le ["Gérer les alertes ou l'autorisation d'accès root"](#) .

Étapes

1. Sélectionnez **ALERTES > Règles**.

La page Règles d'alerte s'affiche.

2. Sélectionnez le bouton radio correspondant à 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 apparaît.

4. Sélectionnez **OK** pour supprimer la règle d'alerte.

Toutes les instances actives de l'alerte seront résolues dans les 10 minutes.

Gérer les notifications d'alerte

Configurer 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 points de terminaison 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, consultez ["Utiliser la surveillance SNMP"](#) .

Après avoir configuré l'agent SNMP StorageGRID , deux types de notifications basées sur des 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 informer le système de gestion qu'un événement s'est produit dans StorageGRID, comme le déclenchement d'une alerte. Les interruptions sont prises 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 délai, il renvoie l'information jusqu'à ce qu'un accusé de réception soit reçu ou que la valeur de nouvelle tentative maximale soit atteinte. Les informations sont prises en charge dans SNMPv2c et SNMPv3.

Les 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 silencieuses"](#) .

Si votre déploiement StorageGRID inclut plusieurs nœuds d'administration, le nœud d'administration principal est l'expéditeur préféré pour les notifications d'alerte, les packages AutoSupport et les interruptions et informations SNMP. Si le nœud d'administration principal devient indisponible, des notifications sont temporairement envoyées par d'autres nœuds d'administration. Voir ["Qu'est-ce qu'un nœud d'administration ?"](#) .

Configurer des 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 les adresses e-mail des 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 avez le ["Gérer les alertes ou l'autorisation d'accès root"](#) .

À propos de cette tâche

La configuration de messagerie utilisée pour les notifications d'alerte n'est pas utilisée pour les packages 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 packages AutoSupport et les interruptions et informations SNMP. Si le nœud d'administration principal devient indisponible, des notifications sont temporairement envoyées par d'autres nœuds d'administration. Voir ["Qu'est-ce qu'un nœud d'administration ?"](#) .

Étapes

1. Sélectionnez **ALERTES > Configuration de la messagerie électronique**.

La page de configuration de la messagerie électronique s'affiche.

2. Cochez la case **Activer les notifications par e-mail** pour indiquer que vous souhaitez que des e-mails de notification soient envoyés lorsque les alertes atteignent les seuils configurés.

Les sections Serveur de messagerie (SMTP), Sécurité de la couche de transport (TLS), Adresses de messagerie et Filtres s'affichent.

3. Dans la section Serveur de messagerie (SMTP), saisissez les informations dont StorageGRID a besoin pour accéder à votre serveur SMTP.

Si votre serveur SMTP nécessite une authentification, vous devez fournir un nom d'utilisateur et un mot de passe.

Champ	Entrer
Serveur de messagerie	Le nom de domaine complet (FQDN) ou l'adresse IP du serveur SMTP.

Champ	Entrer
Port	Le 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, saisissez le nom d'utilisateur avec lequel vous souhaitez vous authentifier.
Mot de passe (facultatif)	Si votre serveur SMTP nécessite une authentification, saisissez le mot de passe pour vous authentifier.

4. Dans la section Adresses e-mail, saisissez les adresses e-mail de l'expéditeur et de chaque destinataire.

- a. Pour l'**Adresse e-mail de l'expéditeur**, spécifiez une adresse e-mail valide à utiliser comme adresse d'expéditeur pour les notifications d'alerte.

Par exemple : `storagegrid-alerts@example.com`

- b. Dans la section Destinataires, saisissez une adresse e-mail pour chaque liste de diffusion ou personne qui doit 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'identité du serveur SMTP.

Vous pouvez copier et coller le contenu dans ce champ, ou sélectionner **Parcourir** et sélectionner le fichier.

Vous devez fournir un fichier unique contenant les certificats de chaque autorité de certification émettrice intermédiaire (CA). Le fichier doit contenir chacun des fichiers de certificat CA codés en PEM, concaténés dans l'ordre de la chaîne de certificats.

- b. Cochez la case **Envoyer un certificat client** si votre serveur de messagerie SMTP exige que les expéditeurs de messagerie fournissent des certificats clients pour l'authentification.

- c. Dans le champ **Certificat client**, indiquez 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 **Clé privée**, saisissez la clé privée du certificat client dans un encodage 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 électronique, sélectionnez l'icône en forme de crayon  pour mettre à jour ce champ.

6. Dans la section Filtres, sélectionnez les niveaux de gravité des alertes qui doivent entraîner des

notifications par e-mail, sauf si la règle d'une alerte spécifique a été désactivée.

Gravité	Description
Mineur, majeur, critique	Une notification par courrier électronique est envoyée lorsque la condition mineure, majeure ou critique d'une règle d'alerte est remplie.
Majeur, critique	Une notification par e-mail est envoyée lorsque la condition majeure ou critique d'une règle d'alerte est remplie. Les notifications ne sont pas envoyées pour les alertes mineures.
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 un e-mail de test**.

Un message de confirmation apparaît, indiquant qu'un e-mail de test a été envoyé.

b. Vérifiez les boîtes de réception de tous les destinataires de courrier électronique et confirmez qu'un courrier électronique de test a été reçu.



Si l'e-mail n'est pas reçu dans les quelques minutes ou si l'alerte **Échec de la notification par e-mail** est déclenchée, vérifiez vos paramètres et réessayez.

c. Sign in à n'importe quel 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'alerte, vous devez vous connecter à chaque nœud d'administration pour vérifier la connectivité. Ceci est en contraste avec les tests des packages AutoSupport , où tous les nœuds d'administration envoient l'e-mail de 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

Une fois le serveur de messagerie SMTP configuré, des notifications par courrier électronique sont envoyées aux destinataires désignés lorsqu'une alerte est déclenchée, sauf si la règle d'alerte est supprimée par un silence. Voir "[Notifications d'alerte silencieuses](#)".

Les notifications par e-mail incluent les informations suivantes :

Low object data storage (6 alerts) 1

The space available for storing object data is low. 2

Recommended actions 3

Perform an expansion procedure. You can add storage volumes (LUNs) to existing Storage Nodes, or you can add new Storage Nodes. See the instructions for expanding a StorageGRID system.

DC1-S1-226

Node DC1-S1-226 4
 Site DC1 225-230
 Severity Minor
 Time triggered Fri Jun 28 14:43:27 UTC 2019
 Job storagegrid
 Service ldr

DC1-S2-227

Node DC1-S2-227
 Site DC1 225-230
 Severity Minor
 Time triggered Fri Jun 28 14:43:27 UTC 2019
 Job storagegrid
 Service ldr

Sent from: DC1-ADM1-225 5

Appeler	Description
1	Le nom de l'alerte, suivi du nombre d'instances actives de cette alerte.
2	La 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 à laquelle la règle d'alerte a été déclenchée et le nom du travail et du service affectés.
5	Le nom d'hôte du nœud d'administration qui a envoyé la notification.

Comment les alertes sont regroupées

Pour éviter 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 courrier électronique.

Comportement	Exemple
Chaque notification d'alerte s'applique uniquement aux alertes portant le même nom. Si deux alertes portant des noms différents sont déclenchées en même temps, deux notifications par e-mail sont envoyées.	• L'alerte A est déclenchée sur deux nœuds en même temps. Une seule notification est envoyée. • L'alerte A est déclenchée sur le nœud 1 et l'alerte B est déclenchée sur le nœud 2 en même temps. Deux notifications sont envoyées : une pour chaque alerte.
Pour une alerte spécifique sur un nœud spécifique, si les seuils sont atteints pour plusieurs niveaux de gravité, une notification est envoyée uniquement pour l'alerte la plus grave.	• L'alerte A est déclenchée et les seuils d'alerte mineure, majeure et critique sont atteints. 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 portant le même nom sont déclenchées pendant cette période, StorageGRID regroupe toutes les alertes dans la notification initiale.	1. L'alerte A est déclenchée sur le nœud 1 à 08h00. Aucune notification n'est envoyée. 2. L'alerte A est déclenchée sur le nœud 2 à 08h01. Aucune notification n'est envoyée. 3. À 08h02, une notification est envoyée pour signaler les deux instances de l'alerte.
Si une autre alerte portant le même nom est déclenchée, StorageGRID attend 10 minutes avant d'envoyer une nouvelle notification. La nouvelle notification signale toutes les alertes actives (alertes actuelles qui n'ont pas été désactivées), même si elles ont été signalées précédemment.	1. L'alerte A est déclenchée sur le nœud 1 à 08h00. Une notification est envoyée à 08h02. 2. L'alerte A est déclenchée sur le nœud 2 à 08h05. Une deuxième notification est envoyée à 08h15 (10 minutes plus tard). Les deux nœuds sont signalés.
S'il existe plusieurs alertes actuelles portant 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 deuxième 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 d'envoyer des notifications par e-mail une fois 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 réduite au silence. Des notifications supplémentaires sont envoyées le 15 mars, le 22 mars, le 29 mars, etc.

Dépannage des notifications d'alerte par e-mail

Si l'alerte **Échec de la notification par e-mail** est déclenchée ou si vous ne parvenez pas à recevoir la notification par e-mail d'alerte de test, suivez ces étapes pour résoudre le problème.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un ["navigateur Web pris en charge"](#) .
- Vous avez le ["Gérer les alertes ou l'autorisation d'accès root"](#) .

Étapes

1. Vérifiez vos paramètres.
 - a. Sélectionnez **ALERTES > Configuration de la messagerie électronique**.
 - 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 anti-spam et assurez-vous que l'e-mail n'a pas été envoyé dans un dossier indésirable.
3. Demandez à votre administrateur de messagerie de confirmer que les e-mails provenant 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 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 que vous avez spécifié.

Voir ["Collecter les fichiers journaux et les données système"](#) .

Notifications d'alerte silencieuses

En option, 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 avez le ["Gérer les alertes ou l'autorisation d'accès root"](#) .

À propos de cette tâche

Vous pouvez désactiver les règles d'alerte sur l'ensemble de la grille, sur un seul site ou sur un seul nœud et pour un ou plusieurs niveaux de gravité. Chaque silence supprime toutes les notifications pour une seule règle d'alerte ou pour toutes les règles d'alerte.

Si vous avez activé l'agent SNMP, les silences suppriment également les interruptions et les informations SNMP.



Soyez prudent lorsque vous décidez de désactiver une règle d'alerte. Si vous désactivez une alerte, vous risquez de ne pas détecter un problème sous-jacent jusqu'à ce qu'il empêche une opération critique de se terminer.

Étapes

1. Sélectionnez **ALERTES > Silences**.

La page Silences apparaît.

Silences

You can configure silences to temporarily suppress alert notifications. Each silence suppresses the notifications for an alert rule at one or more severities. You can suppress an alert rule on the entire grid, a single site, or a single node.

Create

Edit

Remove

Alert Rule	Description	Severity	Time Remaining	Nodes
No results found.				

2. Sélectionnez **Créer**.

La boîte de dialogue Créer un silence s’affiche.

Create Silence

Alert Rule

Description (optional)

Duration

Minutes

Severity

Minor only

Minor, major

Minor, major, critical

Nodes

StorageGRID Deployment

Data Center 1

DC1-ADM1

DC1-G1

DC1-S1

DC1-S2

DC1-S3

Cancel

Save

3. Sélectionnez ou saisissez 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 souhaitez désactiver toutes les règles d'alerte à l'aide des critères spécifiés dans cette boîte de dialogue.

Champ	Description
Description	En option, une description du silence. Par exemple, décrivez le but de ce silence.
Durée	Combien de temps souhaitez-vous que ce silence reste en vigueur, en minutes, en heures ou en 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 pendant une période prolongée. Si une règle d'alerte est désactivée, vous risquez de ne pas détecter un problème sous-jacent jusqu'à ce qu'il empêche une opération critique de se terminer. Cependant, vous devrez peut-être utiliser un silence prolongé si une alerte est déclenchée par une configuration spécifique et intentionnelle, comme cela peut être le cas pour les alertes Lien de l'appliance de services interrompu et les alertes Lien de l'appliance de stockage interrompu.
Gravité	Quelle(s) gravité(s) d'alerte doit(vent) être désactivée(s) ? Si l'alerte est déclenchée à l'un des niveaux de gravité sélectionnés, aucune notification n'est envoyée.
Nœuds	À quel(s) nœud(s) souhaitez-vous que ce silence s'applique. Vous pouvez supprimer une règle d'alerte ou toutes les règles sur l'ensemble de la grille, un seul site ou un seul nœud. Si vous sélectionnez la grille entière, 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. Remarque : 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, la durée restante, les niveaux de gravité sélectionnés ou le nœud affecté. e. Sélectionnez Enregistrer.

Option	Description
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 seront désormais envoyées lorsque cette alerte est déclenchée (sauf si elle est supprimée par un autre silence). Si cette alerte est actuellement déclenchée, l'envoi des notifications par e-mail ou SNMP et la mise à jour de la page Alertes peuvent prendre quelques minutes.

Informations connexes

["Configurer 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.

Selon vos besoins, vous pouvez créer des règles d'alerte personnalisées adaptées à votre approche de gestion du système.

Certaines des alertes par défaut utilisent ["Métriques Prometheus"](#).

Alertes sur les appareils électroménagers

Nom de l'alerte	Description
La batterie de l'appareil est expirée	La batterie du contrôleur de stockage de l'appareil est épuisée.
La batterie de l'appareil est défectueuse	La batterie du contrôleur de stockage de l'appareil est défectueuse.
La batterie de l'appareil a une capacité d'apprentissage insuffisante	La batterie du contrôleur de stockage de l'appareil a une capacité d'apprentissage insuffisante.
Batterie d'appareil presque expirée	La batterie du contrôleur de stockage de l'appareil est sur le point d'expirer.
Batterie de l'appareil retirée	La batterie du contrôleur de stockage de l'appareil est manquante.
La batterie de l'appareil est trop chaude	La batterie du contrôleur de stockage de l'appareil est surchauffée.

Nom de l'alerte	Description
Erreur de communication du BMC de l'appareil	La communication avec le contrôleur de gestion de la carte mère (BMC) a été perdue.
Défaut du périphérique de démarrage de l'appareil détecté	Un problème a été détecté avec le périphérique de démarrage de l'appareil.
Échec du périphérique de sauvegarde du cache de l'appareil	Un périphérique de sauvegarde de cache persistant est tombé en panne.
Capacité insuffisante du périphérique de sauvegarde du cache de l'appareil	La capacité du périphérique de sauvegarde du cache est insuffisante.
Dispositif de sauvegarde du cache de l'appareil protégé en écriture	Un périphérique de sauvegarde de cache est protégé en écriture.
Incompatibilité de taille de mémoire cache de l'appareil	Les deux contrôleurs de l'appareil ont des tailles de cache différentes.
Défaut de batterie CMOS de l'appareil	Un problème a été détecté avec la batterie CMOS de l'appareil.
La température du châssis du contrôleur de calcul de l'appareil est trop élevée	La température du contrôleur de calcul d'un dispositif StorageGRID a dépassé un seuil nominal.
La température du processeur du contrôleur de calcul de l'appareil est trop élevée	La température du processeur dans le contrôleur de calcul d'un dispositif StorageGRID a dépassé un seuil nominal.
Le contrôleur de calcul de l'appareil nécessite une attention particulière	Une panne matérielle a été détectée dans le contrôleur de calcul d'un dispositif StorageGRID .
L'alimentation du contrôleur de calcul de l'appareil A présente un problème	L'alimentation A du contrôleur de calcul présente un problème.
L'alimentation B du contrôleur de calcul de l'appareil présente un problème	L'alimentation B du contrôleur de calcul présente un problème.
Le service de surveillance du matériel informatique de l'appareil est bloqué	Le service qui surveille l'état du matériel de stockage est bloqué.

Nom de l'alerte	Description
Le lecteur DAS de l'appareil dépasse la limite de données écrites par jour	Une quantité excessive de données est écrite sur un lecteur chaque jour, ce qui peut annuler sa garantie.
Défaut détecté sur le lecteur DAS de l'appareil	Un problème a été détecté avec un lecteur de stockage à connexion directe (DAS) dans l'appareil.
Voyant de localisation du lecteur DAS de l'appareil allumé	Le voyant de localisation de lecteur pour un ou plusieurs lecteurs de stockage à connexion directe (DAS) dans un nœud de stockage d'appliance est allumé.
Reconstruction du lecteur DAS de l'appareil	Un lecteur de stockage à connexion directe (DAS) est en cours de reconstruction. Ceci est attendu s'il a été récemment remplacé ou retiré/réinséré.
Défaut du ventilateur de l'appareil détecté	Un problème avec un bloc ventilateur de l'appareil a été détecté.
Défaut de l'appareil Fibre Channel détecté	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'appareil	Un port HBA Fibre Channel est défaillant ou a échoué.
Les lecteurs de cache flash de l'appareil ne sont pas optimaux	Les disques utilisés pour le cache SSD ne sont pas optimaux.
Boîtier d'interconnexion/de batterie de l'appareil retiré	Le boîtier d'interconnexion/batterie est manquant.
Port LACP de l'appareil manquant	Un port sur un dispositif StorageGRID ne participe pas à la liaison LACP.
Défaut de carte réseau de l'appareil détecté	Un problème avec une carte d'interface réseau (NIC) dans l'appareil a été détecté.
Alimentation électrique globale de l'appareil dégradée	La puissance d'un appareil StorageGRID s'écarte de la tension de fonctionnement recommandée.
Avertissement critique du SSD de l'appareil	Un SSD d'appareil signale un avertissement critique.
Défaillance du contrôleur de stockage de l'appareil A	Le contrôleur de stockage A d'un dispositif StorageGRID est tombé en panne.
Défaillance du contrôleur de stockage de l'appareil B	Le contrôleur de stockage B d'un dispositif StorageGRID est en panne.

Nom de l'alerte	Description
Panne du lecteur du contrôleur de stockage de l'appareil	Un ou plusieurs disques d'un dispositif StorageGRID sont en panne ou ne sont pas optimaux.
Problème matériel du contrôleur de stockage de l'appareil	Le logiciel SANtricity signale « Nécessite une attention particulière » pour un composant d'un dispositif StorageGRID .
Panne d'alimentation du contrôleur de stockage de l'appareil	L'alimentation A d'un dispositif StorageGRID s'écarte de la tension de fonctionnement recommandée.
Panne d'alimentation du contrôleur de stockage de l'appareil B	L'alimentation B d'un dispositif StorageGRID s'écarte de la tension de fonctionnement recommandée.
Le service de surveillance du matériel de stockage des appareils est bloqué	Le service qui surveille l'état du matériel de stockage est bloqué.
Étagères de rangement des appareils dégradées	L'état de l'un des composants de l'étagère de stockage d'un dispositif 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 retiré.
Erreur de démarrage sécurisé UEFI de l'appareil	Un appareil n'a pas été démarré en toute sécurité.
Les E/S du disque sont très lentes	Des E/S de disque très lentes peuvent avoir un impact sur les performances de la grille.
Défaut de ventilateur de l'appareil de stockage détecté	Un problème avec une unité de ventilation dans le contrôleur de stockage d'un appareil a été détecté.
Connectivité de stockage dégradée	Il y a un problème avec 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 de syslog

Nom de l'alerte	Description
Les 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 se remplit.

Nom de l'alerte	Description
Erreur de transfert du serveur syslog externe	Le nœud ne peut pas transférer les journaux vers le serveur syslog externe.
Grande file d'attente d'audit	La file d'attente du disque pour les messages d'audit est pleine. Si cette condition n'est pas résolue, les opérations S3 ou Swift peuvent échouer.
Les 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 se remplit.

Alertes de seau

Nom de l'alerte	Description
Le bucket FabricPool a un paramètre de cohérence de bucket non pris en charge	Un bucket FabricPool utilise le niveau de cohérence Disponible ou Site fort, qui n'est pas pris en charge.
Le bucket FabricPool a un paramètre de contrôle de version non pris en charge	Un bucket FabricPool a le contrôle de version ou le verrouillage d'objet S3 activé, qui ne sont pas pris en charge.

Alertes Cassandra

Nom de l'alerte	Description
Erreur du compacteur automatique Cassandra	Le compacteur automatique Cassandra a rencontré une erreur.
Les mesures du compacteur automatique Cassandra sont obsolètes	Les métriques qui décrivent l'auto-compacteur Cassandra sont obsolètes.
Erreur de communication Cassandra	Les nœuds qui exécutent le service Cassandra ont des difficultés à communiquer entre eux.
Les compactions de Cassandra sont surchargées	Le processus de compactage de Cassandra est surchargé.
Erreur d'écriture surdimensionnée de Cassandra	Un processus StorageGRID interne a envoyé une demande d'écriture à Cassandra qui était trop volumineuse.
Les mesures de réparation de Cassandra sont obsolètes	Les métriques qui décrivent les travaux de réparation de Cassandra sont obsolètes.
La réparation de Cassandra progresse lentement	La progression des réparations de la base de données Cassandra est lente.

Nom de l'alerte	Description
Service de réparation Cassandra non disponible	Le service de réparation Cassandra n'est pas disponible.
Corruption de la table Cassandra	Cassandra a détecté une corruption de table. Cassandra redémarre automatiquement s'il détecte une corruption de table.

Alertes du pool de stockage cloud

Nom de l'alerte	Description
Erreur de connectivité du pool de stockage cloud	Le contrôle d'intégrité des pools de stockage cloud a détecté une ou plusieurs nouvelles erreurs.
Expiration de la certification d'entité finale IAM Roles Anywhere	Le certificat d'entité finale IAM Roles Anywhere est sur le point d'expirer.

Alertes de réplication inter-réseaux

Nom de l'alerte	Description
Échec permanent de la réplication inter-réseau	Une erreur de réplication inter-grille s'est produite et nécessite l'intervention de l'utilisateur pour être résolue.
Ressources de réplication inter-réseaux indisponibles	Les demandes de réplication inter-grille sont en attente car une ressource n'est pas disponible.

Alertes DHCP

Nom de l'alerte	Description
Le bail DHCP a expiré	Le bail DHCP sur une interface réseau a expiré.
Le bail 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 traçage

Nom de l'alerte	Description
Impact sur les performances de débogage	Lorsque le mode de 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 négativement.

Alertes par e-mail et AutoSupport

Nom de l'alerte	Description
Échec de l'envoi du message AutoSupport	Le message AutoSupport le plus récent n'a pas pu être envoyé.
Échec de la résolution du nom de domaine	Le nœud StorageGRID n'a pas pu résoudre les noms de domaine.
Échec de la notification par e-mail	La notification par e-mail d'une alerte n'a pas pu être envoyée.
SNMP informe les erreurs	Erreurs lors de l'envoi de notifications d'information SNMP à une destination d'interruption.
Connexion SSH ou console détectée	Au cours des dernières 24 heures, un utilisateur s'est connecté avec la console Web ou SSH.

Alertes de codage d'effacement (EC)

Nom de l'alerte	Description
Échec du rééquilibrage de l'EC	La procédure de rééquilibrage de la CE a échoué ou a été arrêtée.
Échec de la réparation de l'EC	Une tâche de réparation des données EC a échoué ou a été arrêtée.
Réparation de l'EC bloquée	Une tâche de réparation des données EC est bloquée.
Erreur de vérification des fragments codés par effacement	Les fragments codés par effacement ne peuvent plus être vérifiés. Les fragments corrompus peuvent ne pas être réparés.

Alertes d'expiration des certificats

Nom de l'alerte	Description
Expiration du certificat CA du proxy administrateur	Un ou plusieurs certificats du groupe CA du serveur proxy d'administration sont sur le point d'expirer.
Expiration du certificat client	Un ou plusieurs certificats clients 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 du point de terminaison de l'équilibreur de charge	Un ou plusieurs certificats de point de terminaison d'équilibrage de charge sont sur le point d'expirer.

Nom de l'alerte	Description
Expiration du certificat du serveur pour l'interface de gestion	Le certificat du serveur utilisé pour l'interface de gestion est sur le point d'expirer.
Expiration du certificat CA syslog externe	Le certificat de l'autorité de certification (CA) utilisé pour signer le certificat du serveur syslog externe est sur le point d'expirer.
Expiration du certificat 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 du serveur présenté par le serveur syslog externe est sur le point d'expirer.

Alertes du réseau Grid

Nom de l'alerte	Description
Inadéquation du MTU du réseau de grille	Le paramètre MTU pour l'interface du réseau de grille (eth0) diffère considérablement selon les nœuds de la grille.

Alertes de la fédération du réseau

Nom de l'alerte	Description
Expiration du certificat de fédération de réseau	Un ou plusieurs certificats de fédération de grille sont sur le point d'expirer.
Échec de la connexion à la fédération de réseau	La connexion de fédération de réseau entre le réseau local et le réseau distant ne fonctionne pas.

Alertes d'utilisation élevée ou de latence élevée

Nom de l'alerte	Description
Utilisation élevée du tas Java	Un pourcentage élevé de l'espace du tas Java est utilisé.
Latence élevée pour les requêtes de métadonnées	Le temps moyen des requêtes de métadonnées Cassandra est trop long.

Alertes de fédération d'identité

Nom de l'alerte	Description
Échec de la synchronisation de la fédération d'identité	Impossible de synchroniser les groupes fédérés et les utilisateurs à partir de la source d'identité.

Nom de l'alerte	Description
Échec de la synchronisation de la fédération d'identité pour un locataire	Impossible de synchroniser les groupes fédérés et les utilisateurs à partir de la source d'identité configurée par un locataire.

Alertes de gestion du cycle de vie de l'information (ILM)

Nom de l'alerte	Description
Placement ILM irréalisable	Une instruction de placement dans une règle ILM ne peut pas être réalisée pour certains objets.
Taux de balayage ILM faible	Le taux de numérisation ILM est défini sur moins de 100 objets/seconde.

Alertes du serveur de gestion des clés (KMS)

Nom de l'alerte	Description
Expiration du certificat KMS CA	Le certificat de l'autorité de certification (CA) utilisé pour signer le certificat du serveur de gestion de clés (KMS) est sur le point d'expirer.
Expiration du certificat client KMS	Le certificat client d'un serveur de gestion de clés est sur le point d'expirer
Échec du chargement de la configuration KMS	La configuration du serveur de gestion des clés existe mais n'a pas pu être chargée.
Erreur de connectivité KMS	Un nœud d'appareil n'a pas pu se connecter au serveur de gestion des clés de son site.
Nom de la clé de chiffrement KMS introuvable	Le serveur de gestion de clés configuré ne dispose pas de clé de chiffrement correspondant au nom fourni.
Échec de la rotation de la clé de chiffrement KMS	Tous les volumes de l'appareil ont été déchiffrés avec succès, mais un ou plusieurs volumes n'ont pas pu pivoter vers la dernière clé.
KMS n'est pas configuré	Aucun serveur de gestion de clés n'existe pour ce site.
La clé KMS n'a pas réussi à déchiffrer un volume d'appareil	Un ou plusieurs volumes sur un appareil avec chiffrement de nœud activé n'ont pas pu être déchiffrés 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.
Échec de connectivité du serveur KMS	Un nœud d'appareil n'a pas pu se connecter à un ou plusieurs serveurs du cluster de serveurs de gestion de clés pour son site.

Alertes de l'équilibreur de charge

Nom de l'alerte	Description
Connexions d'équilibrage de charge sans demande élevée	Un pourcentage élevé de connexions aux points de terminaison de l'équilibreur de charge se sont déconnectées sans exécuter de requêtes.

Alertes de décalage d'horloge locale

Nom de l'alerte	Description
Grand décalage horaire de l'horloge locale	Le décalage entre l'horloge locale et l'heure du protocole NTP (Network Time Protocol) est trop important.

Alertes de faible mémoire ou d'espace insuffisant

Nom de l'alerte	Description
Faible capacité du disque du journal d'audit	L'espace disponible pour les journaux d'audit est faible. Si cette condition n'est pas résolue, les opérations S3 ou Swift peuvent échouer.
Faible mémoire de nœud disponible	La quantité de RAM disponible sur un nœud est faible.
Faible espace libre pour le pool de stockage	L'espace disponible pour stocker les données d'objet dans le nœud de stockage est faible.
Faible mémoire de nœud installée	La quantité de mémoire installée sur un nœud est faible.
Stockage de métadonnées faibles	L'espace disponible pour stocker les métadonnées des objets est faible.
Faible capacité de disque métrique	L'espace disponible pour la base de données des métriques est faible.
Faible stockage de données d'objets	L'espace disponible pour stocker les données des objets est faible.
Remplacement du filigrane en lecture seule	Le remplacement du filigrane en lecture seule du volume de stockage est inférieur au filigrane optimisé minimum pour un nœud de stockage.
Faible capacité du disque racine	L'espace disponible sur le disque racine est faible.
Faible capacité de données du système	L'espace disponible pour /var/local est faible. Si cette condition n'est pas résolue, les opérations S3 ou Swift peuvent échouer.
Espace libre dans le répertoire tmp faible	L'espace disponible dans le répertoire /tmp est faible.

Alertes de nœud ou de réseau de nœuds

Nom de l'alerte	Description
Utilisation de réception du réseau d'administration	L'utilisation de réception sur le réseau d'administration est élevée.
Utilisation de la transmission du réseau administrateur	L'utilisation de la transmission sur le réseau d'administration est élevée.
Échec de la configuration du pare-feu	Échec de l'application de la configuration du pare-feu.
Points de terminaison de l'interface de gestion en mode de secours	Tous les points de terminaison de l'interface de gestion reviennent depuis trop longtemps aux ports par défaut.
Erreur de connectivité du réseau de nœuds	Des erreurs se sont produites lors du transfert de données entre les nœuds.
Erreur de trame de réception du réseau de nœuds	Un pourcentage élevé de trames réseau reçues par un nœud comportaient des erreurs.
Le nœud n'est pas synchronisé avec le serveur NTP	Le nœud n'est pas synchronisé avec le serveur de protocole de temps réseau (NTP).
Nœud non verrouillé avec le serveur NTP	Le nœud n'est pas verrouillé sur un serveur de protocole de temps réseau (NTP).
Réseau de nœuds non-appareils en panne	Un ou plusieurs périphériques réseau sont en panne ou déconnectés.
Liaison de l'appareil de services en panne sur le réseau d'administration	L'interface de l'appareil avec le réseau d'administration (eth1) est en panne ou déconnectée.
Liaison de l'appareil de services interrompue sur le port 1 du réseau d'administration	Le port réseau administrateur 1 de l'appareil est en panne ou déconnecté.
Liaison de l'appareil de services en panne sur le réseau client	L'interface de l'appareil avec le réseau client (eth2) est en panne ou déconnectée.
Liaison de l'appareil de services interrompue sur le port réseau 1	Le port réseau 1 de l'appareil est hors service ou déconnecté.
Liaison de l'appareil de services interrompue sur le port réseau 2	Le port réseau 2 de l'appareil est hors service ou déconnecté.

Nom de l'alerte	Description
Liaison de l'appareil de services interrompue sur le port réseau 3	Le port réseau 3 de l'appareil est hors service ou déconnecté.
Liaison de l'appareil de services interrompue sur le port réseau 4	Le port réseau 4 de l'appareil est hors service ou déconnecté.
Liaison du dispositif de stockage interrompue sur le réseau d'administration	L'interface de l'appareil avec le réseau d'administration (eth1) est en panne ou déconnectée.
Liaison du dispositif de stockage interrompue sur le port 1 du réseau administrateur	Le port réseau administrateur 1 de l'appareil est en panne ou déconnecté.
Liaison du dispositif de stockage interrompue sur le réseau client	L'interface de l'appareil avec le réseau client (eth2) est en panne ou déconnectée.
Liaison du dispositif de stockage interrompue sur le port réseau 1	Le port réseau 1 de l'appareil est hors service ou déconnecté.
Liaison du dispositif de stockage interrompue sur le port réseau 2	Le port réseau 2 de l'appareil est hors service ou déconnecté.
Liaison du dispositif de stockage interrompue sur le port réseau 3	Le port réseau 3 de l'appareil est hors service ou déconnecté.
Liaison du dispositif de stockage interrompue sur le port réseau 4	Le port réseau 4 de l'appareil est hors service ou déconnecté.
Le nœud de stockage n'est pas dans l'état de stockage souhaité	Le service LDR sur 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
Utilisation de la connexion TCP	Le nombre de connexions TCP sur ce nœud approche le nombre maximum pouvant être suivi.
Impossible de communiquer avec le nœud	Un ou plusieurs services ne répondent pas ou le nœud ne peut pas être atteint.
Redémarrage inattendu du nœud	Un nœud a redémarré de manière inattendue au cours des dernières 24 heures.

Alertes d'objets

Nom de l'alerte	Description
La vérification de l'existence de l'objet a échoué	La tâche de vérification de l'existence de l'objet a échoué.
Vérification de l'existence de l'objet 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 PUT 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 d'objets répliqués qui n'a pas pu être identifié comme un objet répliqué.

Alertes des services de la plateforme

Nom de l'alerte	Description
Faible capacité des demandes en attente des services de la plateforme	Le nombre de demandes de services de plateforme en attente approche de sa capacité.
Services de plateforme indisponibles	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 une attention particulière	Un volume de stockage est hors ligne et nécessite une attention particulière.
Le volume de stockage doit être restauré	Un volume de stockage a été récupéré et doit être restauré.
Volume de stockage hors ligne	Un volume de stockage est hors ligne depuis plus de 5 minutes.
Tentative de remontage du volume de stockage	Un volume de stockage était hors ligne et a déclenché un remontage automatique. Cela pourrait indiquer un problème de lecteur ou des erreurs de système de fichiers.
La restauration du volume n'a pas réussi à 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 désormais utilisée.
service nginx-gw utilisant la configuration de sauvegarde	La configuration du service nginx-gw n'est pas valide. La configuration précédente est désormais utilisée.
Redémarrage requis pour désactiver FIPS	La politique de sécurité ne nécessite pas le mode FIPS, mais le module de sécurité cryptographique NetApp est activé.
Redémarrage requis pour activer FIPS	La politique de sécurité nécessite le mode FIPS, mais le module de sécurité cryptographique NetApp est désactivé.
Service SSH utilisant la configuration de sauvegarde	La configuration du service SSH n'est pas valide. La configuration précédente est désormais utilisée.

Alertes locataires

Nom de l'alerte	Description
Utilisation élevée des quotas des locataires	Un pourcentage élevé d'espace de quota est utilisé. Cette règle est désactivée par défaut car elle pourrait entraîner trop de notifications.

Métriques Prometheus couramment utilisées

Consultez cette liste de mesures Prometheus couramment utilisées pour mieux comprendre les conditions des règles d'alerte par défaut ou pour créer les conditions des règles d'alerte personnalisées.

Vous pouvez également [obtenir une liste complète de toutes les métriques](#) .

Pour plus de détails sur la syntaxe des requêtes Prometheus, voir "[Interroger Prométhée](#)" .

Quelles sont les métriques Prometheus ?

Les métriques Prometheus sont des mesures de séries chronologiques. Le service Prometheus sur les nœuds d'administration collecte ces métriques à partir des services sur tous les nœuds. Les métriques sont stockées sur chaque nœud d'administration jusqu'à ce que l'espace réservé aux données Prometheus soit plein. Quand le `/var/local/mysql_ibdata/` le volume atteint sa capacité, les métriques les plus anciennes sont supprimées en premier.

Où sont utilisées les métriques Prometheus ?

Les métriques collectées par Prometheus sont utilisées à plusieurs endroits dans le Grid Manager :

- **Page Nœuds** : Les graphiques et diagrammes des onglets disponibles sur la page Nœuds utilisent l'outil de visualisation Grafana pour afficher les métriques de séries chronologiques collectées par Prometheus. Grafana affiche les données de séries chronologiques sous forme de graphiques et de tableaux, tandis

que Prometheus sert de source de données principale.



- **Alertes** : les alertes sont déclenchées à des niveaux de gravité spécifiques lorsque les conditions de règle d'alerte qui utilisent les métriques Prometheus sont évaluées comme vraies.
- **API de gestion de grille** : vous pouvez utiliser les métriques Prometheus dans des règles d'alerte personnalisées ou avec des outils d'automatisation externes pour surveiller votre système StorageGRID . Une liste complète des métriques Prometheus est disponible à partir de l'API Grid Management. (En haut du gestionnaire de grille, sélectionnez l'icône d'aide et sélectionnez **Documentation API > métriques**.) Bien que plus d'un millier de mesures soient disponibles, seul un nombre relativement restreint est nécessaire pour surveiller les opérations StorageGRID les plus critiques.



Les métriques qui incluent *private* dans leurs noms sont destinées à un usage interne uniquement et sont susceptibles d'être modifiées entre les versions de StorageGRID sans préavis.

- La page **SUPPORT > Outils > Diagnostics** et la page **SUPPORT > Outils > Métriques** : Ces pages, qui sont principalement destinées à être utilisées par le support technique, fournissent plusieurs outils et graphiques qui utilisent les valeurs des métriques Prometheus.



Certaines fonctionnalités et éléments de menu de la page Métriques sont intentionnellement non fonctionnels et sont susceptibles d'être modifiés.

Liste des mesures les plus courantes

La liste suivante contient les métriques Prometheus les plus couramment utilisées.



Les métriques qui incluent *private* dans leurs noms sont destinées à un usage interne uniquement et sont susceptibles d'être modifiées sans préavis entre les versions de StorageGRID .

alertmanager_notifications_échec_total

Le nombre total de notifications d'alerte ayant échoué.

node_filesystem_avail_bytes

La quantité d'espace du système de fichiers disponible pour les utilisateurs non root en octets.

node_memory_MemAvailable_bytes

Champ d'informations sur la mémoire MemAvailable_bytes.

nœud_réseau_opérateur

Valeur porteuse de `/sys/class/net/iface`.

noeud_réseau_réception_erreurs_total

Statistiques du périphérique réseau `receive_errs`.

erreurs_de_transmission_réseau_nœud_total

Statistiques du périphérique réseau `transmit_errs`.

storagegrid_administrativement_en_arrêt

Le nœud n'est pas connecté au réseau pour une raison attendue. Par exemple, le nœud ou les services sur le nœud ont été arrêtés correctement, le nœud redémarre ou le logiciel est en cours de mise à niveau.

état_matériel_du_contrôleur_de_calcul_de_l'appareil_de_grille_de_stockage

L'état du matériel du contrôleur de calcul dans un appareil.

disques_défaillants_de_l'appareil_de_grille_de_stockage

Pour le contrôleur de stockage d'un appareil, le nombre de lecteurs qui ne sont pas optimaux.

état_matériel_du_contrôleur_de_stockage_de_l'appareil_de_grille_de_stockage

L'état général du matériel du contrôleur de stockage dans un appareil.

buckets_et_conteneurs_de_contenu_de_grille_de_stockage

Le nombre total de buckets S3 et de conteneurs Swift connus par ce nœud de stockage.

objets_de_contenu_de_grille_de_stockage

Le nombre total d'objets de données S3 et Swift connus par ce nœud de stockage. Le comptage est valide uniquement pour les objets de données créés par des applications clientes qui s'interfacent avec le système via S3.

storagegrid_content_objects_lost

Le nombre total d'objets que ce service détecte comme manquants dans le système StorageGRID. Des mesures doivent être prises pour déterminer la cause de la perte et si une récupération est possible.

["Résoudre les problèmes de données d'objets perdues ou manquantes"](#)

storagegrid_http_sessions_entrantes_tentatives

Le nombre total de sessions HTTP qui ont été tentées sur un nœud de stockage.

storagegrid_http_sessions_entrantes_actuellement_établies

Le nombre de sessions HTTP actuellement actives (ouvertes) sur le nœud de stockage.

storagegrid_http_sessions_incoming_failed

Le nombre total de sessions HTTP qui n'ont pas abouti, soit en raison d'une requête HTTP mal formée, soit en raison d'un échec lors du traitement d'une opération.

storagegrid_http_sessions_entrantes_réussies

Le nombre total de sessions HTTP qui se sont terminées avec succès.

storagegrid_ilm_attend_des_objets_d'arrière-plan

Le nombre total d'objets sur ce nœud en attente d'évaluation ILM à partir de l'analyse.

storagegrid_ilm_en_attente_d'évaluation_client_objets_par_seconde

Le taux actuel auquel les objets sont évalués par rapport à la politique ILM sur ce nœud.

storagegrid_ilm_en_attente_d'objets_client

Nombre total d'objets sur ce nœud en attente d'évaluation ILM à partir des opérations client (par exemple, l'ingestion).

storagegrid_ilm_en_attente_du_nombre_total_d'objets

Le nombre total d'objets en attente d'évaluation ILM.

storagegrid_ilm_scan_objets_par_seconde

La vitesse à laquelle les objets appartenant à ce nœud sont analysés et mis en file d'attente pour ILM.

storagegrid_ilm_scan_period_estimated_minutes

Le temps estimé pour effectuer une analyse ILM complète sur ce nœud.

Remarque : une analyse complète ne garantit pas que l'ILM a été appliqué à tous les objets appartenant à ce nœud.

heure d'expiration du certificat du point de terminaison de l'équilibreur de charge de la grille de stockage

Le temps d'expiration du certificat du point de terminaison de l'équilibreur de charge en secondes depuis l'époque.

storagegrid_metadata_queries_average_latency_milliseconds

Le temps moyen requis pour exécuter une requête sur le magasin de métadonnées via ce service.

storagegrid_network_received_bytes

La quantité totale de données reçues depuis l'installation.

octets_transmis_réseau_grille_de_stockage

La quantité totale de données envoyées depuis l'installation.

pourcentage_d'utilisation_du_processeur_du_nœud_de_grille_de_stockage

Le pourcentage de temps CPU disponible actuellement utilisé par ce service. Indique à quel point le service est occupé. La quantité de temps CPU disponible dépend du nombre de CPU du serveur.

storagegrid_ntp_chosen_time_source_offset_milliseconds

Décalage systématique du temps fourni par une source de temps choisie. Le décalage est introduit lorsque le délai pour atteindre une source de temps n'est pas égal au temps nécessaire à la source de temps pour atteindre le client NTP.

storagegrid_ntp_locked

Le nœud n'est pas verrouillé sur un serveur NTP (Network Time Protocol).

storagegrid_s3_data_transfers_bytes_ingested

Quantité totale de données ingérées à partir des clients S3 vers ce nœud de stockage depuis la dernière réinitialisation de l'attribut.

storagegrid_s3_data_transfers_bytes_retrieved

Quantité totale de données récupérées par les clients S3 à partir de ce nœud de stockage depuis la dernière réinitialisation de l'attribut.

storagegrid_s3_operations_failed

Nombre total d'opérations S3 ayant échoué (codes d'état HTTP 4xx et 5xx), à l'exclusion de celles causées par un échec d'autorisation S3.

storagegrid_s3_operations_successful

Nombre total d'opérations S3 réussies (code d'état HTTP 2xx).

storagegrid_s3_operations_unauthorized

Nombre total d'opérations S3 ayant échoué, résultant d'un échec d'autorisation.

jours d'expiration du certificat de l'interface de gestion du certificat du serveur de grille de stockage

Le nombre de jours avant l'expiration du certificat de l'interface de gestion.

certificat_serveur_grille_de_stockage_points_de_termination_API_de_stockage_jours_expansion_du_certificat

Le nombre de jours avant l'expiration du certificat API Object Storage.

service_grille_stockage_cpu_secondes

La durée cumulée pendant laquelle le processeur a été utilisé par ce service depuis l'installation.

utilisation_mémoire_octets_service_grille_de_stockage

La quantité de mémoire (RAM) actuellement utilisée par ce service. Cette valeur est identique à celle affichée par l'utilitaire Linux top sous le nom RES.

service_grille_de_stockage_réseau_octets_reçus

La quantité totale de données reçues par ce service depuis l'installation.

réseau_de_services_de_grille_de_stockage_octets_transmis

La quantité totale de données envoyées par ce service.

redémarrages du service storagegrid

Le nombre total de fois où le service a été redémarré.

storagegrid_service_runtime_seconds

La durée totale d'exécution du service depuis l'installation.

storagegrid_service_uptime_seconds

La durée totale d'exécution du service depuis son dernier redémarrage.

grille_de_stockage_état_courant

L'état actuel des services de stockage. Les valeurs des attributs sont :

- 10 = Hors ligne
- 15 = Entretien
- 20 = Lecture seule

- 30 = En ligne

état_stockage_grille_de_stockage

L'état actuel des services de stockage. Les valeurs des attributs sont :

- 0 = Aucune erreur
- 10 = En transition
- 20 = Espace libre insuffisant
- 30 = Volume(s) indisponible(s)
- 40 = Erreur

grille_de_stockage_utilisation_du_stockage_octets_de_données

Une estimation de la taille totale des données d'objet répliquées et codées par effacement sur le nœud de stockage.

storagegrid_storage_utilisation_métadonnées_autorisées_octets

L'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 la base de données (telles que le compactage et la réparation) et les futures mises à niveau matérielles et logicielles. L'espace autorisé pour les métadonnées d'objet contrôle la capacité globale de l'objet.

grille_de_stockage_utilisation_du_stockage_métadonnées_octets

La quantité de métadonnées d'objet sur le volume de stockage 0, en octets.

storagegrid_storage_utilisation_total_espace_octets

La quantité totale d'espace de stockage allouée à tous les magasins d'objets.

grille_de_stockage_utilisation_espace_utilisable_octets

La quantité totale d'espace de stockage d'objets restant. Calculé en additionnant la quantité d'espace disponible pour tous les magasins d'objets sur le nœud de stockage.

storagegrid_swift_data_transfers_bytes_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_transfers_bytes_récupérés

Quantité totale de données récupérées par les clients Swift à partir de ce nœud de stockage depuis la dernière réinitialisation de l'attribut.

échec des opérations de storagegrid_swift

Nombre total d'opérations Swift ayant échoué (codes d'état HTTP 4xx et 5xx), à l'exclusion de celles causées par un échec d'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, résultant d'un échec d'autorisation (codes d'état HTTP 401, 403, 405).

octets de données d'utilisation du locataire de la grille de stockage

La taille logique de tous les objets pour le locataire.

nombre_d'objets_d'utilisation_locataire_de_grille_de_stockage

Le nombre d'objets pour le locataire.

quota_d'utilisation_locataire_de_grille_de_stockage_octets

La 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 métriques

Pour obtenir la liste complète des métriques, utilisez l'API Grid Management.

1. En haut du gestionnaire de grille, sélectionnez l'icône d'aide et sélectionnez **Documentation API**.
2. Localisez les opérations **métriques**.
3. Exécuter le GET `/grid/metric-names` opération.
4. Téléchargez les résultats.

Référence des fichiers journaux

Référence des fichiers journaux

StorageGRID fournit des journaux utilisés pour capturer des événements, des messages de diagnostic et des conditions d'erreur. Il peut vous être demandé de collecter des fichiers journaux et de les transmettre au support technique pour aider au dépannage.

Les journaux sont classés comme suit :

- ["Journaux du logiciel StorageGRID"](#)
- ["Journaux de déploiement et de maintenance"](#)
- ["À propos du bycast.log"](#)



Les détails fournis pour chaque type de journal sont fournis à titre indicatif 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 d'application dépassent le cadre de ces instructions.

Accéder aux journaux

Pour accéder aux journaux, vous pouvez ["collecter les fichiers journaux et les données système"](#) à partir d'un ou plusieurs nœuds sous forme d'archive de fichier journal unique. Ou, si le nœud d'administration principal n'est pas disponible ou ne peut pas atteindre un nœud spécifique, vous pouvez accéder aux fichiers journaux individuels pour chaque nœud de grille comme suit :

1. Entrez la commande suivante : `ssh admin@grid_node_IP`
2. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.
3. Entrez la commande suivante pour passer en root : `su -`

4. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.

Exporter les journaux vers le serveur syslog

L'exportation des journaux vers le serveur syslog offre les fonctionnalités suivantes :

- Recevez une liste de toutes les demandes Grid Manager et Tenant Manager, en plus des demandes S3 et Swift.
- Meilleure visibilité sur les requêtes S3 qui renvoient des erreurs, sans l'impact sur les performances causé par les méthodes de journalisation d'audit.
- Accès aux requêtes de la couche HTTP et aux codes d'erreur faciles à analyser.
- Meilleure visibilité sur les requêtes bloquées par les classificateurs de trafic au niveau de l'équilibreur de charge.

Pour exporter les journaux, reportez-vous à ["Configurer les messages d'audit et les destinations des journaux"](#).

Catégories de fichiers journaux

L'archive du fichier journal StorageGRID contient les journaux décrits pour chaque catégorie et des fichiers supplémentaires contenant des métriques et la sortie des commandes de débogage.

Emplacement des archives	Description
audit	Messages d'audit générés pendant le fonctionnement normal du système.
journaux du système d'exploitation de base	Informations sur le système d'exploitation de base, y compris les versions d'image StorageGRID .
paquets	Informations de configuration globale (bundles).
Cassandra	Informations sur la base de données Cassandra et journaux de réparation Reaper.
ec	Informations VCS sur le nœud actuel et informations sur le groupe EC par ID de profil.
grille	Journaux de grille généraux, y compris le débogage(<code>broadcast.log</code>) et <code>servermanager</code> journaux.
grille.json	Fichier de configuration de grille partagé entre tous les nœuds. En plus, <code>node.json</code> est spécifique au nœud actuel.
hagroupes	Mesures et journaux des groupes de haute disponibilité.
installer	`Gdu-server` et installer les journaux.
Arbitre lambda	Journaux liés à la demande de proxy S3 Select.

Emplacement des archives	Description
bûcheron.log	Messages de débogage liés à la collecte de journaux.
Métrique	Journaux de service pour Grafana, Jaeger, l'exportateur de nœuds et Prometheus.
divers	Journaux d'accès et d'erreurs Miscd.
MySQL	La configuration de la base de données mariaDB et les journaux associés.
filet	Journaux générés par les scripts liés au réseau et le service Dynip.
nginx	Fichiers et journaux de configuration de l'équilibreur de charge et de la fédération de grille. Inclut également les journaux de trafic Grid Manager et Tenant Manager.
nginx-gw	• <code>access.log</code>: Messages du journal des demandes du gestionnaire de grille et du gestionnaire de locataires. ◦ Ces messages sont préfixés par <code>mgmt</code> : lorsqu'il est exporté à l'aide de <code>syslog</code>. ◦ Le format de ces messages de journal est <code>[\$time_iso8601] \$remote_addr \$status \$bytes_sent \$request_length \$request_time "\$endpointId" "\$request" "\$http_host" "\$http_user_agent" "\$http_referer"</code> • <code>cgr-access.log.gz</code>: Demandes de réplication inter-grille entrantes. ◦ Ces messages sont préfixés par <code>cgr</code> : lorsqu'il est exporté à l'aide de <code>syslog</code>. ◦ Le format de ces messages de journal est <code>[\$time_iso8601] \$remote_addr \$status \$bytes_sent \$request_length \$request_time "\$endpointId" "\$upstream_addr" "\$request" "\$http_host"</code> • <code>endpoint-access.log.gz</code>: S3 et Swift demandent aux points de terminaison de l'équilibreur de charge. ◦ Ces messages sont préfixés par <code>endpoint</code> : lorsqu'il est exporté à l'aide de <code>syslog</code>. ◦ Le format de ces messages de journal est <code>[\$time_iso8601] \$remote_addr \$status \$bytes_sent \$request_length \$request_time "\$endpointId" "\$upstream_addr" "\$request" "\$http_host"</code> • <code>nginx-gw-dns-check.log</code>: En rapport avec la nouvelle alerte de vérification DNS.
ntp	Fichier de configuration et journaux NTP.

Emplacement des archives	Description
Objets orphelins	Journaux relatifs aux objets orphelins.
os	Fichier d'état des nœuds et des grilles, y compris les services <code>pid</code> .
autre	Fichiers journaux sous <code>/var/local/log</code> qui ne sont pas collectés dans d'autres dossiers.
performances	Informations sur les performances du processeur, du réseau et des E/S disque.
données de Prometheus	Métriques Prometheus actuelles, si la collecte de journaux inclut des données Prometheus.
approvisionnement	Journaux liés au processus de provisionnement du réseau.
radeau	Journaux du cluster Raft utilisés dans les services de la plateforme.
ssh	Journaux liés à la configuration et au service SSH.
SNMP	Configuration de l'agent SNMP utilisée pour l'envoi de notifications SNMP.
sockets-données	Données de sockets pour le débogage du réseau.
commandes-système.txt	Sortie des commandes du conteneur StorageGRID . Contient des informations système, telles que la mise en réseau et l'utilisation du disque.
synchronisation-recuperation-package	Lié au maintien de la cohérence du dernier package de récupération sur tous les nœuds d'administration et nœuds de stockage qui hébergent le service ADC.

Journaux du logiciel StorageGRID

Vous pouvez utiliser les journaux StorageGRID pour résoudre les problèmes.



Si vous souhaitez envoyer vos journaux à un serveur syslog externe ou modifier la destination des informations d'audit telles que le `broadcast.log` et `nms.log`, voir ["Configurer les messages d'audit et les destinations des journaux"](#).

Journaux généraux StorageGRID

Nom des fichiers	Remarques	Trouvé sur
/var/local/log/bycast.log	Le fichier de dépannage principal de StorageGRID . Sélectionnez SUPPORT > Outils > Topologie de grille . Sélectionnez ensuite Site > Node > SSM > Événements .	Tous les nœuds
/var/local/log/bycast-err.log	Contient un sous-ensemble de bycast.log (messages de gravité ERREUR et CRITIQUE). Des messages CRITIQUES sont également affichés dans le système. Sélectionnez SUPPORT > Outils > Topologie de grille . Sélectionnez ensuite Site > Node > SSM > Événements .	Tous les nœuds
/var/local/core/	Contient tous les fichiers de vidage de mémoire créés si le programme se termine anormalement. Les causes possibles incluent les échecs d'assertion, les violations ou les délais d'expiration des threads. Remarque : Le fichier <code>/var/local/core/kexec_cmd</code> existe généralement sur les nœuds d'appareil et n'indique pas d'erreur.	Tous les nœuds

Journaux liés au chiffrement

Nom des fichiers	Remarques	Trouvé sur
/var/local/log/ssh-config-generation.log	Contient les journaux liés à la génération de configurations SSH et au rechargement des services SSH.	Tous les nœuds
/var/local/log/nginx/config-generation.log	Contient les journaux liés à la génération de configurations nginx et au rechargement des services nginx.	Tous les nœuds
/var/local/log/nginx-gw/config-generation.log	Contient les journaux liés à la génération de configurations nginx-gw (et au rechargement des services nginx-gw).	Nœuds d'administration et de passerelle
/var/local/log/update-cipher-configurations.log	Contient les journaux liés à la configuration des politiques TLS et SSH.	Tous les nœuds

Journaux de la fédération de grille

Nom des fichiers	Remarques	Trouvé sur
/var/local/log/update_grid_federation_config.log	Contient les journaux liés à la génération de configurations nginx et nginx-gw pour les connexions de fédération de grille.	Tous les nœuds

Journaux NMS

Nom des fichiers	Remarques	Trouvé sur
/var/local/log/nms.log	• Capture les notifications du gestionnaire de grille et du gestionnaire de locataires. • Capture les événements liés au fonctionnement du service NMS. Par exemple, les notifications par e-mail et les modifications de configuration. • Contient les mises à jour du bundle XML résultant des modifications de configuration apportées au système. • Contient des messages d'erreur liés au sous-échantillonnage des attributs effectué une fois par jour. • Contient des messages d'erreur du serveur Web Java, par exemple, des erreurs de génération de page et des erreurs d'état HTTP 500.	Nœuds d'administration
/var/local/log/nms.errlog	Contient des messages d'erreur liés aux mises à niveau de la base de données MySQL. Contient le flux d'erreur standard (stderr) des services correspondants. Il y a un fichier journal par service. Ces fichiers sont généralement vides, sauf en cas de problèmes 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 du gestionnaire de serveur

Nom des fichiers	Remarques	Trouvé sur
/var/local/log/servermanager.log	Fichier journal pour l'application Gestionnaire de serveur exécutée sur le serveur.	Tous les nœuds
/var/local/log/GridstatBackend.errlog	Fichier journal pour l'application backend de l'interface graphique du gestionnaire de serveur.	Tous les nœuds
/var/local/log/gridstat.errlog	Fichier journal pour l'interface graphique du gestionnaire de serveur.	Tous les nœuds

Journaux des services StorageGRID

Nom des fichiers	Remarques	Trouvé sur
/var/local/log/acct.errlog		Nœuds de stockage exécutant le service ADC
/var/local/log/adc.errlog	Contient le flux d'erreur standard (stderr) des services correspondants. Il y a un fichier journal par service. Ces fichiers sont généralement vides, sauf en cas de problèmes avec le service.	Nœuds de stockage exécutant le service ADC
/var/local/log/ams.errlog		Nœuds d'administration
/var/local/log/cassandra/system.log	Informations sur le magasin de métadonnées (base de données Cassandra) qui peuvent être utilisées si des problèmes surviennent lors de l'ajout de nouveaux nœuds de stockage ou si la tâche de réparation de nodetool se bloque.	Nœuds de stockage
/var/local/log/cassandra-reaper.log	Informations sur le service Cassandra Reaper, qui effectue des réparations des données dans 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 des fichiers	Remarques	Trouvé sur
/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/dds.errlog		Nœuds de stockage
/var/local/log/dmv.errlog		Nœuds de stockage
/var/local/log/dynip*	Contient les journaux liés au service dynip, qui surveille la grille pour les changements IP dynamiques et met à jour la configuration locale.	Tous les nœuds
/var/local/log/grafana.log	Le journal associé au service Grafana, qui est utilisé pour la visualisation des métriques dans le gestionnaire de grille.	Nœuds d'administration
/var/local/log/hagroups.log	Le journal associé aux groupes de 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 BACKUP à MASTER ou FAULT.	Nœuds d'administration et nœuds de passerelle
/var/local/log/idnt.errlog		Nœuds de stockage exécutant le service ADC
/var/local/log/jaeger.log	Le 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
/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 le "S3 Sélectionnez les exigences et les limitations pour les nœuds d'administration et de passerelle" .

Nom des fichiers	Remarques	Trouvé sur
/var/local/log/ldr.errlog		Nœuds de stockage
/var/local/log/miscd/*.log	Contient les journaux du service MISCD (Information Service Control Daemon), qui fournit une interface pour interroger et gérer les services sur d'autres nœuds et pour gérer les configurations environnementales sur le nœud, telles que l'interrogation de l'état des services exécutés sur d'autres nœuds.	Tous les nœuds
/var/local/log/nginx/*.log	Contient les journaux du service nginx, qui agit comme un mécanisme d'authentification et de communication sécurisé pour divers services de grille (tels que Prometheus et Dynip) pour pouvoir communiquer avec des services sur d'autres nœuds via des API HTTPS.	Tous les nœuds
/var/local/log/nginx-gw/*.log	Contient les journaux généraux liés 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 les journaux d'accès liés au trafic de réplication inter-grille.	Nœuds d'administration, nœuds de passerelle ou les deux, en fonction de la configuration de la fédération de grille. Trouvé uniquement sur la grille de destination pour la réplication inter-grille.
/var/local/log/nginx-gw/endpoint-access.log.gz	Contient les journaux d'accès pour le service Load Balancer, qui fournit l'équilibrage de la charge du trafic S3 des clients vers les nœuds de stockage.	Nœuds d'administration et nœuds de passerelle
/var/local/log/persistence*	Contient les journaux du service de persistance, qui gère les fichiers sur le disque racine qui doivent persister après un redémarrage.	Tous les nœuds

Nom des fichiers	Remarques	Trouvé sur
/var/local/log/prometheus.log	Pour tous les nœuds, contient le journal du service d'exportation de nœuds et le journal du service de métriques 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 Raft.	Nœuds de stockage avec service RSM
/var/local/log/rms.errlog	Contient les journaux du service Replicated State Machine Service (RSM), qui est utilisé pour les services de la 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 les journaux liés au traitement des mises à jour pour la configuration des noms de domaine hébergés virtuels S3. Consultez les instructions pour implémenter les applications clientes S3.	Nœuds d'administration et de passerelle
/var/local/log/mise à jour-pare-feu-snmpp.*	Contient les journaux liés aux ports de pare-feu gérés pour SNMP.	Tous les nœuds
/var/local/log/update-sysl.log	Contient les journaux liés aux modifications apportées à la configuration syslog du système.	Tous les nœuds
/var/local/log/update-traffic-classes.log	Contient les journaux liés aux modifications apportées à la configuration des classificateurs de trafic.	Nœuds d'administration et de passerelle
/var/local/log/update-utcn.log	Contient les journaux liés au mode réseau client non approuvé sur ce nœud.	Tous les nœuds

Informations connexes

- ["À propos du bycast.log"](#)
- ["Utiliser 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 des fichiers	Remarques	Trouvé sur
/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 lors d'opérations d'agrandissement. Contient un enregistrement des événements d'extension.	Nœuds de stockage
/var/local/log/pa-move.log	Créé lors de l'exécution du <code>pa-move.sh</code> scénario.	Nœud d'administration principal
/var/local/log/pa-move-new_pa.log	Créé lors de l'exécution du <code>pa-move.sh</code> scénario.	Nœud d'administration principal
/var/local/log/pa-move-old_pa.log	Créé lors de l'exécution du <code>pa-move.sh</code> scénario.	Nœud d'administration principal
/var/local/log/gdu-server.log	Créé par le service GDU. Contient les événements liés aux procédures de provisionnement 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
/var/local/log/upgrade.log	Créé lors de la mise à niveau du logiciel. Contient un enregistrement des événements de mise à jour du logiciel.	Tous les nœuds

À propos du `broadcast.log`

Le fichier `/var/local/log/broadcast.log` est le fichier de dépannage principal pour le logiciel StorageGRID. Il y a un `broadcast.log` fichier pour chaque nœud de la grille. Le fichier contient des messages spécifiques à ce nœud de grille.

Le fichier `/var/local/log/broadcast-err.log` est un sous-ensemble de `broadcast.log`. Il contient des messages de gravité ERREUR et CRITIQUE.

En option, vous pouvez modifier la destination des journaux d'audit et envoyer les informations d'audit à un serveur syslog externe. Les journaux locaux des enregistrements d'audit continuent d'être générés et stockés lorsqu'un serveur syslog externe est configuré. Voir ["Configurer les messages d'audit et les destinations des journaux"](#).

Rotation des fichiers pour bycast.log

Quand 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`. Quand 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` il y a 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` il y a sept fichiers.



Si un fichier journal a été compressé, vous ne devez pas le décompresser au même emplacement où il a été écrit. La décompression du fichier au même emplacement peut interférer avec les scripts de rotation des journaux.

En option, vous pouvez modifier la destination des journaux d'audit et envoyer les informations d'audit à un serveur syslog externe. Les journaux locaux des enregistrements d'audit continuent d'être générés et stockés lorsqu'un serveur syslog externe est configuré. Voir "[Configurer les messages d'audit et les destinations des journaux](#)".

Informations connexes

["Collecter les fichiers journaux et les données système"](#)

Messages dans bycast.log

Messages dans `bycast.log` sont écrits par l'ADE (Asynchronous Distributed Environment). ADE est l'environnement d'exécution utilisé par les services de chaque nœud de 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
Nœud ID	12455685
ID du processus ADE	0357819531
Nom du module	SVMR
Identifiant du message	Véhicule électrique à évacuation sanitaire (VEHR)

Segment de message	Valeur dans l'exemple
Heure système UTC	2019-05-05T27T17:10:29.784677 (AAAA-MM-JJTHH:MM:SS.uuuuuu)
Niveau de gravité	ERREUR
Numéro de suivi interne	0906
Message	SVMR : Le contrôle de santé du volume 3 a échoué pour la raison « TOUT »

Gravités des messages dans bycast.log

Les messages dans `bycast.log` Des niveaux de gravité sont attribués.

Par exemple:

- **AVIS** — Un événement qui devrait être enregistré s'est produit. La plupart des messages de journal sont à ce niveau.
- **AVERTISSEMENT** — Une condition inattendue s'est produite.
- **ERREUR** — Une erreur majeure s'est produite et aura un impact sur les opérations.
- **CRITIQUE** — Une condition anormale s'est produite, ce qui a interrompu les opérations normales. Vous devez traiter immédiatement le problème sous-jacent.

Codes d'erreur dans bycast.log

La plupart des messages d'erreur dans `bycast.log` contenir 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 rapporté.

Code d'erreur	Signification
SUCS	Aucune erreur
GERR	Inconnu
CANC	Annulé
ABRT	Avorté
TOUT	Temps mort
INVL	Invalide
NFND	Non trouvé

Code d'erreur	Signification
VERS	Version
CONF	Configuration
ÉCHOUER	Échec
ICPL	Incomplet
FAIT	Fait
SUNV	Service non disponible

Le tableau suivant répertorie les codes d'erreur numériques dans `broadcast.log`.

Numéro d'erreur	Code d'erreur	Signification
001	EPERM	Opération non autorisée
002	ENOENT	Aucun fichier ou répertoire de ce nom
003	ESCRCH	Aucun processus de ce type
004	EINTR	Appel système interrompu
005	EIO	Erreur d'E/S
006	ENXIO	Aucun appareil ou adresse de ce type
007	E2BIG	Liste d'arguments trop longue
008	ENOEXEC	Erreur de format d'exécution
009	EBADF	Numéro de fichier incorrect
010	ECHILD	Aucun processus enfant
011	ENCORE	Essayer à nouveau
012	ÉNOMÈME	Mémoire insuffisante
013	EACCES	Permission refusée

Numéro d'erreur	Code d'erreur	Signification
014	DÉFAUT	Mauvaise adresse
015	ENOTBLK	Dispositif de blocage requis
016	OCCUPÉ	Appareil ou ressource occupé
017	EEXIST	Le fichier existe
018	EXDEV	Lien entre appareils
019	ENODEV	Aucun appareil de ce type
020	ENOTDIR	Pas un répertoire
021	EISDIR	C'est un répertoire
022	EINVAL	Argument invalide
023	ENFILE	Dépassement de capacité de la table de fichiers
024	E-FILE	Trop de fichiers ouverts
025	ÉNORME	Pas une machine à écrire
026	ETXTBSY	Fichier texte occupé
027	EFBIG	Fichier trop volumineux
028	ENOSPC	Plus d'espace disponible sur l'appareil
029	ESPIPE	Recherche illégale
030	EROFS	Système de fichiers en lecture seule
031	EMLINK	Trop de liens
032	ÉPIPE	Tuyau cassé
033	EDOM	Argument mathématique hors du domaine de la fonction
034	ÉRANGE	Résultat mathématique non représentable

Numéro d'erreur	Code d'erreur	Signification
035	EDEADLK	Une impasse sur les ressources se produirait
036	ÉMAILONG	Nom de fichier trop long
037	ENOLCK	Aucun verrou d'enregistrement disponible
038	ENOSYS	Fonction non implémentée
039	ÉNOTEMPTÉ	Le répertoire n'est pas vide
040	BOUCLE	Trop de liens symboliques rencontrés
041		
042	ENOMSG	Aucun message du type souhaité
043	EIDRM	Identifiant supprimé
044	ECHRNG	Numéro de chaîne hors plage
045	EL2NSYNC	Niveau 2 non synchronisé
046	EL3HLT	Niveau 3 arrêté
047	EL3RST	Réinitialisation de niveau 3
048	ELNRNG	Numéro de lien hors limites
049	EUNATCH	Pilote de protocole non connecté
050	ENOC SI	Aucune structure CSI disponible
051	EL2HLT	Niveau 2 arrêté
052	EBADE	Échange invalide
053	EBADR	Descripteur de demande non valide
054	EXCOMPLET	Échange complet
055	ENOANO	Pas d'anode

Numéro d'erreur	Code d'erreur	Signification
056	EBADRQC	Code de demande invalide
057	EBADSLT	Emplacement invalide
058		
059	EBFONT	Mauvais format de fichier de police
060	ENOSTR	L'appareil n'est pas un flux
061	ENODATA	Aucune donnée disponible
062	ETIME	Le temps a expiré
063	ENOSR	Ressources hors flux
064	ENONET	La machine n'est pas sur le réseau
065	ENOPKG	Paquet non installé
066	EREMOTE	L'objet est distant
067	ENOLINK	Le lien a été rompu
068	EADV	Erreur de publicité
069	ESRMNT	Erreur de montage système
070	ECOMM	Erreur de communication lors de l'envoi
071	ÉPROTO	Erreur de protocole
072	ÉMULTIHOP	Tentative de saut multiple
073	EDOTDOT	Erreur spécifique RFS
074	EBADMSG	Pas un message de données
075	DÉBORDEMENT	Valeur trop grande pour le type de données défini
076	ENOTUNIQ	Le nom n'est pas unique sur le réseau

Numéro d'erreur	Code d'erreur	Signification
077	EBADFD	Descripteur de fichier en mauvais état
078	EREMCHG	Adresse distante modifiée
079	ELIBACC	Impossible d'accéder à une bibliothèque partagée nécessaire
080	ÉLIBBAD	Accéder à une bibliothèque partagée corrompue
081	ELIBSCN	
082	ELIBMAX	Tentative de liaison dans trop de bibliothèques partagées
083	ÉLIBEXEC	Impossible d'exécuter directement une bibliothèque partagée
084	EILSEQ	Séquence d'octets illégale
085	ERESTART	L'appel système interrompu doit être redémarré
086	ESTRPIPE	Erreur de tuyau de flux
087	UTILISATEURS	Trop d'utilisateurs
088	ENOTSOCK	Fonctionnement d'un socket sur un non-socket
089	EDESTADDRREQ	Adresse de destination requise
090	TAILLE EMSGS	Message trop long
091	ÉPROTOTYPE	Protocole de type incorrect pour le socket
092	ÉNOPROTOOPE	Protocole non disponible
093	EPROTONOSUPPORT	Protocole non pris en charge
094	ESOCKTNOSUPPORT	Type de socket non pris en charge
095	EOPNOTSUPP	Opération non prise en charge sur le point de terminaison de transport
096	SOUTIEN EPFNOS	Famille de protocoles non prise en charge

Numéro d'erreur	Code d'erreur	Signification
097	SOUTIEN EAFNOS	Famille d'adresses non prise en charge par le protocole
098	UTILISATION D'EADDRIN	Adresse déjà utilisée
099	EADDRNOTAVIL	Impossible d'attribuer l'adresse demandée
100	ENETDOWN	Le réseau est en panne
101	ENETUNREACH	Le réseau est inaccessible
102	ENETRESET	La connexion réseau a été interrompue en raison d'une réinitialisation
103	ÉCONNABORTÉ	Le logiciel a provoqué l'interruption de la connexion
104	RÉINITIALISATION ÉCONOMIQUE	Réinitialisation de la connexion par l'homologue
105	ÉNOBUFS	Aucun espace tampon disponible
106	EISCONN	Le point de terminaison de transport est déjà connecté
107	ENOTCONN	Le point de terminaison de transport n'est pas connecté
108	FERMETURE	Impossible d'envoyer après l'arrêt du point de terminaison de transport
109	ETOOMANYREFS	Trop de références : impossible de les raccorder
110	ETIMEDOUT	La connexion a expiré
111	ÉCONFREINÉ	Connexion rejetée
112	EHOSTDOWN	L'hôte est en panne
113	EHOSTUNREACH	Aucune route vers l'hôte
114	DÉJÀ	Opération déjà en cours
115	PROGRÈS	Opération en cours

Numéro d'erreur	Code d'erreur	Signification
116		
117	EUCLEAN	La structure a besoin d'être nettoyée
118	ENOTNAM	Pas un fichier de type nommé XENIX
119	ENAVAI	Aucun sémaphore XENIX disponible
120	EISNAM	Est un fichier de type nommé
121	EREMOTEIO	Erreur d'E/S à distance
122	EDQUOT	Quota dépassé
123	ÉNOMÉDIUM	Aucun support trouvé
124	TYPE MOYEN	Mauvais type de support
125	ÉANNULÉ	Opération annulée
126	ENOKEY	Clé requise non disponible
127	EKEY EXPIRÉ	La clé a expiré
128	EKEYREVOKED	La clé a été révoquée
129	EKEYREJECTED	La clé a été rejetée par le service
130	PROPRIÉTAIRE MORT	Pour les mutex robustes : le propriétaire est décédé
131	NON RÉCUPÉRABLE	Pour les mutex robustes : état non récupérable

Configurer les destinations des messages d'audit et des journaux

Considérations relatives à l'utilisation d'un serveur syslog externe

Un serveur syslog externe est un serveur extérieur à StorageGRID que vous pouvez utiliser pour collecter des informations d'audit système dans un seul emplacement. L'utilisation d'un serveur syslog externe vous permet de réduire le trafic réseau sur vos nœuds d'administration et de gérer les informations plus efficacement. Pour StorageGRID, le format du paquet de messages syslog sortant est conforme à la RFC 3164.

Les types d'informations d'audit que vous pouvez envoyer au serveur syslog externe incluent :

- 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 les escalades vers la racine
- Journaux d'application qui pourraient être demandés s'il est nécessaire d'ouvrir un dossier d'assistance pour résoudre un problème que vous avez rencontré

Quand utiliser un serveur syslog externe

Un serveur syslog externe est particulièrement utile si vous disposez d'une grande grille, utilisez plusieurs types d'applications S3 ou souhaitez conserver toutes les données d'audit. 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 avoir à passer par un nœud d'administration.



Lorsque les journaux sont envoyés à un serveur syslog externe, les journaux uniques supérieurs à 8 192 octets sont tronqués à la fin du message pour se conformer aux limitations courantes dans les implémentations de serveur syslog externe.



Pour maximiser les options de récupération 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 maintenus sur chaque nœud.

Comment configurer un serveur syslog externe

Pour savoir comment configurer un serveur syslog externe, consultez "[Configurer les messages d'audit et le serveur syslog externe](#)".

Si vous prévoyez de configurer l'utilisation du protocole TLS ou RELP/TLS, vous devez disposer des certificats suivants :

- **Certificats CA du serveur** : un ou plusieurs certificats CA approuvés pour vérifier le serveur syslog externe dans le codage PEM. Si omis, le certificat Grid CA par défaut sera utilisé.
- **Certificat client** : Le certificat client pour l'authentification auprès du serveur syslog externe en codage PEM.
- **Clé privée client** : Clé privée pour le certificat client en 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 secrète. L'utilisation d'une clé privée chiffrée ne présente aucun avantage significatif en termes de sécurité, car la clé et la phrase secrète doivent être stockées. L'utilisation d'une clé privée non chiffrée, si disponible, est recommandée pour plus de simplicité.

Comment estimer la taille du serveur syslog externe

Normalement, votre grille est dimensionnée pour atteindre un débit requis, défini en termes d'opérations S3

par seconde ou d'octets par seconde. Par exemple, vous pouvez avoir besoin que votre grille gère 1 000 opérations S3 par seconde, ou 2 000 Mo par seconde, d'ingestions et de récupérations d'objets. Vous devez dimensionner votre serveur syslog externe en fonction des besoins en données de votre grille.

Cette section fournit quelques formules heuristiques qui vous aident à estimer le taux et la taille moyenne des messages de journal de différents types que votre serveur syslog externe doit être capable de gérer, exprimés en termes de caractéristiques de performances connues ou souhaitées de la grille (opérations S3 par seconde).

Utiliser S3 opérations 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 pour utiliser les formules d'estimation. Pour convertir le débit de la grille, vous devez d'abord déterminer la taille moyenne de votre objet, ce que vous pouvez faire en utilisant les informations des journaux d'audit et des mesures existants (le cas échéant), ou en utilisant vos connaissances des applications qui utiliseront StorageGRID. Par exemple, si votre grille a été dimensionnée pour atteindre un débit de 2 000 Mo/seconde et que la taille moyenne de votre objet est de 2 Mo, alors votre grille a été dimensionnée pour pouvoir gérer 1 000 opérations S3 par seconde (2 000 Mo / 2 Mo).



Les formules de dimensionnement du serveur syslog externe dans les sections suivantes fournissent des estimations de cas courants (plutôt que des estimations de cas les plus défavorables). Selon votre configuration et votre charge de travail, vous pouvez constater un taux de messages syslog ou un volume de données syslog supérieur ou inférieur à celui prévu par les formules. Les formules sont destinées à être utilisées uniquement à titre indicatif.

Formules d'estimation pour les journaux d'audit

Si vous ne disposez d'aucune information sur votre charge de travail S3 autre que le nombre d'opérations S3 par seconde que votre grille est censée prendre en charge, vous pouvez estimer le volume de journaux d'audit que votre serveur syslog externe devra gérer à l'aide des formules suivantes, en supposant que vous laissez les niveaux d'audit définis sur les valeurs par défaut (toutes les catégories définies sur Normal, à l'exception du stockage, qui est défini sur Erreur) :

```
Audit Log Rate = 2 x S3 Operations Rate  
Audit Log Average Size = 800 bytes
```

Par exemple, si votre grille est dimensionnée 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 de stocker) des données de journal d'audit à un débit 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 qui sont des PUT (par rapport aux GETS) et la taille moyenne, en octets, des champs S3 suivants (les abréviations à 4 caractères utilisées dans le tableau sont les noms des champs du journal d'audit) :

Code	Champ	Description
SACC	Nom du compte locataire S3 (expéditeur de la demande)	Le nom du compte locataire de l'utilisateur qui a envoyé la demande. Vide pour les demandes anonymes.
SBAC	Nom du compte locataire S3 (propriétaire du bucket)	Le nom du compte locataire pour le propriétaire du bucket. Utilisé pour identifier l'accès inter-comptes ou anonyme.
S3BK	Godet S3	Le nom du bucket S3.
S3KY	touche S3	Le nom de la clé S3, sans inclure le nom du bucket. Les opérations sur les buckets n'incluent pas ce champ.

Utilisons P pour représenter le pourcentage d'opérations S3 qui sont des PUT, où $0 \leq P \leq 1$ (donc 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 compte S3, du bucket S3 et de la clé S3. Supposons que le nom du compte S3 soit toujours my-s3-account (13 octets), que les buckets aient des noms de longueur fixe comme /my/application/bucket-12345 (28 octets) et que les objets aient des clés de longueur fixe comme 5733a5d7-f069-41ef-8fbd-13247494c69c (36 octets). La valeur de K est alors 90 (13+13+28+36).

Si vous pouvez déterminer les valeurs de P et K, vous pouvez estimer le volume de journaux d'audit que votre serveur syslog externe devra gérer à l'aide des formules suivantes, en supposant que vous laissez les niveaux d'audit définis sur les valeurs par défaut (toutes les catégories définies sur Normal, à l'exception du stockage, 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 votre grille est dimensionnée pour 1 000 opérations S3 par seconde, que votre charge de travail est composée à 50 % de PUT et que vos noms de compte S3, noms de bucket et noms d'objet font en moyenne 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 de stocker) des données de journal d'audit à un débit 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 de niveau d'audit par défaut (toutes les catégories définies sur Normal, à l'exception de Stockage, qui est défini sur Erreur). Les formules détaillées permettant d'estimer le taux et la taille moyenne des messages d'audit pour les paramètres de niveau d'audit non par défaut ne sont pas disponibles. Cependant, 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 est susceptible d'entraîner une surestimation car les messages d'audit «

supplémentaires » sont, en moyenne, plus petits que les messages d'audit par défaut.

Condition	Formule
Réplication : tous les niveaux d'audit sont définis sur Débogage ou Normal	Taux de journal d'audit = 8 x taux d'opérations S3
Codage d'effacement : niveaux d'audit tous définis sur Débogage ou Normal	Utiliser la même formule que pour les paramètres par défaut

Formules d'estimation des événements de sécurité

Les événements de sécurité ne sont pas corrélés aux 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 sur votre charge de travail S3 autre que le nombre d'opérations S3 par seconde que votre grille est censée prendre en charge, vous pouvez estimer le volume de 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
```

Ainsi, par exemple, si votre grille est dimensionnée 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) des données de journal d'application à un débit d'environ 1,2 Mo par seconde.

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 ou codage d'effacement), le pourcentage d'opérations S3 qui sont des PUT (par rapport aux GET/autres) et la taille moyenne, en octets, des champs S3 suivants (les abréviations à 4 caractères utilisées dans le tableau sont les noms des champs du journal d'audit) :

Code	Champ	Description
SACC	Nom du compte locataire S3 (expéditeur de la demande)	Le nom du compte locataire de l'utilisateur qui a envoyé la demande. Vide pour les demandes anonymes.
SBAC	Nom du compte locataire S3 (propriétaire du bucket)	Le nom du compte locataire pour le propriétaire du bucket. Utilisé pour identifier l'accès inter-comptes ou anonyme.
S3BK	Godet S3	Le nom du bucket S3.

Code	Champ	Description
S3KY	touche S3	Le nom de la clé S3, sans inclure le nom du bucket. Les opérations sur les buckets n'incluent pas ce champ.

Exemples d'estimations de dimensionnement

Cette section explique des exemples de cas d'utilisation des formules d'estimation pour les grilles avec les méthodes de protection des données suivantes :

- Réplication
- Codage d'effacement

Si vous utilisez la réplication pour la protection des données

Soit P représente le pourcentage d'opérations S3 qui sont des PUT, où $0 \leq P \leq 1$ (donc pour une charge de travail PUT de 100 %, $P = 1$, et pour une charge de travail GET de 100 %, $P = 0$).

Laissez K représenter la taille moyenne de la somme des noms de compte S3, du bucket S3 et de la clé S3. Supposons que le nom du compte S3 soit toujours my-s3-account (13 octets), que les buckets aient des noms de longueur fixe comme /my/application/bucket-12345 (28 octets) et que les objets aient des clés de longueur fixe comme 5733a5d7-f069-41ef-8fbd-13247494c69c (36 octets). Alors K a une valeur de 90 (13+13+28+36).

Si vous pouvez déterminer les valeurs de P et K , vous pouvez estimer le volume de journaux d'application que votre serveur syslog externe devra être capable de gérer 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
```

Ainsi, par exemple, si votre grille est dimensionnée pour 1 000 opérations S3 par seconde, que votre charge de travail est composée à 50 % de PUT et que vos noms de compte S3, noms de bucket et noms d'objet font en moyenne 90 octets, votre serveur syslog externe doit être dimensionné pour prendre en charge 1 800 journaux d'application par seconde et recevra (et stockera généralement) les données d'application à un débit de 0,5 Mo par seconde.

Si vous utilisez le codage d'effacement pour la protection des données

Soit P représente le pourcentage d'opérations S3 qui sont des PUT, où $0 \leq P \leq 1$ (donc pour une charge de travail PUT de 100 %, $P = 1$, et pour une charge de travail GET de 100 %, $P = 0$).

Laissez K représenter la taille moyenne de la somme des noms de compte S3, du bucket S3 et de la clé S3. Supposons que le nom du compte S3 soit toujours my-s3-account (13 octets), que les buckets aient des noms de longueur fixe comme /my/application/bucket-12345 (28 octets) et que les objets aient des clés de longueur fixe comme 5733a5d7-f069-41ef-8fbd-13247494c69c (36 octets). Alors K a une valeur de 90 (13+13+28+36).

Si vous pouvez déterminer les valeurs de P et K , vous pouvez estimer le volume de journaux d'application que votre serveur syslog externe devra être capable de gérer 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
```

Ainsi, par exemple, si votre grille est dimensionnée pour 1 000 opérations S3 par seconde, que votre charge de travail est composée à 50 % de PUT et que vos noms de compte S3, noms de bucket et noms d'objet font en moyenne 90 octets, votre serveur syslog externe doit être dimensionné pour prendre en charge 2 250 journaux d'application par seconde et doit être capable de recevoir (et généralement de stocker) des données d'application à un débit de 0,6 Mo par seconde.

Configurer les messages d'audit et le serveur syslog externe

Vous pouvez configurer un certain nombre de paramètres liés aux messages d'audit. Vous pouvez ajuster le nombre de messages d'audit enregistrés ; définir les en-têtes de requête HTTP que vous souhaitez inclure dans les messages d'audit de lecture et d'écriture du client ; configurer un serveur Syslog externe ; et spécifier où les journaux d'audit, les journaux d'événements de sécurité et les journaux du logiciel StorageGRID sont envoyés.

Les messages et journaux d'audit enregistrent les activités du système et les événements de sécurité et constituent des outils essentiels pour la surveillance et le dépannage. Tous les nœuds StorageGRID génèrent des messages d'audit et des journaux pour suivre l'activité et les événements du système.

En option, vous pouvez configurer un serveur syslog externe pour enregistrer les informations d'audit à distance. L'utilisation d'un serveur externe minimise l'impact sur les performances de la journalisation des messages d'audit sans réduire l'exhaustivité des données d'audit. Un serveur syslog externe est particulièrement utile si vous disposez d'une grande grille, utilisez plusieurs types d'applications S3 ou souhaitez conserver toutes les données d'audit. Voir ["Configurer les messages d'audit et le serveur syslog externe"](#) pour plus de détails.

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 de maintenance ou root"](#) .
- Si vous envisagez de configurer un serveur syslog externe, vous avez examiné le ["considérations relatives à l'utilisation d'un serveur syslog externe"](#) et s'assurer que le serveur dispose d'une capacité suffisante pour recevoir et stocker les fichiers journaux.
- Si vous prévoyez de configurer un serveur Syslog externe à l'aide du protocole TLS ou RELP/TLS, vous disposez de l'autorité de certification du serveur et des certificats client requis, ainsi que de la clé privée du client.

Modifier les niveaux des messages d'audit

Vous pouvez définir un niveau d'audit différent pour chacune des catégories de messages suivantes dans le journal d'audit :

Catégorie d'audit	Paramètre par défaut	Plus d'informations
Système	Normal	"Messages d'audit du système"

Catégorie d'audit	Paramètre par défaut	Plus d'informations
Stockage	Erreur	"Messages d'audit du stockage d'objets"
Gestion	Normal	"Message d'audit de gestion"
Le client lit	Normal	"Le client lit les messages d'audit"
Le client écrit	Normal	"Le client écrit des messages d'audit"
ILM	Normal	"Messages d'audit ILM"
Réplication inter-réseaux	Erreur	"CGRR : demande de réplication inter-réseau"



Ces valeurs par défaut s'appliquent si vous avez initialement installé StorageGRID à l'aide de la version 10.3 ou ultérieure. Si vous avez initialement utilisé une version antérieure de StorageGRID, la valeur par défaut pour toutes les catégories est définie sur Normal.



Lors des mises à niveau, les configurations de niveau 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
Désactivé	Aucun message d'audit de la catégorie n'est enregistré.
Erreur	Seuls les messages d'erreur sont enregistrés : les messages d'audit pour lesquels le code de résultat n'était pas « réussi » (SUCS).
Normal	Les messages transactionnels standard sont enregistrés : les messages répertoriés dans ces instructions pour la catégorie.
Déboguer	Obsolète. Ce niveau se comporte de la même manière que le niveau d'audit Normal.

Les messages inclus pour un niveau particulier incluent ceux qui seraient enregistrés 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 client pour vos applications S3, vous pouvez éventuellement modifier le paramètre **Lectures client** sur **Erreur** pour réduire le nombre de messages d'audit enregistrés dans le journal d'audit.

3. Sélectionnez **Enregistrer**.

Une bannière verte indique que votre configuration a été enregistrée.

Définir les en-têtes de requête HTTP

Vous pouvez éventuellement définir les en-têtes de requête HTTP que vous souhaitez inclure dans les messages d'audit de lecture et d'écriture du client. Ces en-têtes de protocole s'appliquent uniquement aux requêtes S3.

Étapes

1. Dans la section **En-têtes du 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 correspondre à zéro ou plusieurs caractères. Utilisez la séquence d'échappement (*) pour faire correspondre un astérisque littéral.

2. 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 demande du protocole d'audit sont enregistrés uniquement si le niveau d'audit pour **Lectures client** ou **Écritures client** n'est pas **Désactivé**.

3. Sélectionnez **Enregistrer**

Une bannière verte indique que votre configuration a été enregistrée.

Utiliser un serveur syslog externe

Vous pouvez éventuellement configurer un serveur syslog externe pour enregistrer les journaux d'audit, les journaux d'application et les journaux d'événements de sécurité dans un emplacement extérieur à votre grille.



Si vous ne souhaitez pas utiliser un serveur syslog externe, ignorez cette étape et accédez à [Sélectionner les destinations des informations d'audit](#).



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 la `audit-destinations` points de terminaison, qui se trouvent dans la section API privée du ["API de gestion de grille"](#). Par exemple, vous pouvez utiliser l'API si vous souhaitez utiliser différents serveurs Syslog pour différents groupes de nœuds.

Entrez les informations syslog

Accédez à l'assistant de configuration du serveur Syslog externe et fournissez les informations dont StorageGRID a besoin pour accéder au serveur Syslog externe.

Étapes

1. Depuis la page Serveur d'audit et syslog, sélectionnez **Configurer un serveur syslog externe**. Ou, si vous avez déjà configuré un serveur syslog externe, sélectionnez **Modifier le serveur syslog externe**.

L'assistant de configuration du serveur syslog externe s'affiche.

2. Pour l'étape **Saisir les informations syslog** de l'assistant, saisissez un nom de domaine complet valide ou une adresse IPv4 ou IPv6 pour le serveur syslog externe dans le champ **Hôte**.
3. Saisissez le port de destination sur le serveur syslog externe (doit être un entier compris entre 1 et 65535). Le port par défaut est 514.
4. Sélectionnez le protocole utilisé pour envoyer les informations d'audit au serveur syslog externe.

L'utilisation de **TLS** ou **REL/TLS** est recommandée. 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, consultez la section "[Gérer les certificats de sécurité](#)".

Toutes les options de protocole nécessitent la prise en charge et la configuration du serveur syslog externe. Vous devez choisir une option compatible avec le serveur syslog externe.



Le protocole de journalisation des événements fiable (REL/TLS) étend les fonctionnalités du protocole Syslog pour fournir une livraison fiable des messages d'événements. L'utilisation de REL/TLS peut aider à éviter la perte d'informations d'audit si votre serveur syslog externe doit redémarrer.

5. Sélectionnez **Continuer**.
6. Si vous avez sélectionné **TLS** ou **REL/TLS**, téléchargez les certificats d'autorité de certification du serveur, le certificat client et la clé privée du client.
 - a. Sélectionnez **Parcourir** pour le certificat ou la clé que vous souhaitez utiliser.
 - b. Sélectionnez le certificat ou le fichier clé.
 - c. Sélectionnez **Ouvrir** pour télécharger le fichier.

Une coche verte apparaît à côté du nom du certificat ou du fichier de clé, vous informant qu'il a été téléchargé avec succès.

7. Sélectionnez **Continuer**.

Gérer le contenu du syslog

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 que lorsqu'un utilisateur non autorisé tente de se connecter ou lorsqu'un utilisateur se connecte en tant que root
 - **Envoyer les journaux d'application** : Envoie "[Fichiers journaux du logiciel StorageGRID](#)" utile pour le dépannage, notamment :
 - `broadcast-err.log`
 - `broadcast.log`
 - `jaeger.log`

- `nms.log`(Nœuds d'administration uniquement)
- `prometheus.log`
- `raft.log`
- `hagroups.log`

- **Envoyer les journaux d'accès** : envoie les journaux d'accès HTTP pour les demandes externes à Grid Manager, Tenant Manager, aux points de terminaison d'équilibrage de charge configurés et aux demandes de fédération de grille à partir de systèmes distants.

2. Utilisez les menus déroulants pour sélectionner la gravité et la facilité (type de message) pour chaque catégorie d'informations d'audit que vous souhaitez envoyer.

La définition des valeurs de gravité et d'installation peut vous aider à regrouper les journaux de manière personnalisable pour une analyse plus facile.

a. Pour **Gravité**, sélectionnez **Passthrough** ou sélectionnez une valeur de gravité comprise entre 0 et 7.

Si vous sélectionnez une valeur, la valeur sélectionnée sera appliquée à tous les messages de ce type. Les informations sur les différentes gravités seront perdues si vous remplacez la gravité par une valeur fixe.

Gravité	Description
Passage	Chaque message envoyé au syslog externe doit avoir la même valeur de gravité que lorsqu'il a été enregistré localement sur le nœud : • Pour les journaux d'audit, la gravité est « info ». • Pour les événements de sécurité, les valeurs de gravité sont générées par la distribution Linux sur les nœuds. • Pour les journaux d'application, 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 une valeur « info », tandis que l'arrêt intentionnel du service SSM ou RSM donne une valeur « notice ». • Pour les journaux d'accès, la gravité est « info ».
0	Urgence : le système est inutilisable
1	Alerte : des mesures doivent être prises immédiatement
2	Critique : Conditions critiques
3	Erreur : conditions d'erreur
4	Avertissement : Conditions d'avertissement
5	Avis : État normal mais significatif
6	Informationnel : Messages d'information

Gravité	Description
7	Débogage : messages de niveau débogage

- b. Pour **Facility**, sélectionnez **Passthrough** ou sélectionnez une valeur d'installation comprise entre 0 et 23.

Si vous sélectionnez une valeur, elle sera appliquée à tous les messages de ce type. Les informations sur les différentes installations seront perdues si vous remplacez l'installation par une valeur fixe.

Facilité	Description
Passage	Chaque message envoyé au syslog externe doit avoir la même valeur de fonctionnalité que lorsqu'il a été enregistré localement sur le nœud : • Pour les journaux d'audit, l'installation envoyée au serveur syslog externe est « local7 ». • Pour les événements de sécurité, les valeurs des installations sont générées par la distribution Linux sur les nœuds. • Pour les journaux d'application, les journaux d'application envoyés au serveur syslog externe ont les valeurs de fonctionnalité suivantes : ◦ <code>broadcast.log</code>: utilisateur ou démon ◦ <code>broadcast-err.log</code>: utilisateur, démon, local3 ou local4 ◦ <code>jaeger.log</code>: local2 ◦ <code>nms.log</code>: local3 ◦ <code>prometheus.log</code>: local4 ◦ <code>raft.log</code>: local5 ◦ <code>hagroups.log</code>: local6 • Pour les journaux d'accès, l'installation envoyée au serveur syslog externe est « local0 ».
0	kern (messages du noyau)
1	utilisateur (messages au niveau de l'utilisateur)
2	mail
3	démon (démons système)
4	auth (messages de sécurité/autorisation)
5	syslog (messages générés en interne par syslogd)
6	lpr (sous-système d'imprimante en ligne)

Facilité	Description
7	actualités (sous-système d'actualités du réseau)
8	UUCP
9	cron (démon d'horloge)
10	sécurité (messages de sécurité/autorisation)
11	FTP
12	NTP
13	logaudit (audit des journaux)
14	logalert (alerte de journal)
15	horloge (démon d'horloge)
16	local0
17	local1
18	local2
19	local3
20	local4
21	local5
22	local6
23	local7

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. Vous devez utiliser ces messages de test pour vous aider à valider l'ensemble 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 de 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 indique que la configuration a été enregistrée.

2. Sinon, sélectionnez **Envoyer des messages de test** (recommandé).

Les résultats des tests apparaissent en continu sur la page jusqu'à ce que vous arrêtiez le test. Pendant que le test est en cours, vos messages d'audit continuent d'être envoyés vers vos destinations précédemment configurées.

3. Si vous recevez des erreurs, corrigez-les et sélectionnez à nouveau **Envoyer des messages de test**.

Voir "[Dépanner un serveur syslog externe](#)" pour vous aider à résoudre les erreurs.

4. Attendez de voir une bannière verte indiquant que tous les nœuds ont réussi les tests.
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 êtes renvoyé à la page **Serveur d'audit et syslog**. Une bannière verte indique que la configuration du serveur syslog a été enregistrée.



Les informations d'audit StorageGRID ne sont pas envoyées au serveur Syslog externe tant que vous n'avez pas sélectionné une destination incluant le serveur Syslog externe.

Sélectionner les destinations des informations d'audit

Vous pouvez spécifier où se trouvent les journaux d'audit, les journaux d'événements de sécurité et "[Journaux du logiciel StorageGRID](#)" sont envoyés.



StorageGRID utilise par défaut les destinations d'audit des nœuds locaux et stocke les informations d'audit dans `/var/local/log/localaudit.log`.

Lors de l'utilisation `/var/local/log/localaudit.log`, les entrées du journal d'audit du Grid Manager et du Tenant Manager peuvent être envoyées à un nœud de stockage. Vous pouvez trouver quel nœud contient les entrées les plus récentes en utilisant le `run-each-node --parallel "zgrep MGAU /var/local/log/localaudit.log | tail"` commande.

Certaines destinations ne sont disponibles que si vous avez configuré un serveur syslog externe.

Étapes

1. Sur la page Serveur d'audit et syslog, sélectionnez la destination des informations d'audit.



Les nœuds locaux uniquement et le **serveur syslog externe** offrent généralement de meilleures performances.

Option	Description
Nœuds locaux uniquement (par défaut)	Les messages d'audit, les journaux d'événements de sécurité et les journaux d'application ne sont pas envoyés aux nœuds d'administration. Au lieu de cela, ils sont enregistrés uniquement sur les nœuds qui les ont générés (« le nœud local »). Les informations d'audit générées sur chaque nœud local sont stockées dans <code>/var/local/log/localaudit.log</code>. Remarque : StorageGRID supprime périodiquement les 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 journal sont stockés sur chaque nœud.
Nœuds d'administration/nœuds locaux	Les messages d'audit sont envoyés au journal d'audit sur les nœuds d'administration, et les journaux d'événements de sécurité et les journaux d'application sont stockés sur les nœuds qui les ont générés. Les informations d'audit sont stockées dans les fichiers suivants : • Nœuds d'administration (principaux et non principaux) : <code>/var/local/audit/export/audit.log</code> • Tous les nœuds : Le <code>/var/local/log/localaudit.log</code> le fichier est généralement vide ou manquant. Il peut contenir des informations secondaires, comme une copie supplémentaire de certains messages.
Serveur syslog externe	Les informations d'audit sont envoyées à un serveur syslog externe et enregistrées sur les nœuds locaux(<code>/var/local/log/localaudit.log</code>). Le type d'informations envoyées dépend de la façon dont vous avez configuré le serveur syslog externe. Cette option est activée uniquement après avoir configuré un serveur syslog externe.
Nœud d'administration et serveur syslog externe	Les messages d'audit sont envoyés au journal d'audit(<code>/var/local/audit/export/audit.log</code>) sur les nœuds d'administration, et les informations d'audit sont envoyées au serveur syslog externe et enregistrées sur le nœud local(<code>/var/local/log/localaudit.log</code>). Le type d'informations envoyées dépend de la façon dont vous avez configuré le serveur syslog externe. Cette option est activée uniquement après avoir configuré un serveur syslog externe.

2. Sélectionnez **Enregistrer**.

Un message d'avertissement apparaît.

3. Sélectionnez **OK** pour confirmer que vous souhaitez modifier la destination des informations d'audit.

Une bannière verte indique que la 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.

Utiliser la surveillance SNMP

Utiliser la surveillance SNMP

Si vous souhaitez surveiller StorageGRID à l'aide du protocole SNMP (Simple Network Management Protocol), vous devez configurer l'agent SNMP inclus avec StorageGRID.

- ["Configurer l'agent SNMP"](#)
- ["Mettre 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 table et de notification pour les alertes. La MIB contient également des informations de description du système telles que la plate-forme et le numéro de modèle pour chaque nœud. Chaque nœud StorageGRID prend également en charge un sous-ensemble d'objets MIB-II.



Voir ["Accéder aux fichiers MIB"](#) si vous souhaitez télécharger les fichiers MIB sur vos nœuds de grille.

Initialement, 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 peut envoyer deux types de notifications basées sur des événements à un système de gestion :

Pièges

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 informer le système de gestion qu'un événement s'est produit dans StorageGRID, comme le déclenchement d'une alerte.

Les interruptions sont prises en charge dans les trois versions de SNMP.

Informe

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 délai, il renvoie l'information jusqu'à ce qu'un accusé de réception soit reçu ou que la valeur de nouvelle tentative maximale soit 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 n'importe quel 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 le "[nœud d'administration de l'expéditeur préféré](#)".

Chaque alerte est mappée à l'un des trois types d'interruption en fonction du niveau de gravité de l'alerte : `activeMinorAlert`, `activeMajorAlert` et `activeCriticalAlert`. Pour une liste des alertes qui peuvent déclencher ces pièges, consultez le "[Référence des alertes](#)".

Prise en charge des versions SNMP

Le tableau fournit un résumé de haut niveau de ce qui est pris en charge pour chaque version SNMP.

	SNMPv1	SNMPv2c	SNMPv3
Requêtes (GET et GETNEXT)	Requêtes MIB en lecture seule	Requêtes MIB en lecture seule	Requêtes MIB en lecture seule
Authentification des requêtes	Chaîne communautaire	Chaîne communautaire	Modèle de sécurité basé sur l'utilisateur (USM) utilisateur
Notifications (PIÈGE et INFORME)	Pièges uniquement	Pièges et informations	Pièges et informations
Authentification des notifications	Communauté de piège par défaut ou chaîne de communauté personnalisée pour chaque destination de piège	Communauté de piège par défaut ou chaîne de communauté personnalisée pour chaque destination de piège	Utilisateur USM pour chaque destination de trap

Limites

- StorageGRID prend en charge 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 de support de 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.

Configurer l'agent SNMP

Vous pouvez configurer l'agent SNMP StorageGRID pour 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 avez le ["Autorisation d'accès root"](#) .

À propos de cette tâche

L'agent SNMP StorageGRID prend en charge SNMPv1, SNMPv2c et SNMPv3. Vous pouvez configurer l'agent pour une ou plusieurs versions. Pour SNMPv3, seule l'authentification du modèle de sécurité utilisateur (USM) est prise en charge.

Tous les nœuds de la grille utilisent la même configuration SNMP.

Spécifier la configuration de base

Dans un premier temps, activez l'agent SMNP StorageGRID et fournissez des informations de base.

Étapes

1. Sélectionnez **CONFIGURATION > Surveillance > Agent SNMP**.

La page de l'agent SNMP apparaît.

2. Pour activer l'agent SNMP sur tous les nœuds de grille, cochez la case **Activer SNMP**.
3. Saisissez les informations suivantes dans la section Configuration de base.

Champ	Description
Contact système	Facultatif. Le contact principal du système StorageGRID , qui est renvoyé dans les messages SNMP sous la forme sysContact. Le contact système est généralement une adresse e-mail. Cette valeur s'applique à tous les nœuds du système StorageGRID . Contact système peut contenir jusqu'à 255 caractères.
Emplacement du système	Facultatif. L'emplacement du système StorageGRID , qui est renvoyé dans les messages SNMP sous la forme sysLocation. L'emplacement du système peut être n'importe quelle information utile pour identifier où se trouve votre système StorageGRID . Par exemple, vous pouvez utiliser l'adresse postale d'un établissement. Cette valeur s'applique à tous les nœuds du système StorageGRID . Emplacement du système peut contenir jusqu'à 255 caractères.
Activer les notifications de l'agent SNMP	• Si cette option est sélectionnée, l'agent SNMP StorageGRID envoie des notifications d'interruption et d'information. • Si cette option n'est pas sélectionnée, l'agent SNMP prend en charge l'accès MIB en lecture seule, mais il n'envoie aucune notification SNMP.
Activer les pièges d'authentification	Si cette option est sélectionnée, l'agent SNMP StorageGRID envoie des interruptions d'authentification s'il reçoit des messages de protocole mal authentifiés.

Entrez les chaînes de communauté

Si vous utilisez SNMPv1 ou SNMPv2c, complétez la section Chaînes de communauté.

Lorsque le système de gestion interroge le 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.

Étapes

1. Pour la **Communauté en lecture seule**, saisissez éventuellement une chaîne de communauté pour autoriser l'accès MIB en lecture seule sur les adresses d'agent IPv4 et IPv6.



Pour garantir la sécurité de votre système StorageGRID , n'utilisez pas « public » comme chaîne de communauté. Si vous laissez ce champ vide, l'agent SNMP utilise l'ID de grille de votre système StorageGRID comme chaîne de communauté.

Chaque chaîne de communauté peut comporter un maximum de 32 caractères et ne peut pas contenir de caractères d'espacement.

2. Sélectionnez **Ajouter une autre chaîne de communauté** pour ajouter des chaînes supplémentaires.

Jusqu'à cinq chaînes sont autorisées.

Créer des destinations de pièges

Utilisez l'onglet Destinations d'interruption dans la section Autres configurations pour définir une ou plusieurs destinations pour les notifications d'interruption ou d'information StorageGRID . Lorsque vous activez l'agent SNMP et sélectionnez **Enregistrer**, StorageGRID envoie des notifications à chaque destination définie lorsque des alertes sont déclenchées. Des notifications standard sont également envoyées pour les entités MIB-II prises en charge (par exemple, ifDown et coldStart).

Étapes

1. Pour le champ **Communauté d'interruption par défaut**, saisissez éventuellement la chaîne de communauté par défaut que vous souhaitez utiliser pour les destinations d'interruption SNMPv1 ou SNMPv2.

Si nécessaire, vous pouvez fournir une chaîne de communauté différente (« personnalisée ») lorsque vous définissez une destination d'interruption spécifique.

La communauté de pièges par défaut peut contenir un maximum de 32 caractères et ne peut pas contenir de caractères d'espacement.

2. Pour ajouter une destination de piège, sélectionnez **Créer**.
3. Sélectionnez la version SNMP qui sera utilisée pour cette destination de trap.
4. Remplissez le formulaire Créer une destination de piège pour la version que vous avez sélectionnée.

SNMPv1

Si vous avez sélectionné SNMPv1 comme version, remplissez ces champs.

Champ	Description
Type	Doit être Trap pour SNMPv1.
Hôte	Une adresse IPv4 ou IPv6 ou un nom de domaine complet (FQDN) pour recevoir le piège.
Port	Utilisez 162, qui est le port standard pour les interruptions SNMP, sauf si vous devez utiliser une autre valeur.
Protocole	Utilisez UDP, qui est le protocole de trappe SNMP standard, sauf si vous devez utiliser TCP.
Chaîne communautaire	Utilisez la communauté d'interruption par défaut, si elle a été spécifiée, ou entrez une chaîne de communauté personnalisée pour cette destination d'interruption. La chaîne de communauté personnalisée peut comporter au maximum 32 caractères et ne peut pas contenir d'espaces.

SNMPv2c

Si vous avez sélectionné SNMPv2c comme version, remplissez ces champs.

Champ	Description
Type	Si la destination sera utilisée pour les pièges ou les informations.
Hôte	Une adresse IPv4 ou IPv6 ou FQDN pour recevoir le piège.
Port	Utilisez 162, qui est le port standard pour les interruptions SNMP, sauf si vous devez utiliser une autre valeur.
Protocole	Utilisez UDP, qui est le protocole de trappe SNMP standard, sauf si vous devez utiliser TCP.
Chaîne communautaire	Utilisez la communauté d'interruption par défaut, si elle a été spécifiée, ou entrez une chaîne de communauté personnalisée pour cette destination d'interruption. La chaîne de communauté personnalisée peut comporter au maximum 32 caractères et ne peut pas contenir d'espaces.

SNMPv3

Si vous avez sélectionné SNMPv3 comme version, remplissez ces champs.

Champ	Description
Type	Si la destination sera utilisée pour les pièges ou les informations.
Hôte	Une adresse IPv4 ou IPv6 ou FQDN pour recevoir le piège.
Port	Utilisez 162, qui est le port standard pour les interruptions SNMP, sauf si vous devez utiliser une autre valeur.
Protocole	Utilisez UDP, qui est le protocole de trappe SNMP standard, sauf si vous devez utiliser TCP.
Utilisateur USM	L'utilisateur USM qui sera utilisé pour l'authentification. • Si vous avez sélectionné Trap, seuls les utilisateurs USM sans identifiant de moteur faisant autorité sont affichés. • Si vous avez sélectionné Informer, seuls les utilisateurs USM avec des ID de moteur faisant autorité sont affichés. • Si aucun utilisateur n'est affiché : i. Créez et enregistrez la destination du piège. ii. Aller à Créer des utilisateurs USM et créer l'utilisateur. iii. Revenez à l'onglet Destinations des pièges, sélectionnez la destination enregistrée dans le tableau et sélectionnez Modifier. iv. Sélectionnez l'utilisateur.

5. Sélectionnez **Créer**.

La destination du piège est créée et ajoutée à la table.

Créer des adresses d'agent

Vous pouvez également utiliser l'onglet Adresses des agents dans la section Autres configurations pour spécifier une ou plusieurs « adresses d'écoute ». Il s'agit des adresses StorageGRID sur lesquelles l'agent SNMP peut recevoir des requêtes.

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 .

Étapes

1. Sélectionnez **Créer**.
2. Saisissez les informations suivantes.

Champ	Description
Protocole Internet	Si cette adresse utilisera IPv4 ou IPv6. Par défaut, SNMP utilise IPv4.
Protocole de transport	Si cette adresse utilisera UDP ou TCP. Par défaut, SNMP utilise UDP.
Réseau StorageGRID	Sur quel réseau StorageGRID l'agent écoutera. • Réseaux Grid, Admin et Client : l'agent SNMP écoutera les requêtes sur les trois réseaux. • Réseau de grille • Réseau d'administration • Réseau de clients Remarque : si vous utilisez le réseau client pour des données non sécurisées et que vous créez une adresse d'agent pour le réseau client, sachez que le trafic SNMP sera également non sécurisé.
Port	En option, le numéro de port sur lequel l'agent SNMP doit écouter. Le port UDP par défaut pour un agent SNMP est 161, mais vous pouvez saisir n'importe quel numéro de port inutilisé. Remarque : 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.

3. Sélectionnez **Créer**.

L'adresse de l'agent est créée et ajoutée à la table.

Créer des utilisateurs USM

Si vous utilisez SNMPv3, utilisez l'onglet Utilisateurs USM dans la section Autres configurations pour définir les utilisateurs USM autorisés à interroger la MIB ou à recevoir des interruptions et des informations.



Les destinations SNMPv3 *inform* doivent avoir des utilisateurs avec des ID de moteur. La destination SNMPv3 *trap* ne peut pas avoir d'utilisateurs avec des ID de moteur.

Ces étapes ne s'appliquent pas si vous utilisez uniquement SNMPv1 ou SNMPv2c.

Étapes

1. Sélectionnez **Créer**.

2. Saisissez les informations suivantes.

Champ	Description
Nom d'utilisateur	Un nom unique pour cet utilisateur USM. Les noms d'utilisateur peuvent comporter un maximum de 32 caractères et ne peuvent pas contenir de caractères d'espacement. Le nom d'utilisateur ne peut pas être modifié une fois l'utilisateur créé.
Accès MIB en lecture seule	Si cette option est sélectionnée, cet utilisateur doit avoir un accès en lecture seule au MIB.
ID moteur faisant autorité	Si cet utilisateur doit être utilisé dans une destination d'information, l'ID du moteur faisant autorité pour cet utilisateur. Saisissez 10 à 64 caractères hexadécimaux (5 à 32 octets) sans espaces. Cette valeur est requise pour les utilisateurs USM qui seront sélectionnés dans les destinations d'interruption pour les informations. Cette valeur n'est pas autorisée pour les utilisateurs USM qui seront sélectionnés dans les destinations d'interruption pour les interruptions. Remarque : ce champ n'est pas affiché si vous avez sélectionné Accès MIB en lecture seule car les utilisateurs USM qui ont un accès MIB en lecture seule ne peuvent pas avoir d'ID de moteur.
Niveau de sécurité	Le niveau de sécurité pour l'utilisateur USM : • authPriv : Cet utilisateur communique avec authentification et 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 authentification et sans confidentialité (pas de cryptage). Vous devez spécifier un protocole d'authentification et un mot de passe.
Protocole d'authentification	Toujours défini sur SHA, qui est le seul protocole pris en charge (HMAC-SHA-96).
Mot de passe	Le mot de passe que cet utilisateur utilisera pour l'authentification.
Protocole de confidentialité	Affiché uniquement si vous avez sélectionné authPriv et toujours défini sur AES, qui est le seul protocole de confidentialité pris en charge.
Mot de passe	Affiché uniquement si vous avez sélectionné authPriv. Le mot de passe que cet utilisateur utilisera pour la confidentialité.

3. Sélectionnez **Créer**.

L'utilisateur USM est créé et ajouté à la table.

4. Une fois la configuration de l'agent SNMP terminée, sélectionnez **Enregistrer**.

La nouvelle configuration de l'agent SNMP devient active.

Mettre 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 êtes connecté au Grid Manager à l'aide d'un ["navigateur Web pris en charge"](#) .
- Vous avez le ["Autorisation d'accès root"](#) .

À propos de cette tâche

Voir ["Configurer l'agent SNMP"](#) pour plus de détails sur chaque champ de la page de l'agent SNMP. Vous devez sélectionner **Enregistrer** au bas de la page pour valider les modifications que vous apportez sur chaque onglet.

Étapes

1. Sélectionnez **CONFIGURATION > Surveillance > Agent SNMP**.

La page de l'agent SNMP apparaît.

2. Pour désactiver l'agent SNMP sur tous les nœuds de grille, décochez la case **Activer SNMP** et sélectionnez **Enregistrer**.

Si vous réactivez l'agent SNMP, tous les paramètres de configuration SNMP précédents sont conservés.

3. Vous pouvez également mettre à jour les informations dans la section Configuration de base :
 - a. Si nécessaire, mettez à jour le **Contact système** et l'**Emplacement du système**.
 - b. Vous pouvez également cocher ou décocher la case **Activer les notifications de l'agent SNMP** pour contrôler si l'agent SNMP StorageGRID envoie des notifications d'interruption et d'information.

Lorsque cette case à cocher est décochée, l'agent SNMP prend en charge l'accès MIB en lecture seule, mais il n'envoie pas de notifications SNMP.

- c. Vous pouvez également cocher ou décocher la case **Activer les interruptions d'authentification** pour contrôler si l'agent SNMP StorageGRID envoie des interruptions d'authentification lorsqu'il reçoit des messages de protocole incorrectement authentifiés.
4. Si vous utilisez SNMPv1 ou SNMPv2c, mettez à jour ou ajoutez éventuellement une **Communauté en lecture seule** dans la section Chaînes de communauté.
 5. Pour mettre à jour les destinations des interruptions, sélectionnez l'onglet Destinations des interruptions dans la section Autres configurations.

Utilisez cet onglet pour définir une ou plusieurs destinations pour les notifications d'interruption ou d'information StorageGRID . Lorsque vous activez l'agent SNMP et sélectionnez **Enregistrer**, StorageGRID envoie des notifications à chaque destination définie lorsque des alertes sont déclenchées. Des notifications standard sont également envoyées pour les entités MIB-II prises en charge (par exemple,

ifDown et coldStart).

Pour plus de détails sur ce qu'il faut saisir, voir ["Créer des destinations de pièges"](#) .

- Vous pouvez également mettre à jour ou supprimer la communauté de pièges par défaut.

Si vous supprimez la communauté de trap par défaut, vous devez d'abord vous assurer que toutes les destinations de trap existantes utilisent une chaîne de communauté personnalisée.

- Pour ajouter une destination de piège, sélectionnez **Créer**.
- Pour modifier une destination de piège, sélectionnez le bouton radio, puis sélectionnez **Modifier**.
- Pour supprimer une destination de piège, sélectionnez le bouton radio, puis sélectionnez **Supprimer**.
- Pour valider vos modifications, sélectionnez **Enregistrer** en bas de la page.

6. 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 ». Il s'agit des adresses StorageGRID sur lesquelles l'agent SNMP peut recevoir des requêtes.

Pour plus de détails sur ce qu'il faut saisir, voir ["Créer des adresses d'agent"](#) .

- Pour ajouter une adresse d'agent, sélectionnez **Créer**.
- Pour modifier l'adresse d'un agent, sélectionnez le bouton radio, puis sélectionnez **Modifier**.
- Pour supprimer une adresse d'agent, sélectionnez le bouton radio et sélectionnez **Supprimer**.
- Pour valider vos modifications, sélectionnez **Enregistrer** en bas de la page.

7. 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 le MIB ou à recevoir des interruptions et des informations.

Pour plus de détails sur ce qu'il faut saisir, voir ["Créer des utilisateurs USM"](#) .

- Pour ajouter un utilisateur USM, sélectionnez **Créer**.
- Pour modifier un utilisateur USM, sélectionnez le bouton radio, puis sélectionnez **Modifier**.

Le nom d'utilisateur d'un utilisateur USM existant ne peut pas être modifié. Si vous devez modifier un nom d'utilisateur, vous devez supprimer l'utilisateur et en créer un nouveau.



Si vous ajoutez ou supprimez l'ID de moteur faisant autorité d'un utilisateur et que cet utilisateur est actuellement sélectionné pour une destination, vous devez modifier ou supprimer la destination. Dans le cas contraire, une erreur de validation se produit lorsque vous enregistrez la configuration de l'agent SNMP.

- Pour supprimer un utilisateur USM, sélectionnez le bouton radio et sélectionnez **Supprimer**.



Si l'utilisateur que vous avez supprimé est actuellement sélectionné pour une destination d'interruption, vous devez modifier ou supprimer la destination. Dans le cas contraire, une erreur de validation se produit lorsque vous enregistrez la configuration de l'agent SNMP.

- Pour valider vos modifications, sélectionnez **Enregistrer** en bas de la page.

8. Une fois la configuration de l'agent SNMP mise à jour, sélectionnez **Enregistrer**.

Accéder aux fichiers MIB

Les fichiers MIB contiennent des définitions et des informations sur les propriétés des ressources et des 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 surveiller votre réseau.

Voir "[Utiliser la surveillance SNMP](#)" pour plus d'informations sur les fichiers SNMP et MIB.

Accéder aux fichiers MIB

Suivez ces étapes pour accéder aux fichiers MIB.

Étapes

1. Sélectionnez **CONFIGURATION > Surveillance > Agent SNMP**.
2. Sur la page de l'agent SNMP, sélectionnez le fichier que vous souhaitez télécharger :
 - **NETAPP-STORAGEGRID-MIB.txt**: Définit la table d'alerte et les notifications (traps) accessibles sur tous les nœuds d'administration.
 - **ES-NETAPP-06-MIB.mib**: Définit les objets et les notifications pour les appareils basés sur la série E.
 - **MIB_1_10.zip**: Définit les objets et les notifications pour les appliances avec une interface BMC .



Vous pouvez également accéder aux fichiers MIB à l'emplacement suivant sur n'importe quel nœud StorageGRID : `/usr/share/snmp/mibs`

3. Pour extraire les OID StorageGRID du fichier MIB :

- a. Obtenez l'OID de la racine du 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. Grep pour l'OID StorageGRID dans l'arbre entier (en utilisant `paste` pour joindre des lignes) :

```
root@user-adm1:~ # snmptranslate -Tso | paste -d " " - - | grep 28669
```



Le `snmptranslate` La commande dispose de nombreuses options utiles pour explorer le MIB. Cette commande est disponible sur n'importe quel nœud StorageGRID .

Contenu du fichier MIB

Tous les objets sont sous l'OID StorageGRID .

Nom de l'objet	ID d'objet (OID)	Description
		Le module MIB pour les entités NetApp StorageGRID .

objets MIB

Nom de l'objet	ID d'objet (OID)	Description
nombre d'alertes actives		Le nombre d'alertes actives dans activeAlertTable.
table d'alertes actives		Un tableau des alertes actives dans StorageGRID.
activeAlertId		L'ID de l'alerte. Unique dans l'ensemble actuel d'alertes actives.
activeAlertName		Le nom de l'alerte.
instance d'alerte active		Le nom de l'entité qui a généré l'alerte, généralement le nom du nœud.
gravité de l'alerte active		La gravité de l'alerte.
heure de début d'alerte active		La date et l'heure auxquelles l'alerte a été déclenchée.

Types de notifications (pièges)

Toutes les notifications incluent les variables suivantes en tant que varbinds :

- activeAlertId
- activeAlertName
- instance d'alerte active
- gravité de l'alerte active
- heure de début d'alerte active

Type de notification	ID d'objet (OID)	Description
alerte mineure active		Une alerte de gravité mineure
alerte majeure active		Une alerte de gravité majeure
alerte critique active		Une alerte de gravité critique

Collecter des données StorageGRID supplémentaires

Utiliser des tableaux et des graphiques

Vous pouvez utiliser des graphiques et des rapports pour surveiller l'état du système StorageGRID et résoudre les problèmes.

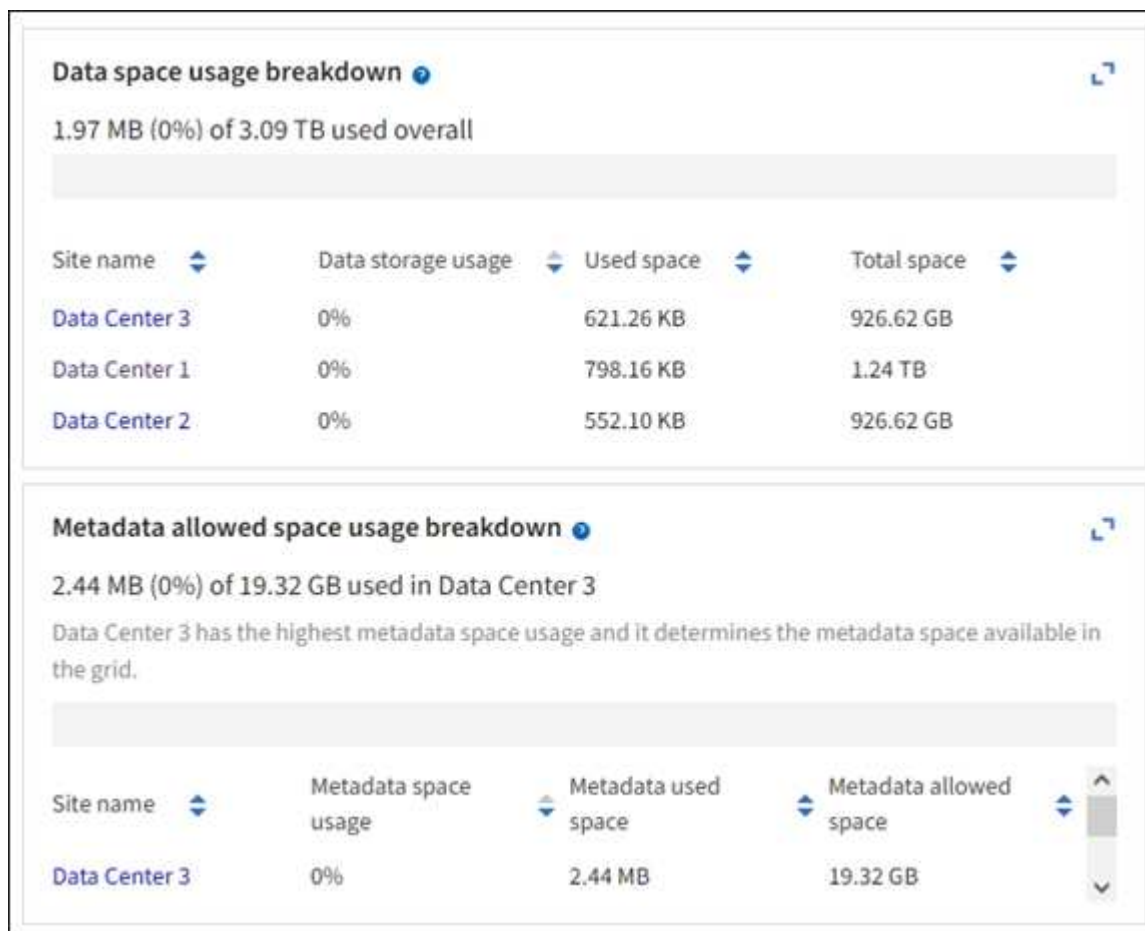


Le gestionnaire de grille est mis à jour à chaque version et peut ne pas correspondre aux exemples de captures d'écran sur cette page.

Types de graphiques

Les graphiques et diagrammes résument les valeurs des métriques et attributs StorageGRID spécifiques.

Le tableau de bord Grid Manager comprend des cartes qui résument le stockage disponible pour la grille et chaque site.



Le panneau d'utilisation du stockage sur le tableau de bord du gestionnaire de locataires affiche les éléments suivants :

- Une liste des plus grands buckets (S3) ou conteneurs (Swift) pour le locataire
- Un graphique à barres qui représente les tailles relatives des plus grands seaux ou conteneurs
- La quantité totale d'espace utilisé et, si un quota est défini, la quantité et le pourcentage d'espace restant

Dashboard

16 Buckets
[View buckets](#)

2 Platform services
endpoints
[View endpoints](#)

0 Groups
[View groups](#)

1 User
[View users](#)

Storage usage ?

6.5 TB of 7.2 TB used

0.7 TB (10.1%) remaining



Bucket name	Space used	Number of objects
Bucket-15	969.2 GB	913,425
Bucket-04	937.2 GB	576,806
Bucket-13	815.2 GB	957,389
Bucket-06	812.5 GB	193,843
Bucket-10	473.9 GB	583,245
Bucket-03	403.2 GB	981,226
Bucket-07	362.5 GB	420,726
Bucket-05	294.4 GB	785,190
8 other buckets	1.4 TB	3,007,036

Top buckets by capacity limit usage ?

Bucket name	Usage
Bucket-10	82%
Bucket-03	57%
Bucket-15	20%

Tenant details ?

Name: Tenant02

ID: 3341 1240 0546 8283 2208

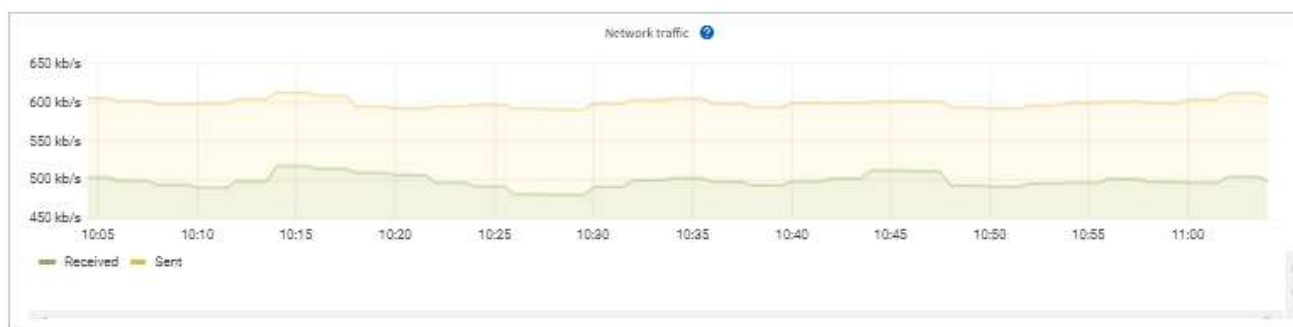
- ✓ Platform services enabled
- ✓ Can use own identity source
- ✓ S3 Select enabled

De plus, des graphiques montrant comment les métriques et les attributs StorageGRID évoluent au fil du temps sont disponibles sur la page Nœuds et sur 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 métriques Prometheus au fil du temps. Par exemple, l'onglet **NODES > Network** pour un nœud de stockage inclut un graphique Grafana pour le trafic réseau.

DC1-S2 (Storage Node)

[Overview](#)[Hardware](#)[Network](#)[Storage](#)[Objects](#)[ILM](#)[Tasks](#)[1 hour](#)[1 day](#)[1 week](#)[1 month](#)[Custom](#)

Network interfaces

Name	Hardware address	Speed	Duplex	Auto-negotiation	Link status
eth0	00:50:56:A7:E8:1D	10 Gigabit	Full	Off	Up

Network communication

Receive

Interface	Data	Packets	Errors	Dropped	Frame overruns	Frames
eth0	3.04 GB	20,403,428	0	24,899	0	0

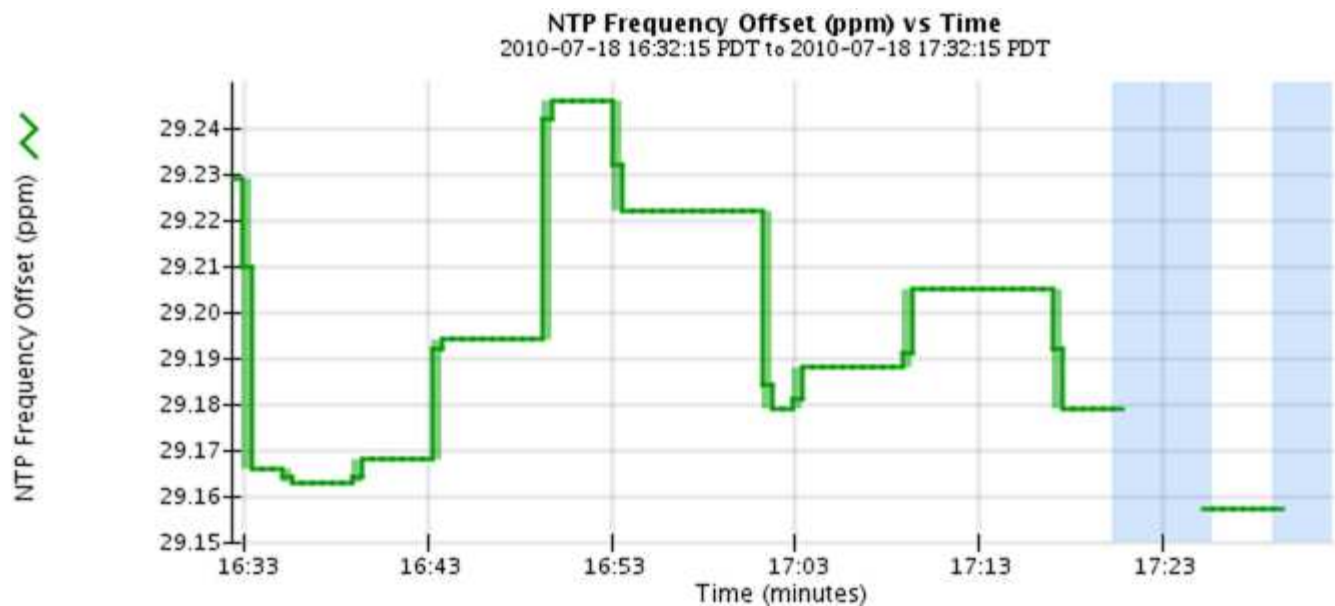
Transmit

Interface	Data	Packets	Errors	Dropped	Collisions	Carrier
eth0	3.65 GB	19,061,947	0	0	0	0

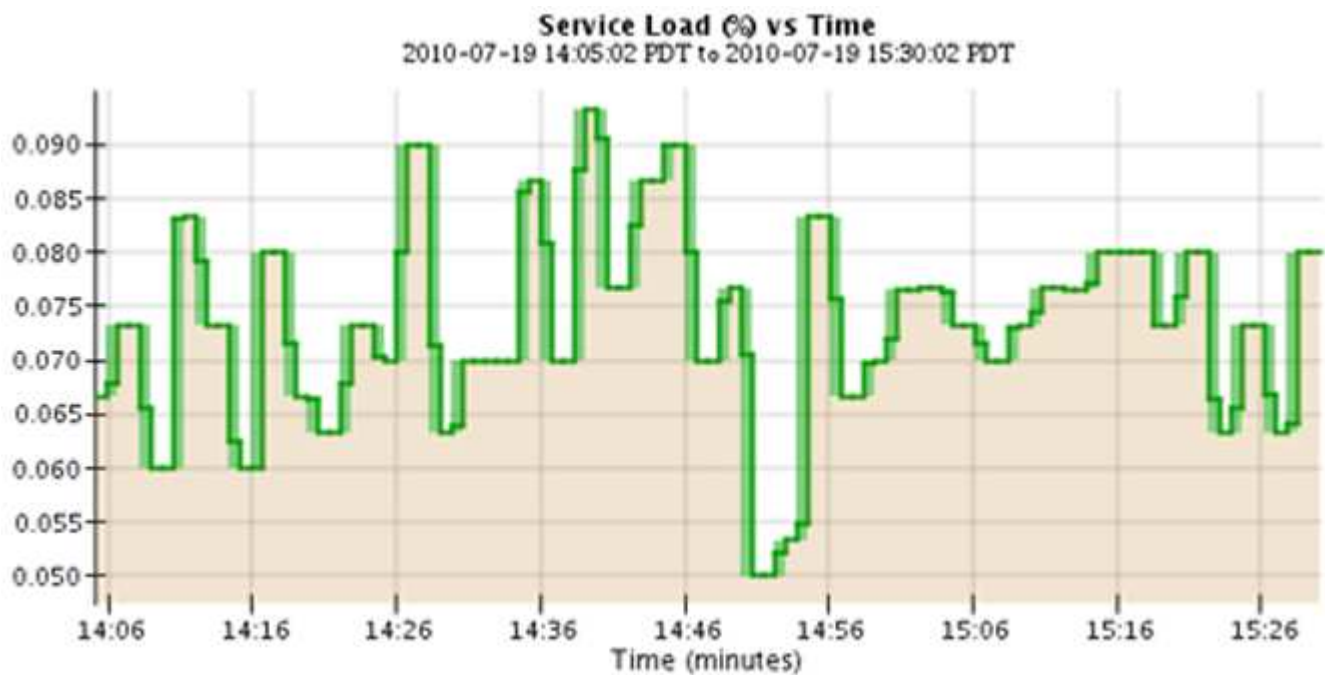


Les graphiques Grafana sont également inclus dans les tableaux de bord pré-construits disponibles sur la page **SUPPORT > Outils > Métriques**.

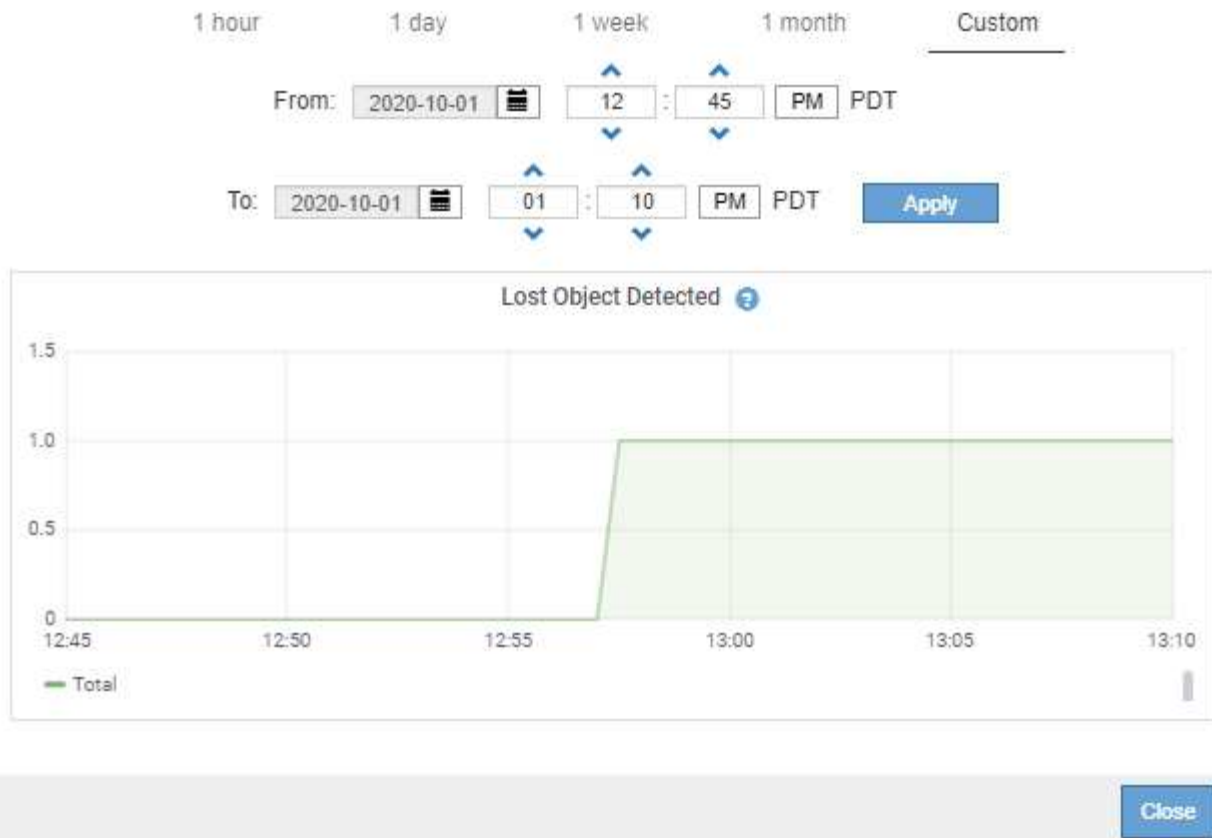
- **Graphiques linéaires** : Disponibles à partir de la page Nœuds et de la page **SUPPORT > Outils > Topologie de grille** (sélectionnez l'icône du graphique  (après une valeur de données), des graphiques linéaires sont utilisés pour tracer les valeurs des attributs StorageGRID qui ont une valeur unitaire (comme le décalage de fréquence NTP, en ppm). Les variations de valeur sont représentées dans des intervalles de données réguliers (bins) au fil du temps.



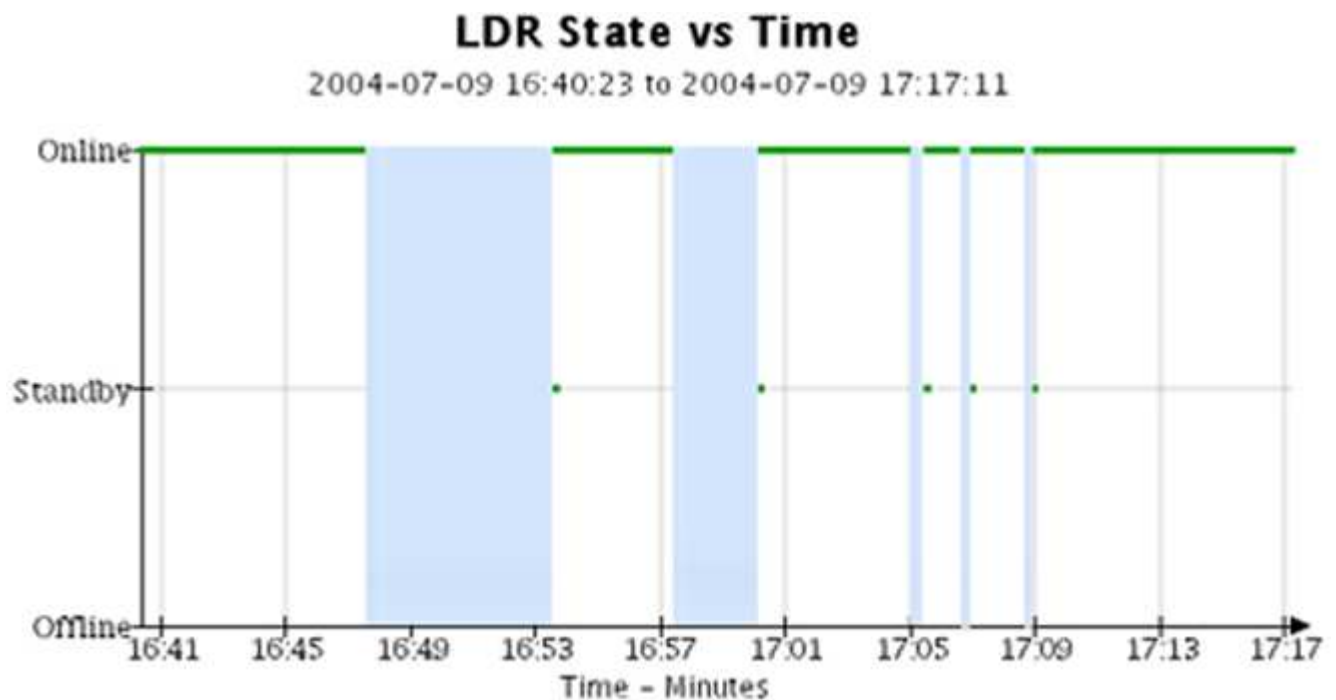
- **Graphiques de zone** : Disponibles à partir de la page Nœuds et de la page **SUPPORT > Outils > Topologie de grille** (sélectionnez l'icône du graphique ) (après une valeur de données), les graphiques de zone sont utilisés pour tracer des quantités d'attributs volumétriques, telles que le nombre d'objets ou les valeurs de charge de service. Les graphiques de surface sont similaires aux graphiques linéaires, mais incluent un ombrage marron clair sous la ligne. Les variations de valeur sont représentées dans des intervalles de données réguliers (bins) au fil du temps.



- Certains graphiques sont indiqués par un type d'icône de graphique différent  et ont un format différent :



- **Graphique d'état** : Disponible à partir de la page **SUPPORT > Outils > Topologie de grille** (sélectionnez l'icône du graphique  (après une valeur de données), les graphiques d'état sont utilisés pour tracer des valeurs d'attribut qui représentent des états distincts tels qu'un état de service qui peut être en ligne, en veille ou hors ligne. Les graphiques d'état sont similaires aux graphiques linéaires, mais la transition est discontinue ; c'est-à-dire que la valeur passe d'une valeur d'état à une autre.



- ["Afficher la page Nœuds"](#)
- ["Afficher l'arborescence de la topologie de la grille"](#)
- ["Examiner les mesures de support"](#)

Légende du graphique

Les lignes et les couleurs utilisées pour dessiner des cartes ont une signification spécifique.

Exemple	Signification
	Les valeurs d'attribut signalées sont tracées à l'aide de lignes vert foncé.
	Un ombrage vert clair autour des lignes vert foncé indique que les valeurs réelles dans cette plage de temps varient et ont été « regroupées » pour un traçage plus rapide. La ligne sombre représente la moyenne pondérée. La plage en vert clair indique les valeurs maximales et minimales dans le bac. Un ombrage marron clair est utilisé pour les graphiques de zone afin d'indiquer les données volumétriques.
	Les zones vides (aucune donnée tracée) indiquent que les valeurs d'attribut n'étaient 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-là étaient indéterminées ; l'attribut ne rapportait pas de valeurs car le service était dans un état inconnu.
	L'ombrage gris indique que certaines ou toutes les valeurs d'attribut à ce moment-là n'étaient pas connues car le service signalant les attributs était administrativement hors service.
	Un mélange de nuances grises et bleues indique que certaines des valeurs d'attribut à ce moment-là étaient indéterminées (car le service était dans un état inconnu), tandis que d'autres n'étaient pas connues car le service signalant les attributs était administrativement en panne.

Afficher des tableaux et des graphiques

La page Nœuds contient les graphiques et diagrammes auxquels vous devez accéder régulièrement pour surveiller des attributs tels que la capacité de stockage et le débit. Dans certains cas, notamment 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

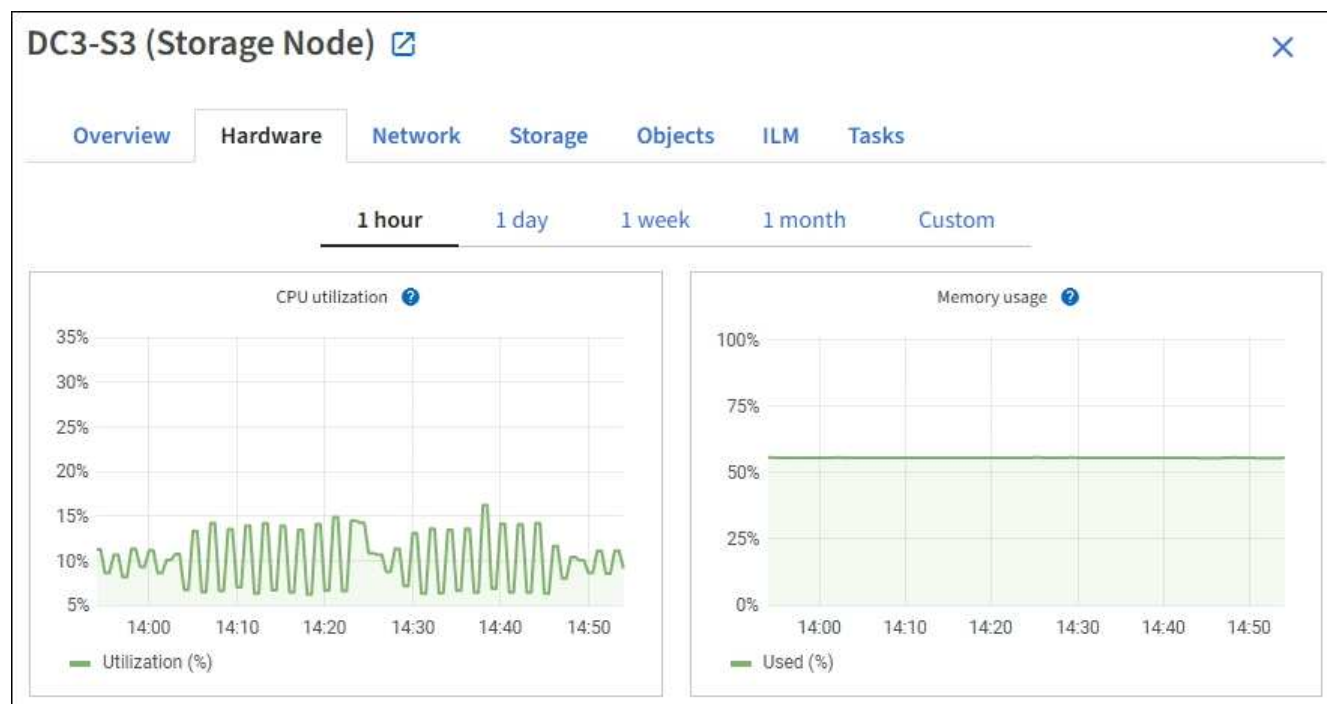
Vous devez être connecté au Grid Manager à l'aide d'un ["navigateur Web pris en charge"](#).

Étapes

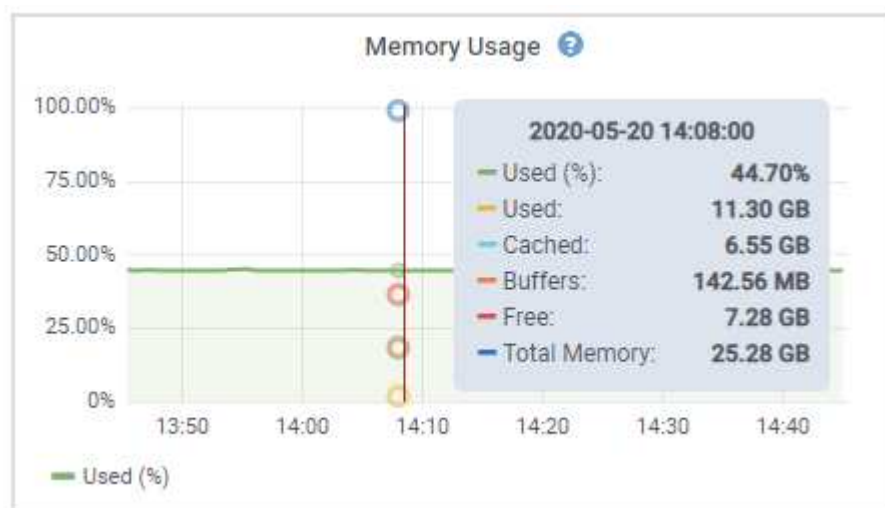
1. Sélectionnez **NODES**. Ensuite, sélectionnez un nœud, un site ou la grille entière.
2. Sélectionnez l'onglet pour lequel vous souhaitez afficher les informations.

Certains onglets incluent un ou plusieurs graphiques Grafana, qui sont utilisés pour tracer les valeurs des

métriques Prometheus au fil du temps. Par exemple, l'onglet **NODES > Hardware** pour un nœud inclut deux graphiques Grafana.



- Vous pouvez également positionner votre curseur sur le graphique pour voir des valeurs plus détaillées pour un moment précis.



- Selon les besoins, 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 métriques et tous les attributs.

Exemple 1 : Dans l'onglet Objets d'un nœud de stockage, vous pouvez sélectionner l'icône de graphique,  pour voir le nombre total de requêtes de stockage de métadonnées réussies pour le nœud de stockage.



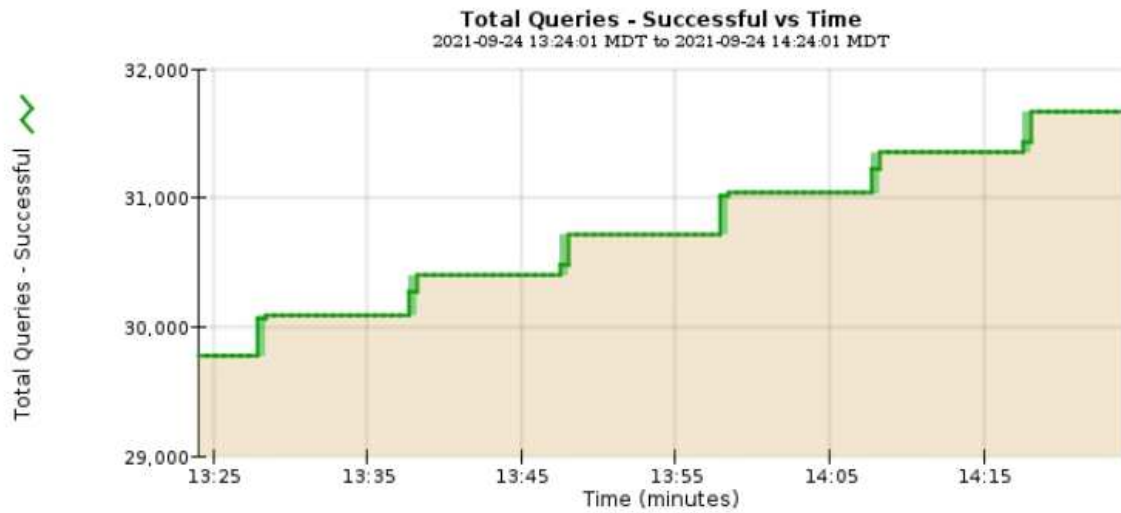
Reports (Charts): DDS (DC1-S1) - Data Store



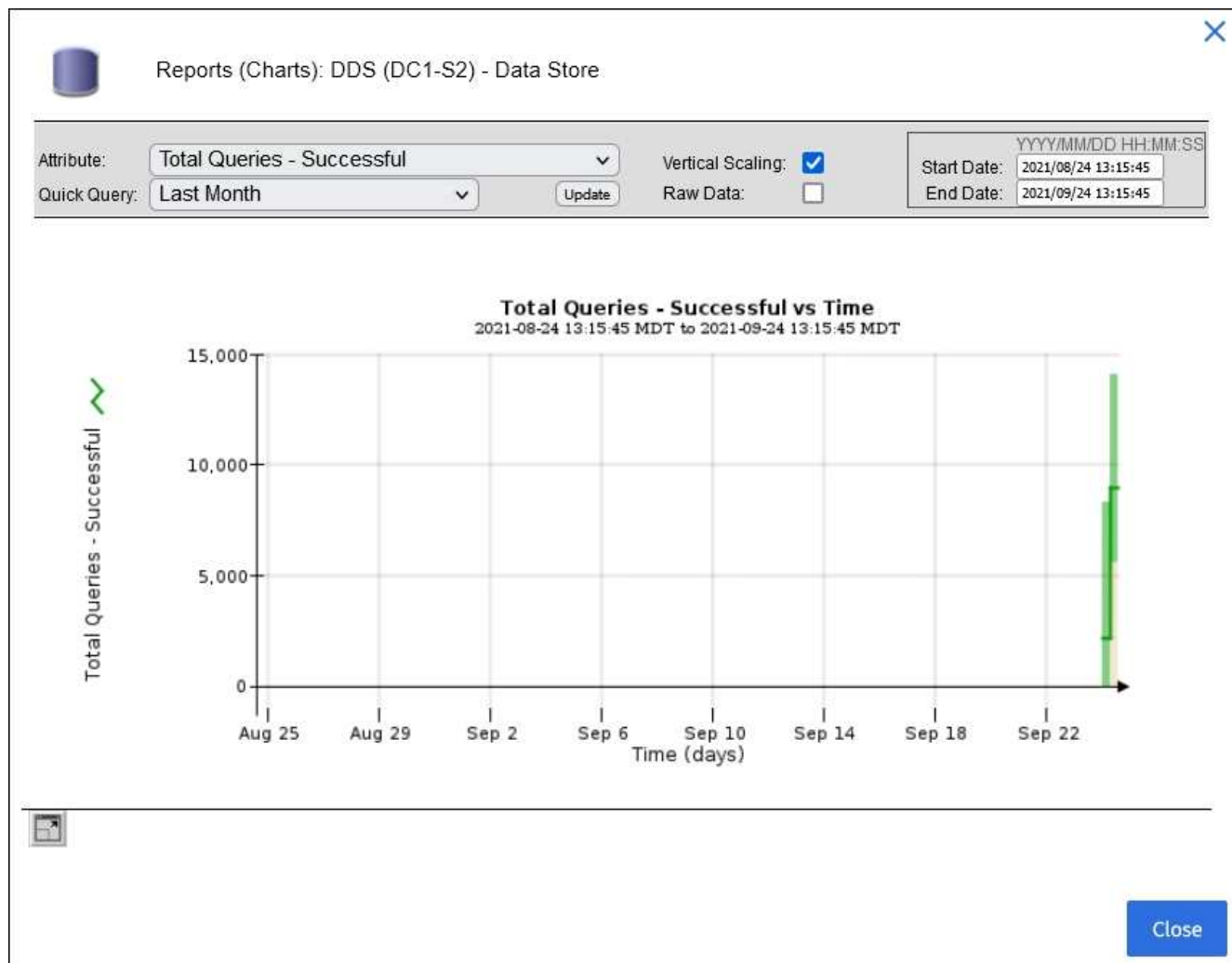
Attribute: Total Queries - Successful ▼
Quick Query: Last Hour ▼ Update

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



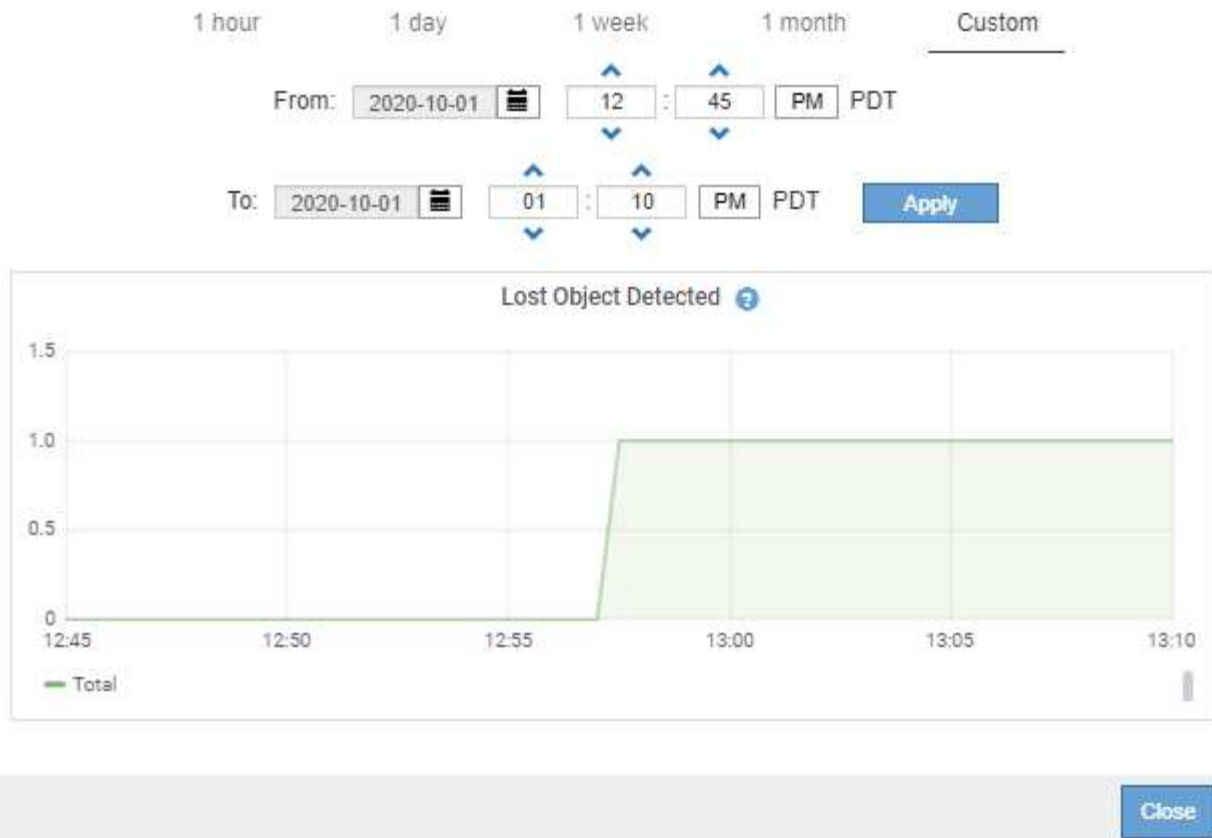
Close



Exemple 2 : Dans l'onglet Objets d'un nœud de stockage, vous pouvez sélectionner l'icône de graphique  pour voir le graphique Grafana du nombre d'objets perdus détectés au fil du temps.

Object Counts	
Total Objects	1
Lost Objects	1
S3 Buckets and Swift Containers	1





5. Pour afficher les graphiques des attributs qui ne sont pas affichés sur la page Nœud, sélectionnez **SUPPORT > Outils > Topologie de grille**.
6. Sélectionnez **nœud de grille > composant ou service > Aperçu > Principal**.

Overview

Alarms

Reports

Configuration

Main



Overview: SSM (DC1-ADM1) - Resources

Updated: 2018-05-07 16:29:52 MDT

Computational Resources

Service Restarts:	1	
Service Runtime:	6 days	
Service Uptime:	6 days	
Service CPU Seconds:	10666 s	
Service Load:	0.266 %	

Memory

Installed Memory:	8.38 GB	
Available Memory:	2.9 GB	

Processors

Processor Number	Vendor	Type	Cache
1	GenuineIntel	Intel(R) Xeon(R) CPU E5-2630 0 @ 2.30GHz	15 MiB
2	GenuineIntel	Intel(R) Xeon(R) CPU E5-2630 0 @ 2.30GHz	15 MiB
3	GenuineIntel	Intel(R) Xeon(R) CPU E5-2630 0 @ 2.30GHz	15 MiB
4	GenuineIntel	Intel(R) Xeon(R) CPU E5-2630 0 @ 2.30GHz	15 MiB
5	GenuineIntel	Intel(R) Xeon(R) CPU E5-2630 0 @ 2.30GHz	15 MiB
6	GenuineIntel	Intel(R) Xeon(R) CPU E5-2630 0 @ 2.30GHz	15 MiB
7	GenuineIntel	Intel(R) Xeon(R) CPU E5-2630 0 @ 2.30GHz	15 MiB
8	GenuineIntel	Intel(R) Xeon(R) CPU E5-2630 0 @ 2.30GHz	15 MiB

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 de la dernière journée.

Générer des graphiques

Les graphiques affichent une représentation graphique des valeurs des données d'attribut. Vous pouvez générer un rapport sur un site de centre de données, un nœud de grille, 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"](#).
- Tu as ["autorisations d'accès spécifiques"](#).

Étapes

1. Sélectionnez **SUPPORT > Outils > Topologie de grille**.
2. Sélectionnez **nœud de grille > composant ou service > Rapports > Graphiques**.
3. Sélectionnez l'attribut sur lequel générer le rapport dans la liste déroulante **Attribut**.
4. Pour forcer l'axe Y à démarrer à zéro, décochez la case **Mise à l'échelle verticale**.
5. Pour afficher les valeurs avec une précision totale, cochez la case **Données brutes** ou pour arrondir les

valeurs à un maximum de trois décimales (par exemple, pour les attributs indiqués sous forme de pourcentages), décochez la case **Données brutes**.

6. Sélectionnez la période sur laquelle porter le rapport dans la liste déroulante **Requête rapide**.

Sélectionnez l'option Requête personnalisée pour sélectionner une plage horaire spécifique.

Le graphique apparaît après quelques instants. Prévoyez quelques minutes pour la tabulation des plages de temps longues.

7. Si vous avez sélectionné Requête personnalisée, personnalisez la période du graphique en saisissant la **Date de début** et la **Date de fin**.

Utiliser le format `YYYY/MM/DDHH:MM:SS` en heure locale. Des zéros non significatifs sont requis pour correspondre au format. Par exemple, 2017/4/6 7:30:00 échoue à la validation. Le format correct est : 2017/04/06 07:30:00.

8. Sélectionnez **Mettre à jour**.

Un graphique est généré après quelques secondes. Prévoyez quelques minutes pour la tabulation des plages de temps longues. En fonction de la durée définie pour la requête, un rapport de texte brut ou un rapport de texte agrégé s'affiche.

Utiliser des rapports textuels

Les rapports textuels affichent une représentation textuelle des valeurs de données d'attribut qui ont été traitées par le service NMS. Il existe deux types de rapports générés en fonction de la période sur laquelle vous effectuez le rapport : les rapports de texte brut pour les périodes inférieures à une semaine et les rapports de texte agrégé pour les périodes supérieures à une semaine.

Rapports de texte brut

Un rapport de 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 d'échantillonnage : date et heure locales auxquelles une valeur d'attribut a été échantillonnée ou modifiée à la source.
- Valeur : valeur de l'attribut au moment de l'échantillonnage.

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 %

Rapports de texte agrégés

Un rapport de texte agrégé affiche des données sur une période plus longue (généralement une semaine) qu'un rapport de texte brut. Chaque entrée est le résultat de la synthèse de plusieurs valeurs d'attribut (un agrégat de valeurs d'attribut) par le service NMS au fil du temps dans 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 auxquelles le service NMS a agrégé (collecté) un ensemble de valeurs d'attribut modifiées.
- Valeur moyenne : la moyenne de la valeur de l'attribut sur la période agrégée.
- Valeur minimale : la valeur minimale sur la période agrégée.
- Valeur maximale : la valeur maximale sur la période 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 textuels

Les rapports textuels affichent une représentation textuelle des valeurs de données d'attribut qui ont été traitées par le service NMS. Vous pouvez générer un rapport sur un site de centre de données, un nœud de grille, 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](#).
- Tu as [autorisations d'accès spécifiques](#).

À propos de cette tâche

Pour les données d'attribut qui sont censées 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 basées sur des événements tels que des changements d'état ou de statut), 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 des périodes supérieures à une semaine.

Le texte gris indique que le service était administrativement hors service pendant la période d'échantillonnage. Le texte bleu indique que le service était dans un état inconnu.

Étapes

1. Sélectionnez **SUPPORT > Outils > Topologie de grille**.
2. Sélectionnez **nœud de grille > composant ou service > Rapports > Texte**.
3. Sélectionnez l'attribut sur lequel générer le rapport 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 indiqués sous forme de pourcentages), décochez la case **Données brutes**.
6. Sélectionnez la période sur laquelle porter le rapport dans la liste déroulante **Requête rapide**.

Sélectionnez l'option Requête personnalisée pour sélectionner une plage horaire spécifique.

Le rapport apparaît après quelques instants. Prévoyez quelques minutes pour la tabulation des plages de temps longues.

- Si vous avez sélectionné Requête personnalisée, vous devez personnaliser la période sur laquelle porter le rapport en saisissant la **Date de début** et la **Date de fin**.

Utiliser le format YYYY/MM/DDHH:MM:SS en heure locale. Des zéros non significatifs sont requis pour correspondre au format. Par exemple, 2017/4/6 7:30:00 échoue à la validation. Le format correct est : 2017/04/06 07:30:00.

- Cliquez sur **Mettre à jour**.

Un rapport texte est généré après quelques instants. Prévoyez quelques minutes pour la tabulation des plages de temps longues. En fonction de la durée définie pour la requête, un rapport de texte brut ou un rapport de texte agrégé s’affiche.

Exporter des rapports de texte

Les rapports de texte exportés ouvrent un nouvel onglet de navigateur, qui vous permet de sélectionner et de copier les données.

À propos de cette 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

- Sélectionnez **SUPPORT > Outils > Topologie de grille**.
- Créer un rapport texte.
- Cliquez sur *Exporter*  .

OverviewAlarmsReportsConfiguration

ChartsText

**Reports (Text): SSM (170-176) - Events**

Attribute: Attribute Send to Relay RateQuick Query: Custom QueryUpdate

Results Per Page: 5Raw Data: ☒

YYYY/MM/DD HH:MM:SSStart Date: 2010/07/19 08:42:09End Date: 2010/07/20 08:42:09

Text Results for Attribute Send to Relay Rate
2010-07-19 08:42:09 PDT To 2010-07-20 08:42:09 PDT

1 - 5 of 254 

Time Received	Sample Time	Value
2010-07-20 08:40:46	2010-07-20 08:40:46	0.274981485 Messages/s
2010-07-20 08:38:46	2010-07-20 08:38:46	0.274989 Messages/s
2010-07-20 08:36:46	2010-07-20 08:36:46	0.283317543 Messages/s
2010-07-20 08:34:46	2010-07-20 08:34:46	0.274982493 Messages/s
2010-07-20 08:32:46	2010-07-20 08:32:46	0.291646426 Messages/s

Previous « 1 2 3 4 5 » Next

La fenêtre Rapport d’exportation de texte s’ouvre et affiche le rapport.

Grid ID: 000 000
 OID: 2.16.124.113590.2.1.400019.1.1.1.1.16996732.200
 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 Rapport de texte d'exportation.

Ces données peuvent désormais être collées dans un document tiers tel qu'une feuille de calcul.

Surveiller les performances PUT et GET

Vous pouvez surveiller les performances de certaines opérations, telles que le stockage et la récupération d'objets, pour aider à identifier les modifications qui pourraient nécessiter une enquête plus approfondie.

À propos de cette tâche

Pour surveiller les performances PUT et GET, vous pouvez exécuter des commandes S3 directement depuis un poste de travail ou en utilisant l'application open source S3tester. L'utilisation de ces méthodes vous permet d'évaluer les performances indépendamment des facteurs externes à StorageGRID, tels que les problèmes avec une application cliente ou les problèmes avec un réseau externe.

Lorsque vous effectuez des tests d'opérations PUT et GET, utilisez les directives suivantes :

- Utilisez des tailles d'objet comparables à celles des objets que vous ingérez généralement dans votre grille.
- Effectuer des opérations sur des sites locaux et distants.

Messages dans le [journal d'audit](#) indique le temps total nécessaire pour exécuter certaines opérations. Par exemple, pour déterminer le temps de traitement total d'une requête S3 GET, vous pouvez consulter la valeur de l'attribut TIME dans le message d'audit SGET. Vous pouvez également trouver l'attribut TIME dans les messages d'audit pour les opérations S3 suivantes : DELETE, GET, HEAD, Metadata Updated, POST, PUT

Lors de l'analyse des résultats, examinez le temps moyen requis pour satisfaire une demande, ainsi que le débit global que vous pouvez atteindre. Répétez régulièrement les mêmes tests et enregistrez les résultats, afin de pouvoir identifier les tendances qui pourraient nécessiter une enquête.

- Tu peux "[télécharger S3tester depuis github](#)".

Surveiller les opérations de vérification des objets

Le système StorageGRID peut vérifier l'intégrité des données d'objet sur les nœuds de stockage, en recherchant les objets corrompus et manquants.

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 de maintenance ou root](#)".

À propos de cette tâche

Deux "[processus de vérification](#)" travailler ensemble pour garantir l'intégrité des données :

- **La vérification en arrière-plan** s'exécute automatiquement, vérifiant en permanence 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 de données d'objet répliquées et codées par effacement. Si des problèmes sont détectés, le système StorageGRID tente automatiquement de remplacer les données d'objet corrompues à partir de copies stockées ailleurs dans le système. La vérification en arrière-plan ne s'exécute pas 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 de l'objet** peut être déclenchée par un utilisateur pour vérifier plus rapidement l'existence (mais pas l'exactitude) des données de l'objet.

La vérification de l'existence de l'objet vérifie si toutes les copies répliquées attendues des objets et des fragments codés par effacement existent sur un nœud de stockage. La vérification de l'existence d'un objet fournit un moyen de vérifier l'intégrité des périphériques de stockage, en particulier si un problème matériel récent a pu affecter l'intégrité des données.

Vous devez examiner régulièrement les résultats des vérifications d'arrière-plan et des contrôles d'existence des objets. Enquêtez immédiatement sur tous les cas de données d'objet corrompues ou manquantes pour déterminer la cause première.

Étapes

1. Examiner les résultats des vérifications des antécédents :
 - a. Sélectionnez **NODES > Storage Node > Objects**.
 - b. Vérifiez les résultats de la vérification :
 - Pour vérifier la vérification des données d'objet répliquées, examinez les attributs dans la section Vérification.

Verification		
Status: ?	No errors	
Percent complete: ?	0.00%	
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	

- Pour vérifier la vérification des fragments codés par effacement, sélectionnez **Storage Node > ILM** et examinez les attributs dans la section Vérification du codage par effacement.

Erasure coding verification		
Status: ?	Idle	
Next scheduled: ?	2021-10-08 10:45:19 MDT	
Fragments verified: ?	0	
Data verified: ?	0 bytes	
Corrupt copies: ?	0	
Corrupt fragments: ?	0	
Missing fragments: ?	0	

Sélectionnez le point d'interrogation ? à côté du nom d'un attribut pour afficher un texte d'aide.

- Examinez les résultats des tâches de vérification de l'existence des objets :
 - Sélectionnez **MAINTENANCE > Vérification de l'existence de l'objet > Historique des tâches**.
 - Analysez la colonne Copies d'objets manquantes détectées. Si des tâches ont entraîné la perte de 100 copies d'objets ou plus et que l'alerte **Objets perdus** a été déclenchée, contactez le support technique.

Object existence check

Perform an object existence check if you suspect storage volumes have been damaged or are corrupt. You can verify that objects defined by your ILM policy, still exist on the volumes.

Active job

Job history

Delete

Search...

☐

Job ID ?

Status ?

Nodes (volumes) ?

Missing object copies detected ?

☐

15816859223101303015

Completed

DC2-S1 (3 volumes)

0

☐

12538643155010477372

Completed

DC1-S3 (1 volume)

0

☐

5490044849774982476

Completed

DC1-S2 (1 volume)

0

☐

3395284277055907678

Completed

DC1-S1 (3 volumes)
DC1-S2 (3 volumes)
DC1-S3 (3 volumes)
and 7 more

0

Surveiller les 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 enregistrés sur le serveur Syslog. Le message Dernier événement affiché dans le Gestionnaire de grille fournit plus d'informations sur l'événement le plus récent.

Les messages d'événements sont également répertoriés dans le `/var/local/log/bycast-err.log` fichier journal. Voir le ["Référence des fichiers journaux"](#).

L'alarme SMTT (Total des événements) 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'enquête sur les événements afin que vous puissiez mieux comprendre pourquoi ces alarmes se sont produites. Si un événement s'est produit en raison d'un problème connu, il est possible de réinitialiser les compteurs d'événements en toute sécurité.

Étapes

1. Passez en revue les événements système pour chaque nœud de grille :
 - a. Sélectionnez **SUPPORT > Outils > Topologie de grille**.
 - b. Sélectionnez **site > nœud de grille > SSM > Événements > Aperçu > Principal**.
2. Générez une liste de messages d'événements précédents pour aider à isoler les problèmes survenus dans

le passé :

- Sélectionnez **SUPPORT > Outils > Topologie de grille.**
- Sélectionnez **site > nœud de grille > SSM > Événements > Rapports.**
- Sélectionnez **Texte.**

L'attribut **Dernier événement** n'est pas affiché dans le "vue des graphiques" . Pour le voir :

- Changez **Attribut** en **Dernier événement.**
- Vous pouvez également sélectionner une période pour la **Requête rapide.**
- Sélectionnez **Mettre à jour.**

Time Received	Sample Time	Value
2009-04-15 15:24:22	2009-04-15 15:24:22	hdc: task_no_data_intr: status=0x51 { DriveReady SeekComplete Error }
2009-04-15 15:24:11	2009-04-15 15:23:39	hdc: task_no_data_intr: status=0x51 { DriveReady SeekComplete Error }

Créer des événements syslog personnalisés

Les événements personnalisés vous permettent de suivre tous les événements utilisateur de niveau noyau, démon, erreur et critique enregistrés 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 pannes matérielles).

À propos de cette tâche

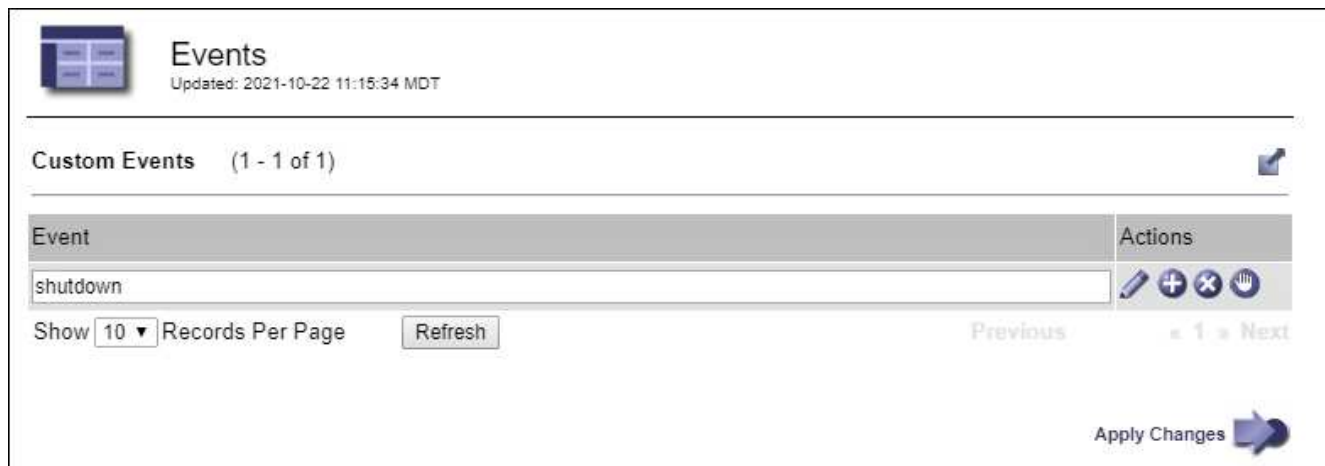
Envisagez de créer des événements personnalisés pour surveiller les problèmes récurrents. Les considérations suivantes s'appliquent aux événements personnalisés.

- Une fois qu'un événement personnalisé est créé, chaque occurrence de celui-ci est surveillée.
- Pour créer un événement personnalisé basé sur des mots-clés dans le `/var/local/log/messages` fichiers, les journaux dans 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 énoncées ci-dessus.

Étapes

1. Sélectionnez **SUPPORT > Alarmes (héritées) > Événements personnalisés**.
2. Cliquez sur *Modifier*  (ou *Insérer*  si ce n'est pas le premier événement).
3. Saisissez une chaîne d'événement personnalisée, par exemple, arrêt



Events
Updated: 2021-10-22 11:15:34 MDT

Custom Events (1 - 1 of 1)

Event	Actions
shutdown	   

Show 10 Records Per Page Refresh Previous « 1 » Next

Apply Changes 

4. Sélectionnez **Appliquer les modifications**.
5. Sélectionnez **SUPPORT > Outils > Topologie de grille**.
6. Sélectionnez **nœud de grille > SSM > Événements**.
7. Recherchez l'entrée pour les événements personnalisés dans la table Événements et surveillez la valeur de **Count**.

Si le nombre augmente, un événement personnalisé que vous surveillez est déclenché sur ce nœud de grille.

OverviewAlarmsReportsConfiguration

Main



Overview: SSM (DC1-ADM1) - Events

Updated: 2021-10-22 11:19:18 MDT

System Events

Log Monitor State:Connected

Total Events:0

Last Event:No Events

Description	Count
Abnormal Software Events	0
Account Service Events	0
Cassandra Errors	0
Cassandra Heap Out Of Memory Errors	0
Chunk Service Events	0
Custom Events	0
Data-Mover Service Events	0
File System Errors	0
Forced Termination Events	0
Grid Node Errors	0
Hotfix Installation Failure Events	0
I/O Errors	0
IDE Errors	0
Identity Service Events	0
Kernel Errors	0
Kernel Memory Allocation Failure	0
Keystone Service Events	0
Network Receive Errors	0
Network Transmit Errors	0
Out Of Memory Errors	0
Replicated State Machine Service Events	0
SCSI Errors	0

Réinitialiser le nombre d'événements personnalisés à zéro

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 provoque le déclenchement de l'alarme par l'événement suivant. En revanche, lorsque vous reconnaissez une alarme, celle-ci n'est redéclenchée que si le niveau de seuil suivant est atteint.

Étapes

1. Sélectionnez **SUPPORT > Outils > Topologie de grille**.
2. Sélectionnez **nœud de grille > SSM > Événements > Configuration > Principal**.
3. Cochez la case **Réinitialiser** pour les événements personnalisés.

Overview

Alarms

Reports

Configuration

Main

Alarms



Configuration: SSM (DC2-ADM1) - Events

Updated: 2018-04-11 10:35:44 MDT

Description	Count	Reset
Abnormal Software Events	0	☐
Account Service Events	0	☐
Cassandra Errors	0	☐
Cassandra Heap Out Of Memory Errors	0	☐
Custom Events	0	☒
File System Errors	0	☐
Forced Termination Events	0	☐

4. Sélectionnez **Appliquer les modifications**.

Examiner les messages d'audit

Les messages d'audit peuvent vous aider à mieux comprendre les opérations détaillées 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 du système sont liés au système d'audit lui-même, aux états des nœuds de grille, à l'activité des tâches à l'échelle du système et aux opérations de sauvegarde de service.
- Les messages d'audit du stockage d'objets sont liés au stockage et à la gestion des objets dans StorageGRID, y compris le stockage et les récupérations d'objets, les transferts de nœud de grille à nœud de grille et les vérifications.
- Les messages d'audit de lecture et d'écriture du client sont enregistrés lorsqu'une application client S3 effectue une demande de création, de modification ou de récupération d'un objet.
- Les messages d'audit de gestion enregistrent les demandes des utilisateurs adressées à 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.

Vous pouvez accéder aux fichiers journaux d'audit directement à partir de la ligne de commande du nœud d'administration.

StorageGRID peut envoyer des informations d'audit par défaut, ou vous pouvez modifier la destination :

- StorageGRID utilise par défaut les destinations d'audit des nœuds locaux.
- Les entrées du journal d'audit de Grid Manager et de Tenant Manager peuvent être envoyées à un nœud

de stockage.

- En option, vous pouvez modifier la destination des journaux d'audit et envoyer les informations d'audit à un serveur syslog externe. Les journaux locaux des enregistrements d'audit continuent d'être générés et stockés lorsqu'un serveur syslog externe est configuré.
- ["En savoir plus sur la configuration des messages d'audit et des 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, consultez ["Examiner les journaux d'audit"](#) .

Collecter les fichiers journaux et les données système

Vous pouvez utiliser Grid Manager 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"](#) .
- Tu as ["autorisations d'accès spécifiques"](#) .
- Vous devez disposer de la phrase secrète de provisionnement.

À propos de cette tâche

Vous pouvez utiliser le gestionnaire de grille pour collecter ["fichiers journaux"](#) , les données système et les données de configuration de n'importe quel nœud de grille pour la période que vous sélectionnez. Les données sont collectées et archivées dans un fichier .tar.gz que vous pouvez ensuite télécharger sur votre ordinateur local.

En option, vous pouvez modifier la destination des journaux d'audit et envoyer les informations d'audit à un serveur syslog externe. Les journaux locaux des enregistrements d'audit continuent d'être générés et stockés lorsqu'un serveur syslog externe est configuré. Voir ["Configurer 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.

Selon vos besoins, vous pouvez collecter des fichiers journaux pour l'ensemble de la grille ou pour l'ensemble d'un site de centre de données.

3. Sélectionnez une **Heure de début** et une **Heure de fin** pour définir la plage horaire des données à inclure dans les fichiers journaux.

Si vous sélectionnez une période très longue ou collectez les journaux de tous les nœuds d'une grande grille, l'archive des journaux peut devenir trop volumineuse pour être stockée sur un nœud ou trop volumineuse pour être collectée sur le nœud d'administration principal pour téléchargement. Si cela se produit, vous devez redémarrer la collecte des journaux avec un ensemble de données plus petit.

4. Sélectionnez les types de journaux que vous souhaitez collecter.

- **Journaux d'application** : journaux spécifiques aux applications 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 du réseau.
- **Base de données Prometheus** : métriques de séries chronologiques provenant des services sur tous les nœuds.

5. Vous pouvez également saisir des notes sur les fichiers journaux que vous collectez dans la zone de texte **Notes**.

Vous pouvez utiliser ces notes pour fournir au support technique des informations sur le problème qui vous a incité à collecter les fichiers journaux. Vos notes sont ajoutées à un fichier appelé `info.txt`, ainsi que d'autres informations sur la collecte de fichiers journaux. Le `info.txt` le fichier est enregistré dans le package d'archive du fichier journal.

6. Saisissez la phrase secrète de provisionnement de votre système StorageGRID dans la zone de texte **Phrase secrète 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 grille.

Si vous recevez un message d'erreur concernant la taille du journal, essayez de collecter les journaux pendant une période plus courte ou pour moins de nœuds.

8. Sélectionnez **Télécharger** lorsque la collecte du fichier journal est terminée.

Le fichier `.tar.gz` contient tous les fichiers journaux de tous les nœuds de grille où la collecte des journaux a réussi. À l'intérieur du fichier combiné `.tar.gz`, il y a une archive de fichier journal pour chaque nœud de grille.

Après avoir terminé

Vous pouvez retélécharger le package d'archive du fichier journal ultérieurement si vous en avez besoin.

En option, vous pouvez sélectionner **Supprimer** pour supprimer le package d'archive du fichier journal et libérer de l'espace disque. Le package d'archive de fichiers journaux actuel est automatiquement supprimé la prochaine fois que vous collectez des fichiers journaux.

Déclencher manuellement un package AutoSupport

Pour aider le support technique à résoudre les problèmes liés à votre système StorageGRID, vous pouvez déclencher manuellement l'envoi d'un package AutoSupport

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 root ou de l'autorisation de configuration d'une autre grille.

Étapes

1. Sélectionnez **SUPPORT > Outils > * AutoSupport***.
2. Dans l'onglet **Actions**, sélectionnez **Envoyer AutoSupport déclenchée par l'utilisateur**.

StorageGRID tente d'envoyer un package AutoSupport au site de support NetApp. Si la tentative réussit, les valeurs **Résultat le plus récent** et **Dernière heure de réussite** dans l'onglet **Résultats** sont mises à jour. En cas de problème, la valeur **Résultat le plus récent** est mise à jour sur « Échec » et StorageGRID n'essaie pas d'envoyer à nouveau le package AutoSupport.

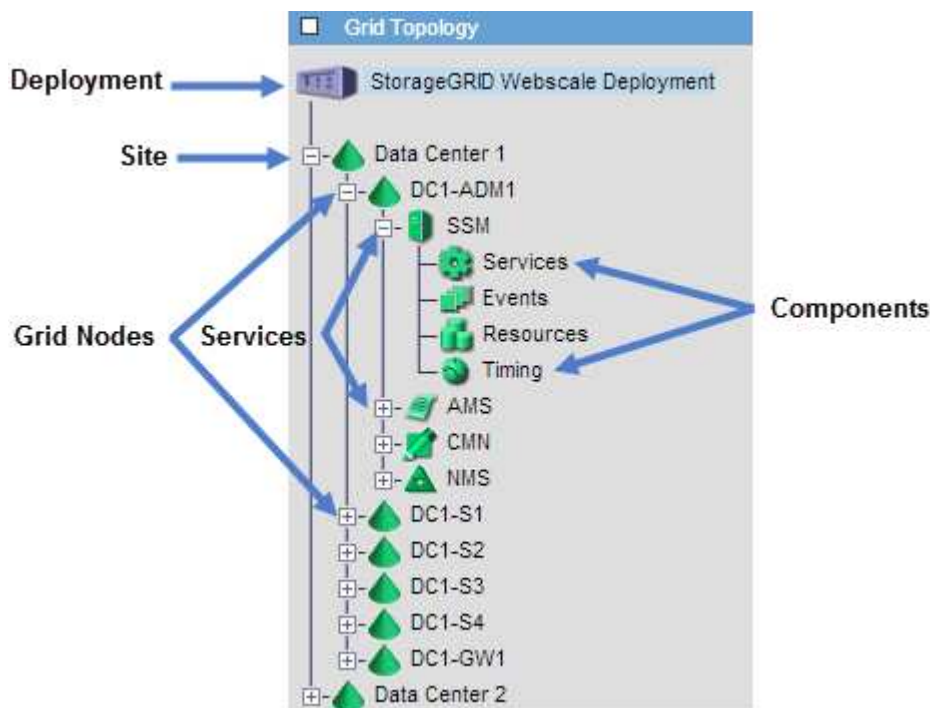


Après avoir envoyé un package AutoSupport déclenché par l'utilisateur, actualisez la page AutoSupport dans votre navigateur après 1 minute pour accéder aux résultats les plus récents.

Afficher l'arborescence de la topologie de la grille

L'arborescence de topologie de grille donne accès à des informations détaillées sur les éléments du système StorageGRID , notamment les sites, les nœuds de grille, les services et les composants. Dans la plupart des cas, vous n'avez besoin d'accéder à l'arborescence de la topologie de la grille que lorsque cela est indiqué dans la documentation ou lorsque vous travaillez avec le support technique.

Pour accéder à l'arborescence de 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 du site, du nœud ou du service. Pour développer ou réduire tous les éléments de l'ensemble du site ou de chaque nœud, maintenez la touche **<Ctrl>** enfoncée et cliquez.

Attributs StorageGRID

Les attributs signalent les valeurs et les statuts de nombreuses fonctions du système StorageGRID . Les 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 Grid Manager :

- **Page Nœuds** : de nombreuses valeurs affichées sur la page Nœuds sont des attributs StorageGRID . (Les métriques Prometheus sont également affichées sur les pages Nœuds.)
- **Arborescence de topologie de grille** : les valeurs d'attribut sont affichées dans l'arborescence de topologie de grille (**SUPPORT > Outils > Topologie de grille**).
- **Événements** : des événements système se produisent lorsque certains attributs enregistrent une condition

d'erreur ou de défaut pour un nœud, y compris des erreurs telles que des erreurs réseau.

Valeurs d'attribut

Les attributs sont rapportés dans la mesure du possible et sont approximativement corrects. Les mises à jour d'attributs peuvent être perdues dans certaines circonstances, comme le crash d'un service ou l'échec et la reconstruction d'un nœud de grille.

De plus, les délais de propagation peuvent ralentir la génération de rapports sur les attributs. Les valeurs mises à jour pour la plupart des attributs sont envoyées au système StorageGRID à intervalles fixes. Il peut s'écouler plusieurs minutes 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.

Examiner les mesures de support

Lors du dépannage d'un problème, vous pouvez travailler avec le support technique pour examiner les métriques et les graphiques détaillés de votre système StorageGRID .

Avant de commencer

- Vous devez être connecté au Grid Manager à l'aide d'un [navigateur Web pris en charge](#) .
- Tu as ["autorisations d'accès spécifiques"](#) .

À propos de cette tâche

La page Métriques vous permet d'accéder aux interfaces utilisateur de Prometheus et Grafana. Prometheus est un logiciel open source de collecte de métriques. Grafana est un logiciel open source de visualisation de métriques.



Les outils disponibles sur la page Métriques sont destinés à être utilisés par le support technique. Certaines fonctionnalités et éléments de menu de ces outils sont intentionnellement non fonctionnels et sont susceptibles d'être modifiés. Voir la liste des ["métriques Prometheus couramment utilisées"](#) .

Étapes

1. Comme indiqué par le support technique, sélectionnez **SUPPORT > Outils > Métriques**.

Un exemple de la page Métriques est présenté ici :

Metrics

Access charts and metrics to help troubleshoot issues.

 The tools available on this page are intended for use by technical support. Some features and menu items within these tools are intentionally non-functional.

Prometheus

Prometheus is an open-source toolkit for collecting metrics. The Prometheus interface allows you to query the current values of metrics and to view charts of the values over time.

Access the Prometheus UI using the link below. You must be signed in to the Grid Manager.

- [https://\[redacted\]](https://[redacted])

Grafana

Grafana is open-source software for metrics visualization. The Grafana interface provides pre-constructed dashboards that contain graphs of important metric values over time.

Access the Grafana dashboards using the links below. You must be signed in to the Grid Manager.

ADE	EC Overview	Replicated Read Path Overview
Account Service Overview	Grid	S3 - Node
Alertmanager	ILM	S3 Overview
Audit Overview	Identity Service Overview	S3 Select
Cassandra Cluster Overview	Ingests	Site
Cassandra Network Overview	Node	Support
Cassandra Node Overview	Node (Internal Use)	Traces
Cross Grid Replication	OSL - AsyncIO	Traffic Classification Policy
Cloud Storage Pool Overview	Platform Services Commits	Usage Processing
EC - ADE	Platform Services Overview	Virtual Memory (vmstat)
EC - Chunk Service	Platform Services Processing	

-
2. Pour interroger les valeurs actuelles des métriques StorageGRID et afficher les graphiques des valeurs au fil du temps, cliquez sur le lien dans la section Prometheus.

L'interface Prometheus apparaît. Vous pouvez utiliser cette interface pour exécuter des requêtes sur les métriques StorageGRID disponibles et pour représenter graphiquement les métriques StorageGRID au fil du temps.



Les métriques qui incluent *private* dans leurs noms sont destinées à un usage interne uniquement et sont susceptibles d'être modifiées entre les versions de StorageGRID sans préavis.

-
-
3. Pour accéder aux tableaux de bord pré-construits contenant des graphiques des métriques StorageGRID au fil du temps, cliquez sur les liens dans la section Grafana.

L'interface Grafana pour le lien que vous avez sélectionné apparaît.



Exécuter les diagnostics

Lors du dépannage d'un problème, vous pouvez travailler avec le support technique pour exécuter des diagnostics sur votre système StorageGRID et examiner les résultats.

- ["Examiner les mesures de support"](#)
- ["Métriques Prometheus couramment utilisées"](#)

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un ["navigateur Web pris en charge"](#).
- Tu as ["autorisations d'accès spécifiques"](#).

À propos de cette tâche

La page Diagnostics effectue un ensemble de vérifications de diagnostic sur l'état actuel de la grille. Chaque contrôle de diagnostic peut avoir l'un des trois statuts suivants :

-

✓ **Normal** : Toutes les valeurs sont dans la plage normale.

• ⚠ **Attention** : Une ou plusieurs valeurs sont en dehors de la plage normale.

• ✖ **Attention** : Une ou plusieurs valeurs sont significativement en dehors de la plage normale.

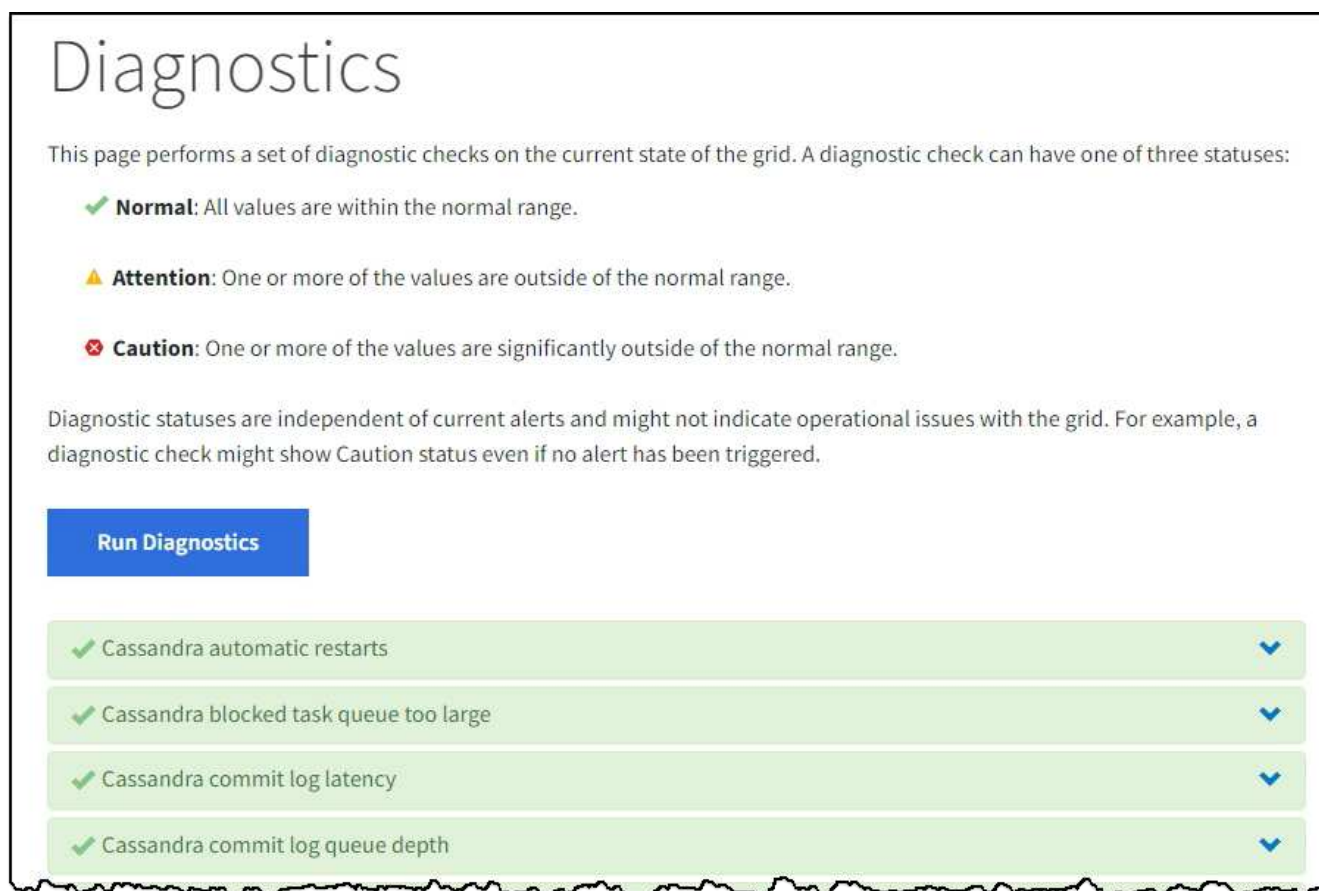
Les états de diagnostic sont indépendants des alertes actuelles et peuvent ne pas indiquer de problèmes opérationnels avec le réseau. Par exemple, un contrôle de diagnostic peut afficher le statut Attention même si aucune alerte n'a été déclenchée.

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 Normal). Au sein de chaque gravité, les résultats sont triés par ordre alphabétique.

Dans cet exemple, tous les diagnostics ont un statut Normal.



The screenshot shows a web interface titled "Diagnostics". Below the title, a paragraph explains that the page performs diagnostic checks on the current state of the grid and that checks can have one of three statuses: Normal, Attention, or Caution. Each status is accompanied by a small icon and a brief description. Below this explanation is a blue button labeled "Run Diagnostics". Underneath the button is a list of four diagnostic checks, each in a light green box with a green checkmark icon on the left and a blue downward arrow on the right. The checks are: "Cassandra automatic restarts", "Cassandra blocked task queue too large", "Cassandra commit log latency", and "Cassandra commit log queue depth".

Diagnostics

This page performs a set of diagnostic checks on the current state of the grid. A diagnostic check can have one of three statuses:

- ✓ **Normal:** All values are within the normal range.
- ⚠ **Attention:** One or more of the values are outside of the normal range.
- ✖ **Caution:** One or more of the values are significantly outside of the normal range.

Diagnostic statuses are independent of current alerts and might not indicate operational issues with the grid. For example, a diagnostic check might show Caution status even if no alert has been triggered.

Run Diagnostics

- ✓ Cassandra automatic restarts
- ✓ Cassandra blocked task queue too large
- ✓ Cassandra commit log latency
- ✓ Cassandra commit log queue depth

2. Pour en savoir plus sur un diagnostic spécifique, cliquez n'importe où sur la ligne.

Les détails sur le diagnostic et ses résultats actuels s'affichent. Les détails suivants sont répertoriés :

- **Statut** : L'état actuel de ce diagnostic : Normal, Attention ou Attention.
- **Requête Prometheus** : si elle est utilisée 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

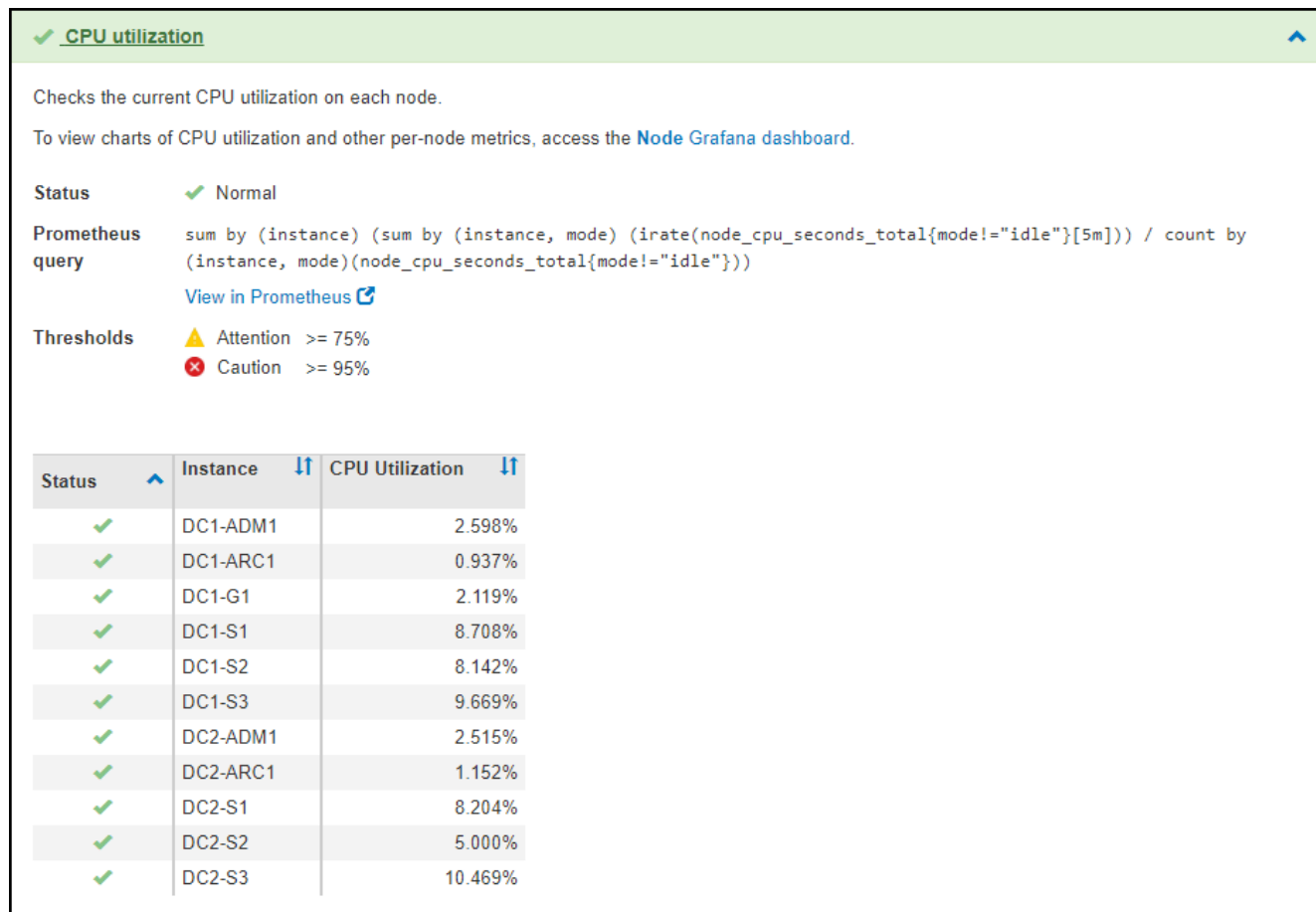
diagnostics.)

- **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** : un 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 affichée. Toutes les valeurs des nœuds sont inférieures aux seuils d'attention et de prudence, donc l'état global du diagnostic est Normal.



3. **Facultatif** : Pour voir les graphiques Grafana liés à ce diagnostic, cliquez sur le lien **Tableau de bord Grafana**.

Ce lien n'est pas affiché pour tous les diagnostics.

Le tableau de bord Grafana associé apparaît. Dans cet exemple, le tableau de bord du nœud s'affiche, affichant l'utilisation du processeur au fil du temps pour ce nœud ainsi que d'autres graphiques Grafana pour le nœud.



Vous pouvez également accéder aux tableaux de bord Grafana pré-construits à partir de la section Grafana de la page **SUPPORT > Outils > Métriques**.



4. **Facultatif** : Pour voir 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 apparaît.

☐ Enable query history

```
sum by (instance) (sum by (instance, mode) (irate(node_cpu_seconds_total{mode!="idle"}[5m])) / count by (instance, mode))
```

Load time: 547ms
Resolution: 14s
Total time series: 13

Execute

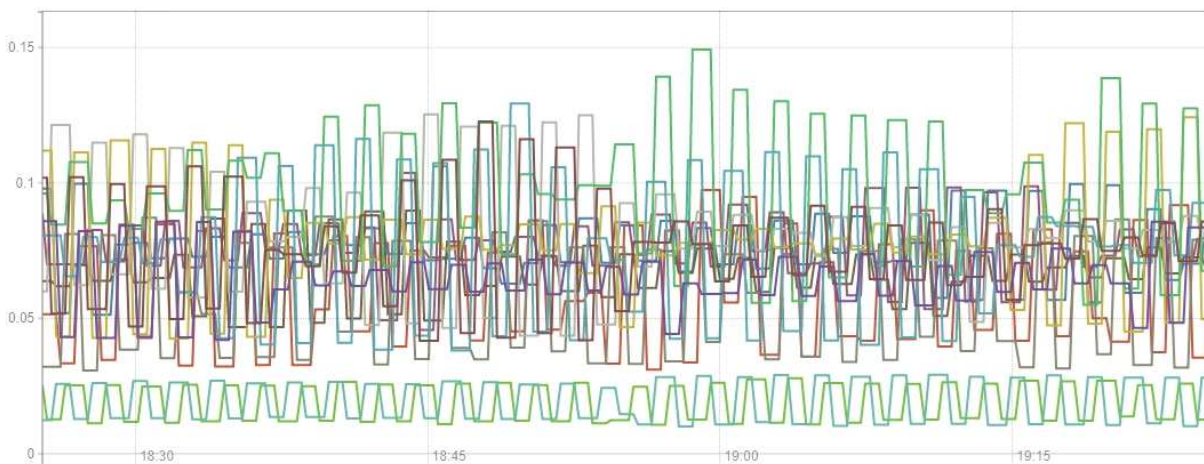
- insert metric at cursor - ▾

Graph Console

- 1h +

◀ Until ▶

Res. (s)

☐ stacked

- ✓ {instance="DC3-S3"}
- ✓ {instance="DC3-S2"}
- ✓ {instance="DC3-S1"}
- ✓ {instance="DC2-S3"}
- ✓ {instance="DC2-S2"}
- ✓ {instance="DC2-S1"}
- ✓ {instance="DC2-ADM1"}
- ✓ {instance="DC1-S3"}
- ✓ {instance="DC1-S2"}
- ✓ {instance="DC1-S1"}
- ✓ {instance="DC1-G1"}
- ✓ {instance="DC1-ARC1"}
- ✓ {instance="DC1-ADM1"}

Remove Graph

Add Graph

Créer des applications de surveillance personnalisées

Vous pouvez créer des applications de surveillance et des tableaux de bord personnalisés à l'aide des mesures StorageGRID disponibles à partir de l'API Grid Management.

Si vous souhaitez surveiller des métriques qui ne sont pas affichées sur une page existante du Grid Manager, ou si vous souhaitez créer des tableaux de bord personnalisés pour StorageGRID, vous pouvez utiliser l'API Grid Management pour interroger les métriques StorageGRID .

Vous pouvez également accéder aux métriques Prometheus directement avec un outil de surveillance externe, tel que Grafana. L'utilisation d'un outil externe nécessite que vous téléchargiez ou génériez un certificat client administratif pour permettre à StorageGRID d'authentifier l'outil pour des raisons de sécurité. Voir [le "instructions pour administrer StorageGRID"](#) .

Pour afficher les opérations de l'API des métriques, y compris la liste complète des métriques disponibles, accédez au gestionnaire de grille. En haut de la page, sélectionnez l'icône d'aide et sélectionnez

metrics

Operations on metrics

GET

/grid/metric-labels/{label}/values

Lists the values for a metric label

GET

/grid/metric-names

Lists all available metric names

GET

/grid/metric-query

Performs an instant metric query at a single point in time

GET

/grid/metric-query-range

Performs a metric query over a range of time

Les détails sur la manière de mettre en œuvre une application de surveillance personnalisée dépassent le cadre de cette documentation.

Dépannage du système StorageGRID

Dépanner un système StorageGRID

Si vous rencontrez un problème lors de l'utilisation d'un système StorageGRID , reportez-vous aux conseils et instructions de cette section pour obtenir de l'aide pour déterminer et résoudre le problème.

Souvent, vous pouvez résoudre les problèmes par vous-même ; cependant, vous devrez peut-être faire appel au support technique pour résoudre certains problèmes.

Définir le problème

La première étape pour résoudre un problème est de le définir clairement.

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 clientes signalent que les objets ne peuvent pas être ingérés dans StorageGRID.
Quand le problème a-t-il commencé ?	L'ingestion d'objets a été refusée pour la première fois vers 14h50 le 8 janvier 2020.
Comment avez-vous remarqué le problème pour la première fois ?	Notifié par l'application client. J'ai également reçu des notifications d'alerte par e-mail.
Le problème survient-il systématiquement ou seulement parfois ?	Le problème persiste.

Question	Exemple de réponse
Si le problème se produit régulièrement, quelles sont les étapes qui le provoquent ?	Le problème se produit chaque fois qu'un client tente d'ingérer un objet.
Si le problème survient par intermittence, quand se produit-il ? Enregistrez les heures de chaque incident dont vous avez connaissance.	Le problème n'est pas intermittent.
Avez-vous déjà vu ce problème ? À quelle fréquence avez-vous eu ce problème dans le passé ?	C'est la première fois que je vois ce problème.

Évaluer le risque et l'impact sur le système

Après avoir défini le problème, évaluez son risque et son impact sur le système StorageGRID . Par exemple, la présence d'alertes critiques ne signifie pas nécessairement que le système ne fournit pas de services essentiels.

Ce tableau résume l'impact que l'exemple de problème a sur les opérations du système :

Question	Exemple de réponse
Le système StorageGRID peut-il ingérer du contenu ?	Non.
Les applications clientes peuvent-elles récupérer du contenu ?	Certains objets peuvent être récupérés et d'autres non.
Les données sont-elles en danger ?	Non.
La capacité à mener des affaires est-elle gravement affectée ?	Oui, car les applications clientes ne peuvent pas stocker d'objets dans le système StorageGRID et les données ne peuvent pas être récupérées de manière cohérente.

Collecter des données

Après avoir défini le problème et évalué son risque et son impact, collectez des données pour analyse. Le type de données qu'il est le plus utile de collecter dépend de la nature du problème.

Type de données à collecter	Pourquoi collecter ces données	Instructions
Créer une chronologie des changements récents	Les modifications apportées à votre système StorageGRID , à sa configuration ou à son environnement peuvent entraîner un nouveau comportement.	• Créer une chronologie des changements récents

Type de données à collecter	Pourquoi collecter ces données	Instructions
Avis sur les alertes	Les alertes peuvent vous aider à déterminer rapidement la cause première d'un problème en fournissant des indices importants sur les problèmes sous-jacents qui pourraient en être la cause. Consultez la liste des alertes actuelles pour voir si StorageGRID a identifié la cause première d'un problème pour vous. Consultez les alertes déclenchées dans le passé pour obtenir des informations supplémentaires.	• "Afficher les alertes actuelles et résolues"
Surveiller les événements	Les événements incluent toutes les erreurs système ou tous les événements de défaut pour un nœud, y compris les erreurs telles que les erreurs réseau. Surveillez les événements pour en savoir plus sur les problèmes ou pour aider au dépannage.	• "Surveiller les événements"
Identifier les tendances à l'aide de graphiques et de rapports textuels	Les tendances peuvent fournir des indices précieux sur le moment où les problèmes sont apparus pour la première fois et peuvent vous aider à comprendre à quelle vitesse les choses évoluent.	• "Utiliser des tableaux et des graphiques" • "Utiliser des rapports textuels"
Établir des lignes de base	Recueillir des informations sur les niveaux normaux de diverses valeurs opérationnelles. Ces valeurs de référence et les écarts par rapport à ces valeurs de référence peuvent fournir des indices précieux.	• Établir des lignes de base
Effectuer des tests d'ingestion et de récupération	Pour résoudre les problèmes de performances liés à l'ingestion et à la récupération, utilisez une station de travail pour stocker et récupérer des objets. Comparez les résultats avec ceux observés lors de l'utilisation de l'application cliente.	• "Surveiller les performances PUT et GET"
Examiner les messages d'audit	Consultez les messages d'audit pour suivre en détail les opérations StorageGRID . Les détails des messages d'audit peuvent être utiles pour résoudre de nombreux types de problèmes, y compris les problèmes de performances.	• "Examiner les messages d'audit"

Type de données à collecter	Pourquoi collecter ces données	Instructions
Vérifier l'emplacement des objets et l'intégrité du stockage	Si vous rencontrez des problèmes de stockage, vérifiez que les objets sont placés là où vous le souhaitez. Vérifiez l'intégrité des données d'objet sur un nœud de stockage.	• "Surveiller les opérations de vérification des objets" • "Confirmer les emplacements des données d'objet" • "Vérifier l'intégrité de l'objet"
Collecter des données pour le support technique	Le support technique peut vous demander de collecter des données ou d'examiner des informations spécifiques pour vous aider à résoudre les problèmes.	• "Collecter les fichiers journaux et les données système" • "Déclencher manuellement un package AutoSupport" • "Examiner les mesures de support"

Créer une chronologie des modifications récentes

Lorsqu'un problème survient, vous devez tenir compte de ce qui a changé récemment et du moment où ces changements se sont produits.

- Les modifications apportées à votre système StorageGRID , à sa configuration ou à son environnement peuvent entraîner un nouveau comportement.
- Une chronologie des changements peut vous aider à identifier les changements qui pourraient être responsables d'un problème et comment chaque changement pourrait avoir affecté son développement.

Créez un tableau des modifications récentes apportées à votre système qui comprend des informations sur le moment où chaque modification s'est produite et tous les détails pertinents sur la modification, tels que des informations sur ce qui se passait d'autre pendant que la modification était en cours :

L'heure du changement	Type de changement	Détails
Par exemple: • Quand avez-vous commencé la récupération du nœud ? • Quand la mise à niveau du logiciel a-t-elle été terminée ? • Avez-vous interrompu le processus ?	Ce qui s'est passé? Qu'est-ce que tu as fait?	Documentez tous les détails pertinents concernant le changement. Par exemple: • Détails des changements du réseau. • Quel correctif a été installé. • Comment les charges de travail des clients ont changé. Assurez-vous de noter si plusieurs changements se produisent en même temps. Par exemple, ce changement a-t-il été effectué alors 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 changé récemment ?
- La politique ILM a-t-elle été mise à jour ?
- La charge de travail du client a-t-elle changé ?
- L'application cliente ou son comportement a-t-il changé ?
- Avez-vous modifié les équilibres de charge ou ajouté ou supprimé un groupe de haute disponibilité de nœuds d'administration ou de nœuds de passerelle ?
- Des tâches ont-elles été commencées qui pourraient prendre beaucoup de temps à terminer ? Voici quelques exemples :
 - Récupération d'un nœud de stockage défaillant
 - Déclassement du nœud de stockage
- Des modifications ont-elles été apportées à l'authentification des utilisateurs, telles que l'ajout d'un locataire ou la modification de la configuration LDAP ?
- La migration des données est-elle en cours ?
- Les services de la plateforme ont-ils été récemment activés ou modifiés ?
- La conformité a-t-elle été activée récemment ?
- Des pools de stockage cloud ont-ils été ajoutés ou supprimés ?
- Des modifications ont-elles été apportées à la compression ou au cryptage du stockage ?
- Y a-t-il eu des changements dans l'infrastructure du réseau ? Par exemple, les VLAN, les routeurs ou les DNS.
- Des modifications ont-elles été apportées aux sources NTP ?
- Des modifications ont-elles été apportées aux interfaces Grid, Admin ou Client Network ?
- D'autres modifications ont-elles été apportées au système StorageGRID ou à son environnement ?

Établir des lignes de base

Vous pouvez établir des lignes de base pour votre système en enregistrant les niveaux normaux de diverses valeurs opérationnelles. À l'avenir, vous pourrez comparer les valeurs actuelles à ces lignes de base pour aider à détecter et à résoudre les valeurs anormales.

Propriété	Valeur	Comment obtenir
Consommation moyenne de stockage	Go consommés/jour Pourcentage consommé/jour	Accédez au gestionnaire de grille. Sur la page Nœuds, sélectionnez la grille entière ou un site et accédez à l'onglet Stockage. Sur le graphique Stockage utilisé - Données d'objet, recherchez une période où la ligne est assez stable. Positionnez votre curseur sur le graphique pour estimer la quantité de stockage consommée chaque jour Vous pouvez collecter ces informations pour l'ensemble du système ou pour un centre de données spécifique.
Consommation moyenne de métadonnées	Go consommés/jour Pourcentage consommé/jour	Accédez au gestionnaire de grille. Sur la page Nœuds, sélectionnez la grille entière ou un site et accédez à l'onglet Stockage. Sur le graphique Stockage utilisé - Métadonnées d'objet, recherchez une période où la ligne est assez stable. Positionnez votre curseur sur le graphique pour estimer la quantité de stockage de métadonnées consommée chaque jour Vous pouvez collecter ces informations pour l'ensemble du système ou pour un centre de données spécifique.
Taux d'opérations S3/Swift	Opérations/seconde	Dans le tableau de bord du gestionnaire de grille, sélectionnez Performances > Opérations S3 ou Performances > Opérations Swift. Pour voir les taux et les nombres d'ingestion et de récupération pour un site ou un nœud spécifique, sélectionnez NODES > site ou Storage Node > Objects. Placez votre curseur sur le graphique Ingérer et récupérer pour S3.
Échec des opérations S3/Swift	Opérations	Sélectionnez SUPPORT > Outils > Topologie de grille . Dans l'onglet Présentation de la section Opérations API, affichez la valeur de Opérations S3 - Échec ou Opérations Swift - Échec.
Taux d'évaluation ILM	Objets/seconde	Depuis la page Nœuds, sélectionnez grid > ILM. Sur le graphique de la file d'attente ILM, recherchez une période où la ligne est assez stable. Placez votre curseur sur le graphique pour estimer une valeur de référence pour le taux d'évaluation de votre système.

Propriété	Valeur	Comment obtenir
Taux de balayage ILM	Objets/seconde	Sélectionnez NODES > grid > ILM . Sur le graphique de la file d'attente ILM, recherchez une période où la ligne est assez stable. Placez votre curseur sur le graphique pour estimer une valeur de référence pour le taux d'analyse pour votre système.
Objets mis en file d'attente à partir des opérations client	Objets/seconde	Sélectionnez NODES > grid > ILM . Sur le graphique de la file d'attente ILM, recherchez une période où la ligne est assez stable. Placez votre curseur sur le graphique pour estimer une valeur de référence pour 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 la table Requêtes, affichez la valeur de la latence moyenne.

Analyser les données

Utilisez les informations que vous collectez pour déterminer la cause du problème et les solutions potentielles.

L'analyse dépend du problème, mais en général :

- Localisez les points de défaillance et les goulots d'étranglement à l'aide des alertes.
- Reconstituez l'historique du problème à l'aide de l'historique des alertes et des graphiques.
- Utilisez des graphiques pour trouver des anomalies et comparer la situation problématique avec le fonctionnement normal.

Liste de contrôle des informations d'escalade

Si vous ne parvenez pas à résoudre le problème vous-même, contactez le support technique. Avant de contacter le support technique, rassemblez les informations répertoriées dans le tableau suivant pour faciliter la résolution du problème.

	Article	Remarques
	Énoncé du problème	Quels sont les symptômes du problème ? Quand le problème a-t-il commencé ? Cela se produit-il régulièrement ou par intermittence ? Si c'est par intermittence, à quelles heures cela s'est-il produit ? Définir le problème

	Article	Remarques
	Évaluation d'impact	Quelle est la gravité du problème ? Quel est l'impact sur l'application cliente ? • Le client s'est-il déjà connecté avec succès ? • Le client peut-il ingérer, récupérer et supprimer des données ?
	ID système StorageGRID	Sélectionnez MAINTENANCE > Système > Licence . L'ID système StorageGRID est affiché dans le cadre de la licence actuelle.
	Version du logiciel	En haut du gestionnaire de grille, sélectionnez l'icône d'aide et sélectionnez À propos pour voir la version de StorageGRID .
	Personnalisation	Résumez la configuration de votre système StorageGRID . Par exemple, énumérez les éléments suivants : • Le réseau utilise-t-il la compression du stockage, le cryptage du stockage ou la conformité ? • ILM crée-t-il des objets répliqués ou codés par effacement ? L'ILM assure-t-il la redondance du site ? Les règles ILM utilisent-elles les comportements d'ingestion équilibrés, stricts ou à double engagement ?
	Fichiers journaux et données système	Collectez les fichiers journaux et les données système de votre système. Sélectionnez SUPPORT > Outils > Journaux. Vous pouvez collecter des journaux pour l'ensemble de la grille ou pour des nœuds sélectionnés. Si vous collectez des journaux uniquement pour des nœuds sélectionnés, assurez-vous d'inclure au moins un nœud de stockage doté du service ADC. (Les trois premiers nœuds de stockage d'un site incluent le service ADC.) "Collecter les fichiers journaux et les données système"
	Informations de base	Collectez des informations de base concernant les opérations d'ingestion, les opérations de récupération et la consommation de stockage. Établir des lignes de base
	Chronologie des changements récents	Créez une chronologie qui résume tous les changements récents apportés au système ou à son environnement. Créer une chronologie des changements récents

✓	Article	Remarques
	Historique des efforts déployés pour diagnostiquer le problème	Si vous avez pris des mesures pour diagnostiquer ou résoudre le problème vous-même, assurez-vous d'enregistrer les étapes que vous avez suivies et le résultat.

Résoudre les problèmes d'objets et de stockage

Confirmer les emplacements des données d'objet

En fonction du problème, vous souhaitez peut-être ["confirmer où les données de l'objet sont stockées"](#) . Par exemple, vous souhaitez peut-être vérifier que la politique ILM fonctionne comme prévu et que les données d'objet sont stockées là où prévu.

Avant de commencer

- Vous devez avoir un identifiant d'objet, qui peut être l'un des suivants :
 - **UUID** : l'identifiant unique universel de l'objet. Entrez le UUID en majuscules.
 - **CBID** : l'identifiant unique de l'objet dans StorageGRID . Vous pouvez obtenir le CBID d'un objet à partir du journal d'audit. Entrez le CBID en majuscules.
 - **Seau S3 et clé d'objet** : Lorsqu'un objet est ingéré via le ["Interface S3"](#) , l'application cliente utilise une combinaison de clés de bucket et d'objet pour stocker et identifier l'objet.

Étapes

1. Sélectionnez **ILM > Recherche de métadonnées d'objet**.
2. Tapez l'identifiant de l'objet dans le champ **Identifiant**.

Vous pouvez saisir un UUID, un CBID, une clé de bucket/objet S3 ou un nom de conteneur/objet 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 :

- 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 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 clé-valeur de métadonnées utilisateur personnalisées associées à l'objet.
- Pour les objets S3, toutes les paires clé-valeur de balise d'objet associées à l'objet.
- Pour les copies d'objets répliquées, l'emplacement de stockage actuel de chaque copie.
- Pour les copies d'objets codées par effacement, l'emplacement de stockage actuel de chaque fragment.
- Pour les copies d'objet dans un pool de stockage Cloud, l'emplacement de l'objet, y compris le nom du bucket externe et l'identifiant unique de l'objet.
- Pour les objets segmentés et les objets en plusieurs parties, une liste de segments d'objet comprenant les identifiants de segment et les tailles de données. Pour les objets comportant plus de 100 segments, seuls les 100 premiers segments sont affichés.
- Toutes les métadonnées d'objet au format de stockage interne non traité. Ces métadonnées brutes incluent des métadonnées système internes dont la persistance d'une version à l'autre n'est pas garantie.

L'exemple suivant montre 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": {
      "PAHS": "2",

```

Pannes du magasin d'objets (volume de stockage)

Le stockage sous-jacent sur 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 du magasin d'objets pour chaque nœud de stockage. Les magasins d'objets sont affichés en bas de la page **NODES > 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

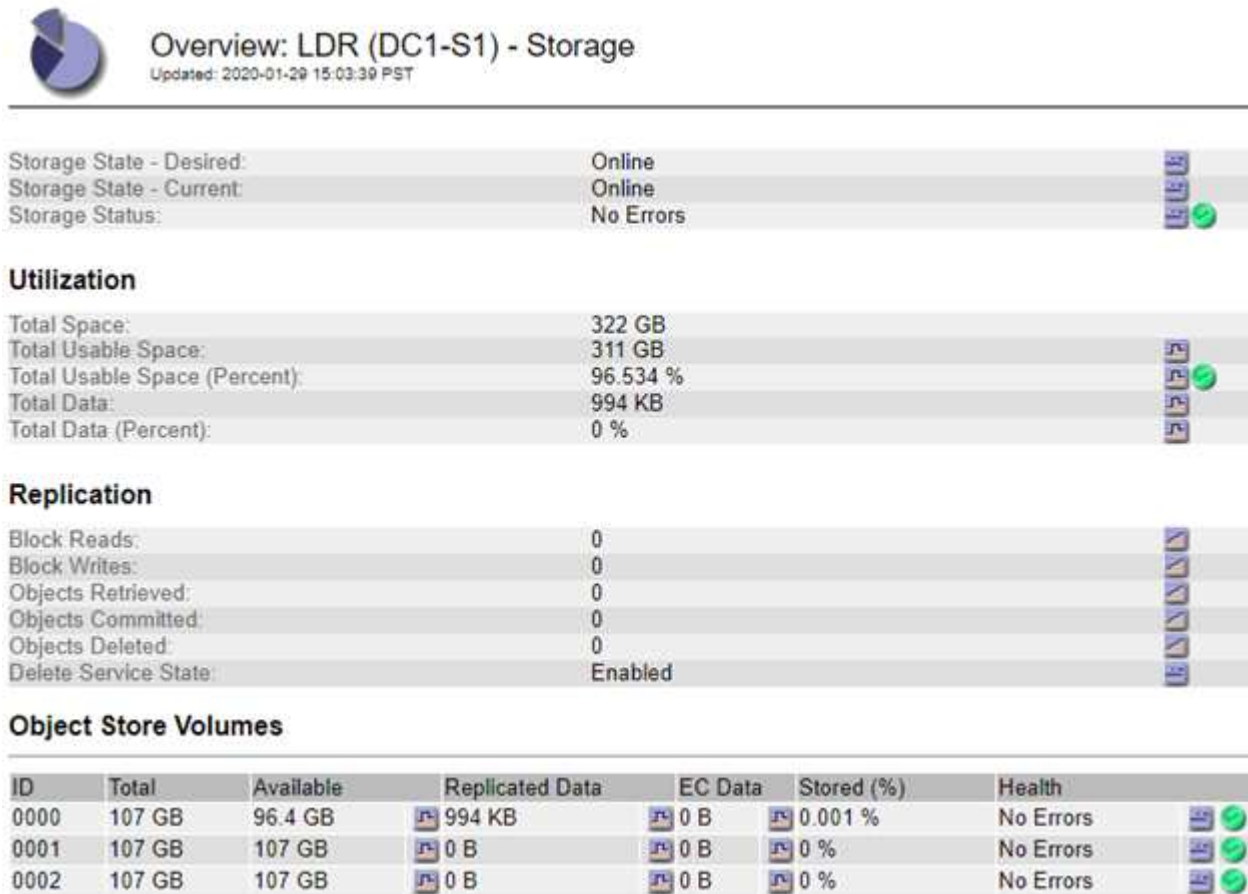
Mount point ? ⇅	Device ? ⇅	Status ? ⇅	Size ? ⇅	Available ? ⇅	Write cache status ? ⇅
/	croot	Online	21.00 GB	14.73 GB 	Unknown
/var/local	cvloc	Online	85.86 GB	80.94 GB 	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.17 GB 	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB 	Enabled
/var/local/rangedb/2	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 voir plus "détails sur chaque nœud de stockage", suivez ces étapes :

1. Sélectionnez **SUPPORT > Outils > Topologie de grille.**
2. Sélectionnez **site > Nœud de stockage > LDR > Stockage > Aperçu > Principal.**



Selon la nature de la panne, les défauts d'un volume de stockage peuvent se refléter dans "alertes de volume de stockage". Si un volume de stockage tombe en panne, vous devez réparer le volume de stockage défaillant pour restaurer le nœud de stockage à toutes ses fonctionnalités dès que possible. Si nécessaire, vous pouvez aller dans l'onglet **Configuration** et "placer le nœud de stockage dans un état de lecture seule" afin que le système StorageGRID puisse l'utiliser pour la récupération des données pendant que vous vous préparez à une récupération complète du serveur.

Vérifier l'intégrité de l'objet

Le système StorageGRID vérifie l'intégrité des données d'objet sur les nœuds de stockage, en recherchant les objets corrompus et manquants.

Il existe deux processus de vérification : la vérification en arrière-plan et la vérification de l'existence de l'objet (anciennement appelée vérification au premier plan). Ils travaillent ensemble pour garantir l'intégrité des données. La vérification en arrière-plan s'exécute automatiquement et vérifie en permanence l'exactitude des données de l'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) des 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 les copies corrompues des données d'objet et tente automatiquement de réparer tous les problèmes qu'il détecte.

La vérification en arrière-plan vérifie l'intégrité des objets répliqués et des objets codés par effacement, comme suit :

- **Objets répliqués** : si le processus de vérification en arrière-plan détecte un objet répliqué corrompu, la copie corrompue est supprimée de son emplacement et mise en quarantaine ailleurs sur le nœud de stockage. Ensuite, une nouvelle copie non corrompue est générée et placée pour satisfaire les politiques ILM actives. La nouvelle copie peut ne pas être placée sur le nœud de stockage qui a été utilisé pour la copie d'origine.



Les données d'objet corrompues sont mises en quarantaine plutôt que supprimées du système, de sorte qu'elles restent accessibles. Pour plus d'informations sur l'accès aux données des objets mis en quarantaine, contactez le support technique.

- **Objets codés par effacement** : si le processus de vérification en arrière-plan détecte qu'un fragment d'un objet codé par effacement est corrompu, StorageGRID tente automatiquement de reconstruire le fragment manquant en place sur le même nœud de stockage, en utilisant les fragments de données et de parité restants. Si le fragment corrompu ne peut pas être reconstruit, une tentative est effectuée pour récupérer une autre copie de l'objet. Si la récupération réussit, une évaluation ILM est effectuée pour créer une copie de remplacement de l'objet codé par effacement.

Le processus de vérification en arrière-plan vérifie les objets sur les nœuds de stockage uniquement. Il ne vérifie pas les objets 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 rythme continu conçu pour ne pas interférer avec les activités ordinaires du système. La vérification des antécédents ne peut pas être arrêtée. Cependant, vous pouvez augmenter le taux de vérification en arrière-plan pour vérifier plus rapidement le contenu d'un nœud de stockage si vous suspectez un problème.

Alertes 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'identification de l'objet), l'alerte **Objet corrompu non identifié détecté** est déclenchée.

Si la vérification en arrière-plan ne peut pas remplacer un objet corrompu car elle 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 inquiétudes concernant l'intégrité des données.

Avant de commencer

- Vous devez être connecté au Grid Manager à l'aide d'un ["navigateur Web pris en charge"](#) .
- Tu as ["autorisations d'accès spécifiques"](#) .

À propos de cette 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 valeur dépassée).

- Élevé : la vérification du stockage se déroule rapidement, à un rythme qui peut ralentir les activités ordinaires du système.

Utilisez le taux de vérification élevé uniquement lorsque vous suspectez qu'une panne matérielle ou logicielle a pu corrompre les données de l'objet. Une fois la vérification d'arrière-plan haute priorité terminée, le taux de vérification est automatiquement réinitialisé sur Adaptatif.

Étapes

1. Sélectionnez **SUPPORT > Outils > Topologie de grille**.
2. Sélectionnez **Nœud de stockage > LDR > Vérification**.
3. Sélectionnez **Configuration > Principal**.
4. Accédez à **LDR > Vérification > Configuration > Principal**.
5. Sous Vérification en arrière-plan, sélectionnez **Taux de vérification > Élevé** ou **Taux de vérification > Adaptatif**.

The screenshot displays the 'Configuration: LDR () - Verification' page. At the top, there are tabs for 'Overview', 'Alarms', 'Reports', and 'Configuration', with 'Configuration' being the active tab. Below the tabs is a 'Main' header. The main content area shows a title 'Configuration: LDR () - Verification' with a sub-header 'Updated: 2021-11-11 07:13:00 MST'. The page is divided into sections: 'Reset Missing Objects Count' with an unchecked checkbox, 'Background Verification' with a 'Verification Rate' dropdown menu set to 'Adaptive' (highlighted with a green box), 'Reset Corrupt Objects Count' with an unchecked checkbox, 'Quarantined Objects' with a 'Delete Quarantined Objects' checkbox (unchecked), and an 'Apply Changes' button at the bottom right.

6. Cliquez sur **Appliquer les modifications**.
7. Surveillez les résultats de la vérification en arrière-plan pour les objets répliqués.
 - a. Accédez à **NODES > Storage Node > Objects**.
 - b. Dans la section Vérification, surveillez les valeurs pour **Objets corrompus** et **Objets corrompus non identifiés**.

Si la vérification en arrière-plan détecte des données d'objet répliquées corrompues, la mesure **Objets corrompus** est incrémentée et StorageGRID tente d'extraire l'identifiant d'objet des données, comme suit :

- Si l'identifiant de l'objet peut être extrait, StorageGRID crée automatiquement une nouvelle copie des données de l'objet. La nouvelle copie peut être effectuée n'importe où dans le système

StorageGRID qui satisfait aux politiques ILM actives.

- 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 répliquées corrompues sont détectées, contactez le support technique pour déterminer la cause première de la corruption.

8. Surveillez les résultats de la vérification en arrière-plan pour les objets codés par 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 récupère en reconstruisant le fragment corrompu en place sur le même nœud de stockage.

- a. Sélectionnez **SUPPORT > Outils > Topologie de grille**.

- b. Sélectionnez **Nœud de stockage > LDR > Codage d'effacement**.

- c. Dans le tableau Résultats de vérification, surveillez l'attribut Fragments corrompus détectés (ECCD).

9. Une fois les objets corrompus restaurés automatiquement par le système StorageGRID, réinitialisez le nombre d'objets corrompus.

- a. Sélectionnez **SUPPORT > Outils > Topologie de grille**.

- b. Sélectionnez **Nœud de stockage > LDR > Vérification > 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** a été déclenchée, le support technique peut souhaiter accéder aux objets mis en quarantaine pour aider à déboguer le problème sous-jacent ou pour tenter de récupérer des données.

- a. Sélectionnez **SUPPORT > Outils > Topologie de grille**.

- b. Sélectionnez **Nœud de stockage > LDR > Vérification > Configuration**.

- c. Sélectionnez **Supprimer les objets mis en quarantaine**.

- d. Sélectionnez **Appliquer les modifications**.

Qu'est-ce que la vérification de l'existence d'un objet ?

La vérification de l'existence d'un objet vérifie si toutes les copies répliquées attendues des objets et des fragments codés par effacement existent sur un nœud de stockage. La vérification de l'existence d'un objet ne vérifie pas les données de l'objet lui-même (la vérification en arrière-plan le fait) ; au lieu de cela, elle fournit un moyen de vérifier l'intégrité des périphériques de stockage, en particulier si un problème matériel récent a pu affecter l'intégrité des données.

Contrairement à la vérification en arrière-plan, qui se produit automatiquement, vous devez démarrer manuellement une tâche de vérification de l'existence d'un objet.

La vérification de l'existence des objets lit les métadonnées de chaque objet stocké dans StorageGRID et vérifie l'existence des copies d'objets répliquées et des fragments d'objets codés par effacement. Toute donnée manquante est traitée comme suit :

- **Copies répliquées** : si une copie des données d'objet répliquées est manquante, StorageGRID tente

automatiquement de remplacer la copie à partir d'une copie stockée ailleurs dans le système. Le nœud de stockage exécute une copie existante via une évaluation ILM, qui déterminera 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 les politiques ILM actives 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 en place sur le même nœud de stockage à l'aide des fragments restants. Si le fragment manquant ne peut pas être reconstruit (parce que trop de fragments ont été perdus), ILM tente de trouver une autre copie de l'objet, qu'il peut utiliser pour générer un nouveau fragment codé par effacement.

Exécuter la vérification de l'existence de l'objet

Vous créez et exécutez une tâche de vérification de l'existence d'un objet à la fois. Lorsque vous créez une tâche, vous sélectionnez les nœuds de stockage et les volumes que vous souhaitez vérifier. Vous sélectionnez également la consistance du travail.

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 de maintenance ou root"](#) .
- Vous avez vérifié que les nœuds de stockage que vous souhaitez vérifier sont en ligne. Sélectionnez **NODES** pour afficher le tableau des nœuds. Assurez-vous qu'aucune icône d'alerte n'apparaît à côté du nom du nœud pour les nœuds que vous souhaitez vérifier.
- Vous avez vérifié que les procédures suivantes ne sont **pas** en cours d'exécution sur les nœuds que vous souhaitez vérifier :
 - Extension du réseau pour ajouter un nœud de stockage
 - Mise hors service du nœud de stockage
 - Récupération d'un volume de stockage défaillant
 - Récupération d'un nœud de stockage avec un lecteur système défaillant
 - Rééquilibrage de la CE
 - Clonage de nœud d'appareil

La vérification de l'existence de l'objet ne fournit pas d'informations utiles pendant que ces procédures sont en cours.

À propos de cette tâche

Une tâche de vérification de l'existence d'un objet peut prendre des jours ou des semaines, selon le nombre d'objets dans la grille, les nœuds et volumes de stockage sélectionnés et la cohérence sélectionnée. 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 de l'existence de l'objet**.
2. Sélectionnez **Créer un travail**. L'assistant Créer une tâche de vérification de l'existence d'un objet s'affiche.
3. Sélectionnez les nœuds contenant les volumes que vous souhaitez vérifier. Pour sélectionner tous les nœuds en ligne, cochez la case **Nom du nœud** dans l'en-tête de la colonne.

Vous pouvez rechercher par nom de nœud ou par site.

Vous ne pouvez pas sélectionner des nœuds qui ne sont pas connectés au réseau.

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 de volume de stockage ou du nom du nœud.

Pour sélectionner tous les volumes pour chaque nœud sélectionné, cochez la case **Volume de stockage** dans l'en-tête de colonne.

6. Sélectionnez **Continuer**.

7. Sélectionnez la consistance pour le travail.

La 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.
- **Strong-global** : Deux copies de métadonnées sur chaque site.
- **Tous** (par défaut) : les trois copies de métadonnées sur chaque site.

Pour plus d'informations sur la cohérence, consultez les descriptions dans l'assistant.

8. Sélectionnez **Continuer**.

9. Vérifiez et révisiez vos sélections. Vous pouvez sélectionner **Précédent** pour accéder à une étape précédente de l'assistant afin de mettre à jour vos sélections.

Une tâche de vérification de l'existence d'un objet est générée et s'exécute jusqu'à ce que l'un des événements suivants se produise :

- Le travail est terminé.
- Vous mettez en pause ou annulez le travail. Vous pouvez reprendre un travail que vous avez suspendu, mais vous ne pouvez pas reprendre un travail que vous avez annulé.
- Le travail stagne. L'alerte **La vérification de l'existence de l'objet est bloquée** est déclenchée. Suivez les actions correctives spécifiées pour l'alerte.
- Le travail échoue. L'alerte **La vérification de l'existence de l'objet a échoué** est déclenchée. Suivez les actions correctives spécifiées pour l'alerte.
- Un message « Service indisponible » ou « Erreur interne du serveur » s'affiche. Après une minute, actualisez la page pour continuer à surveiller le travail.



Si nécessaire, vous pouvez quitter la page de vérification de l'existence de l'objet et y revenir pour continuer à surveiller le travail.

10. Pendant l'exécution du travail, affichez l'onglet **Tâche active** et notez la valeur de Copies d'objets manquantes détectées.

Cette valeur représente le nombre total de copies manquantes d'objets répliqués et d'objets codés par effacement avec un ou plusieurs fragments manquants.

Si le nombre de copies d'objets manquants détectées est supérieur à 100, il peut y avoir un problème avec le stockage du nœud de stockage.

Object existence check

Perform an object existence check if you suspect some storage volumes have been damaged or are corrupt and you want to verify that objects still exist on these volumes.

If you have questions about running object existence check, contact technical support.

Active job

Job history

Status: Accepted

Consistency control: All

Job ID: 2334602652907829302

Start time: 2021-11-10 14:43:02 MST

Missing object copies detected: 0

Elapsed time: —

Progress: 0%

Estimated time to completion: —

Pause

Cancel

Volumes

Details

Selected node	Selected storage volumes	Site
DC1-S1	0, 1, 2	Data Center 1
DC1-S2	0, 1, 2	Data Center 1
DC1-S3	0, 1, 2	Data Center 1

11. Une fois le travail terminé, effectuez les actions supplémentaires requises :

- Si le nombre de copies d'objets manquantes détectées est nul, aucun problème n'a été détecté. Aucune action n'est requise.
- Si le nombre de copies d'objets manquantes détectées est supérieur à zéro et que l'alerte **Objets perdus** n'a pas été déclenchée, alors toutes les copies manquantes ont été réparées par le système. Vérifiez que tous les problèmes matériels ont été corrigés pour éviter de futurs dommages aux copies d'objets.
- Si le nombre de copies d'objets manquantes détectées est supérieur à zéro et que l'alerte **Objets perdus** a été déclenchée, l'intégrité des données peut être affectée. Contactez le support technique.
- Vous pouvez enquêter sur les copies d'objets perdues en utilisant grep pour extraire les messages d'audit LLST : `grep LLST audit_file_name`.

Cette procédure est similaire à celle pour "[enquête sur les objets perdus](#)", bien que pour les copies d'objets, vous recherchez LLST au lieu de OLST.

12. Si vous avez sélectionné la cohérence Strong-Site ou Strong-Global pour le travail, attendez environ trois semaines pour la cohérence des métadonnées, puis réexécutez 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 la tâche, la réexécution de la tâche peut effacer les copies d'objets manquantes signalées par erreur ou entraîner la vérification de copies d'objets supplémentaires si elles ont été manquées.

- Sélectionnez **MAINTENANCE > Vérification de l'existence de l'objet > Historique des tâches**.

- b. Déterminer les tâches prêtes à être réexécutées :
 - i. Consultez la colonne **Heure de fin** pour déterminer quelles tâches ont été exécutées il y a plus de trois semaines.
 - ii. Pour ces tâches, scannez la colonne de contrôle de cohérence pour strong-site ou strong-global.
- c. Cochez la case correspondant à chaque tâche que vous souhaitez réexécuter, puis sélectionnez **Réexécuter**.

Object existence check

Perform an object existence check if you suspect some storage volumes have been damaged or are corrupt and you want to verify that objects still exist on these volumes.

If you have questions about running object existence check, contact technical support.

Active job

Job history

Delete

Rerun

Search by Job ID/ node name/ consistency control/ start time

Displaying 4 results

☐	Job ID ?	Status	Nodes (volumes) ?	Missing object copies detected ?	Consistency control	Start time ?	End time ?
☒	2334602652907829302	Completed	DC1-S1 (3 volumes) DC1-S2 (3 volumes) DC1-S3 (3 volumes) and 7 more	0	All	2021-11-10 14:43:02 MST	2021-11-10 14:43:06 MST (3 weeks ago)
☐	11725651898848823235 (Rerun job)	Completed	DC1-S2 (2 volumes) DC1-S3 (2 volumes) DC1-S4 (2 volumes) and 4 more	0	Strong-site	2021-11-10 14:42:10 MST	2021-11-10 14:42:11 MST (17 minutes ago)

- d. Dans l'assistant de réexécution des tâches, vérifiez les nœuds et les volumes sélectionnés ainsi que la cohérence.
- e. Lorsque vous êtes prêt à réexécuter les tâches, sélectionnez **Réexécuter**.

L'onglet Travail actif apparaît. Tous les travaux que vous avez sélectionnés sont réexécutés comme un seul travail avec une cohérence de site forte. Un champ **Tâches associées** dans la section Détails répertorie les identifiants de tâche pour les tâches d'origine.

Après avoir terminé

Si vous avez encore des inquiétudes concernant l'intégrité des données, accédez à **SUPPORT > Outils > Topologie de grille > site > Nœud de stockage > LDR > Vérification > Configuration > Principal** 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 tous les problèmes qu'elle détecte. Trouver et réparer les problèmes potentiels le plus rapidement possible réduit le risque de perte de données.

Dépannage de l'alerte S3 PUT : taille de l'objet trop grande

L'alerte de taille d'objet S3 PUT trop grande est déclenchée si un locataire tente une opération PutObject non multipartite qui dépasse la limite de taille S3 de 5 Gio.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un"navigateur Web pris en charge" .
- Tu as"autorisations d'accès spécifiques" .

Déterminez quels locataires utilisent des objets supérieurs à 5 Gio, afin de pouvoir les avertir.

Étapes

1. Accédez à **CONFIGURATION > Surveillance > Serveur d'audit et syslog.**
2. Si les écritures du client sont normales, accédez au journal d'audit :
 - a. Entrer `ssh admin@primary_Admin_Node_IP`
 - b. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.
 - c. Entrez la commande suivante pour passer en root : `su -`
 - d. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.

Lorsque vous êtes connecté en tant que root, l'invite passe de \$ à # .

- e. Accédez au répertoire dans lequel se trouvent les journaux d'audit.

Le répertoire du journal d'audit et les nœuds applicables dépendent de vos paramètres de destination d'audit.

Option	Destination
Nœuds locaux (par défaut)	<code>/var/local/log/localaudit.log</code>
Nœuds d'administration/nœuds locaux	• Nœuds d'administration (principaux et non principaux) : <code>/var/local/audit/export/audit.log</code> • Tous les nœuds : Le <code>/var/local/log/localaudit.log</code> le fichier est généralement vide ou manquant dans ce mode.
Serveur syslog externe	<code>/var/local/log/localaudit.log</code>

En fonction des paramètres de destination de votre audit, saisissez : `cd /var/local/log` ou `/var/local/audit/export/`

Pour en savoir plus, consultez" Sélectionner les destinations des informations d'audit" .

- f. Identifiez les locataires qui utilisent des objets supérieurs à 5 Gio.
 - i. Entrer `zgrep SPUT * | egrep "CSIZ\ (UI64\): ([5-9] | [1-9] [0-9]+) [0-9]{9}"`
 - ii. Pour chaque message d'audit dans les résultats, regardez `S3AI` champ pour déterminer l'ID du compte locataire. Utilisez les autres champs du message pour déterminer quelle adresse IP a été utilisée par le client, le bucket et l'objet :

Code	Description
SAIP	IP source
S3AI	ID du locataire
S3BK	Seau
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 client ne sont pas normales, utilisez l'ID de locataire de l'alerte pour identifier le locataire :

- Accédez à **SUPPORT > Outils > Journaux**. Collectez les journaux d'application pour le nœud de stockage dans l'alerte. Précisez 15 minutes avant et après l'alerte.
- Extrayez le fichier et accédez à `bycast.log` :

```
/GID<grid_id>_<time_stamp>/<site_node>/<time_stamp>/grid/bycast.log
```

- Rechercher dans le journal pour `method=PUT` et identifier le client dans le `clientIP` champ.

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. Informez les locataires que la taille maximale de `PutObject` est de 5 Gio et qu'ils doivent utiliser des téléchargements en plusieurs parties pour les objets supérieurs à 5 Gio.

5. Ignorez l'alerte pendant une semaine si l'application a été modifiée.

Résoudre les problèmes de données d'objets perdues ou manquantes

Résoudre les problèmes de données d'objets perdues ou manquantes

Les objets peuvent être récupérés pour plusieurs raisons, notamment les demandes de lecture à partir d'une application cliente, les vérifications en arrière-plan des données d'objet répliquées, les réévaluations ILM et la restauration des données d'objet lors de la récupération d'un nœud de stockage.

Le système StorageGRID utilise les informations de localisation dans les métadonnées d'un objet pour déterminer à partir de quel emplacement récupérer l'objet. Si aucune copie de l'objet n'est trouvée à l'emplacement prévu, le système tente de récupérer une autre copie de l'objet ailleurs dans le système, en supposant que la politique ILM contient une règle permettant de créer deux ou plusieurs copies de l'objet.

Si cette récupération réussit, le système StorageGRID remplace la copie manquante de l'objet. Dans le cas contraire, 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 à code d'effacement, si une copie ne peut pas être récupérée à partir de l'emplacement prévu, l'attribut Copies corrompues détectées (ECOR) est incrémenté de un avant qu'une tentative de récupération d'une copie à partir d'un autre emplacement ne soit effectuée. Si aucune autre copie n'est trouvée, l'alerte est déclenchée.

Vous devez examiner immédiatement toutes les alertes **Objets perdus** pour déterminer la cause première de la perte et déterminer si l'objet peut toujours exister dans un nœud de stockage hors ligne ou actuellement indisponible. Voir "[Enquêter sur les objets perdus](#)".

Dans le cas où les données de l'objet sans copies sont perdues, il n'existe aucune solution de récupération. Cependant, vous devez réinitialiser le compteur d'objets perdus pour éviter que les objets perdus connus ne masquent les nouveaux objets perdus. Voir "[Réinitialiser le nombre d'objets perdus et manquants](#)".

Enquêter sur 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](#)".
- Tu as "[autorisations d'accès spécifiques](#)".
- Vous devez avoir le `Passwords.txt` déposer.

À propos de cette tâche

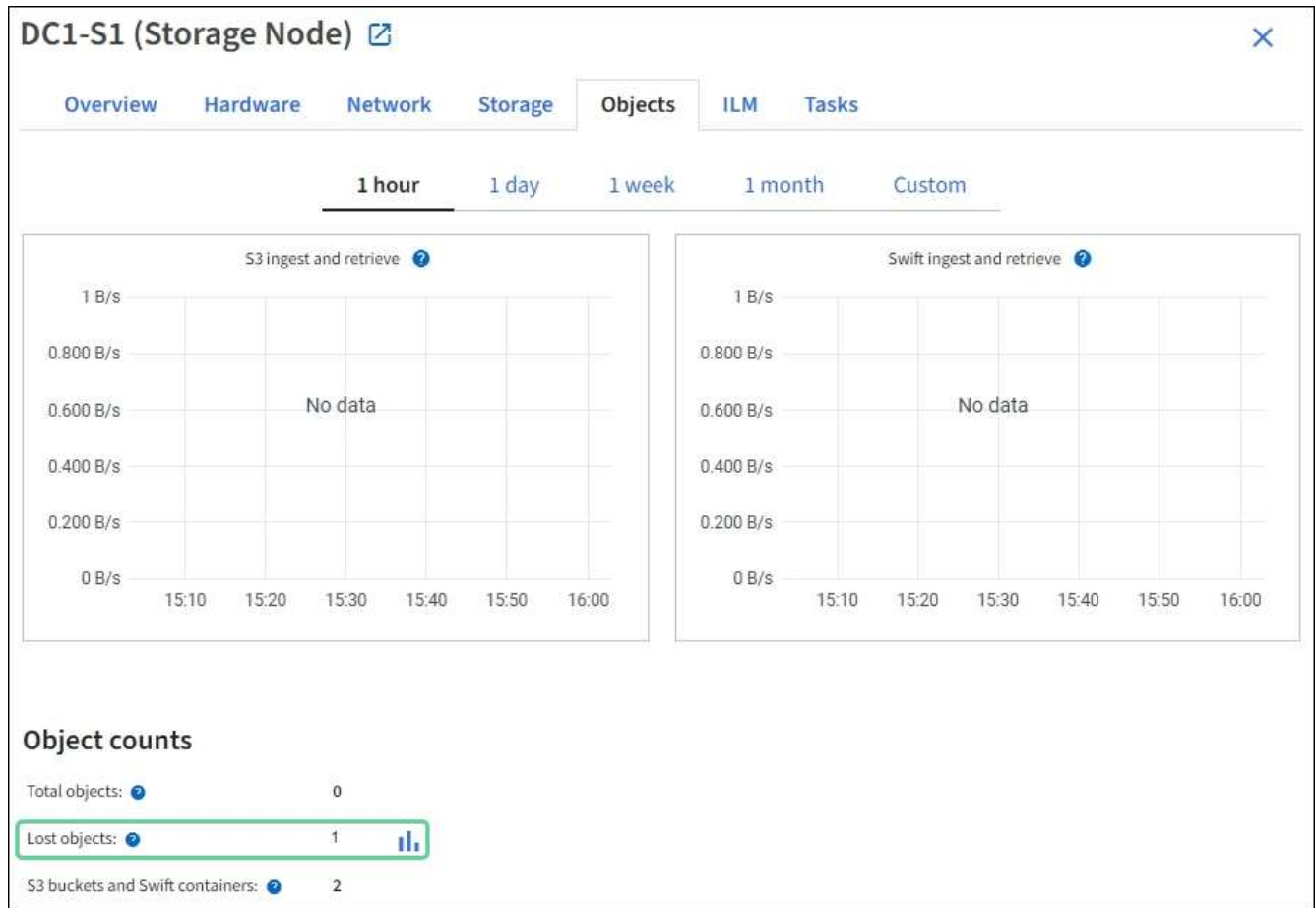
L'alerte **Objets perdus** indique que StorageGRID estime qu'il n'existe aucune copie d'un objet dans la grille. Les données ont peut-être été définitivement perdues.

Enquêtez immédiatement sur les alertes d'objets perdus. Vous devrez peut-être prendre des mesures pour éviter toute perte de données supplémentaire. Dans certains cas, vous pourrez peut-être restaurer un objet perdu si vous agissez rapidement.

Étapes

1. Sélectionnez **NODES**.
2. Sélectionnez **Nœud de stockage > Objets**.
3. Consultez le nombre d'objets perdus affiché dans le tableau Nombre d'objets.

Ce nombre indique le nombre total d'objets que ce nœud de grille détecte comme manquants dans l'ensemble du système StorageGRID . La valeur est la somme des compteurs d'objets perdus du composant de magasin de données dans les services LDR et DDS.



4. À partir d'un nœud d'administration, "[accéder 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 de grille :
 - i. Entrez la commande suivante : `ssh admin@grid_node_IP`
 - ii. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.
 - iii. Entrez la commande suivante pour passer en root : `su -`
 - iv. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer. 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.

Le répertoire du journal d'audit et les nœuds applicables dépendent de vos paramètres de destination d'audit.

Option	Destination
Nœuds locaux (par défaut)	/var/local/log/localaudit.log
Nœuds d'administration/nœuds locaux	- Nœuds d'administration (principaux et non principaux) : /var/local/audit/export/audit.log - Tous les nœuds : Le /var/local/log/localaudit.log le fichier est généralement vide ou manquant dans ce mode.
Serveur syslog externe	/var/local/log/localaudit.log

En fonction des paramètres de destination de votre audit, saisissez : `cd /var/local/log` ou `/var/local/audit/export/`

Pour en savoir plus, consultez "[Sélectionner les destinations des informations d'audit](#)".

- c. Utilisez `grep` pour extraire les messages d'audit d'objet perdu (OLST). Entrer: `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] [AMID(FC32):ILMX] [ATID(UI64):7729403978647354233]]
```

5. Recherchez les métadonnées de l'objet perdu en utilisant l'UUID :

- a. Sélectionnez **ILM > Recherche de métadonnées d'objet**.
- b. Saisissez l'UUID et sélectionnez **Rechercher**.
- c. Vérifiez les emplacements dans les métadonnées et prenez les mesures appropriées :

Métadonnées	Conclusion
Objet <object_identifieur> non trouvé	Si l'objet n'est pas trouvé, le message « ERROR:" » est renvoyé. Si l'objet n'est pas trouvé, vous pouvez réinitialiser le nombre d'Objets perdus pour effacer l'alerte. L'absence d'un objet indique que l'objet a été intentionnellement supprimé.

Métadonnées	Conclusion
Emplacements > 0	Si des emplacements sont répertoriés dans la sortie, l'alerte Objets perdus peut être un faux positif. Confirmer que les objets existent. Utilisez l'ID de nœud et le chemin de fichier répertoriés dans la sortie pour confirmer que le fichier objet se trouve à l'emplacement répertorié. (La procédure pour recherche d'objets potentiellement perdus explique comment utiliser l'ID de nœud pour trouver le nœud de stockage correct.) Si les objets existent, vous pouvez réinitialiser le nombre d'Objets perdus pour effacer l'alerte.
Emplacements = 0	S'il n'y a aucun emplacement répertorié dans la sortie, l'objet est potentiellement manquant. Vous pouvez essayer de rechercher et restaurer l'objet vous-même, ou vous pouvez contacter le support technique. Le support technique peut vous demander de déterminer si une procédure de récupération de 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 sur un volume de stockage.

Rechercher et restaurer des objets potentiellement perdus

Il peut être possible de trouver et de restaurer des objets qui ont déclenché une alerte **Objet perdu** et une alarme Objets perdus (LOST) héritée et que vous avez identifiés comme potentiellement perdus.

Avant de commencer

- Vous avez l'UUID de tout objet perdu, tel qu'identifié dans ["Enquêter sur les objets perdus"](#).
- Vous avez le `Passwords.txt` déposer.

À propos de cette tâche

Vous pouvez suivre cette procédure pour rechercher des copies répliquées de l'objet perdu ailleurs dans la grille. Dans la plupart des cas, l'objet perdu ne sera pas retrouvé. Cependant, dans certains cas, vous pourrez peut-être retrouver et restaurer un objet répliqué perdu si vous agissez rapidement.



Contactez le support technique pour obtenir de l'aide sur cette procédure.

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 de grille :
 - i. Entrez la commande suivante : `ssh admin@grid_node_IP`

- ii. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.
 - iii. Entrez la commande suivante pour passer en root : `su -`
 - iv. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer. Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.
- b. Accédez au répertoire où se trouvent les journaux d'audit.

Le répertoire du journal d'audit et les nœuds applicables dépendent de vos paramètres de destination d'audit.

Option	Destination
Nœuds locaux (par défaut)	<code>/var/local/log/localaudit.log</code>
Nœuds d'administration/nœuds locaux	• Nœuds d'administration (principaux et non principaux) : <code>/var/local/audit/export/audit.log</code> • Tous les nœuds : Le <code>/var/local/log/localaudit.log</code> le fichier est généralement vide ou manquant dans ce mode.
Serveur syslog externe	<code>/var/local/log/localaudit.log</code>

En fonction des paramètres de destination de votre audit, saisissez : `cd /var/local/log` ou `/var/local/audit/export/`

Pour en savoir plus, consultez "[Sélectionner les destinations des informations d'audit](#)".

- c. Utilisez `grep` pour extraire le "[messages d'audit associés à l'objet potentiellement perdu](#)" et les envoyer vers un fichier de sortie. Entrer: `grep uuid-value audit_file_name > output_file_name`

Par exemple:

```
Admin: # grep 926026C4-00A4-449B-AC72-BCCA72DD1311 audit.log >
/var/local/tmp/messages_about_lost_object.txt
```

- d. Utilisez `grep` pour extraire les messages d'audit d'emplacement perdu (LLST) de ce fichier de sortie. Entrer: `grep LLST output_file_name`

Par exemple:

```
Admin: # grep LLST /var/local/tmp/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) :15815351
34379225]
[ATYP (FC32) :LLST] [ANID (UI32) :12448208] [AMID (FC32) :CLSM] [ATID (UI64) :70
86871083190743409]]
```

e. Recherchez le champ PCLD et le champ NOID dans le message LLST.

Si elle est présente, la valeur de PCLD est le chemin complet sur le disque vers la copie de l'objet répliqué manquant. La valeur de NOID est l'ID du nœud du LDR où une copie de l'objet peut être trouvée.

Si vous trouvez l'emplacement d'un 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 pour le service LDR se trouve dans la table Informations sur le nœud. Passez en revue les informations de 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 de grille :

- i. Entrez la commande suivante : `ssh admin@grid_node_IP`
- ii. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.
- iii. Entrez la commande suivante pour passer en root : `su -`
- iv. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.

Lorsque vous êtes connecté en tant que root, l'invite passe de \$ à # .

b. Déterminez si le chemin d'accès au fichier de l'objet existe.

Pour le chemin d'accès au fichier de l'objet, utilisez la valeur de PCLD du message d'audit LLST.

Par exemple, saisissez :

```
ls '/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA#3tN6'
```



Placez toujours le chemin du fichier objet entre guillemets simples dans les commandes pour échapper aux caractères spéciaux.

- Si le chemin de l'objet n'est pas trouvé, l'objet est perdu et ne peut pas être restauré à l'aide de cette procédure. Contactez le support technique.
- Si le chemin de l'objet est trouvé, passez à l'étape suivante. Vous pouvez tenter de restaurer l'objet

trouvé dans StorageGRID.

3. Si le chemin de l'objet a été trouvé, essayez de restaurer l'objet dans StorageGRID:
 - a. À partir du même nœud de stockage, modifiez la propriété du fichier objet afin qu'il puisse être géré par StorageGRID. Entrer: `chown ldr-user:bycast 'file_path_of_object'`
 - b. Connectez-vous à Telnet sur localhost 1402 pour accéder à la console LDR. Entrer: `telnet 0 1402`
 - c. Entrer: `cd /proc/STOR`
 - d. Entrer: `Object_Found 'file_path_of_object'`

Par exemple, saisissez :

```
Object_Found '/var/local/rangedb/1/p/17/11/00rH0%DkRs&LgA%#3tN6'
```

Délivrance du `Object_Found` la commande notifie la grille de l'emplacement de l'objet. Il déclenche également les politiques ILM actives, qui effectuent des copies supplémentaires comme spécifié dans chaque politique.



Si le nœud de stockage sur lequel vous avez trouvé l'objet est hors ligne, vous pouvez copier l'objet sur n'importe quel nœud de stockage en ligne. Placez l'objet dans n'importe quel répertoire `/var/local/rangedb` du nœud de stockage en ligne. Ensuite, émettez le `Object_Found` commande utilisant ce chemin de fichier vers l'objet.

- Si l'objet ne peut pas être restauré, le `Object_Found` la commande échoue. Contactez le support technique.
- Si l'objet a été restauré avec succès sur 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 avec succès sur StorageGRID, vérifiez que les nouveaux emplacements ont été créés :
 - a. Sign in au Grid Manager à l'aide d'un [navigateur Web pris en charge](#) .
 - b. Sélectionnez **ILM > Recherche de métadonnées d'objet**.
 - c. Saisissez l'UUID et sélectionnez **Rechercher**.
 - d. Vérifiez les métadonnées et les nouveaux emplacements.
5. À partir d'un nœud d'administration, recherchez dans les journaux d'audit le message d'audit ORLM pour cet objet afin de confirmer que la gestion du cycle de vie des informations (ILM) a placé des copies comme

requis.

- a. Connectez-vous au nœud de grille :
 - i. Entrez la commande suivante : `ssh admin@grid_node_IP`
 - ii. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.
 - iii. Entrez la commande suivante pour passer en root : `su -`
 - iv. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer. 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. Se référer à [sous-étape 1. b](#).
- c. Utilisez `grep` pour extraire les messages d'audit associés à l'objet dans un fichier de sortie. Entrer:
`grep uuid-value audit_file_name > output_file_name`

Par exemple:

```
Admin: # grep 926026C4-00A4-449B-AC72-BCCA72DD1311 audit.log >
/var/local/tmp/messages_about_restored_object.txt
```

- d. Utilisez `grep` pour extraire les messages d'audit des règles d'objet respectées (ORLM) de ce fichier de sortie. Entrer: `grep ORLM output_file_name`

Par exemple:

```
Admin: # grep ORLM /var/local/tmp/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 `LOCS` dans le message d'audit.

Si elle est présente, la valeur de `CLDI` dans `LOCS` est l'ID du nœud et l'ID du volume où une copie d'objet a été créée. Ce message indique que l'ILM a été appliqué et que deux copies d'objet ont été créées à deux emplacements dans la grille.

6. ["Réinitialiser 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 à zéro.

Avant de commencer

- Vous devez être connecté au Grid Manager à l'aide d'un [navigateur Web pris en charge](#) .
- Tu as ["autorisations d'accès spécifiques"](#) .

À propos de cette tâche

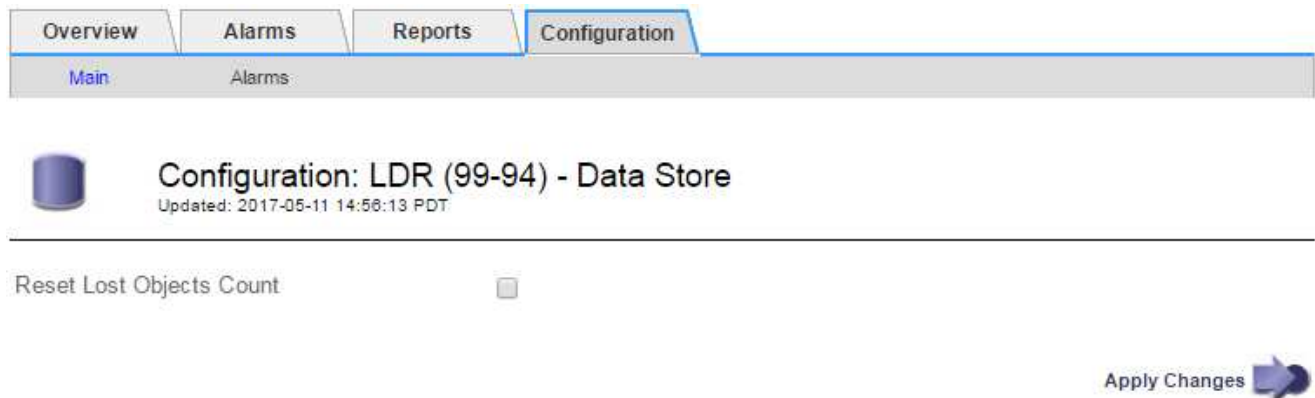
Vous pouvez réinitialiser le compteur d'objets perdus à partir de l'une des pages suivantes :

- **SUPPORT > Outils > Topologie de grille > Site > Nœud de stockage > LDR > Magasin de données > Présentation > Principal**
- **SUPPORT > Outils > Topologie de grille > Site > Nœud de stockage > DDS > Magasin de données > Présentation > Principal**

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 > Nœud de stockage > LDR > Magasin de données > Configuration** pour le nœud de stockage qui a l'alerte **Objets perdus** ou l'alarme **PERDU**.
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** ainsi que l'alarme **PERDU** s'effacent, ce qui peut prendre quelques minutes.

5. Vous pouvez également réinitialiser d'autres valeurs d'attributs associés qui pourraient avoir été incrémentées au cours du processus d'identification de l'objet perdu.
 - a. Sélectionnez **Site > Nœud de stockage > LDR > Codage d'effacement > Configuration**.
 - b. Sélectionnez **Réinitialiser le nombre d'échecs de lecture** et **Réinitialiser le nombre de copies corrompues détectées**.
 - c. Cliquez sur **Appliquer les modifications**.

- d. Sélectionnez **Site > Nœud de stockage > LDR > Vérification > 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 nécessaires, vous pouvez sélectionner **Supprimer les objets mis en quarantaine**.

Les 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 possible de supprimer en toute sécurité les objets mis en quarantaine. Cependant, si l'alerte **Objets perdus** ou l'alarme PERDU est déclenchée, le support technique peut souhaiter 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**.

Dépannage de l'alerte de faible stockage de données d'objet

L'alerte **Faible stockage de données d'objet** surveille la quantité d'espace disponible pour stocker les 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](#) .
- Tu as ["autorisations d'accès spécifiques"](#) .

À propos de cette tâche

L'alerte **Faible stockage de données d'objet** est déclenchée lorsque la quantité totale de données d'objet répliquées et codées par effacement sur un nœud de stockage répond à l'une des conditions configurées dans la règle d'alerte.

Par défaut, une alerte majeure est déclenchée lorsque cette condition est évaluée comme vraie :

```
(storagegrid_storage_utilization_data_bytes/  
(storagegrid_storage_utilization_data_bytes +  
storagegrid_storage_utilization_usable_space_bytes)) >=0.90
```

Dans cet état :

- `storagegrid\_storage\_utilization\_data\_bytes` est une estimation de la taille totale des données d'objet répliquées et codées par effacement pour un nœud de stockage.
- `storagegrid\_storage\_utilization\_usable\_space\_bytes` est la quantité totale d'espace de stockage d'objets restant pour un nœud de stockage.

Si une alerte majeure ou mineure de **Faible stockage de données d'objet** est déclenchée, vous devez effectuer une procédure d'extension dès que possible.

Étapes

1. Sélectionnez **ALERTES > Actuel**.

La page Alertes apparaît.

2. Dans le tableau des alertes, développez le groupe d'alertes **Faible stockage de données d'objet**, si nécessaire, et sélectionnez l'alerte que vous souhaitez afficher.

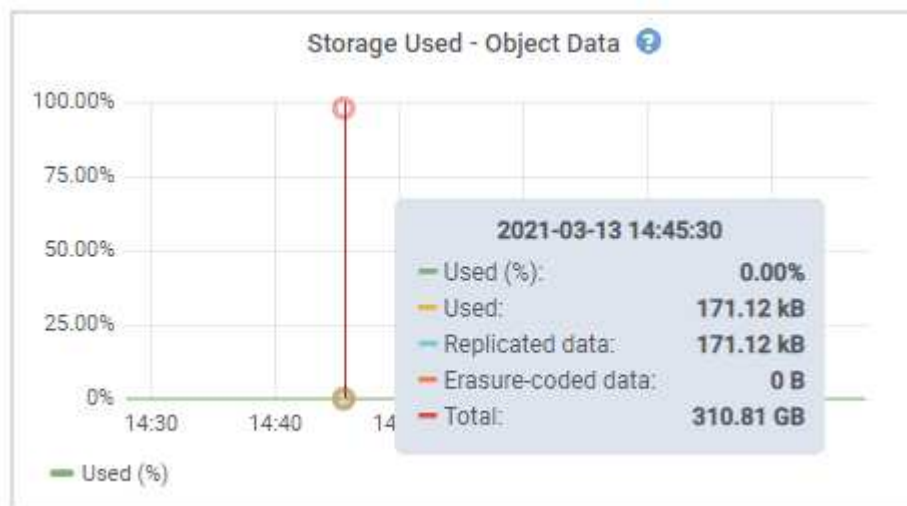


Sélectionnez l'alerte, pas l'en-tête d'un groupe d'alertes.

3. Vérifiez les détails dans la boîte de dialogue et notez les points suivants :
 - Le temps déclenché
 - Le nom du site et du nœud
 - Les valeurs actuelles des métriques pour cette alerte
4. Sélectionnez **NODES > Storage Node ou Site > Storage**.
5. Placez votre curseur sur le graphique Stockage utilisé - Données de l'objet.

Les valeurs suivantes sont affichées :

- **Utilisé (%)** : Le pourcentage de l'espace total utilisable qui a été utilisé pour les données de l'objet.
- **Utilisé** : la quantité d'espace total utilisable qui a été utilisée pour les données de l'objet.
- **Données répliquées** : une estimation de la quantité de données d'objet répliquées sur ce nœud, ce site ou cette grille.
- **Données codées par effacement** : une estimation de la quantité de données d'objet codées par effacement sur ce nœud, ce site ou cette grille.
- **Total** : La quantité totale d'espace utilisable sur ce nœud, ce site ou cette grille. La valeur utilisée est la `storagegrid_storage_utilization_data_bytes` métrique.



6. Sélectionnez les contrôles de temps au-dessus du graphique pour afficher l'utilisation du stockage sur différentes périodes.

L'analyse de l'utilisation du stockage au fil du temps peut vous aider à comprendre la quantité de stockage utilisée avant et après le déclenchement de l'alerte et peut vous aider à estimer le temps nécessaire pour que l'espace restant du nœud soit plein.

7. Dès que possible, "[ajouter de la capacité de stockage](#)" à votre réseau.

Vous pouvez ajouter des volumes de stockage (LUN) aux nœuds de stockage existants ou ajouter de

nouveaux nœuds de stockage.



Pour plus d'informations, consultez la section "[Gérer des nœuds de stockage complets](#)".

Dépannage des alertes de remplacement du 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 **Remplacement du 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](#)" les paramètres globaux étaient les mêmes valeurs appliquées 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, les 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 maximale et ne pourrait pas accepter de nouvelles données si des filigranes optimisés étaient appliqués. StorageGRID ne modifiera pas les paramètres de filigrane dans ce cas.
- Vous avez précédemment défini l'un des filigranes du volume de stockage sur une valeur personnalisée. StorageGRID ne remplacera pas les paramètres de filigrane personnalisés par des valeurs optimisées. Cependant, StorageGRID peut déclencher l'alerte **Remplacement du filigrane en lecture seule faible** si votre valeur personnalisée pour le filigrane en lecture seule logicielle du volume de stockage est trop petite.

Comprendre l'alerte

Si vous utilisez des valeurs personnalisées pour les filigranes de volume de stockage, l'alerte **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 en lecture seule du volume de stockage est inférieure à la valeur optimisée minimale pour ce nœud de stockage. Si vous continuez à utiliser le paramètre personnalisé, le nœud de stockage risque de manquer cruellement d'espace avant de pouvoir passer en toute sécurité à l'état de lecture seule. Certains volumes de stockage peuvent devenir inaccessibles (démontés automatiquement) lorsque le nœud atteint sa capacité.

Par exemple, supposons que vous ayez précédemment défini le filigrane de lecture seule logicielle du volume de stockage sur 5 Go. Supposons maintenant que StorageGRID a calculé les valeurs optimisées suivantes pour les quatre volumes de stockage du nœud de stockage A :

Volume 0	12 Go
Volume 1	12 Go
Volume 2	11 Go

L'alerte **Remplacement du filigrane en lecture seule faible** est déclenchée pour le nœud de stockage A, car votre filigrane personnalisé (5 Go) est inférieur à la valeur optimisée minimale pour tous les volumes de ce nœud (11 Go). Si vous continuez à utiliser le paramètre personnalisé, le nœud risque de manquer cruellement d'espace avant de pouvoir passer en toute sécurité à l'état de lecture seule.

Résoudre l'alerte

Suivez ces étapes si une ou plusieurs alertes de **remplacement du filigrane en lecture seule faible** 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 supérieur.
- Vous êtes connecté au Grid Manager à l'aide d'un ["navigateur Web pris en charge"](#).
- Vous avez le ["Autorisation d'accès root"](#).

À propos de cette tâche

Vous pouvez résoudre l'alerte **Remplacement du filigrane en lecture seule faible** en mettant à jour les paramètres de filigrane personnalisés avec les nouveaux remplacements de filigrane. Toutefois, si un ou plusieurs nœuds de stockage sont presque pleins ou si vous avez des exigences ILM particulières, vous devez d'abord afficher 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 **NODES**.
2. Pour chaque site de la grille, développez la liste des nœuds.
3. Consultez les valeurs de pourcentage affichées dans la colonne **Données d'objet utilisées** pour chaque nœud de stockage sur chaque site.

Nodes

View the list and status of sites and grid nodes.

Search... Total node count: 13

Name	Type	Object data used	Object metadata used	CPU usage
StorageGRID	Grid	61%	4%	—
▲ Data Center 1	Site	56%	3%	—
DC1-ADM	Primary Admin Node	—	—	6%
DC1-GW	Gateway Node	—	—	1%
! DC1-SN1	Storage Node	71%	3%	30%
! DC1-SN2	Storage Node	25%	3%	42%
! DC1-SN3	Storage Node	63%	3%	42%
! DC1-SN4	Storage Node	65%	3%	41%

4. Suivez l'étape appropriée :

- Si aucun des nœuds de stockage n'est presque plein (par exemple, toutes les valeurs **Données d'objet utilisées** sont inférieures à 80 %), vous pouvez commencer à utiliser les paramètres de remplacement. Aller à [Utiliser des filigranes optimisés](#) .
- Si les règles ILM utilisent un comportement d'ingestion strict ou si des pools de stockage spécifiques sont presque pleins, effectuez les étapes décrites dans [Afficher les filigranes de stockage optimisés](#) et [Déterminez si vous pouvez utiliser des filigranes optimisés](#) .

Afficher les filigranes de stockage optimisés

StorageGRID utilise deux mesures Prometheus pour afficher les valeurs optimisées qu'il a calculées pour le filigrane en lecture seule du volume de stockage. Vous pouvez afficher les valeurs optimisées minimales et maximales pour chaque nœud de stockage de votre grille.

Étapes

- Sélectionnez **SUPPORT > Outils > Métriques**.
- Dans la section Prometheus, sélectionnez le lien pour accéder à l'interface utilisateur de Prometheus.
- Pour voir le filigrane en lecture seule minimal recommandé, entrez la métrique Prometheus suivante et sélectionnez **Exécuter** :

```
storagegrid_storage_volume_minimum_optimized_soft_readonly_watermark
```

La dernière colonne affiche la valeur optimisée minimale du filigrane en lecture seule souple pour tous les

volumes de stockage sur chaque nœud de stockage. Si cette valeur est supérieure au paramètre personnalisé pour le filigrane en lecture seule logicielle du volume de stockage, l'alerte **Remplacement du filigrane en lecture seule faible** est déclenchée pour le nœud de stockage.

4. Pour voir le filigrane en lecture seule maximal recommandé, entrez la métrique Prometheus suivante et sélectionnez **Exécuter** :

```
storagegrid_storage_volume_maximum_optimized_soft_readonly_watermark
```

La dernière colonne affiche la valeur optimisée maximale du filigrane en lecture seule pour tous les volumes de stockage sur chaque nœud de stockage.

5. Notez la valeur optimisée maximale pour chaque nœud de stockage.

Déterminez si vous pouvez utiliser des filigranes optimisés

Étapes

1. Sélectionnez **NODES**.
2. Répétez ces étapes pour chaque nœud de stockage en ligne :
 - a. Sélectionnez **Nœud de stockage > Stockage**.
 - b. Faites défiler jusqu'au tableau Magasins d'objets.
 - c. Comparez la valeur **Disponible** pour chaque magasin d'objets (volume) au filigrane optimisé maximal que vous avez noté pour ce nœud de stockage.
3. Si au moins un volume sur chaque nœud de stockage en ligne dispose de plus d'espace disponible que le filigrane optimisé maximal pour ce nœud, accédez à [Utiliser des filigranes optimisés](#) pour commencer à utiliser les filigranes optimisés.

Sinon, étendez la grille dès que possible. Soit ["ajouter des volumes de stockage"](#) à un nœud existant ou ["ajouter de nouveaux nœuds de stockage"](#). Ensuite, allez à [Utiliser des filigranes optimisés](#) pour mettre à jour les paramètres du filigrane.

4. Si vous devez continuer à utiliser des valeurs personnalisées pour les filigranes du volume de stockage, ["silence"](#) ou ["désactiver"](#) l'alerte **Remplacement du 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 à celles recommandées pour les filigranes de volume de stockage peut entraîner l'inaccessibilité de certains volumes de stockage (démontage automatique) lorsque le nœud atteint sa capacité.

Utiliser des filigranes optimisés

Étapes

1. Accédez à **SUPPORT > Autre > Filigranes de stockage**.
2. Cochez la case **Utiliser les valeurs optimisées**.
3. Sélectionnez **Enregistrer**.

Les paramètres de filigrane de volume de stockage optimisés 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.

Résoudre les problèmes de métadonnées

Si des problèmes de métadonnées surviennent, des alertes vous informeront de la source des problèmes et des mesures recommandées à prendre. En particulier, vous devez ajouter de nouveaux nœuds de stockage si l'alerte de faible stockage de métadonnées est déclenchée.

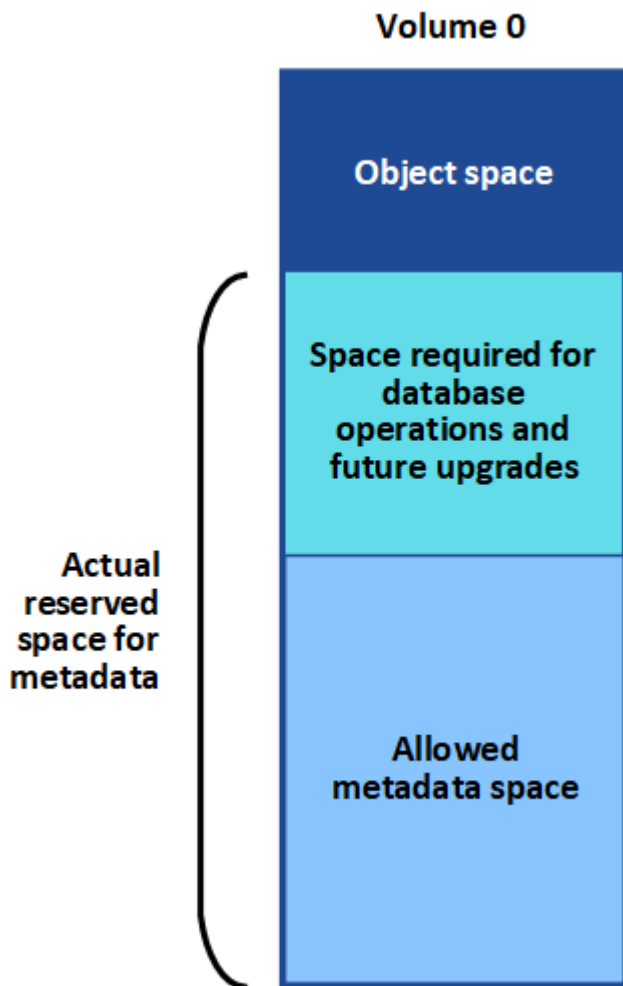
Avant de commencer

Vous êtes connecté au Grid Manager à l'aide d'un [navigateur Web pris en charge](#) .

À propos de cette tâche

Suivez les actions recommandées pour chaque alerte liée aux métadonnées déclenchée. Si l'alerte **Faible stockage de métadonnées** est déclenchée, vous devez ajouter de nouveaux nœuds de stockage.

StorageGRID réserve une certaine quantité d'espace sur le volume 0 de chaque nœud de stockage pour les métadonnées d'objet. Cet espace, appelé *espace réservé réel*, est subdivisé en espace autorisé pour les métadonnées d'objet (l'espace de métadonnées autorisé) et l'espace requis pour les opérations essentielles de la base de données, telles que le compactage et la réparation. L'espace de métadonnées autorisé régit la capacité globale de l'objet.



Si les métadonnées de l'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 produiront.

Tu peux "[surveiller la capacité des métadonnées des objets pour chaque nœud de stockage](#)" pour vous aider à anticiper les erreurs et à les corriger avant qu'elles ne surviennent.

StorageGRID utilise la métrique Prometheus suivante pour mesurer le degré de remplissage de l'espace de métadonnées autorisé :

```
storagegrid_storage_utilization_metadata_bytes/storagegrid_storage_utilization_metadata_allowed_bytes
```

Lorsque cette expression Prometheus atteint certains seuils, l'alerte **Faible stockage de métadonnées** est déclenchée.

- **Mineur** : les métadonnées de l'objet utilisent 70 % ou plus de l'espace de métadonnées autorisé. Vous devez ajouter de nouveaux nœuds de stockage dès que possible.
- **Majeur** : les métadonnées de l'objet utilisent 90 % ou plus de l'espace de métadonnées autorisé. Vous devez ajouter de nouveaux nœuds de stockage immédiatement.



Lorsque les métadonnées d'objet utilisent 90 % ou plus de l'espace de métadonnées autorisé, un avertissement apparaît sur le tableau de bord. Si cet avertissement apparaît, vous devez ajouter immédiatement de nouveaux nœuds de stockage. Vous ne devez jamais autoriser les métadonnées d'objet à utiliser plus de 100 % de l'espace autorisé.

- **Critique** : les métadonnées de l'objet utilisent 100 % ou plus 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 de nouveaux objets et ajouter immédiatement de nouveaux nœuds de stockage.



Si la taille du volume 0 est inférieure à l'option de stockage d'espace réservé aux métadonnées (par exemple, dans un environnement hors production), le calcul de l'alerte **Faible stockage de métadonnées** peut être inexact.

Étapes

1. Sélectionnez **ALERTES > Actuel**.
2. Dans le tableau des alertes, développez le groupe d'alertes **Faible stockage de métadonnées**, si nécessaire, et sélectionnez l'alerte spécifique que vous souhaitez afficher.
3. Consultez les détails dans la boîte de dialogue d'alerte.
4. Si une alerte majeure ou critique de **stockage de métadonnées faible** a été déclenchée, effectuez une extension pour ajouter immédiatement des nœuds de stockage.



Étant donné que StorageGRID conserve des copies complètes de toutes les métadonnées d'objet sur chaque site, la capacité des métadonnées de l'ensemble de la grille est limitée par la capacité des métadonnées du plus petit site. Si vous devez ajouter une capacité de métadonnées à un site, vous devez également "[développer d'autres sites](#)" par le même nombre de nœuds de stockage.

Une fois l'extension effectuée, StorageGRID redistribue les métadonnées d'objet existantes aux nouveaux nœuds, ce qui augmente la capacité globale des métadonnées de la grille. Aucune action de l'utilisateur n'est requise. L'alerte **Faible stockage de métadonnées** est effacée.

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 d'un outil de surveillance externe, vous devez vérifier le certificat.

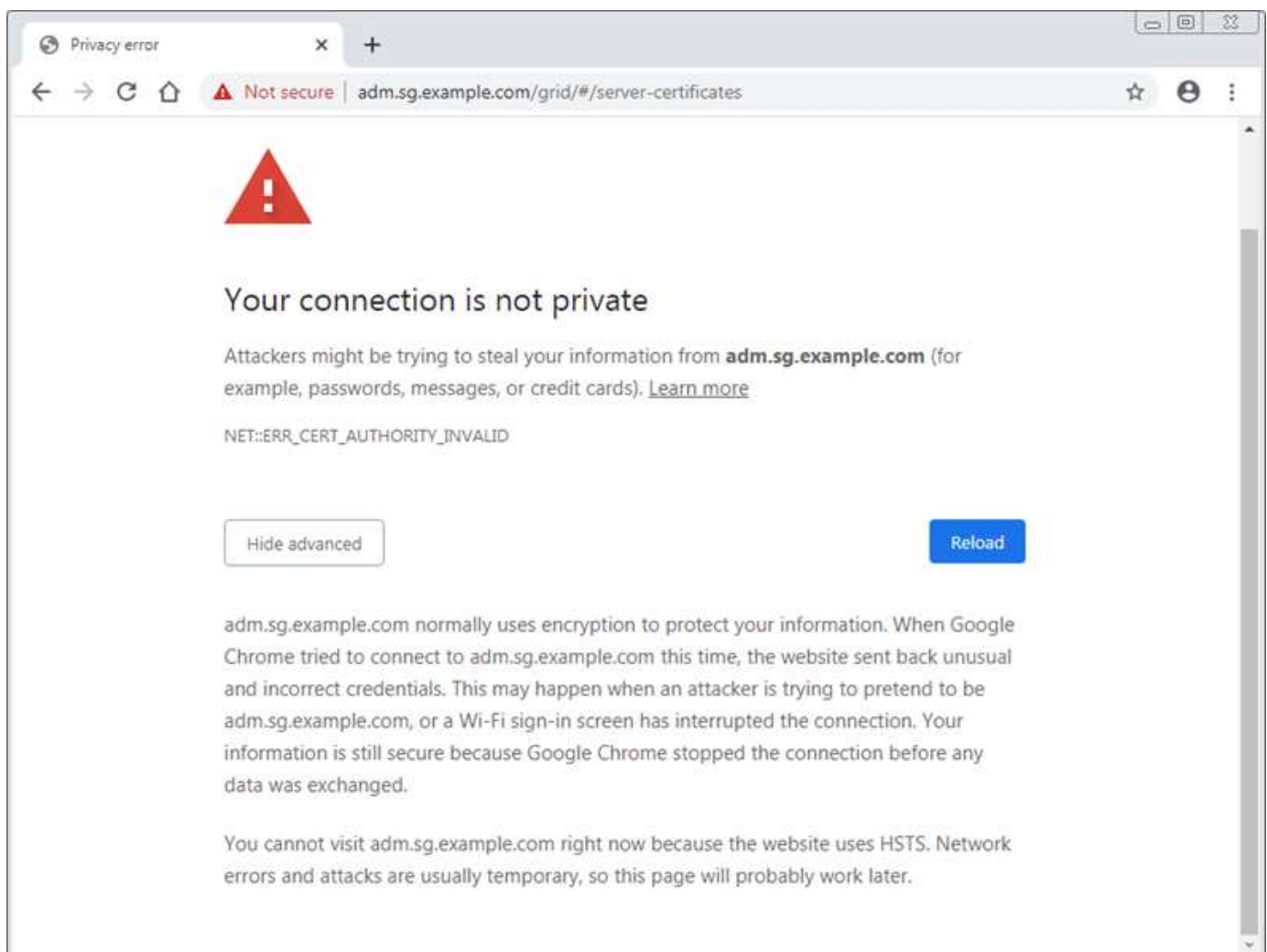
À propos de cette tâche

Les erreurs de certificat peuvent entraîner des problèmes lorsque vous essayez de vous connecter à StorageGRID à l'aide de Grid Manager, de l'API Grid Management, de Tenant Manager ou de l'API Tenant Management. Des erreurs de certificat peuvent également se produire lorsque vous essayez de vous connecter à un client S3 ou à un outil de surveillance externe.

Si vous accédez au Grid Manager ou au Tenant Manager 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'une des situations suivantes se produit :

- Votre certificat d'interface de gestion personnalisée expire.
- Vous revenez d'un certificat d'interface de gestion personnalisé au 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 perturbées 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 clients pour l'intégration Prometheus externe, des erreurs de certificat peuvent être provoquées par le certificat de l'interface de gestion StorageGRID ou par des certificats clients. L'alerte **Expiration des certificats clients configurés sur la page Certificats** est déclenchée lorsqu'un certificat client est sur le point d'expirer.

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 de certificat approprié](#)" .

1. Vérifiez la période de validité du certificat. + Certains navigateurs Web et clients S3 n'acceptent pas les certificats dont la période de validité est supérieure à 398 jours.
2. Si le certificat a expiré ou expirera bientôt, téléchargez ou générez un nouveau certificat.
 - Pour un certificat de serveur, consultez les étapes pour "[configuration d'un certificat de serveur personnalisé pour le Grid Manager et le Tenant Manager](#)" .
 - Pour un certificat client, consultez les étapes pour "[configuration d'un certificat client](#)" .
3. Pour les erreurs de certificat de serveur, essayez l'une ou les deux options suivantes :
 - Assurez-vous que le nom alternatif du sujet (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 essayez de vous connecter à StorageGRID à l'aide d'un nom de domaine :
 - i. Saisissez l'adresse IP du nœud d'administration au lieu du nom de domaine pour contourner l'erreur de connexion et accéder au gestionnaire de grille.
 - ii. Depuis le Gestionnaire de grille, sélectionnez **CONFIGURATION** > **Sécurité** > **Certificats** puis "[sélectionnez l'onglet de certificat approprié](#)" pour installer un nouveau certificat personnalisé ou continuer avec le certificat par défaut.
 - iii. Dans les instructions d'administration de StorageGRID, consultez les étapes pour "[configuration d'un certificat de serveur personnalisé pour le Grid Manager et le Tenant Manager](#)" .

Résoudre les problèmes liés au nœud d'administration et à l'interface utilisateur

Vous pouvez effectuer plusieurs tâches pour aider à déterminer la source des problèmes liés aux nœuds d'administration et à l'interface utilisateur de StorageGRID .

Erreurs de connexion au nœud d'administration

Si vous rencontrez une erreur lorsque vous vous connectez à un nœud d'administration StorageGRID , votre système peut avoir un problème avec un "[réseautage](#)" ou "[matériel](#)" problème, un problème avec "[Services du nœud d'administration](#)" , ou un "[problème avec la base de données Cassandra](#)" sur les nœuds de stockage connectés.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "[navigateur Web pris en charge](#)" .
- Vous avez le `Passwords.txt` déposer.
- Tu as "[autorisations d'accès spécifiques](#)" .

À propos de cette tâche

Utilisez ces instructions de dépannage si vous voyez l'un des messages d'erreur suivants lorsque vous tentez de vous connecter à un nœud 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 de vous connecter à nouveau.

Si l'erreur n'est pas résolue automatiquement, passez à l'étape suivante.

2. Si votre système StorageGRID possède plusieurs nœuds d'administration, essayez de vous connecter au gestionnaire de grille à partir d'un autre nœud d'administration pour vérifier l'état d'un nœud d'administration indisponible.
 - Si vous parvenez à vous connecter, vous pouvez utiliser les options **Tableau de bord**, **NODES**, **Alerts** et **SUPPORT** pour vous aider à déterminer la cause de l'erreur.
 - Si vous n'avez qu'un seul nœud d'administration ou si vous ne parvenez toujours pas à 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 pour "[configuration de l'authentification unique](#)".

Vous devrez peut-être désactiver et réactiver temporairement SSO pour un seul nœud d'administration afin de résoudre les problèmes.



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 utilisateur fédéré ne fonctionne pas, essayez de vous connecter au gestionnaire de grille en tant qu'utilisateur local, tel que root.

- Si l'utilisateur local peut se connecter :
 - i. Consultez les alertes.
 - ii. Sélectionnez **CONFIGURATION > Contrôle d'accès > Fédération d'identité**.
 - iii. Cliquez sur **Tester la connexion** pour valider vos paramètres de connexion au serveur LDAP.
 - iv. Si le test échoue, résolvez toutes les erreurs 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 Secure Shell (ssh) pour vous connecter au nœud d'administration :

- a. Entrez la commande suivante : `ssh admin@Admin_Node_IP`

- b. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.
- c. Entrez la commande suivante pour passer en root : `su -`
- d. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.

Lorsque vous êtes connecté en tant que root, l'invite passe de \$ à # .

7. Afficher l'état de tous les services exécutés sur le nœud de grille : `storagegrid-status`

Assurez-vous que les services nms, mi, nginx et mgmt api sont tous en cours d'exécution.

La sortie est mise à jour immédiatement 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. Confirmez que le service nginx-gw est en cours d'exécution # `service nginx-gw status`
- 9. Utilisez Lumberjack pour collecter des journaux : # `/usr/local/sbin/lumberjack.rb`

Si l'échec d'authentification s'est produit dans le passé, vous pouvez utiliser les options de script Lumberjack `--start` et `--end` pour spécifier la plage horaire appropriée. Utilisez `lumberjack -h` pour plus de détails sur ces options.

La sortie vers le terminal indique où l'archive du 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 ne parvenez pas à identifier de problèmes avec le nœud d'administration, exécutez l'une des commandes suivantes pour déterminer les adresses IP des trois nœuds de stockage qui exécutent le service ADC sur votre site. En règle générale, il s'agit des trois premiers nœuds de stockage installés sur le site.

```
# cat /etc/hosts
```

```
# gpt-list-services adc
```

Les nœuds d'administration utilisent le service ADC pendant le processus d'authentification.

12. Depuis le nœud d'administration, utilisez `ssh` pour vous connecter à chacun des nœuds de stockage ADC, en utilisant les adresses IP que vous avez identifiées.

13. Afficher l'état de tous les services exécutés sur le nœud de grille : `storagegrid-status`

Assurez-vous que les services `idnt`, `acct`, `nginx` et `cassandra` sont tous en cours d'exécution.

14. Répéter les étapes [Utilisez le bûcheron pour collecter des bûches](#) et [Réviser les journaux](#) 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 d'interface utilisateur

L'interface utilisateur du Grid Manager ou du Tenant Manager peut ne pas répondre comme prévu après la mise à niveau du logiciel StorageGRID .

Étapes

1. Assurez-vous que vous utilisez un ["navigateur Web pris en charge"](#) .
2. Videz le cache de votre navigateur Web.

La suppression du cache supprime les ressources obsolètes utilisées par la version précédente du logiciel StorageGRID et permet à l'interface utilisateur de fonctionner à nouveau correctement. Pour obtenir des

instructions, consultez la documentation de votre navigateur Web.

Résoudre les problèmes de réseau, de matériel et de plate-forme

Il existe plusieurs tâches que vous pouvez effectuer pour vous aider à déterminer la source des problèmes liés au réseau, au matériel et à la plate-forme StorageGRID .

Erreur « 422 : Entité non traitable »

L'erreur 422 : Entité non traitable peut se produire pour différentes raisons. Vérifiez le message d'erreur pour déterminer la cause de votre problème.

Si vous voyez l'un des messages d'erreur répertoriés, prenez l'action recommandée.

Message d'erreur	Cause profonde et action corrective
<pre>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</pre>	Ce message peut s'afficher si vous sélectionnez l'option Ne pas utiliser TLS pour Transport Layer Security (TLS) lors de la configuration de la fédération d'identité à l'aide de Windows Active Directory (AD). L'utilisation de l'option Ne pas utiliser TLS n'est pas prise en charge pour une utilisation avec des serveurs AD qui appliquent la signature LDAP. Vous devez sélectionner l'option Utiliser STARTTLS ou l'option Utiliser LDAPS pour TLS.

Message d'erreur	Cause profonde et action corrective
<pre>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)</pre>	Ce message s'affiche si vous essayez d'utiliser un chiffrement non pris en charge pour établir une connexion TLS (Transport Layer Security) depuis StorageGRID vers un système externe utilisé pour identifier la fédération ou les pools de stockage 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 grille

L'alerte **Incompatibilité MTU du réseau de grille** est déclenchée lorsque le paramètre d'unité de transmission maximale (MTU) pour l'interface du réseau de grille (eth0) diffère considérablement entre les nœuds de la grille.

À propos de cette tâche

Les différences dans les paramètres MTU peuvent indiquer que certains réseaux eth0, mais pas tous, sont configurés pour les trames jumbo. Une non-concordance de taille MTU supérieure à 1 000 peut entraîner des problèmes de performances réseau.

Étapes

1. Répertoriez les paramètres MTU pour eth0 sur tous les nœuds.
 - Utilisez la requête fournie dans le gestionnaire de grille.
 - Accéder à *primary Admin Node IP address/metrics/graph* et entrez la requête suivante :
node_network_mtu_bytes{device="eth0"}
2. ["Modifier les paramètres MTU"](#) si nécessaire pour garantir qu'ils sont les mêmes pour l'interface du réseau Grid (eth0) sur tous les nœuds.
 - Pour les nœuds basés sur 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 avoir la valeur MTU souhaitée, puis utiliser le change-ip.py script pour changer la valeur MTU du réseau dans le conteneur.

Utilisez les arguments suivants pour modifier le MTU sur les nœuds basés sur Linux ou VMware.

Arguments positionnels	Description
mtu	Le MTU à définir. Doit être compris entre 1280 et 9216.
network	Les réseaux auxquels appliquer le MTU. Inclure un ou plusieurs des types de réseaux suivants : • grille • administrateur • client

+

Arguments optionnels	Description
-h, - help	Afficher le message d'aide et quitter.
-n node, --node node	Le nœud. La valeur par défaut est le nœud local.

Alerte d'erreur de réception de trame de réseau de nœuds

Les alertes **Erreur de réception de trame de réseau de nœuds** peuvent être provoquées par des problèmes de connectivité entre StorageGRID et votre matériel réseau. Cette alerte disparaît d'elle-même une fois le problème sous-jacent résolu.

À propos de cette tâche

Les alertes **Erreur de réception de trame de réseau de nœud** peuvent être provoquées par les problèmes suivants avec le matériel réseau qui se connecte à StorageGRID:

- La correction d'erreur directe (FEC) est requise et n'est pas utilisée
- Incompatibilité entre le port du commutateur et le MTU de la carte réseau
- Taux d'erreur de lien élevés
- Dépassement de mémoire tampon en anneau de la carte réseau

Étapes

1. Suivez les étapes de dépannage pour toutes les causes potentielles de cette alerte en fonction de la configuration de votre réseau.
2. Effectuez les étapes suivantes en fonction de la cause de l'erreur :

Incompatibilité FEC



Ces étapes s'appliquent uniquement aux alertes **Erreur de trame de réception du réseau de nœuds** causées par une incompatibilité FEC sur les appliances StorageGRID .

- a. Vérifiez l'état FEC du port dans le commutateur connecté à votre appliance StorageGRID .
- b. Vérifiez l'intégrité physique des câbles reliant l'appareil au commutateur.
- c. Si vous souhaitez modifier les paramètres FEC pour tenter de résoudre l'alerte, assurez-vous d'abord que l'appliance est configurée pour le mode **Auto** sur la page Configuration de liaison du programme d'installation de l'appliance StorageGRID (consultez les instructions de votre appliance :
 - "SG6160"
 - "SGF6112"
 - "SG6000"
 - "SG5800"
 - "SG5700"
 - "SG110 et SG1100"
 - "SG100 et SG1000"
- d. Modifiez les paramètres FEC sur les ports du commutateur. Les ports de l'appliance StorageGRID ajusteront leurs paramètres FEC pour correspondre, si possible.

Vous ne pouvez pas configurer les paramètres FEC sur les appliances StorageGRID . Au lieu de cela, les appareils tentent de découvrir et de refléter les paramètres FEC sur les ports de commutateur auxquels ils sont connectés. Si les liaisons sont forcées à des vitesses de réseau de 25 GbE ou 100 GbE, le commutateur et la carte réseau risquent de ne pas parvenir à négocier un paramètre FEC commun. Sans paramètre FEC commun, le réseau reviendra au mode « sans FEC ». Lorsque FEC n'est pas activé, les connexions sont plus sensibles aux erreurs causées par le bruit électrique.



Les appliances StorageGRID prennent en charge Firecode (FC) et Reed Solomon (RS) FEC, ainsi que l'absence de FEC.

Incompatibilité entre le port du commutateur et le MTU de la carte réseau

Si l'alerte est provoquée par une incompatibilité entre le port de commutateur et le MTU de la carte réseau, vérifiez que la taille du MTU configurée sur le nœud est la même que le paramètre MTU du port de commutateur.

La taille MTU configurée sur le nœud peut être inférieure au paramètre sur le port de commutateur auquel le nœud est connecté. Si un nœud StorageGRID reçoit une trame Ethernet supérieure à son MTU, ce qui est possible avec cette configuration, l'alerte **Erreur de trame de réception du réseau du nœud** peut être signalée. Si vous pensez que c'est ce qui se passe, modifiez le MTU du port du commutateur pour qu'il corresponde au MTU de l'interface réseau StorageGRID ou modifiez le MTU de l'interface réseau StorageGRID pour qu'il corresponde au port du commutateur, en fonction de vos objectifs ou exigences en matière de MTU de bout en bout.



Pour des performances réseau optimales, tous les nœuds doivent être configurés avec des valeurs MTU similaires sur leurs interfaces Grid Network. L'alerte **Incompatibilité MTU du réseau de grille** est déclenchée s'il existe une différence significative dans les paramètres MTU du réseau de grille sur des nœuds individuels. Les valeurs MTU ne doivent pas nécessairement être les mêmes pour tous les types de réseaux. Voir [Dépannage de l'alerte de non-concordance MTU du réseau de grille](#) pour plus d'informations.



Voir aussi ["Modifier le paramètre MTU"](#) .

Taux d'erreur de lien élevés

- Activez FEC, si ce n'est pas déjà fait.
- Vérifiez que votre câblage réseau est de bonne qualité et qu'il n'est pas endommagé ou mal connecté.
- Si les câbles ne semblent pas être le problème, contactez le support technique.



Vous remarquerez peut-être des taux d'erreur élevés dans un environnement avec un bruit électrique élevé.

Dépassement de mémoire tampon en anneau de la carte réseau

Si l'erreur est un dépassement de mémoire tampon en anneau de la carte réseau, contactez le support technique.

La mémoire tampon en anneau peut être saturée lorsque le système StorageGRID est surchargé et incapable de traiter les événements réseau en temps opportun.

3. Surveillez le problème et contactez le support technique si l'alerte ne se résout pas.

Erreurs de synchronisation horaire

Vous pourriez rencontrer des problèmes de synchronisation horaire dans votre grille.

Si vous rencontrez des problèmes de synchronisation horaire, 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 de haute précision, tels que StorageGRID.

Linux : problèmes de connectivité réseau

Vous pourriez rencontrer des problèmes de connectivité réseau pour les nœuds StorageGRID hébergés sur des hôtes Linux.

Clonage d'adresse MAC

Dans certains cas, les problèmes de réseau peuvent être résolus en utilisant le clonage d'adresse MAC. Si vous utilisez des hôtes virtuels, définissez la valeur de la clé de clonage d'adresse MAC pour chacun de vos réseaux sur « true » dans votre fichier de configuration de nœud. Ce paramètre oblige l'adresse MAC du conteneur StorageGRID à utiliser l'adresse MAC de l'hôte. Pour créer des fichiers de configuration de nœud, consultez les instructions pour ["Red Hat Enterprise Linux"](#) ou ["Ubuntu ou Debian"](#) .



Créez des interfaces réseau virtuelles distinctes à utiliser par 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 promiscuité n'a pas été activé sur l'hyperviseur.

Pour plus d'informations sur l'activation du clonage MAC, consultez les instructions de ["Red Hat Enterprise Linux"](#) ou ["Ubuntu ou Debian"](#) .

Mode promiscuité

Si vous ne souhaitez pas utiliser le clonage d'adresse MAC et préférez autoriser toutes les interfaces à recevoir et à transmettre des données pour des 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 **Accepter** pour le mode promiscuité, les modifications d'adresse MAC et les transmissions falsifiées. Les valeurs définies sur le commutateur virtuel peuvent être remplacées par les valeurs au niveau du groupe de ports. Assurez-vous donc que les paramètres sont les mêmes aux deux endroits.

Pour plus d'informations sur l'utilisation du mode Promiscuous, consultez les instructions de ["Red Hat Enterprise Linux"](#) ou ["Ubuntu ou Debian"](#) .

Linux : l'état du nœud est « orphelin »

Un nœud Linux dans un état orphelin indique généralement que le service StorageGrid ou le démon du nœud StorageGRID contrôlant le conteneur du nœud est mort de manière inattendue.

À propos de cette tâche

Si un nœud Linux signale qu'il est dans un état orphelin, vous devez :

- Vérifiez les journaux pour les erreurs et les messages.
- Essayez de redémarrer le nœud.
- Si nécessaire, utilisez les commandes du moteur de conteneur pour arrêter le conteneur de nœud existant.
- Redémarrez le nœud.

Étapes

1. Vérifiez les journaux du démon de service et du nœud orphelin pour détecter d'éventuelles erreurs évidentes ou des messages concernant une sortie inattendue.
2. Connectez-vous à l'hôte en tant que root ou en utilisant un compte avec l'autorisation sudo.
3. Essayez de redémarrer le nœud 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 contrôle du nœud de grille de stockage. Par exemple : `sudo docker stop --time secondscontainer-name`

Pour `seconds` , entrez le nombre de secondes pendant lesquelles vous souhaitez attendre que le conteneur s'arrête (généralement 15 minutes ou moins). Par exemple:

```
sudo docker stop --time 900 storagegrid-DC1-S1-172-16-1-172
```

5. Redémarrer le nœud : `storagegrid node start node-name`

```
storagegrid node start DC1-S1-172-16-1-172
```

Linux : Dépannage de la prise en charge d'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.

À propos de cette tâche

Pour voir l'adresse IPv6 qui a été attribuée à un nœud de grille :

1. Sélectionnez **NODES** et sélectionnez le nœud.
2. Sélectionnez **Afficher les adresses IP supplémentaires** à côté de **Adresses IP** dans l'onglet Présentation.

Si l'adresse IPv6 n'est pas affichée et que le nœud est installé sur un hôte Linux, suivez ces étapes 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 devrait être 0.

```
net.ipv6.conf.all.disable_ipv6 = 0
```



Si le résultat n'est pas 0, consultez la documentation de votre système d'exploitation pour modifier `sysctl` paramètres. Ensuite, changez la valeur à 0 avant de continuer.

3. Entrez le conteneur de nœud 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 devrait être 1.

```
net.ipv6.conf.all.disable_ipv6 = 1
```



Si le résultat n'est pas 1, cette procédure ne s'applique pas. Contactez le support technique.

5. Sortir du conteneur : `exit`

```
root@DC1-S1:~ # exit
```

6. En tant que root, éditez 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 qui peuvent être liés à l'utilisation d'un serveur syslog externe et répertorie les actions correctives.

Pour plus d'informations sur l'envoi d'informations d'audit à un serveur syslog externe, consultez :

- ["Considérations relatives à l'utilisation d'un serveur syslog externe"](#)
- ["Configurer les messages d'audit et le serveur syslog externe"](#)

Message d'erreur	Description et actions recommandées
Ne peut pas résoudre le nom d'hôte	Le nom de domaine complet que vous avez saisi pour le serveur syslog n'a pas pu être résolu en une adresse IP. 1. Vérifiez le nom d'hôte que vous avez entré. Si vous avez saisi une adresse IP, assurez-vous qu'il s'agit d'une adresse IP valide en notation WXYZ (« décimale à points »). 2. Vérifiez que les serveurs DNS sont correctement configurés. 3. Confirmez que chaque nœud peut accéder aux adresses IP du serveur DNS.
Connexion rejetée	Une connexion TCP ou TLS au serveur syslog a été refusée. Il se peut qu'aucun service n'écoute sur le port TCP ou TLS pour l'hôte, ou qu'un pare-feu bloque l'accès. 1. Vérifiez que vous avez entré le nom de domaine complet ou l'adresse IP, le port et le protocole corrects pour le serveur Syslog. 2. Confirmez que l'hôte du service Syslog exécute un démon Syslog qui écoute sur le port spécifié. 3. Confirmez qu'un pare-feu ne bloque pas l'accès aux connexions TCP/TLS des nœuds à l'IP et au port du serveur syslog.
Réseau inaccessible	Le serveur syslog n'est pas sur un sous-réseau directement connecté. Un routeur a renvoyé un message d'échec ICMP pour indiquer qu'il ne pouvait pas transmettre les messages de test des nœuds répertoriés au serveur Syslog. 1. Vérifiez que vous avez entré le nom de domaine complet ou l'adresse IP correct pour le serveur syslog. 2. Pour chaque nœud répertorié, vérifiez la liste des sous-réseaux du réseau de grille, les listes de sous-réseaux des réseaux d'administration et les passerelles du réseau client. Confirmez qu'ils sont configurés pour acheminer le trafic vers le serveur Syslog via l'interface réseau et la passerelle attendues (Grille, Admin ou Client).

Message d'erreur	Description et actions recommandées
Hôte inaccessible	Le serveur syslog se trouve sur un sous-réseau directement connecté (sous-réseau utilisé par les nœuds répertoriés pour leurs adresses IP de grille, d'administration ou de 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 entré le nom de domaine complet ou l'adresse IP correct pour le serveur syslog. 2. Vérifiez que l'hôte exécutant le service syslog est opérationnel.
La connexion a expiré	Une tentative de connexion TCP/TLS a été effectuée, mais aucune réponse n'a été reçue du serveur syslog pendant une longue période. Il peut y avoir une mauvaise configuration du routage ou un pare-feu peut abandonner le trafic sans envoyer de réponse (une configuration courante). 1. Vérifiez que vous avez entré le nom de domaine complet ou l'adresse IP correct pour le serveur syslog. 2. Pour chaque nœud répertorié, vérifiez la liste des sous-réseaux du réseau de grille, les listes de sous-réseaux des réseaux d'administration et les passerelles du réseau client. Confirmez qu'ils sont configurés pour acheminer le trafic vers le serveur Syslog à l'aide de l'interface réseau et de la passerelle (Grille, Admin ou Client) sur lesquelles vous prévoyez que le serveur Syslog sera atteint. 3. Confirmez 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 a été fermée ultérieurement. Les raisons peuvent être les suivantes : • 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 peut fermer les connexions TCP inactives. • Un serveur non-syslog écoutant sur le port du serveur syslog a peut-être fermé la connexion. Pour résoudre ce problème : 1. Vérifiez que vous avez entré le nom de domaine complet ou l'adresse IP, le port et le protocole corrects pour le serveur Syslog. 2. Si vous utilisez TLS, vérifiez que le serveur syslog utilise également TLS. Si vous utilisez TCP, vérifiez que le serveur syslog utilise également TCP. 3. Vérifiez qu'un pare-feu intermédiaire n'est pas configuré pour fermer les connexions TCP inactives.

Message d'erreur	Description et actions recommandées
Erreur de certificat TLS	Le certificat de serveur reçu du serveur syslog n'était pas compatible avec le groupe de certificats CA et le certificat client que vous avez fournis. 1. Confirmez que le groupe de certificats CA et le certificat client (le cas échéant) sont compatibles avec le certificat du serveur sur le serveur Syslog. 2. Confirmez que les identités dans le certificat du serveur du serveur syslog incluent les valeurs IP ou FQDN attendues.
Transfert suspendu	Les enregistrements Syslog ne sont plus transmis au serveur Syslog et StorageGRID n'est pas en mesure de détecter la raison. Consultez les journaux de débogage fournis avec cette erreur pour tenter de déterminer la cause première.
Session TLS terminée	Le serveur Syslog a mis fin à la session TLS et StorageGRID n'est pas en mesure de détecter la raison. 1. Consultez les journaux de débogage fournis avec cette erreur pour tenter de déterminer la cause première. 2. Vérifiez que vous avez entré le nom de domaine complet ou l'adresse IP, le port et le protocole corrects pour le serveur Syslog. 3. Si vous utilisez TLS, vérifiez que le serveur syslog utilise également TLS. Si vous utilisez TCP, vérifiez que le serveur syslog utilise également TCP. 4. Confirmez que le groupe de certificats CA et le certificat client (le cas échéant) sont compatibles avec le certificat du serveur du serveur Syslog. 5. Confirmez que les identités dans le certificat du serveur du serveur syslog incluent les valeurs IP ou FQDN attendues.
La requête de résultats a échoué	Le nœud d'administration utilisé pour la configuration et les tests du serveur Syslog ne peut pas demander les résultats des tests aux nœuds répertoriés. Un ou plusieurs nœuds peuvent 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 miscd sur les nœuds répertoriés.

Examiner les journaux d'audit

Messages d'audit et journaux

Ces instructions contiennent des informations sur la structure et le contenu des messages d'audit et des journaux d'audit StorageGRID . Vous pouvez utiliser ces informations pour lire et analyser la piste d'audit de l'activité du système.

Ces instructions sont destinées aux administrateurs chargés de produire des rapports d'activité et d'utilisation du système qui nécessitent l'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, consultez ["Configurer les messages d'audit et les destinations des journaux"](#) .

Auditer le flux et la rétention des messages

Tous les services StorageGRID génèrent des messages d'audit pendant le fonctionnement normal du système. Vous devez comprendre comment ces messages d'audit circulent à travers le système StorageGRID vers le `audit.log` déposer.

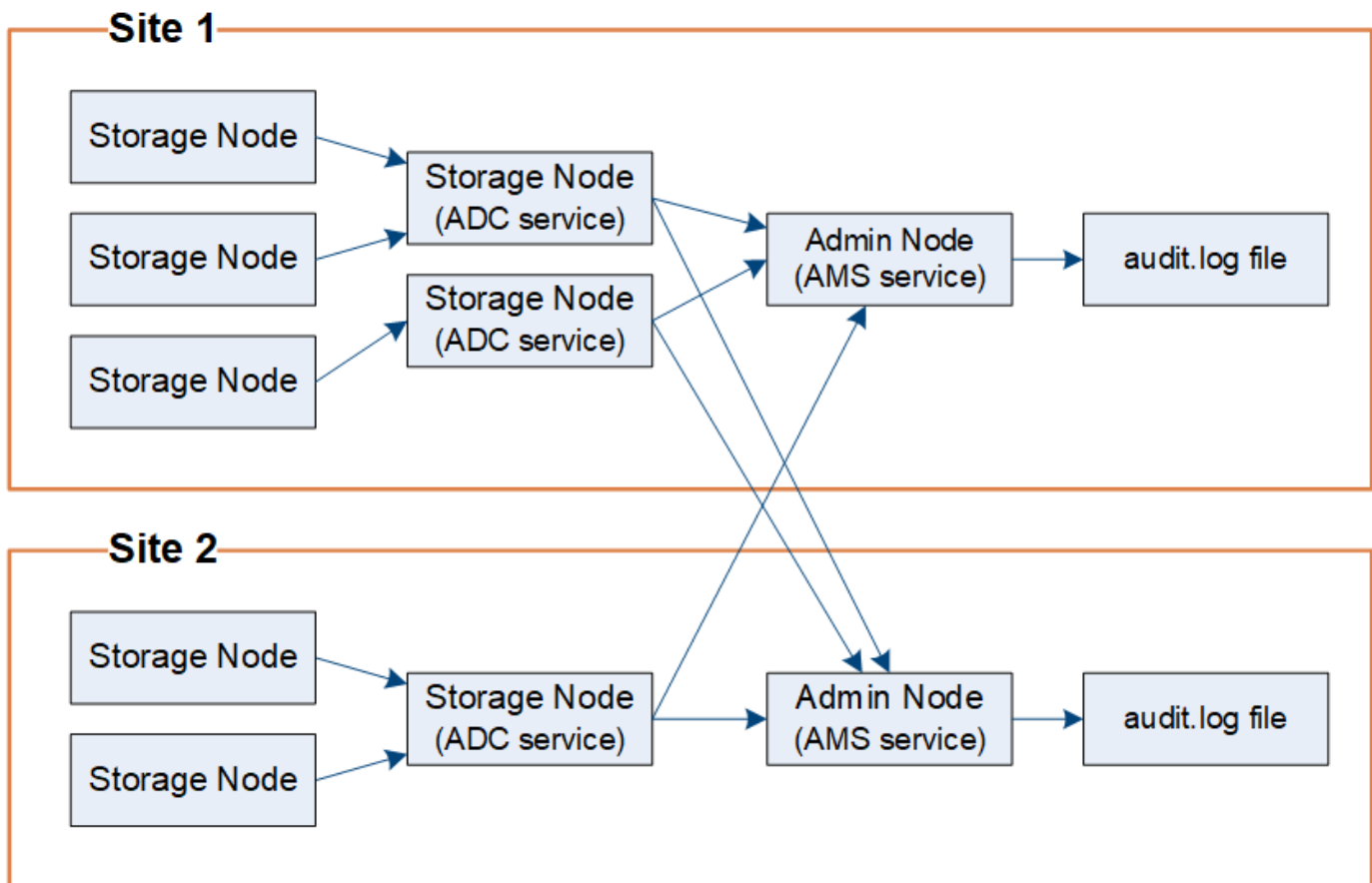
Flux de messages d'audit

Les messages d'audit sont traités par les nœuds d'administration et par les nœuds de stockage dotés d'un service de contrôleur de domaine administratif (ADC).

Comme indiqué dans le diagramme de flux de messages d'audit, chaque nœud StorageGRID envoie ses messages d'audit à l'un des services ADC sur le site du centre de données. Le service ADC est automatiquement activé pour les trois premiers nœuds de stockage installés sur chaque site.

À 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.

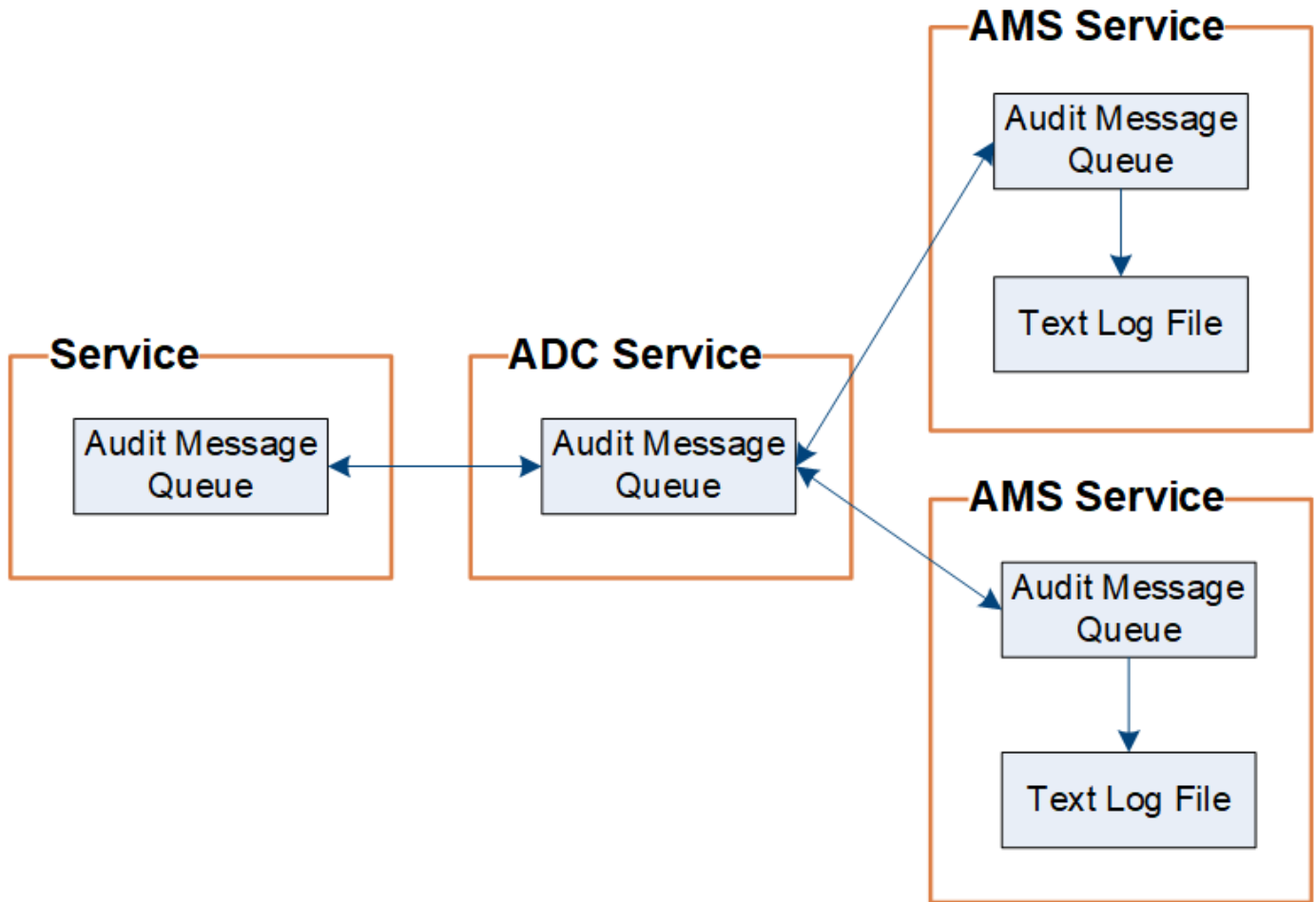
Chaque nœud d'administration stocke les messages d'audit dans des fichiers journaux texte ; le fichier journal actif est nommé `audit.log` .



Rétention des messages d'audit

StorageGRID utilise un processus de copie et de suppression pour garantir qu'aucun message d'audit n'est perdu avant de pouvoir être écrit dans le journal d'audit.

Lorsqu'un nœud génère ou relaie un message d'audit, le message est stocké dans une file d'attente de messages d'audit sur le disque système du nœud de 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/log` annuaire. 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. À mesure que les files d'attente augmentent, elles consomment davantage d'espace disponible dans chaque nœud. `/var/local/` annuaire. Si le problème persiste et que le répertoire des messages d'audit d'un nœud devient trop plein, les nœuds individuels donneront la priorité au traitement de leur arriéré et deviendront temporairement indisponibles pour les nouveaux messages.

Plus précisément, vous pourriez observer les comportements suivants :

- Si le `/var/local/log` le répertoire utilisé par un nœud d'administration devient plein, le nœud d'administration sera marqué comme indisponible pour les nouveaux messages d'audit jusqu'à ce que le répertoire ne soit plus plein. Les demandes des clients S3 ne sont pas affectées. L'alarme XAMS (Unreachable Audit Repositories) 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 marqué comme indisponible pour les messages d'audit jusqu'à ce que le répertoire ne soit plein qu'à 87 %. Les demandes des clients S3 adressées à d'autres nœuds ne sont pas affectées. L'alarme NRLY (relais d'audit disponibles) est déclenchée lorsque les relais d'audit sont inaccessibles.



S'il n'y a pas de nœuds de stockage disponibles avec le service ADC, les nœuds de stockage stockent les messages d'audit localement dans le `/var/local/log/localaudit.log` déposer.

- Si le `/var/local/` répertoire utilisé par un nœud de stockage devient plein à 85 %, le nœud commencera à refuser les demandes des clients S3 avec `503 Service Unavailable`.

Les types de problèmes suivants peuvent entraîner une augmentation considérable de la taille des files d'attente de messages d'audit :

- La 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 être en retard.
- Un taux d'activité soutenu qui dépasse la capacité d'audit du système.
- Le `/var/local/` l'espace sur un nœud de stockage ADC devient plein pour des raisons sans rapport avec les messages d'audit. Lorsque cela se produit, le nœud cesse d'accepter de nouveaux messages d'audit et donne la priorité à son arriéré actuel, ce qui peut entraîner des arriérés sur d'autres nœuds.

Alerte de file d'attente d'audit volumineuse 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 au fil du 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 devraient se résoudre au fil du temps et peuvent être ignorées.

Si l'alerte ou l'alarme persiste et augmente en gravité, affichez un graphique de la taille de la file d'attente. Si le nombre 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 enregistrés en modifiant le niveau d'audit pour les écritures et les lectures du client sur Erreur ou Désactivé. Voir "[Configurer les messages d'audit et les destinations des journaux](#)".

Messages en double

Le système StorageGRID adopte une approche conservatrice en cas de défaillance d'un réseau ou d'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 les éléments actifs `audit.log` fichier et tous les fichiers journaux d'audit compressés. Vous pouvez accéder aux fichiers journaux d'audit directement à partir de la ligne de commande du nœud d'administration.

Avant de commencer

- Tu as "[autorisations d'accès spécifiques](#)".
- Vous devez avoir le `Passwords.txt` déposer.
- Vous devez connaître l'adresse IP d'un nœud d'administration.

Étapes

1. Connectez-vous à un nœud d'administration :
 - a. Entrez la commande suivante : `ssh admin@primary_Admin_Node_IP`
 - b. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.
 - c. Entrez la commande suivante pour passer en root : `su -`
 - d. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.

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/log
```

3. Affichez 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/log` annuaire. Les fichiers journaux d'audit actifs sont nommés `audit.log` .



En option, vous pouvez modifier la destination des journaux d'audit et envoyer les informations d'audit à un serveur syslog externe. Les journaux locaux des enregistrements d'audit continuent d'être générés et stockés lorsqu'un serveur syslog externe est configuré. Voir "[Configurer les messages d'audit et les destinations des journaux](#)" .

Une fois par jour, l'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 en une seule journée, les noms de fichiers utilisent la date d'enregistrement du fichier, suivie d'un numéro, au 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 une journée, le fichier enregistré est compressé et renommé, au format `yyyy-mm-dd.txt.gz` , qui préserve la date originale. Au fil du temps, cela entraîne une consommation de stockage allouée 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/log` annuaire. Les journaux d'audit sont supprimés en fonction de la date de leur création, le plus ancien étant supprimé en premier. Vous pouvez surveiller les actions du script dans le fichier suivant : `/var/local/log/manage-audit.log` .

Cet exemple montre l'actif `audit.log` fichier, le fichier de la veille(`2018-04-15.txt`), et le fichier compressé du jour précédent(`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

Les fichiers journaux d'audit se trouvent sur chaque nœud d'administration et contiennent une collection de messages d'audit individuels.

Chaque message d'audit contient les éléments suivants :

- Le 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, placé 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 plus de lisibilité). Ces messages ont été générés lorsqu'un locataire a créé un bucket S3 et ajouté deux objets à ce bucket.

2019-08-07T18:43:30.247711

```
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991681][TIME(UI64):73520][SAIP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::17530064241597054718:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"bucket1"][AVER(UI32):10][ATIM(UI64):1565203410247711]
[ATYP(FC32):SPUT][ANID(UI32):12454421][AMID(FC32):S3RQ][ATID(UI64):7074142142472611085]]
```

2019-08-07T18:43:30.783597

```
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991696][TIME(UI64):120713][SAIP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::17530064241597054718:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"bucket1"][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(FC32):S3RQ][ATID(UI64):8439606722108456022]]
```

2019-08-07T18:43:30.784558

```
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991693][TIME(UI64):121666][SAIP(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::17530064241597054718:root"]
[SBAI(CSTR):"17530064241597054718"][SBAC(CSTR):"s3tenant"][S3BK(CSTR):"bucket1"][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(FC32):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](#) pour résumer combien d’opérations d’écriture, de lecture et de suppression ont été enregistrées et combien de temps ces opérations ont pris.

Utiliser l’outil d’audit-explication

Vous pouvez utiliser le `audit-explain` outil permettant de traduire les messages

d'audit du journal d'audit dans un format facile à lire.

Avant de commencer

- Tu as "[autorisations d'accès spécifiques](#)".
- Vous devez avoir le `Passwords.txt` déposer.
- Vous devez connaître l'adresse IP du nœud d'administration principal.

À propos de cette tâche

Le `audit-explain` L'outil, disponible sur le nœud d'administration principal, fournit des résumés simplifiés des messages d'audit dans un journal d'audit.



Le `audit-explain` L'outil est principalement destiné à être utilisé par le support technique lors des opérations de dépannage. Traitement `audit-explain` les requêtes peuvent consommer une grande quantité de puissance CPU, ce qui peut avoir un impact sur les opérations `StorageGRID`.

Cet exemple montre une sortie typique de la `audit-explain` outil. Ces quatre "**CRACHER**" des messages d'audit ont été générés lorsque le locataire S3 avec l'ID de compte 92484777680322627870 a utilisé des requêtes S3 PUT pour créer un bucket nommé « bucket1 » et ajouter trois objets à ce bucket.

```
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 simples ou compressés. Par exemple:

```
audit-explain audit.log
```

```
audit-explain 2019-08-12.txt.gz
```

- Traiter plusieurs fichiers simultanément. Par exemple:

```
audit-explain audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz
```

```
audit-explain /var/local/log/*
```

- Acceptez l'entrée d'un tube, ce qui vous permet de filtrer et de prétraiter l'entrée à l'aide du `grep` commandement ou autres moyens. Par exemple:

```
grep SPUT audit.log | audit-explain
```

```
grep bucket-name audit.log | audit-explain
```

Étant donné que les journaux d'audit peuvent être très volumineux et lents à analyser, vous pouvez gagner du temps en filtrant les parties que vous souhaitez consulter et en les exécutant. `audit-explain` sur les parties, au lieu du fichier entier.



Le `audit-explain` l'outil n'accepte pas les fichiers compressés comme entrée canalisée. Pour traiter les fichiers compressés, fournissez leurs noms de fichiers comme arguments de ligne de commande ou utilisez le `zcat` outil pour décompresser les fichiers en premier. Par exemple:

```
zcat audit.log.gz | audit-explain
```

Utilisez le `help` (`-h`) option pour voir les options disponibles. Par exemple:

```
$ audit-explain -h
```

Étapes

1. Connectez-vous au nœud d'administration principal :

- Entrez la commande suivante : `ssh admin@primary_Admin_Node_IP`
- Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.
- Entrez la commande suivante pour passer en root : `su -`
- Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.

Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

2. Entrez la commande suivante, où `/var/local/log/audit.log` représente le nom et l'emplacement du ou des fichiers que vous souhaitez analyser :

```
$ audit-explain /var/local/log/audit.log
```

Le `audit-explain` L'outil imprime des interprétations lisibles par l'homme de tous les messages dans le ou les fichiers spécifiés.



Pour réduire la longueur des lignes et améliorer la lisibilité, les horodatages ne sont pas affichés par défaut. Si vous souhaitez voir les horodatages, utilisez l'horodatage(`-t`) option.

Utiliser l'outil d'audit-somme

Vous pouvez utiliser le `audit-sum` outil permettant de compter les messages d'audit d'écriture, de lecture, d'en-tête et de suppression et de voir le temps minimum, maximum et moyen (ou la taille) pour chaque type d'opération.

Avant de commencer

- Tu as "[autorisations d'accès spécifiques](#)".
- Vous devez avoir le `Passwords.txt` déposer.
- Vous devez connaître l'adresse IP du nœud d'administration principal.

À propos de cette tâche

Le `audit-sum` L'outil, disponible sur le nœud d'administration principal, résume 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 à être utilisé par le support technique lors des opérations de dépannage. Traitement `audit-sum` les requêtes peuvent consommer une grande quantité de puissance CPU, ce qui peut avoir un impact sur les opérations StorageGRID .

Cet exemple montre une sortie typique de la `audit-sum` outil. Cet exemple montre combien de temps ont pris les opérations du protocole.

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` L'outil fournit les décomptes et les heures des messages d'audit S3, Swift et ILM suivants dans un journal d'audit.



Les codes d'audit sont supprimés du produit et de la documentation à mesure que les fonctionnalités sont obsolètes. Si vous rencontrez un code d'audit qui n'est pas répertorié ici, vérifiez les versions précédentes de cette rubrique pour les anciennes versions de SG. Par exemple : "[Documentation de l'outil d'audit de StorageGRID 11.8](#)".

Code	Description	Se référer à
IDEL	Suppression initiée par ILM : enregistre le moment où ILM démarre le processus de suppression d'un objet.	" IDEL : suppression initiée par ILM "
SDEL	S3 DELETE : enregistre une transaction réussie pour supprimer un objet ou un bucket.	" SDEL : SUPPRESSION S3 "
SGET	S3 GET : enregistre une transaction réussie pour récupérer un objet ou répertorier les objets dans un bucket.	" SGET : S3 OBTENIR "
KARITÉ	S3 HEAD : enregistre une transaction réussie pour vérifier l'existence d'un objet ou d'un bucket.	" SHEA : TÊTE S3 "

Code	Description	Se référer à
CRACHER	S3 PUT : enregistre une transaction réussie pour créer un nouvel objet ou un nouveau bucket.	"SPUT : S3 PUT"
WDEL	Swift DELETE : enregistre une transaction réussie pour supprimer un objet ou un conteneur.	"WDEL : SUPPRESSION rapide"
WGET	Swift GET : enregistre une transaction réussie pour récupérer un objet ou répertorier les objets dans un conteneur.	"WGET : Swift GET"
WHEA	Swift HEAD : enregistre une transaction réussie pour vérifier l'existence d'un objet ou d'un conteneur.	"WHEA : TÊTE RAPIDE"
WPUT	Swift PUT : enregistre une transaction réussie pour créer un nouvel objet ou conteneur.	"WPUT : Swift PUT"

Le `audit-sum` L'outil peut effectuer les opérations suivantes :

- Traiter les journaux d'audit simples ou compressés. Par exemple:

```
audit-sum audit.log
```

```
audit-sum 2019-08-12.txt.gz
```

- Traiter plusieurs fichiers simultanément. Par exemple:

```
audit-sum audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz
```

```
audit-sum /var/local/log/*
```

- Acceptez l'entrée d'un tube, ce qui vous permet de filtrer et de prétraiter l'entrée à l'aide du `grep` commandement ou autres moyens. 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 canalisée. Pour traiter les fichiers compressés, fournissez leurs noms de fichiers comme arguments de ligne de commande ou utilisez le `zcat` outil pour décompresser les fichiers en premier. Par exemple:

```
audit-sum audit.log.gz
```

```
zcat audit.log.gz | audit-sum
```

Vous pouvez utiliser des options de ligne de commande pour résumer les opérations sur les buckets séparément des opérations sur les objets ou pour regrouper les résumés de messages par nom de bucket, par

période ou par type de cible. Par défaut, les résumés affichent le temps de fonctionnement minimum, maximum et moyen, mais vous pouvez utiliser le `size (-s)` option permettant de regarder la taille de l’objet à la place.

Utilisez le `help (-h)` option pour voir les options disponibles. Par exemple:

```
$ audit-sum -h
```

Étapes

- 1. Connectez-vous au nœud d’administration principal :
 - a. Entrez la commande suivante : `ssh admin@primary_Admin_Node_IP`
 - b. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.
 - c. Entrez la commande suivante pour passer en root : `su -`
 - d. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.

Lorsque vous êtes connecté en tant que root, l’invite passe de `$` à `#` .

- 2. Si vous souhaitez analyser tous les messages liés aux opérations d’écriture, de lecture, de lecture et de suppression, suivez ces étapes :
 - a. Entrez la commande suivante, où `/var/local/log/audit.log` représente le nom et l’emplacement du ou des fichiers que vous souhaitez analyser :

```
$ audit-sum /var/local/log/audit.log
```

Cet exemple montre une sortie typique de la `audit-sum` outil. Cet exemple montre combien de temps ont pris les opérations du protocole.

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 plus lentes en moyenne avec 1,13 seconde, mais les opérations SGET et SPUT (S3 PUT) affichent toutes deux des temps de pire cas longs d’environ 1 770 secondes.

- b. Pour afficher les 10 opérations de récupération les plus lentes, utilisez la commande `grep` pour sélectionner uniquement les messages SGET et ajoutez l’option de sortie longue (`-l`) pour inclure les

chemins d'objet :

```
grep SGET audit.log | audit-sum -l
```

Les résultats incluent le type (objet ou bucket) et le chemin, ce qui vous permet de rechercher dans le journal d'audit d'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/r9010aQ8JB-1566861764-4519.iso
    1624414429      10.96.101.125      object     5375001556
backup/r9010aQ8JB-1566861764-6618.iso
    1533143793      10.96.101.125      object     5183661466
backup/r9010aQ8JB-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
```

+

À partir de cet exemple de sortie, vous pouvez voir que les trois requêtes S3 GET les plus lentes concernaient des objets d'une taille d'environ 5 Go, ce qui est beaucoup plus grand que les autres objets. La grande taille explique les temps de récupération les plus lents dans le pire des cas.

3. Si vous souhaitez déterminer les tailles des objets ingérés et récupérés dans votre grille, utilisez l'option de taille(-s):

```
audit-sum -s audit.log
```


message group average (MB)	count	min (MB)	max (MB)
=====	=====	=====	=====
IDEL 1654.502	274	0.004	5000.000
SDEL 1.695	213371	0.000	10.504
SGET 14.920	201906	0.000	5000.000
SHEA 2.967	22716	0.001	10.504
SPUT 2.495	1771398	0.000	5000.000

Dans cet exemple, la taille moyenne de l'objet pour SPUT est inférieure à 2,5 Mo, mais la taille moyenne pour SGET est beaucoup plus grande. Le nombre de messages SPUT est bien supérieur au nombre de messages SGET, ce qui indique que la plupart des objets ne sont jamais récupérés.

4. Si vous souhaitez déterminer si les récupérations ont été lentes hier :
 - a. Émettez la commande sur le journal d'audit approprié et utilisez l'option de regroupement par heure(`-gt`), suivi de la période (par exemple, 15M, 1H, 10S) :

```
grep SGET audit.log | audit-sum -gt 1H
```

message group average(sec)	count	min(sec)	max(sec)
=====	=====	=====	=====
2019-09-05T00 1.254	7591	0.010	1481.867
2019-09-05T01 1.115	4173	0.011	1740.290
2019-09-05T02 1.562	20142	0.011	1274.961
2019-09-05T03 1.254	57591	0.010	1383.867
2019-09-05T04 1.405	124171	0.013	1740.290
2019-09-05T05 1.562	420182	0.021	1274.511
2019-09-05T06 5.562	1220371	0.015	6274.961
2019-09-05T07 2.002	527142	0.011	1974.228
2019-09-05T08 1.105	384173	0.012	1740.290
2019-09-05T09 1.354	27591	0.010	1481.867

Ces résultats montrent que le trafic S3 GET a augmenté entre 06h00 et 07h00. Les temps maximum et moyen sont également considérablement plus élevés à ces moments-là, et ils n'augmentent pas progressivement à mesure que le nombre augmente. Cela suggère que la capacité a été dépassée quelque part, peut-être dans le réseau ou dans la capacité du réseau à traiter les demandes.

- b. Pour déterminer la taille des objets récupérés chaque heure hier, ajoutez l'option de taille(-s) à la commande :

```
grep SGET audit.log | audit-sum -gt 1H -s
```

message group average(B)	count	min(B)	max(B)
=====	=====	=====	=====
2019-09-05T00 1.976	7591	0.040	1481.867
2019-09-05T01 2.062	4173	0.043	1740.290
2019-09-05T02 2.303	20142	0.083	1274.961
2019-09-05T03 1.182	57591	0.912	1383.867
2019-09-05T04 1.528	124171	0.730	1740.290
2019-09-05T05 2.398	420182	0.875	4274.511
2019-09-05T06 51.328	1220371	0.691	5663711385.961
2019-09-05T07 2.147	527142	0.130	1974.228
2019-09-05T08 1.878	384173	0.625	1740.290
2019-09-05T09 1.354	27591	0.689	1481.867

Ces résultats indiquent que certaines récupérations très importantes ont eu lieu lorsque le trafic de récupération global était à son maximum.

- c. Pour voir plus de détails, utilisez le ["outil d'audit-explication"](#) pour passer en revue toutes les opérations SGET pendant cette heure :

```
grep 2019-09-05T06 audit.log | grep SGET | audit-explain | less
```

Si la sortie de la commande `grep` doit comporter plusieurs 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 buckets sont plus lentes que les opérations SPUT pour les objets :

- a. Commencez par utiliser le `-go` option, qui regroupe séparément les messages pour les opérations d'objet et de compartiment :

```
grep SPUT sample.log | audit-sum -go
```

message group average(sec)	count	min(sec)	max(sec)
=====	=====	=====	=====
SPUT.bucket 0.125	1	0.125	0.125
SPUT.object 0.236	12	0.025	1.019

Les résultats montrent que les opérations SPUT pour les buckets ont des caractéristiques de performances différentes des opérations SPUT pour les objets.

- b. Pour déterminer quels buckets ont les opérations SPUT les plus lentes, utilisez le `-gb` option, qui regroupe les messages par bucket :

```
grep SPUT audit.log | audit-sum -gb
```

message group average(sec)	count	min(sec)	max(sec)
=====	=====	=====	=====
SPUT.cho-non-versioning 1.571	71943	0.046	1770.563
SPUT.cho-versioning 1.415	54277	0.047	1736.633
SPUT.cho-west-region 1.329	80615	0.040	55.557
SPUT.ldt002 0.361	1564563	0.011	51.569

- c. Pour déterminer quels buckets ont la plus grande taille d'objet SPUT, utilisez à la fois le `-gb` et le `-s` options:

```
grep SPUT audit.log | audit-sum -gb -s
```

message group average (B)	count	min (B)	max (B)
=====	=====	=====	=====
SPUT.cho-non-versioning 21.672	71943	2.097	5000.000
SPUT.cho-versioning 21.120	54277	2.097	5000.000
SPUT.cho-west-region 14.433	80615	2.097	800.000
SPUT.ltd002 0.352	1564563	0.000	999.972

Format du message d'audit

Format du message d'audit

Les messages d'audit échangés au sein du système StorageGRID incluent des informations standard communes à tous les messages et un contenu spécifique décrivant l'événement ou l'activité signalé.

Si les informations récapitulatives fournies par le ["audit-explication"](#) et ["somme d'audit"](#) les outils sont insuffisants, reportez-vous à cette section pour comprendre le format général de tous les messages d'audit.

Voici un exemple de message d'audit tel qu'il pourrait apparaître dans le fichier journal d'audit :

```
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):9445736326500603516]]
```

Chaque message d'audit contient une chaîne d'éléments d'attribut. La chaîne entière est entourée de crochets([]), et chaque élément d'attribut dans la chaîne a les caractéristiques suivantes :

- Entouré de parenthèses []
- 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 saut de ligne \n

Chaque élément comprend un code d'attribut, un type de données et une valeur qui sont rapportés 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 signalé. Certains attributs sont communs à tous les messages d'audit et d'autres sont spécifiques à chaque événement.
- `type` est un identifiant à quatre caractères du type de données de programmation de la valeur, tel que UI64, FC32, etc. Le type est entre parenthèses `( )`.
- `value` est le contenu de l'attribut, généralement une valeur numérique ou textuelle. Les valeurs suivent toujours deux points `:`. Les valeurs de type de données CSTR sont entourées de guillemets doubles « ».

Types de données

Différents types de données sont utilisés pour stocker des informations dans les messages d'audit.

Type	Description
UI32	Entier long non signé (32 bits) ; il peut stocker les nombres de 0 à 4 294 967 295.
UI64	Entier long double non signé (64 bits) ; il peut stocker les nombres de 0 à 18 446 744 073 709 551 615.
FC32	Constante à quatre caractères ; une valeur entière non signée de 32 bits représentée par quatre caractères ASCII tels que « ABCD ».
iPad	Utilisé pour les adresses IP.
CSTR	Un tableau de longueur variable de caractères UTF-8. Les caractères peuvent être échappés avec les conventions suivantes : • La barre oblique inverse est \. • Le retour chariot est \r. • Les guillemets doubles sont \". • Le saut de ligne (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 l'événement

Chaque message d'audit dans le journal d'audit enregistre des 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 :

```
2018-12-05T08:24:45.921845 [AUDT:*[RSLT\FC32\):SUCS\]*  
\[TIME\UI64\):11454\]\[SAIP\IPAD\):"10.224.0.100"\]\[S3AI\CSTR\):"60025621595611246499"\]  
\[SACC\CSTR\):"compte"\]\[S3AK\CSTR\):"SGKH4_Nc8SO1H6w3w0nCOFCGgk__E6dYzKlumRsK  
JA=="\]\[SUSR\CSTR\):"urn:sgws:identity::60025621595611246499:root"\]  
\[SBAI\UI64\):"60025621595611246499"\]\[SBAC\CSTR\):"account"\]\[S3BK\CSTR\):"bucket"\]  
\[S3KY\CSTR\):"object"\]\[CBID\UI64\):0xCC128B9B9E428347\]\[UUID\CSTR\):"B975D2CE-E4DA-  
4D14-8A23-1CB4B83F2CD8"\]\[CSIZ\UI64\):30720\]\[AVER\UI32\):10]  
\[ATIM\UI64\):1543998285921845\]\[ATYP\FC32\):SHEA\]\[ANID\UI32\):12281045\]\[AMID\FC32\):S3RQ]  
\[ATID\UI64\):15552417629170647261\]
```

Le **ATYP** L'élément (souligné dans l'exemple) identifie quel événement a généré le message. Cet exemple de message inclut le **"KARITÉ"** code de message ([ATYP(FC32):SHEA]), indiquant qu'il a été généré par une demande S3 HEAD réussie.

Éléments communs aux messages d'audit

Tous les messages d'audit contiennent les éléments communs.

Code	Type	Description
AU MILIEU DE	FC32	ID du module : identifiant à quatre caractères de l'ID du module qui a généré le message. Cela indique le segment de code dans lequel le message d'audit a été généré.
ANID	UI32	ID de nœud : l'ID de nœud de grille attribué au service qui a généré le message. Chaque service se voit attribuer un identifiant unique au moment de la configuration et de l'installation du système StorageGRID . Cet identifiant ne peut pas être modifié.
ASES	UI64	Identifiant de session d'audit : dans les versions précédentes, cet élément indiquait l'heure à laquelle le système d'audit était 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.

Code	Type	Description
ASQN	UI64	Nombre de séquences : dans les versions précédentes, ce compteur était incrémenté pour chaque message d'audit généré sur le nœud de grille (ANID) et réinitialisé à zéro au redémarrage du service. Remarque : cet élément est obsolète et n'apparaît plus dans les messages d'audit.
ATID	UI64	ID de trace : un identifiant partagé par l'ensemble des messages déclenchés par un événement unique.
ATIM	UI64	Horodatage : l'heure à laquelle l'événement a été généré et a déclenché le message d'audit, mesurée 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. L'arrondi ou la troncature de l'horodatage enregistré peut être nécessaire. L'heure lisible par l'homme qui apparaît au début du message d'audit dans le <code>audit.log</code> le fichier est l'attribut ATIM au format ISO 8601. La date et l'heure sont représentées comme <code>YYYY-MMDDTHH:MM:SS.UUUUUU</code>, où le T est une chaîne de caractères littérale indiquant le début du segment de temps de la date. <code>UUUUUU</code> sont des microsecondes.
ATYP	FC32	Type d'événement : identifiant à quatre caractères de l'événement enregistré. Cela régit le contenu de la « charge utile » du message : les attributs qui sont inclus.
MOYENNE	UI32	Version : la version du message d'audit. À mesure que le logiciel StorageGRID évolue, de nouvelles versions de services peuvent intégrer de nouvelles fonctionnalités dans les rapports d'audit. Ce champ permet la compatibilité descendante dans le service AMS pour traiter les messages provenant d'anciennes versions de services.
RSLT	FC32	Résultat : le résultat d'un événement, d'un processus ou d'une transaction. Si ce n'est pas pertinent pour un message, NONE est utilisé plutôt que SUCS afin que le message ne soit pas filtré accidentellement.

Exemples de messages d'audit

Vous pouvez trouver des informations détaillées dans chaque message d'audit. Tous les messages d'audit utilisent le même format.

Ce qui suit est un exemple de message d'audit tel qu'il pourrait apparaître dans le `audit.log` déposer:


```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"] [
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"] [S3BK(CSTR):"s3small11"] [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 enregistré, ainsi que des informations sur le message d'audit lui-même.

Pour identifier quel événement est 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):"s3small11"] [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. **"CRACHER"** représente une transaction S3 PUT, qui enregistre l'ingestion d'un objet dans un bucket.

Le message d'audit suivant indique également le compartiment auquel 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\):"s3small11"] [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 UTC (Universal Coordinated Time) au début du message d'audit. Cette valeur est une version lisible par l'homme 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):"bc644d381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"][S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"][S3BK(CSTR):"s3small11"][S3KY(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):1579224144102530435]]
```

ATIM enregistre le temps, en microsecondes, depuis le début de l'époque UNIX. Dans l'exemple, la valeur 1405631878959669 se traduit par jeudi 17 juillet 2014 21:17:59 UTC.

Messages d'audit et cycle de vie des objets

Quand les messages d'audit sont-ils générés ?

Des messages d'audit sont générés chaque fois qu'un objet est ingéré, récupéré ou supprimé. Vous pouvez identifier ces transactions dans le journal d'audit en localisant les messages d'audit spécifiques à l'API S3.

Les messages d'audit sont liés via des identifiants spécifiques à chaque protocole.

Protocole	Code
Liaison des opérations S3	S3BK (godet), S3KY (clé) ou les deux
Lier les opérations Swift	WCON (conteneur), WOBJ (objet) ou les deux
Lier les opérations internes	CBID (identifiant interne de l'objet)

Moment des messages d'audit

En raison de facteurs tels que les différences de synchronisation entre les nœuds de grille, la taille des objets et les délais du réseau, l'ordre des messages d'audit générés par les différents services peut varier par rapport à celui indiqué dans les exemples de cette section.

Transactions d'ingestion d'objets

Vous pouvez identifier les transactions d'ingestion client dans le journal d'audit en localisant les messages d'audit spécifiques à l'API S3.

Tous les messages d'audit générés lors d'une transaction d'ingestion ne sont pas répertoriés dans les tableaux suivants. Seuls les messages nécessaires au suivi de la transaction d'ingestion sont inclus.

Messages d'audit d'ingestion S3

Code	Nom	Description	Tracer	Voir
CRACHER	Transaction S3 PUT	Une transaction d'ingestion S3 PUT s'est terminée avec succès.	CBID, S3BK, S3KY	"SPUT : S3 PUT"
ORLM	Règles d'objet respectées	La politique ILM a été satisfaite pour cet objet.	CBID	"ORLM : Règles d'objet respectées"

Messages d'audit d'ingestion rapide

Code	Nom	Description	Tracer	Voir
WPUT	Transaction PUT rapide	Une transaction d'ingestion Swift PUT a été effectuée avec succès.	CBID, WCON, WOBJ	"WPUT : Swift PUT"
ORLM	Règles d'objet respectées	La politique ILM a été satisfaite pour cet objet.	CBID	"ORLM : Règles d'objet respectées"

Exemple : ingestion d'objets 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 dans un nœud de stockage (service LDR).

Dans cet exemple, la stratégie ILM active inclut la règle ILM « Créer 2 copies ».



Tous les messages d'audit générés lors d'une transaction ne sont pas répertoriés dans l'exemple ci-dessous. Seuls ceux liés à la transaction d'ingestion S3 (SPUT) sont répertoriés.

Cet exemple suppose qu'un bucket S3 a été précédemment créé.

SPUT : S3 PUT

Le message SPUT est généré pour indiquer qu'une transaction S3 PUT 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):"SGKHya1RU_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 qui a été appliquée.

Pour les objets répliqués, le champ LOCS inclut l'ID du nœud LDR et l'ID du volume des emplacements des 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 à codage d'effacement, le champ LOCS inclut l'ID du profil de codage d'effacement et l'ID du groupe de codage 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 PATH inclut des informations sur le bucket S3 et la clé ou des informations sur le conteneur et l'objet Swift, 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'objets

Vous pouvez identifier les transactions de suppression d'objet dans le journal d'audit en localisant les messages d'audit spécifiques à l'API S3.

Tous les messages d'audit générés lors d'une transaction de suppression ne sont pas répertoriés dans les tableaux suivants. Seuls les messages nécessaires au suivi de la transaction de suppression sont inclus.

S3 supprime les messages d'audit

Code	Nom	Description	Tracer	Voir
SDEL	S3 Supprimer	Demande effectuée pour supprimer l'objet d'un bucket.	CBID, S3KY	"SDEL : SUPPRESSION S3"

Suppression rapide des messages d'audit

Code	Nom	Description	Tracer	Voir
WDEL	Suppression rapide	Demande effectuée pour supprimer l'objet d'un conteneur, ou le 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 d'audit.



Tous les messages d'audit générés lors d'une transaction de suppression ne sont pas répertoriés dans l'exemple ci-dessous. Seuls ceux liés à la transaction de suppression S3 (SDEL) sont répertoriés.

SDEL : Suppression S3

La suppression d'objet commence lorsque le client envoie une demande DeleteObject à un service LDR. Le message contient le bucket à partir duquel supprimer l'objet et la clé S3 de l'objet, qui est utilisée pour 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'objets

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.

Tous les messages d'audit générés lors d'une transaction de récupération ne sont pas répertoriés dans les

tableaux suivants. Seuls les messages nécessaires au suivi de la transaction de récupération sont inclus.

Messages d'audit de récupération S3

Code	Nom	Description	Tracer	Voir
SGET	GET S3	Demande effectuée pour récupérer un objet d'un bucket.	CBID, S3BK, S3KY	"SGET : S3 OBTENIR"

Messages d'audit de récupération rapide

Code	Nom	Description	Tracer	Voir
WGET	Swift GET	Demande effectuée pour récupérer un objet d'un conteneur.	CBID, WCON, WOBJ	"WGET : Swift GET"

Exemple : récupération d'objet 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 lors d'une transaction ne sont pas répertoriés dans l'exemple ci-dessous. Seuls ceux liés à la transaction de récupération S3 (SGET) sont répertoriés.

SGET : S3 OBTENIR

La récupération d'objet commence lorsque le client envoie une demande GetObject à un service LDR. Le message contient le bucket à partir duquel récupérer l'objet et la clé S3 de l'objet, qui est utilisée pour 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 politique de compartiment le permet, un client peut récupérer des objets de manière anonyme ou récupérer des objets à partir d'un compartiment appartenant à un autre compte de locataire. Le message d'audit contient des informations sur le compte locataire du propriétaire du bucket afin que vous puissiez suivre ces demandes anonymes et inter-comptes.

Dans l'exemple de message suivant, le client envoie une requête GetObject pour un objet stocké dans un bucket dont il n'est pas propriétaire. Les valeurs de SBAI et SBAC enregistrent l'ID et le nom du compte locataire du propriétaire du bucket, qui diffèrent de l'ID et du nom du compte locataire du client enregistrés

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 Sélectionner 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 lors d'une transaction ne sont pas répertoriés dans l'exemple ci-dessous. Seuls ceux liés à la transaction S3 Select (SelectObjectContent) sont répertoriés.

Chaque requête génère deux messages d'audit : l'un qui exécute l'autorisation de la demande S3 Select (le champ S3SR est défini sur « select ») et une opération GET standard ultérieure 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

Les messages d'audit sont générés lorsqu'un client S3 met à jour les métadonnées d'un objet.

Messages d'audit de mise à jour des métadonnées S3

Code	Nom	Description	Tracer	Voir
SUPD	Métadonnées S3 mises à jour	Généré 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 montre une transaction réussie pour mettre à jour les métadonnées d'un objet S3 existant.

SUPD : mise à jour des métadonnées S3

Le client S3 fait une demande (SUPD) pour 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 il a été configuré comme en-tête de protocole d'audit (**CONFIGURATION > Surveillance > Serveur d'audit et syslog**). Voir ["Configurer 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

Descriptions des messages d'audit

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 de filtrage des messages d'audit souhaité.

Les messages d'audit sont également répertoriés par ordre alphabétique en fonction de leurs codes à quatre caractères. Cette liste alphabétique vous permet de trouver des informations sur des messages spécifiques.

Les codes à quatre caractères utilisés tout au long de 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, consultez ["Configurer les](#)

Catégories de messages d'audit

Messages d'audit du système

Les messages d'audit appartenant à la catégorie d'audit système sont utilisés pour les événements liés au système d'audit lui-même, aux états des nœuds de grille, à l'activité des tâches à l'échelle du système (tâches de grille) et aux opérations de sauvegarde de service.

Code	Titre et description du message	Voir
ECMC	Fragment de données codées par effacement manquant : indique qu'un fragment de données codées par effacement manquant a été détecté.	"ECMC : Fragment de données codées par effacement manquant"
ECOC	Fragment de données codées par effacement corrompu : indique qu'un fragment de données codées par effacement corrompu a été détecté.	"ECOC : fragment de données corrompu et codé par effacement"
ETAF	Échec de l'authentification de sécurité : une tentative de connexion utilisant Transport Layer Security (TLS) a échoué.	"ETAF : échec de l'authentification de sécurité"
GNRG	Enregistrement GNDS : un service a mis à jour ou enregistré des informations le concernant dans le système StorageGRID .	"GNRG : Enregistrement GNDS"
GNUR	Désinscription GNDS : un service s'est désinscrit du système StorageGRID .	"GNUR : Désinscription 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 soumise au service CMN.	"GTSU : tâche de grille soumise"
LLST	Emplacement perdu : ce message d'audit est généré lorsqu'un emplacement est perdu.	"LLST : Localisation perdue"
OLST	Objet perdu : un objet demandé ne peut pas être localisé dans le système StorageGRID .	"OLST : le système a détecté un objet perdu"
SADD	Désactivation de l'audit de sécurité : la journalisation des messages d'audit a été désactivée.	"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 : un bloc de contenu a échoué aux contrôles de vérification.	"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 inconnu"
SYSD	Arrêt du nœud : un arrêt a été demandé.	"SYSD : arrêt du nœud"
SYST	Arrêt du nœud : un service a initié un arrêt gracieux.	"SYST : arrêt du nœud"
SYSU	Démarrage du nœud : un service a démarré ; la nature de l'arrêt précédent est indiquée dans le message.	"SYSU : démarrage du nœud"

Messages d'audit du stockage d'objets

Les messages d'audit appartenant à la catégorie d'audit de stockage d'objets sont utilisés pour les événements liés au stockage et à la gestion des objets au sein du système StorageGRID . Il s'agit notamment du stockage et de la récupération d'objets, des transferts de nœud de grille à nœud de grille et des vérifications.



Les codes d'audit sont supprimés du produit et de la documentation à mesure que les fonctionnalités sont obsolètes. Si vous rencontrez un code d'audit qui n'est pas répertorié ici, vérifiez les versions précédentes de cette rubrique pour les anciennes versions de SG. Par exemple : ["Messages d'audit du stockage d'objets StorageGRID 11.8"](#) .

Code	Description	Voir
FRÈRE	Demande de lecture seule de bucket : un bucket est entré ou sorti du mode lecture seule.	"BROR : demande de lecture seule du bucket"
CBSE	Fin d'envoi de l'objet : l'entité source a terminé une opération de transfert de données de nœud de grille à nœud de grille.	"CBSE : Fin d'envoi d'objet"
CBRE	Fin de réception de l'objet : l'entité de destination a terminé une opération de transfert de données de nœud de grille à nœud de grille.	"CBRE : extrémité de réception d'objet"

Code	Description	Voir
CGRR	Demande de réplication inter-grille : StorageGRID a tenté une opération de réplication inter-grille pour répliquer des objets entre des buckets dans une connexion de fédération de grille.	"CGRR : demande de réplication inter-réseau"
EBDL	Suppression d'un compartiment vide : le scanner ILM a supprimé un objet dans un compartiment qui supprime tous les objets (effectuant une opération de vidage de compartiment).	"EBDL : Suppression du bucket vide"
EBKR	Demande de compartiment vide : un utilisateur a envoyé une demande pour activer ou désactiver le compartiment vide (c'est-à-dire pour supprimer des objets du compartiment ou pour arrêter la suppression d'objets).	"EBKR : demande de seau vide"
SCMT	Validation du magasin d'objets : un bloc de contenu a été entièrement stocké et vérifié et peut désormais être demandé.	"SCMT : demande de validation du magasin d'objets"
SREM	Supprimer le 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"

Le client lit les messages d'audit

Les messages d'audit de lecture du client sont enregistrés lorsqu'une application client S3 effectue une demande de récupération d'un objet.

Code	Description	Utilisé par	Voir
S3SL	Requête S3 Select : enregistre une fin après qu'une requête S3 Select a été renvoyée au client. Le message S3SL peut inclure des détails sur le message d'erreur et le code d'erreur. La demande n'a peut-être pas abouti.	Client S3	"S3SL : Demande de sélection S3"
SGET	S3 GET : enregistre une transaction réussie pour récupérer un objet ou répertorier les objets dans un bucket. Remarque : si la transaction fonctionne sur une sous-ressource, le message d'audit inclura le champ S3SR.	Client S3	"SGET : S3 OBTENIR"
KARITÉ	S3 HEAD : enregistre une transaction réussie pour vérifier l'existence d'un objet ou d'un bucket.	Client S3	"SHEA : TÊTE S3"

Code	Description	Utilisé par	Voir
WGET	Swift GET : enregistre une transaction réussie pour récupérer un objet ou répertorier les objets dans un conteneur.	Client Swift	"WGET : Swift GET"
WHEA	Swift HEAD : enregistre une transaction réussie pour vérifier l'existence d'un objet ou d'un conteneur.	Client Swift	"WHEA : TÊTE RAPIDE"

Le client écrit des messages d'audit

Les messages d'audit d'écriture client sont enregistrés lorsqu'une application client S3 effectue une demande de création ou de modification d'un objet.

Code	Description	Utilisé par	Voir
OVWR	Écrasement d'objet : enregistre une transaction pour écraser un objet par un autre objet.	Clients S3 et Swift	"OVWR : écrasement d'objet"
SDEL	S3 DELETE : enregistre une transaction réussie pour supprimer un objet ou un bucket. Remarque : si la transaction fonctionne sur une sous-ressource, le message d'audit inclura le champ S3SR.	Client S3	"SDEL : SUPPRESSION S3"
SPOS	S3 POST : enregistre une transaction réussie pour restaurer un objet du stockage AWS Glacier vers un pool de stockage cloud.	Client S3	"SPOS : POST S3"
CRACHER	S3 PUT : enregistre une transaction réussie pour créer un nouvel objet ou un nouveau bucket. Remarque : si la transaction fonctionne sur une sous-ressource, le message d'audit inclura le champ S3SR.	Client S3	"SPUT : S3 PUT"
SUPD	Métadonnées S3 mises à jour : enregistre une transaction réussie pour mettre à jour les métadonnées d'un objet ou d'un compartiment existant.	Client S3	"SUPD : Métadonnées S3 mises à jour"
WDEL	Swift DELETE : enregistre une transaction réussie pour supprimer un objet ou un conteneur.	Client Swift	"WDEL : SUPPRESSION rapide"
WPUT	Swift PUT : enregistre une transaction réussie pour créer un nouvel objet ou conteneur.	Client Swift	"WPUT : Swift PUT"

Message d'audit de gestion

La catégorie Gestion enregistre les demandes des utilisateurs dans l'API de gestion.

Code	Titre et description du message	Voir
MGAU	Message d'audit de l'API de gestion : un journal des demandes des utilisateurs.	"MGAU : Message d'audit de gestion"

Messages d'audit 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 de l'information (ILM).

Code	Titre et description du message	Voir
IDEL	Suppression initiée par ILM : ce message d'audit est généré lorsque ILM démarre le processus de suppression d'un objet.	"IDEL : suppression initiée par ILM"
LKCU	Nettoyage des objets écrasés. Ce message d'audit est généré lorsqu'un objet écrasé est automatiquement supprimé pour libérer de l'espace de stockage.	"LKCU : Nettoyage des objets écrasés"
ORLM	Règles d'objet respectées : ce message d'audit est généré lorsque les données d'objet sont stockées comme spécifié par les règles ILM.	"ORLM : Règles d'objet respectées"

Référence du message d'audit

BROR : demande de lecture seule du bucket

Le service LDR génère ce message d'audit lorsqu'un bucket entre ou sort du mode lecture seule. Par exemple, un bucket entre en mode lecture seule pendant que tous les objets sont supprimés.

Code	Champ	Description
BKHD	UUID du bucket	L'ID du bucket.
BROV	Valeur de la demande en lecture seule du bucket	Si le bucket est mis en lecture seule ou quitte l'état de lecture seule (1 = lecture seule, 0 = non en lecture seule).
FRÈRES	Raison de lecture seule du bucket	La raison pour laquelle le bucket est mis en lecture seule ou quitte l'état de lecture seule. Par exemple, emptyBucket.

Code	Champ	Description
S3AI	ID de compte locataire S3	L'ID du compte locataire qui a envoyé la demande. Une valeur vide indique un accès anonyme.
S3BK	Godet S3	Le nom du bucket S3.

CBRB : Début de la réception de l'objet

Lors du fonctionnement normal du système, les blocs de contenu sont continuellement transférés entre différents nœuds à mesure que les données sont consultées, répliquées et conservées. Lorsque le transfert d'un bloc de contenu d'un nœud à un autre est initié, ce message est émis par l'entité de destination.

Code	Champ	Description
CNID	Identifiant de connexion	L'identifiant unique de la session/connexion nœud à nœud.
CBID	Identifiant du bloc de contenu	L'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. PULL : L'opération de transfert a été demandée par l'entité réceptrice.
CTSR	Entité source	L'ID du nœud de la source (expéditeur) du transfert CBID.
CTDS	Entité de destination	L'ID du nœud de destination (récepteur) du transfert CBID.
CTSS	Démarrage du comptage de séquences	Indique le premier nombre de séquences demandé. En cas de succès, le transfert commence à partir de ce décompte de séquence.
CTES	Nombre de séquences de fin attendu	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 de transfert	Statut au moment du début du transfert : SUCS : Le transfert a démarré avec succès.

Ce message d'audit signifie qu'une opération de transfert de données de nœud à nœud a été lancée sur un seul élément de contenu, tel qu'identifié par son identifiant de bloc de contenu. L'opération demande des données allant du « Nombre de séquences de début » au « Nombre de séquences de fin attendu ». Les nœuds d'envoi et de réception sont identifiés par leurs identifiants de nœud. Ces informations peuvent être

utilisées pour suivre le flux de données du système et, lorsqu'elles sont combinées avec des messages d'audit de stockage, pour vérifier le nombre de réplicas.

CBRE : extrémité de réception d'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	Identifiant de connexion	L'identifiant unique de la session/connexion nœud à nœud.
CBID	Identifiant du bloc de contenu	L'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. PULL : L'opération de transfert a été demandée par l'entité réceptrice.
CTSR	Entité source	L'ID du nœud de la source (expéditeur) du transfert CBID.
CTDS	Entité de destination	L'ID du nœud de destination (récepteur) du transfert CBID.
CTSS	Démarrage du comptage de séquences	Indique le nombre de séquences sur lequel le transfert a commencé.
CTAS	Nombre réel de séquences finales	Indique le dernier nombre de séquences transférées avec succès. Si le nombre réel de séquences de fin est identique au nombre réel de séquences de début et que le résultat du transfert n'a pas réussi, aucune donnée n'a été échangée.
RSLT	Résultat du transfert	Le résultat de l'opération de transfert (du point de vue de l'entité expéditrice) : SUCS : transfert terminé avec succès ; tous les comptages de séquences demandés ont été envoyés. CONL : connexion perdue pendant le transfert CTMO : connexion expirée lors de l'établissement ou du transfert UNRE : ID du nœud de destination inaccessible CRPT : transfert terminé en raison de la réception de données corrompues ou invalides

Ce message d'audit signifie qu'une opération de transfert de données de nœud à nœud a été effectuée. Si le résultat du transfert a réussi, l'opération a transféré les données de « Nombre de séquences de départ » vers « Nombre de séquences de fin réel ». Les nœuds d'envoi et de réception sont identifiés par leurs identifiants de nœud. Ces informations peuvent être utilisées pour suivre le flux de données du système et pour localiser, tabuler et analyser les erreurs. Associé à des messages d'audit de stockage, il peut également être utilisé pour vérifier le nombre de réplicas.

CBSB : Début de l'envoi de l'objet

Lors du fonctionnement normal du système, les blocs de contenu sont continuellement transférés entre différents nœuds à mesure que les données sont consultées, répliquées et conservées. Lorsque le transfert d'un bloc de contenu d'un nœud à un autre est initié, ce message est émis par l'entité source.

Code	Champ	Description
CNID	Identifiant de connexion	L'identifiant unique de la session/connexion nœud à nœud.
CBID	Identifiant du bloc de contenu	L'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. PULL : L'opération de transfert a été demandée par l'entité réceptrice.
CTSR	Entité source	L'ID du nœud de la source (expéditeur) du transfert CBID.
CTDS	Entité de destination	L'ID du nœud de destination (récepteur) du transfert CBID.
CTSS	Démarrage du comptage de séquences	Indique le premier nombre de séquences demandé. En cas de succès, le transfert commence à partir de ce décompte de séquence.
CTES	Nombre de séquences de fin attendu	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 de transfert	Statut au moment du début du transfert : SUCS : le transfert a démarré avec succès.

Ce message d'audit signifie qu'une opération de transfert de données de nœud à nœud a été lancée sur un seul élément de contenu, tel qu'identifié par son identifiant de bloc de contenu. L'opération demande des données allant du « Nombre de séquences de début » au « Nombre de séquences de fin attendu ». Les nœuds d'envoi et de réception sont identifiés par leurs identifiants de nœud. Ces informations peuvent être utilisées pour suivre le flux de données du système et, lorsqu'elles sont combinées avec des messages d'audit

de stockage, pour vérifier le nombre de réplicas.

CBSE : Fin d'envoi d'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	Identifiant de connexion	L'identifiant unique de la session/connexion nœud à nœud.
CBID	Identifiant du bloc de contenu	L'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. PULL : L'opération de transfert a été demandée par l'entité réceptrice.
CTSR	Entité source	L'ID du nœud de la source (expéditeur) du transfert CBID.
CTDS	Entité de destination	L'ID du nœud de destination (récepteur) du transfert CBID.
CTSS	Démarrage du comptage de séquences	Indique le nombre de séquences sur lequel le transfert a commencé.
CTAS	Nombre réel de séquences finales	Indique le dernier nombre de séquences transférées avec succès. Si le nombre réel de séquences de fin est identique au nombre réel de séquences de début et que le résultat du transfert n'a pas réussi, aucune donnée n'a été échangée.
RSLT	Résultat du transfert	Le résultat de l'opération de transfert (du point de vue de l'entité expéditrice) : SUCS : transfert terminé avec succès ; tous les comptages de séquences demandés ont été envoyés. CONL : connexion perdue pendant le transfert CTMO : connexion expirée lors de l'établissement ou du transfert UNRE : ID du nœud de destination inaccessible CRPT : transfert terminé en raison de la réception de données corrompues ou invalides

Ce message d'audit signifie qu'une opération de transfert de données de nœud à nœud a été effectuée. Si le

résultat du transfert a réussi, l'opération a transféré les données de « Nombre de séquences de départ » vers « Nombre de séquences de fin réel ». Les nœuds d'envoi et de réception sont identifiés par leurs identifiants de nœud. Ces informations peuvent être utilisées pour suivre le flux de données du système et pour localiser, tabuler et analyser les erreurs. Associé à des messages d'audit de stockage, il peut également être utilisé pour vérifier le nombre de réplicas.

CGRR : demande de réplication inter-réseau

Ce message est généré lorsque StorageGRID tente une opération de réplication inter-grille pour répliquer des objets entre des buckets dans une connexion de fédération de grille.

Code	Champ	Description
CSIZ	Taille de l'objet	La taille de l'objet en octets. L'attribut CSIZ a été introduit dans StorageGRID 11.8. Par conséquent, les demandes de réplication inter-grille couvrant une mise à niveau de StorageGRID 11.7 vers 11.8 peuvent avoir une taille d'objet totale inexacte.
S3AI	ID de compte locataire S3	L'ID du compte locataire propriétaire du bucket à partir duquel l'objet est répliqué.
GFID	ID de connexion à la fédération de grille	L'ID de la connexion de fédération de grille utilisée pour la réplication inter-grille.
OPÉRER	Opération CGR	Le type d'opération de réplication inter-grille qui a été tenté : • 0 = Répliquer l'objet • 1 = Répliquer l'objet en plusieurs parties • 2 = Répliquer le marqueur de suppression
S3BK	Godet S3	Le nom du bucket S3.
S3KY	Touche S3	Le nom de la clé S3, sans inclure le nom du bucket.
VSID	ID de version	L'ID de version de la version spécifique d'un objet en cours de réplication.
RSLT	Code de résultat	Renvoie une erreur réussie (SUCS) ou générale (GERR).

EBDL : Suppression du bucket vide

Le scanner ILM a supprimé un objet dans un bucket qui supprime tous les objets (effectuant une opération de bucket vide).

Code	Champ	Description
CSIZ	Taille de l'objet	La taille de l'objet en octets.
CHEMIN	Seau/clé S3	Le nom du compartiment S3 et le nom de la clé S3.
SEGC	UUID du conteneur	UUID du conteneur pour l'objet segmenté. Cette valeur n'est disponible que si l'objet est segmenté.
UUID	Identifiant unique universel	L'identifiant de l'objet dans le système StorageGRID .
RSLT	Résultat de l'opération de suppression	Le résultat d'un événement, d'un processus ou d'une transaction. Si ce n'est pas pertinent pour un message, NONE est utilisé plutôt que SUCS afin que le message ne soit pas filtré accidentellement.

EBKR : demande de seau vide

Ce message indique qu'un utilisateur a envoyé une demande pour activer ou désactiver le compartiment vide (c'est-à-dire pour supprimer des objets du compartiment ou pour arrêter la suppression d'objets).

Code	Champ	Description
CONSTRUIRE	UUID du bucket	L'ID du bucket.
EBJS	Configuration JSON du bucket vide	Contient le JSON représentant la configuration actuelle du bucket vide.
S3AI	ID de compte locataire S3	L'ID du compte locataire de l'utilisateur qui a envoyé la demande. Une valeur vide indique un accès anonyme.
S3BK	Godet S3	Le nom du bucket S3.

ECMC : Fragment de données codées par effacement manquant

Ce message d'audit indique que le système a détecté un fragment de données codé par effacement manquant.

Code	Champ	Description
VCMC	ID VCS	Le nom du VCS qui contient le bloc manquant.
MCID	ID de bloc	L'identifiant du fragment codé par effacement manquant.

Code	Champ	Description
RSLT	Résultat	Ce champ a la valeur « AUCUN ». RSLT est un champ de message obligatoire, mais n'est pas pertinent pour ce message particulier. « NONE » est utilisé plutôt que « SUCS » afin que ce message ne soit pas filtré.

ECOC : fragment de données corrompu et codé par effacement

Ce message d'audit indique que le système a détecté un fragment de données codé par effacement corrompu.

Code	Champ	Description
VCCO	ID VCS	Le nom du VCS qui contient le bloc corrompu.
VLID	ID du volume	Le volume RangeDB qui contient le fragment codé par effacement corrompu.
CCID	ID de bloc	L'identifiant du fragment codé par effacement corrompu.
RSLT	Résultat	Ce champ a la valeur « AUCUN ». RSLT est un champ de message obligatoire, mais n'est pas pertinent pour ce message particulier. « NONE » est utilisé plutôt que « SUCS » afin que ce message ne soit pas filtré.

ETAF : échec de l'authentification de sécurité

Ce message est généré lorsqu'une tentative de connexion utilisant Transport Layer Security (TLS) a échoué.

Code	Champ	Description
CNID	Identifiant de connexion	L'identifiant système unique pour la connexion TCP/IP sur laquelle l'authentification a échoué.
RUID	Identité de l'utilisateur	Un identifiant dépendant du service représentant l'identité de l'utilisateur distant.

Code	Champ	Description
RSLT	Code de raison	La raison de l'échec : SCNI : l'établissement de la connexion sécurisée a échoué. CERM : Le certificat était 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'était pas valide. CSGU : le signataire du certificat était inconnu. UCRM : les informations d'identification de l'utilisateur étaient manquantes. UCRI : les informations d'identification de l'utilisateur n'étaient pas valides. UCRU : les informations d'identification de l'utilisateur n'ont pas été autorisées. TOUT : L'authentification a expiré.

Lorsqu'une connexion est établie avec un service sécurisé qui utilise TLS, les informations d'identification de l'entité distante sont vérifiées à l'aide du profil TLS et d'une logique supplémentaire intégrée au service. Si cette authentification échoue en raison de certificats ou d'informations d'identification non valides, inattendus ou non autorisés, un message d'audit est enregistré. Cela permet d'effectuer des requêtes sur les tentatives d'accès non autorisées et d'autres problèmes de connexion liés à la sécurité.

Le message peut résulter d'une entité distante ayant une configuration incorrecte ou de tentatives de présentation d'informations d'identification non valides ou non autorisées 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 le concernant dans le système StorageGRID .

Code	Champ	Description
RSLT	Résultat	Le résultat de la demande de mise à jour : • SUCS : Réussi • SUNV : Service indisponible • GERR : Autre échec

Code	Champ	Description
GNID	Nœud ID	L'ID de nœud du service qui a initié la demande de mise à jour.
GNTTP	Type d'appareil	Le type de périphérique du nœud de grille (par exemple, BLDR pour un service LDR).
GNDV	Version du modèle d'appareil	La chaîne identifiant la version du modèle de périphérique du nœud de grille dans le bundle DMDL.
GNGP	Groupe	Le groupe auquel appartient le nœud de grille (dans le contexte des coûts de liaison et du classement des requêtes de service).
GNIA	Adresse IP	L'adresse IP du nœud de grille.

Ce message est généré chaque fois qu'un nœud de grille met à jour son entrée dans le bundle de nœuds de grille.

GNUR : Désinscription GNDS

Le service CMN génère ce message d'audit lorsqu'un service dispose d'informations non enregistrées le concernant auprès du système StorageGRID .

Code	Champ	Description
RSLT	Résultat	Le résultat de la demande de mise à jour : • SUCS : Réussi • SUNV : Service indisponible • GERR : Autre échec
GNID	Nœud ID	L'ID de nœud du service qui a initié 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 SUCS, ABRT ou ROLF, un message d'audit correspondant indiquant que la tâche de grille a démarré s'affichera. Les autres résultats indiquent que le traitement de cette tâche de grille n'a jamais commencé.

Code	Champ	Description
TSID	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. Il est possible qu'une tâche de grille donnée soit soumise plusieurs fois et, dans ce cas, le champ ID de tâche n'est pas suffisant pour lier de manière unique les messages d'audit Soumis, Démarré et Terminé.
RSLT	Résultat	Le résultat final de la tâche de grille : • SUCS : la tâche de grille s'est terminée avec succès. • ABRT : la tâche de grille a été terminée sans erreur de restauration. • ROLF : La tâche de grille a été interrompue et n'a pas pu terminer le processus de restauration. • CANC : la tâche de grille a été annulée par l'utilisateur avant d'être démarrée. • EXPR : La tâche de grille a expiré avant d'avoir été démarrée. • 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 comme doublon.

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 Tâche de grille soumise pour les tâches de grille initiées par le service de soumission de tâche de grille interne 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
TSID	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. Il est possible qu'une tâche de grille donnée soit soumise plusieurs fois et, dans ce cas, le champ ID de tâche n'est pas suffisant pour lier de manière unique les messages d'audit Soumis, Démarré et Terminé.
RSLT	Résultat	Le résultat. Ce champ n'a qu'une seule valeur : • SUCS : la tâche de grille a été démarrée avec succès.

Ce message d'audit indique qu'une tâche de grille a été soumise au service CMN.

Code	Champ	Description
TSID	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. Il est possible qu'une tâche de grille donnée soit soumise plusieurs fois et, dans ce cas, le champ ID de tâche n'est pas suffisant pour lier de manière unique les messages d'audit Soumis, Démarré et Terminé.
TTYP	Type de tâche	Le type de tâche de grille.
TVER	Version de la tâche	Un numéro indiquant la version de la tâche de grille.
TDSC	Description de la tâche	Une description lisible par l'homme de la tâche de grille.
TVA	Valide après l'horodatage	L'heure la plus ancienne (UINT64 microsecondes à partir du 1er janvier 1970 - heure UNIX) à laquelle la tâche de grille est valide.
VBTS	Valide avant l'horodatage	La dernière heure (UINT64 microsecondes à partir du 1er janvier 1970 - heure UNIX) à laquelle la tâche de grille est valide.
TSRC	Source	La source de la tâche : • TXTB : la tâche de grille a été soumise via le système StorageGRID sous la forme d'un bloc de texte signé. • GRILLE : la tâche de grille a été soumise via le service de soumission de tâches de grille interne.
ACTV	Type d'activation	Le type d'activation : • AUTO : La tâche de grille a été soumise à une activation automatique. • PEND : la tâche de grille a été soumise dans la table en attente. C'est la seule possibilité pour la source TXTB.
RSLT	Résultat	Le résultat de la soumission : • SUCS : la tâche de grille a été soumise avec succès. • ÉCHEC : La tâche a été déplacée directement vers la table historique.

Ce message est généré lorsque ILM démarre le processus de suppression d'un objet.

Le message IDEL est généré dans l'une de ces situations :

- **Pour les objets dans les compartiments S3 conformes** : ce message est généré lorsque ILM démarre le processus de suppression automatique d'un objet car 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 les buckets S3 non conformes**. Ce message est généré lorsque ILM démarre le processus de suppression d'un objet car aucune instruction de placement dans les stratégies ILM actives ne s'applique actuellement à l'objet.

Code	Champ	Description
CBID	Identifiant du bloc de contenu	Le CBID de l'objet.
CMPA	Conformité : Suppression automatique	Pour les objets dans les buckets S3 conformes uniquement. 0 (faux) ou 1 (vrai), indiquant si un objet conforme doit être supprimé automatiquement à la fin de sa période de conservation, à moins que le bucket ne soit soumis à une suspension légale.
CMPL	Conformité : Conservation légale	Pour les objets dans les buckets S3 conformes uniquement. 0 (faux) ou 1 (vrai), indiquant si le bucket est actuellement sous une suspension légale.
CMPR	Conformité : Durée de conservation	Pour les objets dans les buckets S3 conformes uniquement. La durée de la période de rétention de l'objet en minutes.
CTME	Conformité : Heure d'ingestion	Pour les objets dans les buckets S3 conformes uniquement. L'heure 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 bucket.
DMRK	Supprimer l'ID de version du marqueur	L'ID de version du marqueur de suppression créé lors de la suppression d'un objet d'un bucket versionné. Les opérations sur les buckets n'incluent pas ce champ.
CSIZ	Taille du contenu	La taille de l'objet en octets.

Code	Champ	Description
LOC	Emplacements	L'emplacement de stockage des données d'objet dans le système StorageGRID . La valeur de LOCS est "" si l'objet n'a aucun emplacement (par exemple, il a été supprimé). CLEC : pour les objets à codage d'effacement, l'ID de profil de codage d'effacement et l'ID de groupe de codage d'effacement appliqué aux données de l'objet. CLDI : pour les objets répliqués, l'ID du nœud LDR et l'ID du volume de l'emplacement de l'objet. CLNL : ID du nœud ARC de l'emplacement de l'objet si les données de l'objet sont archivées.
CHEMIN	Seau/clé S3	Le nom du compartiment S3 et le nom de la clé S3.
RSLT	Résultat	Le résultat de l'opération ILM. SUCS : L'opération ILM a réussi.
RÈGLE	Étiquette des règles	• Si un objet dans un compartiment S3 conforme est supprimé automatiquement parce que sa période de conservation a expiré, ce champ est vide. • Si l'objet est supprimé parce qu'il n'existe 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 qui s'appliquait à l'objet.
SGRP	Site (Groupe)	Si présent, l'objet a été supprimé sur le site spécifié, qui n'est pas le site où l'objet a été ingéré.
UUID	Identifiant unique universel	L'identifiant de l'objet dans le système StorageGRID .
VSID	ID de version	L'ID de version de la version spécifique d'un objet qui a été supprimé. Les opérations sur les buckets et les objets dans les buckets non versionnés n'incluent pas ce champ.

LKCU : Nettoyage des objets écrasés

Ce message est généré lorsque StorageGRID supprime un objet écrasé qui nécessitait auparavant un nettoyage pour libérer de l'espace de stockage. Un objet est écrasé lorsqu'un client S3 écrit un objet dans un chemin contenant déjà un objet. Le processus de suppression se produit automatiquement et en arrière-plan.

Code	Champ	Description
CSIZ	Taille du contenu	La taille de l'objet en octets.
LTyp	Type de nettoyage	<i>Usage interne uniquement.</i>
LUID	UUID de l'objet supprimé	L'identifiant de l'objet qui a été supprimé.
CHEMIN	Seau/clé S3	Le nom du compartiment S3 et le nom de la clé S3.
SEGC	UUID du conteneur	UUID du conteneur pour l'objet segmenté. Cette valeur n'est disponible que si l'objet est segmenté.
UUID	Identifiant unique universel	L'identifiant de l'objet qui existe encore. Cette valeur n'est disponible que si l'objet n'a pas été supprimé.

LKDM : Nettoyage des objets divulgués

Ce message est généré lorsqu'un fragment divulgué a été nettoyé ou supprimé. Un bloc peut faire partie d'un objet répliqué ou d'un objet codé par effacement.

Code	Champ	Description
CLOC	Emplacement du bloc	Le chemin du fichier du morceau divulgué qui a été supprimé.
CTYP	Type de morceau	Type de morceau : ec: Erasure-coded object chunk repl: Replicated object chunk

Code	Champ	Description
LTyp	Type de fuite	Les cinq types de fuites qui peuvent être détectées : <code>object_leaked</code>: Object doesn't exist in the grid <code>location_leaked</code>: Object exists in the grid, but found location doesn't belong to object <code>mup_seg_leaked</code>: Multipart upload was stopped or not completed, and the segment/part was left out <code>segment_leaked</code>: Parent UUID/CBID (associated container object) is valid but doesn't contain this segment <code>no_parent</code>: Container object is deleted, but object segment was left out and not deleted
CTIM	Temps de création du bloc	Il est temps que le morceau divulgué soit créé.
UUID	Identifiant unique universel	L'identifiant de l'objet auquel appartient le bloc.
CBID	Identifiant du bloc de contenu	CBID de l'objet auquel appartient le fragment divulgué.
CSIZ	Taille du contenu	La taille du bloc en octets.

LLST : Localisation perdue

Ce message est généré chaque fois qu'un emplacement pour une copie d'objet (répliquée ou codée par effacement) ne peut pas être trouvé.

Code	Champ	Description
CBIL	CBID	Le CBID affecté.
ECPR	Profil de codage d'effacement	Pour les données d'objet codées par effacement. L'ID du profil de codage d'effacement utilisé.
LTyp	Type d'emplacement	CLDI (en ligne) : pour les données d'objets répliquées CLEC (en ligne) : pour les données d'objets codées par effacement CLNL (Nearline) : pour les données d'objets répliquées archivées

Code	Champ	Description
NOID	ID du nœud source	L'ID du nœud sur lequel les emplacements ont été perdus.
PCLD	Chemin vers l'objet répliqué	Le 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 <code>/var/local/rangedb/2/p/13/13/00oJs6X%{h{U)SeUFxE@</code>
RSLT	Résultat	Toujours AUCUN. RSLT est un champ de message obligatoire, mais n'est pas pertinent pour ce message. NONE est utilisé plutôt que SUCS afin que ce message ne soit pas filtré.
TSRC	Source de déclenchement	UTILISATEUR : Déclenché par l'utilisateur SYST : système déclenché
UUID	ID unique universel	L'identifiant de l'objet affecté dans le système StorageGRID .

MG AU : Message d'audit de gestion

La catégorie Gestion enregistre les demandes des utilisateurs dans l'API de gestion. Chaque requête HTTP qui n'est pas une requête GET ou HEAD vers un URI d'API valide enregistre une réponse contenant le nom d'utilisateur, l'IP et le type de requête vers l'API. Les URI d'API non valides (tels que /api/v3-authorize) et les demandes non valides adressées à des URI d'API valides ne sont pas enregistrées.

Code	Champ	Description
MDIP	Adresse IP de destination	L'adresse IP du serveur (destination).
MDNA	Nom de domaine	Le nom de domaine de l'hôte.
MPAT	Demande PATH	Le chemin de la demande.
MPQP	Paramètres de requête de demande	Les paramètres de requête pour la demande.

Code	Champ	Description
MRBD	Corps de la requête	Le contenu du corps de la requête. Alors que le corps de la réponse est enregistré par défaut, le corps de la demande est enregistré dans certains cas lorsque le corps de la réponse est vide. Étant donné que les informations suivantes ne sont pas disponibles dans le corps de la réponse, elles sont extraites du corps de la requête pour les méthodes POST suivantes : • Nom d'utilisateur et identifiant de compte dans POST authorize • Nouvelle configuration des sous-réseaux dans POST /grid/grid-networks/update • Nouveaux serveurs NTP dans POST /grid/ntp-servers/update • ID de serveur mis hors service dans POST /grid/servers/decommission 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).
MRMD	Méthode de requête	La méthode de requête HTTP : • POSTE • METTRE • SUPPRIMER • CORRECTIF
MRSC	Code de réponse	Le code de réponse.
MRSP	Corps de la réponse	Le contenu de la réponse (le corps de la réponse) est enregistré 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	L'adresse IP du client (source).
MUUN	URN de l'utilisateur	L'URN (nom de ressource uniforme) de l'utilisateur qui a envoyé la demande.
RSLT	Résultat	Renvoie une réussite (SUCS) ou l'erreur signalée par le backend.

OLST : le système a détecté un objet perdu

Ce message est généré lorsque le service DDS ne parvient pas à localiser de copies

d'un objet dans le système StorageGRID .

Code	Champ	Description
CBID	Identifiant du bloc de contenu	Le CBID de l'objet perdu.
NOID	Nœud ID	Si disponible, le dernier emplacement direct ou proche connu de l'objet perdu. Il est possible d'avoir uniquement l'ID de nœud sans ID de volume si les informations de volume ne sont pas disponibles.
CHEMIN	Seau/clé S3	Si disponible, le nom du compartiment S3 et le nom de la clé S3.
RSLT	Résultat	Ce champ a la valeur AUCUN. RSLT est un champ de message obligatoire, mais n'est pas pertinent pour ce message. NONE est utilisé plutôt que SUCS afin que ce message ne soit pas filtré.
UUID	ID unique universel	L'identifiant de l'objet perdu dans le système StorageGRID .
VOLI	ID du volume	Si disponible, l'ID de volume du nœud de stockage 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 avec succès comme spécifié par les règles ILM.



Le message ORLM n'est pas généré lorsqu'un objet est stocké avec succès par la règle par défaut Créer 2 copies si une autre règle de la stratégie utilise le filtre avancé Taille de l'objet.

Code	Champ	Description
CONSTRUIRE	En-tête de godet	Champ d'ID du bucket. Utilisé pour les opérations internes. Apparaît uniquement si STAT est PRGD.
CBID	Identifiant du bloc de contenu	Le CBID de l'objet.
CSIZ	Taille du contenu	La taille de l'objet en octets.

Code	Champ	Description
LOC	Emplacements	L'emplacement de stockage des données d'objet dans le système StorageGRID . La valeur de LOCS est "" si l'objet n'a aucun emplacement (par exemple, il a été supprimé). CLEC : pour les objets à codage d'effacement, l'ID de profil de codage d'effacement et l'ID de groupe de codage d'effacement appliqué aux données de l'objet. CLDI : pour les objets répliqués, l'ID du nœud LDR et l'ID du volume de l'emplacement de l'objet. CLNL : ID du nœud ARC de l'emplacement de l'objet si les données de l'objet sont archivées.
CHEMIN	Seau/clé S3	Le nom du compartiment S3 et le nom de la clé S3.
RSLT	Résultat	Le résultat de l'opération ILM. SUCS : L'opération ILM a réussi.
RÈGLE	Étiquette des règles	L'étiquette lisible par l'homme attribuée à la règle ILM appliquée à cet objet.
SEGC	UUID du conteneur	UUID du conteneur pour l'objet segmenté. Cette valeur n'est disponible que si l'objet est segmenté.
SGCB	Conteneur CBID	CBID du conteneur pour l'objet segmenté. Cette valeur est disponible uniquement pour les objets segmentés et en plusieurs parties.
STAT	Statut	L'état de fonctionnement de l'ILM. TERMINÉ : les opérations ILM sur l'objet sont terminées. DFER : L'objet a été marqué pour une future réévaluation ILM. PRGD : l'objet a été supprimé du système StorageGRID . NLOC : les données de l'objet ne peuvent plus être trouvées dans le système StorageGRID . Ce statut peut indiquer que toutes les copies des données de l'objet sont manquantes ou endommagées.
UUID	Identifiant unique universel	L'identifiant de l'objet dans le système StorageGRID .
VSID	ID de version	L'ID de version d'un nouvel objet créé dans un bucket versionné. Les opérations sur les buckets et les objets dans les buckets non versionnés n'incluent pas ce champ.

Le message d'audit ORLM peut être émis plusieurs fois pour un même objet. Par exemple, il est émis chaque

fois que l'un des événements suivants se produit :

- Les règles ILM pour l'objet sont satisfaites pour toujours.
- Les règles ILM pour 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 répliquées est corrompue. Le système StorageGRID effectue une évaluation ILM pour remplacer l'objet corrompu.

Informations connexes

- ["Transactions d'ingestion d'objets"](#)
- ["Transactions de suppression d'objets"](#)

OVWR : écrasement d'objet

Ce message est généré lorsqu'une opération externe (demandée par le client) entraîne l'écrasement d'un objet par un autre objet.

Code	Champ	Description
CBID	Identifiant du bloc de contenu (nouveau)	Le CBID du nouvel objet.
CSIZ	Taille de l'objet précédent	La taille, en octets, de l'objet écrasé.
trouble obsessionnel compulsif (TOC)	Identifiant du bloc de contenu (précédent)	Le CBID de l'objet précédent.
UUID	ID unique universel (nouveau)	L'identifiant du nouvel objet dans le système StorageGRID .
OUID	ID unique universel (précédent)	L'identifiant de l'objet précédent dans le système StorageGRID .
CHEMIN	Chemin de l'objet S3	Le chemin d'accès à l'objet S3 utilisé pour l'objet précédent et le nouvel objet
RSLT	Code de résultat	Résultat de la transaction d'écrasement d'objet. Le résultat est toujours : SUCS : Réussi
SGRP	Site (Groupe)	Si présent, l'objet écrasé a été supprimé sur le site spécifié, qui n'est pas le site où l'objet écrasé a été ingéré.

S3SL : Demande de sélection S3

Ce message enregistre une fin après qu'une demande S3 Select a été renvoyée au client. Le message S3SL peut inclure des détails sur le message d'erreur et le 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 sera le nombre d'octets après décompression.
BYPR	Octets traités	Nombre d'octets traités. Indique combien d'octets de « Octets analysés » ont été réellement traités ou traités par une tâche S3 Select.
BYRT	Octets renvoyés	Nombre d'octets qu'une tâche S3 Select a renvoyé au client.
REPR	Enregistrements traités	Nombre d'enregistrements ou de lignes qu'une tâche S3 Select a reçus des nœuds de stockage.
RERT	Dossiers retournés	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 cela est faux, la tâche n'a pas pu se terminer et les champs d'erreur contiendront probablement des données. Le client a peut-être reçu des résultats partiels, voire aucun résultat du tout.
REID	ID de la demande	Identifiant de la demande S3 Select.
EXTM	Temps d'exécution	Le temps, en secondes, qu'il a fallu pour terminer la tâche S3 Select.
ERMG	Message d'erreur	Message d'erreur généré par la tâche S3 Select.
ERTY	Type d'erreur	Type d'erreur généré par le travail S3 Select.
ERST	Trace de pile d'erreurs	Erreur Stacktrace générée par le travail S3 Select.
S3BK	Godet S3	Le nom du bucket S3.

Code	Champ	Description
S3AK	ID de clé d'accès S3 (expéditeur de la demande)	L'ID de clé d'accès S3 pour l'utilisateur qui a envoyé la demande.
S3AI	ID de compte locataire S3 (expéditeur de la demande)	L'ID du compte locataire de l'utilisateur qui a envoyé la demande.
S3KY	Touche S3	Le nom de la clé S3, sans inclure le nom du bucket.

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 ni livrés.

Code	Champ	Description
AETM	Méthode d'activation	La méthode utilisée pour désactiver l'audit.
AEUN	Nom d'utilisateur	Le nom d'utilisateur qui a exécuté la commande pour désactiver la journalisation d'audit.
RSLT	Résultat	Ce champ a la valeur AUCUN. RSLT est un champ de message obligatoire, mais n'est pas pertinent pour ce message. NONE est utilisé plutôt que SUCS afin que ce message ne soit pas filtré.

Le message implique que la journalisation était auparavant activée, mais qu'elle est désormais désactivée. Ceci est généralement utilisé uniquement lors de l'ingestion en masse pour améliorer les performances du système. Suite à l'activité en masse, l'audit est restauré (SADE) et la possibilité de désactiver l'audit est alors définitivement bloquée.

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 à nouveau collectés et livrés.

Code	Champ	Description
AETM	Méthode d'activation	La méthode utilisée pour permettre l'audit.
AEUN	Nom d'utilisateur	Le nom d'utilisateur qui a exécuté la commande pour activer la journalisation d'audit.

Code	Champ	Description
RSLT	Résultat	Ce champ a la valeur AUCUN. RSLT est un champ de message obligatoire, mais n'est pas pertinent pour ce message. NONE est utilisé plutôt que SUCS afin que ce message ne soit pas filtré.

Le message implique que la journalisation était auparavant désactivée (SADD), mais qu'elle a maintenant été restaurée. Ceci est généralement utilisé uniquement lors de l'ingestion en masse pour améliorer les performances du système. Après l'activité en masse, l'audit est restauré et la possibilité de désactiver l'audit est alors définitivement bloquée.

SCMT : validation du magasin d'objets

Le contenu de la grille n'est pas rendu disponible ou reconnu comme stocké tant qu'il n'a pas été validé (ce qui signifie qu'il a été stocké de manière persistante). Le contenu stocké de manière persistante a été entièrement écrit sur le disque et a réussi les contrôles d'intégrité associés. Ce message est émis lorsqu'un bloc de contenu est validé dans le stockage.

Code	Champ	Description
CBID	Identifiant du bloc de contenu	L'identifiant unique du bloc de contenu dédié au stockage permanent.
RSLT	Code de résultat	État au moment où l'objet a été stocké sur le disque : SUCS : Objet stocké avec succès.

Ce message signifie qu'un bloc de contenu donné a été entièrement stocké et vérifié et peut désormais être demandé. Il peut être utilisé pour suivre le flux de données au sein du système.

SDEL : SUPPRESSION S3

Lorsqu'un client S3 émet une transaction DELETE, une demande est effectuée pour supprimer l'objet ou le bucket spécifié, ou pour supprimer une sous-ressource bucket/objet. Ce message est émis par le serveur si la transaction réussit.

Code	Champ	Description
CBID	Identifiant du bloc de contenu	L'identifiant unique du bloc de contenu demandé. Si le CBID est inconnu, ce champ est défini sur 0. Les opérations sur les buckets n'incluent pas ce champ.
CNCH	En-tête de contrôle de cohérence	La valeur de l'en-tête de requête HTTP Consistency-Control, si présent dans la requête.
CNID	Identifiant de connexion	L'identifiant système unique pour la connexion TCP/IP.

Code	Champ	Description
CSIZ	Taille du contenu	La taille de l'objet supprimé en octets. Les opérations sur les buckets n'incluent pas ce champ.
DMRK	Supprimer l'ID de version du marqueur	L'ID de version du marqueur de suppression créé lors de la suppression d'un objet d'un bucket versionné. Les opérations sur les buckets n'incluent pas ce champ.
GFID	ID de connexion à la fédération de grille	L'ID de connexion de la connexion de fédération de grille associée à une demande de suppression de réplication inter-grille. Uniquement inclus dans les journaux d'audit sur la grille de destination.
GFSA	ID du compte source de la Grid Federation	L'ID de compte du locataire sur la grille source pour une demande de suppression de réplication inter-grille. Uniquement inclus 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 enregistrés tels que sélectionnés lors de la configuration. <code>`X-Forwarded-For`</code> est automatiquement inclus s'il est présent dans la demande et si le <code>`X-Forwarded-For`</code> la valeur est différente de l'adresse IP de l'expéditeur de la demande (champ d'audit SAIP). <code>`x-amz-bypass-governance-retention`</code> est automatiquement inclus s'il est présent dans la demande.
MTME	Heure de la dernière modification	L'horodatage Unix, en microsecondes, indiquant quand l'objet a été modifié pour la dernière fois.
RSLT	Code de résultat	Résultat de la transaction DELETE. Le résultat est toujours : SUCS : Réussi
S3AI	ID de compte locataire S3 (expéditeur de la demande)	L'ID du compte 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)	L'ID de clé d'accès S3 haché pour l'utilisateur qui a envoyé la demande. Une valeur vide indique un accès anonyme.
S3BK	Godet S3	Le nom du bucket S3.

Code	Champ	Description
S3KY	Touche S3	Le nom de la clé S3, sans inclure le nom du bucket. Les opérations sur les buckets n'incluent pas ce champ.
S3SR	Sous-ressource S3	Le compartiment ou la sous-ressource d'objet sur lequel l'opération est effectuée, le cas échéant.
SACC	Nom du compte locataire S3 (expéditeur de la demande)	Le nom du compte locataire de l'utilisateur qui a envoyé la demande. Vide pour les demandes anonymes.
SAIP	Adresse IP (expéditeur de la requête)	L'adresse IP de l'application cliente qui a effectué la demande.
SBAC	Nom du compte locataire S3 (propriétaire du bucket)	Le nom du compte locataire pour le propriétaire du bucket. Utilisé pour identifier l'accès inter-comptes ou anonyme.
SBAI	ID de compte locataire S3 (propriétaire du bucket)	L'ID de compte locataire du propriétaire du bucket cible. Utilisé pour identifier l'accès inter-comptes ou anonyme.
SGRP	Site (Groupe)	Si présent, l'objet a été supprimé sur le site spécifié, qui n'est pas le site où l'objet a été ingéré.
SUSR	URN utilisateur S3 (expéditeur de la requête)	L'ID du compte locataire et le nom d'utilisateur de l'utilisateur effectuant la demande. L'utilisateur peut être un utilisateur local ou un utilisateur LDAP. Par exemple : urn:sgws:identity::03393893651506583485:root Vide pour les demandes anonymes.
TEMPS	Durée	Temps total de traitement de la demande en microsecondes.
TLIP	Adresse IP de l'équilibreur de charge approuvé	Si la demande a été acheminée par un équilibreur de charge de couche 7 approuvé, l'adresse IP de l'équilibreur de charge.
UUDM	Identifiant unique universel pour un marqueur de suppression	L'identifiant d'un marqueur de suppression. Les messages du journal d'audit spécifient UUDM ou UUID, où UUDM indique un marqueur de suppression créé à la suite d'une demande de suppression d'objet et UUID indique un objet.

Code	Champ	Description
UUID	Identifiant unique universel	L'identifiant de l'objet dans le système StorageGRID .
VSID	ID de version	L'ID de version de la version spécifique d'un objet qui a été supprimé. Les opérations sur les buckets et les objets dans les buckets non versionnés n'incluent pas ce champ.

SGET : S3 OBTENIR

Lorsqu'un client S3 émet une transaction GET, une demande est effectuée pour récupérer un objet ou répertorier les objets dans un bucket, ou pour supprimer une sous-ressource bucket/objet. Ce message est émis par le serveur si la transaction réussit.

Code	Champ	Description
CBID	Identifiant du bloc de contenu	L'identifiant unique du bloc de contenu demandé. Si le CBID est inconnu, ce champ est défini sur 0. Les opérations sur les buckets n'incluent pas ce champ.
CNCH	En-tête de contrôle de cohérence	La valeur de l'en-tête de requête HTTP Consistency-Control, si présent dans la requête.
CNID	Identifiant de connexion	L'identifiant système unique pour la connexion TCP/IP.
CSIZ	Taille du contenu	La taille de l'objet récupéré en octets. Les opérations sur les buckets n'incluent pas ce champ.
HTRH	En-tête de requête HTTP	Liste des noms et valeurs d'en-tête de requête HTTP enregistrés tels que sélectionnés lors de la configuration. `X-Forwarded-For` est automatiquement inclus s'il est présent dans la demande et si le `X-Forwarded-For` la valeur est différente de l'adresse IP de l'expéditeur de la demande (champ d'audit SAIP) .
LITÉ	ListObjectsV2	Une réponse au format v2 a été demandée. Pour plus de détails, voir "AWS ListObjectsV2" . Pour les opérations de bucket GET uniquement.
NCHD	Nombre d'enfants	Inclut les clés et les préfixes courants. Pour les opérations de bucket GET uniquement.

Code	Champ	Description
RANG	Lecture de la portée	Pour les opérations de lecture de plage uniquement. Indique la plage d'octets lus par cette requête. 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 : SUCS : Réussi
S3AI	ID de compte locataire S3 (expéditeur de la demande)	L'ID du compte 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)	L'ID de clé d'accès S3 haché pour l'utilisateur qui a envoyé la demande. Une valeur vide indique un accès anonyme.
S3BK	Godet S3	Le nom du bucket S3.
S3KY	Touche S3	Le nom de la clé S3, sans inclure le nom du bucket. Les opérations sur les buckets n'incluent pas ce champ.
S3SR	Sous-ressource S3	Le compartiment ou la sous-ressource d'objet sur lequel l'opération est effectuée, le cas échéant.
SACC	Nom du compte locataire S3 (expéditeur de la demande)	Le nom du compte locataire de l'utilisateur qui a envoyé la demande. Vide pour les demandes anonymes.
SAIP	Adresse IP (expéditeur de la requête)	L'adresse IP de l'application cliente qui a effectué la demande.
SBAC	Nom du compte locataire S3 (propriétaire du bucket)	Le nom du compte locataire pour le propriétaire du bucket. Utilisé pour identifier l'accès inter-comptes ou anonyme.
SBAI	ID de compte locataire S3 (propriétaire du bucket)	L'ID de compte locataire du propriétaire du bucket cible. Utilisé pour identifier l'accès inter-comptes ou anonyme.

Code	Champ	Description
SUSR	URN utilisateur S3 (expéditeur de la requête)	L'ID du compte locataire et le nom d'utilisateur de l'utilisateur effectuant la demande. L'utilisateur peut être un utilisateur local ou un utilisateur LDAP. Par exemple : <code>urn:sgws:identity::03393893651506583485:root</code> Vide pour les demandes anonymes.
TEMPS	Durée	Temps total de traitement de la demande en microsecondes.
TLIP	Adresse IP de l'équilibreur de charge approuvé	Si la demande a été acheminée par un équilibreur de charge de couche 7 approuvé, l'adresse IP de l'équilibreur de charge.
RTCN	Tronqué ou non tronqué	Définissez sur faux si tous les résultats ont été renvoyés. Définissez sur vrai si davantage de résultats sont disponibles à renvoyer. Pour les opérations de bucket GET uniquement.
UUID	Identifiant unique universel	L'identifiant de l'objet dans le système StorageGRID .
VSID	ID de version	L'ID de version de la version spécifique d'un objet qui a été demandé. Les opérations sur les buckets et les objets dans les buckets non versionnés n'incluent pas ce champ.

SHEA : TÊTE S3

Lorsqu'un client S3 émet une transaction HEAD, une demande est effectuée pour vérifier l'existence d'un objet ou d'un bucket et récupérer les métadonnées relatives à un objet. Ce message est émis par le serveur si la transaction réussit.

Code	Champ	Description
CBID	Identifiant du bloc de contenu	L'identifiant unique du bloc de contenu demandé. Si le CBID est inconnu, ce champ est défini sur 0. Les opérations sur les buckets n'incluent pas ce champ.
CNID	Identifiant de connexion	L'identifiant système unique pour la connexion TCP/IP.
CSIZ	Taille du contenu	La taille de l'objet vérifié en octets. Les opérations sur les buckets 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 enregistrés tels que sélectionnés lors de la configuration. `X-Forwarded-For` est automatiquement inclus s'il est présent dans la demande et si le `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 : SUCS : Réussi
S3AI	ID de compte locataire S3 (expéditeur de la demande)	L'ID du compte 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)	L'ID de clé d'accès S3 haché pour l'utilisateur qui a envoyé la demande. Une valeur vide indique un accès anonyme.
S3BK	Godet S3	Le nom du bucket S3.
S3KY	Touche S3	Le nom de la clé S3, sans inclure le nom du bucket. Les opérations sur les buckets n'incluent pas ce champ.
SACC	Nom du compte locataire S3 (expéditeur de la demande)	Le nom du compte locataire de l'utilisateur qui a envoyé la demande. Vide pour les demandes anonymes.
SAIP	Adresse IP (expéditeur de la requête)	L'adresse IP de l'application cliente qui a effectué la demande.
SBAC	Nom du compte locataire S3 (propriétaire du bucket)	Le nom du compte locataire pour le propriétaire du bucket. Utilisé pour identifier l'accès inter-comptes ou anonyme.
SBAI	ID de compte locataire S3 (propriétaire du bucket)	L'ID de compte locataire du propriétaire du bucket cible. Utilisé pour identifier l'accès inter-comptes ou anonyme.

Code	Champ	Description
SUSR	URN utilisateur S3 (expéditeur de la requête)	L'ID du compte locataire et le nom d'utilisateur de l'utilisateur effectuant la demande. L'utilisateur peut être un utilisateur local ou un utilisateur LDAP. Par exemple : <code>urn:sgws:identity::03393893651506583485:root</code> Vide pour les demandes anonymes.
TEMPS	Durée	Temps total de traitement de la demande en microsecondes.
TLIP	Adresse IP de l'équilibreur de charge approuvé	Si la demande a été acheminée par un équilibreur de charge de couche 7 approuvé, l'adresse IP de l'équilibreur de charge.
UUID	Identifiant unique universel	L'identifiant de l'objet dans le système StorageGRID .
VSID	ID de version	L'ID de version de la version spécifique d'un objet qui a été demandé. Les opérations sur les buckets et les objets dans les buckets non versionnés n'incluent pas ce champ.

SPOS : POST S3

Lorsqu'un client S3 émet une demande d'objet POST, ce message est émis par le serveur si la transaction réussit.

Code	Champ	Description
CBID	Identifiant du bloc de contenu	L'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	La valeur de l'en-tête de requête HTTP Consistency-Control, si présent dans la requête.
CNID	Identifiant de connexion	L'identifiant système unique pour la connexion TCP/IP.
CSIZ	Taille du contenu	La 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 enregistrés tels que sélectionnés lors de la configuration. `X-Forwarded-For` est automatiquement inclus s'il est présent dans la demande et si le `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 requête RestoreObject. Le résultat est toujours : SUCS : Réussi
S3AI	ID de compte locataire S3 (expéditeur de la demande)	L'ID du compte 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)	L'ID de clé d'accès S3 haché pour l'utilisateur qui a envoyé la demande. Une valeur vide indique un accès anonyme.
S3BK	Godet S3	Le nom du bucket S3.
S3KY	Touche S3	Le nom de la clé S3, sans inclure le nom du bucket. Les opérations sur les buckets n'incluent pas ce champ.
S3SR	Sous-ressource S3	Le compartiment ou la sous-ressource d'objet sur lequel l'opération est effectuée, le cas échéant. Réglez sur « sélectionner » pour une opération de sélection S3.
SACC	Nom du compte locataire S3 (expéditeur de la demande)	Le nom du compte locataire de l'utilisateur qui a envoyé la demande. Vide pour les demandes anonymes.
SAIP	Adresse IP (expéditeur de la requête)	L'adresse IP de l'application cliente qui a effectué la demande.

Code	Champ	Description
SBAC	Nom du compte locataire S3 (propriétaire du bucket)	Le nom du compte locataire pour le propriétaire du bucket. Utilisé pour identifier l'accès inter-comptes ou anonyme.
SBAI	ID de compte locataire S3 (propriétaire du bucket)	L'ID de compte locataire du propriétaire du bucket cible. Utilisé pour identifier l'accès inter-comptes ou anonyme.
SRCF	Configuration des sous-ressources	Restaurer les informations.
SUSR	URN utilisateur S3 (expéditeur de la requête)	L'ID du compte locataire et le nom d'utilisateur de l'utilisateur effectuant la demande. L'utilisateur peut être un utilisateur local ou un utilisateur LDAP. Par exemple : <code>urn:sgws:identity::03393893651506583485:root</code> Vide pour les demandes anonymes.
TEMPS	Durée	Temps total de traitement de la demande en microsecondes.
TLIP	Adresse IP de l'équilibreur de charge approuvé	Si la demande a été acheminée par un équilibreur de charge de couche 7 approuvé, l'adresse IP de l'équilibreur de charge.
UUID	Identifiant unique universel	L'identifiant de l'objet dans le système StorageGRID .
VSID	ID de version	L'ID de version de la version spécifique d'un objet qui a été demandé. Les opérations sur les buckets et les objets dans les buckets non versionnés n'incluent pas ce champ.

SPUT : S3 PUT

Lorsqu'un client S3 émet une transaction PUT, une demande est effectuée pour créer un nouvel objet ou un nouveau compartiment, ou pour supprimer une sous-ressource de compartiment/objet. Ce message est émis par le serveur si la transaction réussit.

Code	Champ	Description
CBID	Identifiant du bloc de contenu	L'identifiant unique du bloc de contenu demandé. Si le CBID est inconnu, ce champ est défini sur 0. Les opérations sur les buckets n'incluent pas ce champ.

Code	Champ	Description
CMPS	Paramètres de conformité	Les paramètres de conformité utilisés lors de la création du bucket, s'ils sont présents dans la demande (tronqués aux 1024 premiers caractères).
CNCH	En-tête de contrôle de cohérence	La valeur de l'en-tête de requête HTTP Consistency-Control, si présent dans la requête.
CNID	Identifiant de connexion	L'identifiant système unique pour la connexion TCP/IP.
CSIZ	Taille du contenu	La taille de l'objet récupéré en octets. Les opérations sur les buckets n'incluent pas ce champ.
GFID	ID de connexion à la fédération de grille	L'ID de connexion de la connexion de la fédération de grille associée à une demande PUT de réplication inter-grille. Uniquement inclus dans les journaux d'audit sur la grille de destination.
GFSA	ID du compte source de la Grid Federation	L'ID de compte du locataire sur la grille source pour une demande PUT de réplication inter-grille. Uniquement inclus 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 enregistrés tels que sélectionnés lors de la configuration. <code>`X-Forwarded-For`</code> est automatiquement inclus s'il est présent dans la demande et si le <code>`X-Forwarded-For`</code> la valeur est différente de l'adresse IP de l'expéditeur de la demande (champ d'audit SAIP). <code>`x-amz-bypass-governance-retention`</code> est automatiquement inclus s'il est présent dans la demande.
LKEN	Verrouillage d'objet activé	Valeur de l'en-tête de la requête <code>x-amz-bucket-object-lock-enabled</code> , si présent dans la demande.
LKLH	Verrouillage d'objet Conservation légale	Valeur de l'en-tête de la requête <code>x-amz-object-lock-legal-hold</code> , s'il est présent dans la requête PutObject.

Code	Champ	Description
LKMD	Mode de rétention du verrouillage des objets	Valeur de l'en-tête de la requête <code>x-amz-object-lock-mode</code> , s'il est présent dans la requête PutObject.
LKRU	Verrouillage d'objet Conserver jusqu'à la date	Valeur de l'en-tête de la requête <code>x-amz-object-lock-retain-until-date</code> , s'il est présent dans la requête PutObject. Les valeurs sont limitées à 100 ans à compter de la date d'ingestion de l'objet.
MTME	Heure de la dernière modification	L'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 : SUCS : Réussi
S3AI	ID de compte locataire S3 (expéditeur de la demande)	L'ID du compte 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)	L'ID de clé d'accès S3 haché pour l'utilisateur qui a envoyé la demande. Une valeur vide indique un accès anonyme.
S3BK	Godet S3	Le nom du bucket S3.
S3KY	Touche S3	Le nom de la clé S3, sans inclure le nom du bucket. Les opérations sur les buckets n'incluent pas ce champ.
S3SR	Sous-ressource S3	Le compartiment ou la sous-ressource d'objet sur lequel l'opération est effectuée, le cas échéant.
SACC	Nom du compte locataire S3 (expéditeur de la demande)	Le nom du compte locataire de l'utilisateur qui a envoyé la demande. Vide pour les demandes anonymes.
SAIP	Adresse IP (expéditeur de la requête)	L'adresse IP de l'application cliente qui a effectué la demande.

Code	Champ	Description
SBAC	Nom du compte locataire S3 (propriétaire du bucket)	Le nom du compte locataire pour le propriétaire du bucket. Utilisé pour identifier l'accès inter-comptes ou anonyme.
SBAI	ID de compte locataire S3 (propriétaire du bucket)	L'ID de compte locataire du propriétaire du bucket cible. Utilisé pour identifier l'accès inter-comptes ou anonyme.
SRCF	Configuration des sous-ressources	La nouvelle configuration de sous-ressource (tronquée aux 1024 premiers caractères).
SUSR	URN utilisateur S3 (expéditeur de la requête)	L'ID du compte locataire et le nom d'utilisateur de l'utilisateur effectuant la demande. L'utilisateur peut être un utilisateur local ou un utilisateur LDAP. Par exemple : <code>urn:sgws:identity::03393893651506583485:root</code> Vide pour les demandes anonymes.
TEMPS	Durée	Temps total de traitement de la demande en microsecondes.
TLIP	Adresse IP de l'équilibreur de charge approuvé	Si la demande a été acheminée par un équilibreur de charge de couche 7 approuvé, l'adresse IP de l'équilibreur de charge.
ULID	ID de téléchargement	Inclus uniquement dans les messages SPUT pour les opérations CompleteMultipartUpload. Indique que toutes les pièces ont été téléchargées et assemblées.
UUID	Identifiant unique universel	L'identifiant de l'objet dans le système StorageGRID .
VSID	ID de version	L'ID de version d'un nouvel objet créé dans un bucket versionné. Les opérations sur les buckets et les objets dans les buckets non versionnés n'incluent pas ce champ.
VSST	État de versionnage	Le nouvel état de version d'un bucket. 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 les API standard.

Code	Champ	Description
CBID	Identifiant du bloc de contenu	L'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 au sein du système.

SUPD : Métadonnées S3 mises à jour

Ce message est généré par l'API S3 lorsqu'un client S3 met à jour les métadonnées d'un objet ingéré. Le message est émis par le serveur si la mise à jour des métadonnées est réussie.

Code	Champ	Description
CBID	Identifiant du bloc de contenu	L'identifiant unique du bloc de contenu demandé. Si le CBID est inconnu, ce champ est défini sur 0. Les opérations sur les buckets n'incluent pas ce champ.
CNCH	En-tête de contrôle de cohérence	La valeur de l'en-tête de requête HTTP Consistency-Control, si présent dans la requête, lors de la mise à jour des paramètres de conformité d'un bucket.
CNID	Identifiant de connexion	L'identifiant système unique pour la connexion TCP/IP.
CSIZ	Taille du contenu	La taille de l'objet récupéré en octets. Les opérations sur les buckets n'incluent pas ce champ.
HTRH	En-tête de requête HTTP	Liste des noms et valeurs d'en-tête de requête HTTP enregistrés tels que sélectionnés lors de la configuration. `X-Forwarded-For` est automatiquement inclus s'il est présent dans la demande et si le `X-Forwarded-For` la valeur est différente de l'adresse IP de l'expéditeur de la demande (champ d'audit SAIP) .

Code	Champ	Description
RSLT	Code de résultat	Résultat de la transaction GET. Le résultat est toujours : SUCS : réussi
S3AI	ID de compte locataire S3 (expéditeur de la demande)	L'ID du compte 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)	L'ID de clé d'accès S3 haché pour l'utilisateur qui a envoyé la demande. Une valeur vide indique un accès anonyme.
S3BK	Godet S3	Le nom du bucket S3.
S3KY	Touche S3	Le nom de la clé S3, sans inclure le nom du bucket. Les opérations sur les buckets n'incluent pas ce champ.
SACC	Nom du compte locataire S3 (expéditeur de la demande)	Le nom du compte locataire de l'utilisateur qui a envoyé la demande. Vide pour les demandes anonymes.
SAIP	Adresse IP (expéditeur de la requête)	L'adresse IP de l'application cliente qui a effectué la demande.
SBAC	Nom du compte locataire S3 (propriétaire du bucket)	Le nom du compte locataire pour le propriétaire du bucket. Utilisé pour identifier l'accès inter-comptes ou anonyme.
SBAI	ID de compte locataire S3 (propriétaire du bucket)	L'ID de compte locataire du propriétaire du bucket cible. Utilisé pour identifier l'accès inter-comptes ou anonyme.
SUSR	URN utilisateur S3 (expéditeur de la requête)	L'ID du compte locataire et le nom d'utilisateur de l'utilisateur effectuant la demande. L'utilisateur peut être un utilisateur local ou un utilisateur LDAP. Par exemple : <code>urn:sgws:identity::03393893651506583485:root</code> Vide pour les demandes anonymes.
TEMPS	Durée	Temps total de traitement de la demande en microsecondes.

Code	Champ	Description
TLIP	Adresse IP de l'équilibreur de charge approuvé	Si la demande a été acheminée par un équilibreur de charge de couche 7 approuvé, l'adresse IP de l'équilibreur de charge.
UUID	Identifiant unique universel	L'identifiant de l'objet dans le système StorageGRID .
VSID	ID de version	L'ID de version de la version spécifique d'un objet dont les métadonnées ont été mises à jour. Les opérations sur les buckets et les objets dans les buckets 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 des données d'objet répliquées sont lues ou écrites sur le disque, plusieurs contrôles de vérification et d'intégrité sont effectués pour garantir que les données envoyées à l'utilisateur demandeur sont identiques aux données initialement ingérées dans le système. Si l'une de ces vérifications échoue, le système met automatiquement en quarantaine les données de l'objet répliqué corrompu pour empêcher leur récupération ultérieure.

Code	Champ	Description
CBID	Identifiant du bloc de contenu	L'identifiant unique du bloc de contenu dont la vérification a échoué.
RSLT	Code de résultat	Type d'échec de vérification : CRCF : échec du contrôle de redondance cyclique (CRC). HMAC : la vérification du code d'authentification de message basé sur le hachage (HMAC) a échoué. EHSB : hachage de contenu chiffré inattendu. PHSH : hachage de contenu original inattendu. SEQC : séquence de données incorrecte sur le disque. PERR : structure non valide du fichier disque. DERR : Erreur de disque. FNAM : Mauvais nom de fichier.



Ce message doit être surveillé de près. Les échecs de vérification du contenu peuvent indiquer des pannes matérielles imminentes.

Pour déterminer quelle opération a déclenché le message, consultez la valeur du champ AMID (ID du module). Par exemple, une valeur SVFY indique que le message a été généré par le module Storage Verifier, c'est-à-dire une vérification en arrière-plan, et STOR indique que le message a été déclenché par une récupération de contenu.

SVRU : Vérification du magasin d'objets inconnu

Le composant Stockage du service LDR analyse en continu toutes les copies des données d'objet répliquées dans le magasin d'objets. Ce message est émis lorsqu'une copie inconnue ou inattendue des données d'objet répliquées est détectée dans le magasin d'objets et déplacée vers le répertoire de quarantaine.

Code	Champ	Description
FPTH	Chemin du fichier	Le chemin du fichier de la copie d'objet inattendue.
RSLT	Résultat	Ce champ a la valeur « AUCUN ». RSLT est un champ de message obligatoire, mais n'est pas pertinent pour ce message. « NONE » est utilisé plutôt que « SUCS » afin que ce message ne soit pas filtré.



Le message d'audit SVRU : Object Store Verify Unknown doit être surveillé de près. Cela signifie que des copies inattendues de données d'objet ont été détectées dans le magasin d'objets. Cette situation doit être étudiée immédiatement pour déterminer comment ces copies ont été créées, car elle peut indiquer des pannes matérielles imminentes.

SYSD : arrêt du nœud

Lorsqu'un service est arrêté correctement, ce message est généré pour indiquer que l'arrêt a été demandé. En général, 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	Arrêt propre	La nature de l'arrêt : SUCS : Le système a été arrêté proprement.

Le message n'indique pas si le serveur hôte est arrêté, uniquement le service de reporting. Le RSLT d'un SYSD ne peut pas indiquer un arrêt « sale », car le message est généré uniquement par des arrêts « propres ».

SYST : arrêt du nœud

Lorsqu'un service est arrêté correctement, 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	Arrêt propre	La nature de l'arrêt : SUCS : Le système a été arrêté proprement.

Le message n'indique pas si le serveur hôte est arrêté, uniquement le service de reporting. Le code RSLT d'un message SYST ne peut pas indiquer un arrêt « sale », car le message est généré uniquement par des arrêts « propres ».

SYSU : démarrage du nœud

Lorsqu'un service est redémarré, ce message est généré pour indiquer si l'arrêt précédent était propre (commandé) ou désordonné (inattendu).

Code	Champ	Description
RSLT	Arrêt propre	La nature de l'arrêt : SUCS : Le système a été arrêté proprement. DSDN : le système n'a pas été arrêté correctement. 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, uniquement le service de reporting. Ce message peut être utilisé pour :

- Détecter la discontinuité dans la piste d'audit.
- Déterminez si un service échoue pendant son fonctionnement (car la nature distribuée du système StorageGRID peut masquer ces échecs). Le Gestionnaire de serveur redémarre automatiquement un service défaillant.

WDEL : SUPPRESSION rapide

Lorsqu'un client Swift émet une transaction DELETE, une demande est effectuée pour supprimer l'objet ou le conteneur spécifié. Ce message est émis par le serveur si la transaction réussit.

Code	Champ	Description
CBID	Identifiant du bloc de contenu	L'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	La 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 enregistrés tels que sélectionnés lors de la configuration. `X-Forwarded-For` est automatiquement inclus s'il est présent dans la demande et si le `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	L'horodatage Unix, en microsecondes, indiquant quand l'objet a été modifié pour la dernière fois.
RSLT	Code de résultat	Résultat de la transaction DELETE. Le résultat est toujours : SUCS : Réussi
SAIP	Adresse IP du client demandeur	L'adresse IP de l'application cliente qui a effectué la demande.
SGRP	Site (Groupe)	Si présent, l'objet a été supprimé sur le site spécifié, qui n'est pas le site où l'objet a été ingéré.
TEMPS	Durée	Temps total de traitement de la demande en microsecondes.
TLIP	Adresse IP de l'équilibreur de charge approuvé	Si la demande a été acheminée par un équilibreur de charge de couche 7 approuvé, l'adresse IP de l'équilibreur de charge.
UUID	Identifiant unique universel	L'identifiant de l'objet dans le système StorageGRID .
CMPC	ID de compte Swift	L'ID de compte unique tel que spécifié par le système StorageGRID .
WCON	Conteneur Swift	Le nom du conteneur Swift.
WOBJ	Objet Swift	L'identifiant de l'objet Swift. Les opérations sur les conteneurs n'incluent pas ce champ.
WUSR	Utilisateur du compte Swift	Le 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 effectuée 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 réussit.

Code	Champ	Description
CBID	Identifiant du bloc de contenu	L'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	La 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 enregistrés tels que sélectionnés lors de la configuration. <code>`X-Forwarded-For` est automatiquement inclus s'il est présent dans la demande et si le `X-Forwarded-For` la valeur est différente de l'adresse IP de l'expéditeur de la demande (champ d'audit SAIP).</code>
RSLT	Code de résultat	Résultat de la transaction GET. Le résultat est toujours SUCS : réussi
SAIP	Adresse IP du client demandeur	L'adresse IP de l'application cliente qui a effectué la demande.
TEMPS	Durée	Temps total de traitement de la demande en microsecondes.
TLIP	Adresse IP de l'équilibreur de charge approuvé	Si la demande a été acheminée par un équilibreur de charge de couche 7 approuvé, l'adresse IP de l'équilibreur de charge.
UUID	Identifiant unique universel	L'identifiant de l'objet dans le système StorageGRID .
CMPC	ID de compte Swift	L>ID de compte unique tel que spécifié par le système StorageGRID .
WCON	Conteneur Swift	Le nom du conteneur Swift. Les opérations sur les comptes n'incluent pas ce champ.

Code	Champ	Description
WOBJ	Objet Swift	L'identifiant de l'objet Swift. Les opérations sur les comptes et les conteneurs n'incluent pas ce champ.
WUSR	Utilisateur du compte Swift	Le nom d'utilisateur du compte Swift qui identifie de manière unique le client effectuant la transaction.

WHEA : TÊTE RAPIDE

Lorsqu'un client Swift émet une transaction HEAD, une demande est effectuée pour vérifier l'existence d'un compte, d'un conteneur ou d'un objet et récupérer toutes les métadonnées pertinentes. Ce message est émis par le serveur si la transaction réussit.

Code	Champ	Description
CBID	Identifiant du bloc de contenu	L'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	La 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 enregistrés tels que sélectionnés lors de la configuration. `X-Forwarded-For` est automatiquement inclus s'il est présent dans la demande et si le `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 HEAD. Le résultat est toujours : SUCS : réussi
SAIP	Adresse IP du client demandeur	L'adresse IP de l'application cliente qui a effectué la demande.
TEMPS	Durée	Temps total de traitement de la demande en microsecondes.
TLIP	Adresse IP de l'équilibreur de charge approuvé	Si la demande a été acheminée par un équilibreur de charge de couche 7 approuvé, l'adresse IP de l'équilibreur de charge.

Code	Champ	Description
UUID	Identifiant unique universel	L'identifiant de l'objet dans le système StorageGRID .
CMPC	ID de compte Swift	L'ID de compte unique tel que spécifié par le système StorageGRID .
WCON	Conteneur Swift	Le nom du conteneur Swift. Les opérations sur les comptes n'incluent pas ce champ.
WOBJ	Objet Swift	L'identifiant de l'objet Swift. Les opérations sur les comptes et les conteneurs n'incluent pas ce champ.
WUSR	Utilisateur du compte Swift	Le nom d'utilisateur du compte Swift qui identifie de manière unique le client effectuant la transaction.

WPUT : Swift PUT

Lorsqu'un client Swift émet une transaction PUT, une demande est effectuée pour créer un nouvel objet ou conteneur. Ce message est émis par le serveur si la transaction réussit.

Code	Champ	Description
CBID	Identifiant du bloc de contenu	L'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	La 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 enregistrés tels que sélectionnés lors de la configuration. `X-Forwarded-For` est automatiquement inclus s'il est présent dans la demande et si le `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	L'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 : SUCS : réussi
SAIP	Adresse IP du client demandeur	L'adresse IP de l'application cliente qui a effectué la demande.
TEMPS	Durée	Temps total de traitement de la demande en microsecondes.
TLIP	Adresse IP de l'équilibreur de charge approuvé	Si la demande a été acheminée par un équilibreur de charge de couche 7 approuvé, l'adresse IP de l'équilibreur de charge.
UUID	Identifiant unique universel	L'identifiant de l'objet dans le système StorageGRID .
CMPC	ID de compte Swift	L'ID de compte unique tel que spécifié par le système StorageGRID .
WCON	Conteneur Swift	Le nom du conteneur Swift.
WOBJ	Objet Swift	L'identifiant de l'objet Swift. Les opérations sur les conteneurs n'incluent pas ce champ.
WUSR	Utilisateur du compte Swift	Le nom d'utilisateur du compte Swift qui identifie de manière unique le client effectuant la transaction.

Développer une grille

Types d'extension

Vous pouvez étendre la capacité ou les fonctionnalités de votre système StorageGRID sans interrompre les opérations du système.

Une extension StorageGRID vous permet d'ajouter :

- Volumes de stockage vers nœuds de stockage
- Nouveaux nœuds de grille sur un site existant
- Un tout nouveau site

La raison pour laquelle vous effectuez 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 de métadonnées ou ajouter de la redondance ou de nouvelles fonctionnalités.

Suivez les étapes correspondant au type d'extension que vous effectuez :

Ajouter des volumes de stockage

Suivez les étapes pour [ajout de volumes de stockage aux nœuds de stockage](#) .

Ajouter des nœuds de grille

1. Suivez les étapes pour [ajout de nœuds de grille à un site existant](#) .
2. ["Mettre à jour les sous-réseaux"](#) .
3. Déployer les nœuds de grille :
 - ["appareils électroménagers"](#)
 - ["VMware"](#)
 - ["Linux"](#)



« Linux » fait référence à un déploiement Red Hat Enterprise Linux, Ubuntu ou Debian. Pour une liste des versions prises en charge, consultez le ["Outil de matrice d'interopérabilité NetApp \(IMT\)"](#) .

4. ["Effectuer l'expansion"](#) .
5. ["Configurer le système étendu"](#) .

Ajouter un nouveau site

1. Suivez les étapes pour [Ajout d'un nouveau site](#) .
2. ["Mettre à jour les sous-réseaux"](#) .
3. Déployer les nœuds de grille :
 - ["appareils électroménagers"](#)
 - ["VMware"](#)
 - ["Linux"](#)



« Linux » fait référence à un déploiement Red Hat Enterprise Linux, Ubuntu ou Debian. Pour une liste des versions prises en charge, consultez le ["Outil de matrice d'interopérabilité NetApp \(IMT\)"](#) .

4. ["Effectuer l'expansion"](#) .
5. ["Configurer le système étendu"](#) .

Planifier l'extension de StorageGRID

Ajouter de la capacité de stockage

Directives pour l'ajout de capacité d'objet

Vous pouvez étendre la capacité de stockage d'objets de votre système StorageGRID en ajoutant des volumes de stockage aux nœuds de stockage existants ou en ajoutant de nouveaux nœuds de stockage aux sites existants. Vous devez ajouter une capacité de stockage d'une manière qui répond aux exigences de votre politique de gestion du cycle

de vie des informations (ILM).

Directives pour l'ajout de volumes de stockage

Avant d'ajouter des volumes de stockage aux nœuds de stockage existants, consultez les directives et limitations suivantes :

- Vous devez examiner vos règles ILM actuelles pour déterminer où et quand ["ajouter des volumes de stockage"](#) pour augmenter le stockage disponible pour ["objets répliqués"](#) ou ["objets à code d'effacement"](#) .
- Vous ne pouvez pas augmenter la capacité des métadonnées de votre système en ajoutant des volumes de stockage, car les métadonnées des objets sont stockées uniquement sur le volume 0.
- Chaque nœud de stockage basé sur un logiciel peut prendre en charge un maximum de 48 volumes de stockage. Si vous devez ajouter une capacité au-delà de cela, vous devez ajouter de nouveaux nœuds de stockage.
- Vous pouvez ajouter une ou deux étagères d'extension à chaque appareil SG6060. Chaque étagère d'extension ajoute 16 volumes de stockage. Avec les deux étagères d'extension installées, le SG6060 peut prendre en charge un total de 48 volumes de stockage.
- Vous pouvez ajouter une ou deux étagères d'extension à chaque appareil SG6160. Chaque étagère d'extension ajoute 60 volumes de stockage. Avec les deux étagères d'extension installées, le SG6160 peut prendre en charge un total de 180 volumes de stockage.
- Vous ne pouvez pas ajouter de volumes de stockage à un autre dispositif 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 récupération ou une autre extension.

Après avoir décidé d'ajouter des volumes de stockage et déterminé les nœuds de stockage que vous devez étendre pour satisfaire à votre politique ILM, suivez les instructions correspondant à votre type de nœud de stockage :

- Pour ajouter une ou deux étagères d'extension à un dispositif de stockage SG6060, accédez à ["Ajouter une étagère d'extension au SG6060 déployé"](#) .
- Pour ajouter une ou deux étagères d'extension à un dispositif de stockage SG6160, accédez à ["Ajouter une étagère d'extension au SG6160 déployé"](#)
- Pour un nœud basé sur un logiciel, suivez les instructions pour ["ajout de volumes de stockage aux nœuds de stockage"](#) .

Directives pour l'ajout de nœuds de stockage

Avant d'ajouter des nœuds de stockage à des sites existants, consultez les directives et limitations suivantes :

- Vous devez examiner vos règles ILM actuelles pour déterminer où et quand ajouter des nœuds de stockage pour augmenter le stockage disponible pour ["objets répliqués"](#) ou ["objets à code d'effacement"](#) .
- Vous ne devez pas ajouter plus de 10 nœuds de stockage dans une seule procédure d'extension.
- Vous pouvez ajouter des nœuds de stockage à plusieurs sites dans une seule procédure d'extension.
- Vous pouvez ajouter des nœuds de stockage et d'autres types de nœuds dans une seule procédure d'extension.
- Avant de démarrer la procédure d'extension, vous devez confirmer que toutes les opérations de réparation de données effectuées dans le cadre d'une récupération sont terminées. Voir ["Vérifier les tâches de réparation de données"](#) .

- Si vous devez supprimer des nœuds de stockage avant ou après avoir effectué une extension, vous ne devez pas mettre hors service plus de 10 nœuds de stockage dans une seule procédure de mise hors service de nœud.

Directives pour le service ADC sur les nœuds de stockage

Lors de la configuration de l'extension, vous devez choisir d'inclure ou non le service de contrôleur de domaine administratif (ADC) sur chaque nouveau nœud de stockage. Le service ADC suit l'emplacement et la disponibilité des services du réseau.

- Le système StorageGRID nécessite un ["quorum des services ADC"](#) être disponible sur chaque site et à tout moment.
- Au moins trois nœuds de stockage sur chaque site doivent inclure le service ADC.
- L'ajout du service ADC à chaque nœud de stockage n'est pas recommandé. L'inclusion d'un trop grand nombre de services ADC peut entraîner des ralentissements en raison de la quantité accrue de communication entre les nœuds.
- Une seule grille ne doit pas avoir 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. Étant donné que vous ne pouvez pas mettre hors service un nœud de stockage s'il reste trop peu de services ADC, 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.

Ajouter une capacité de stockage pour les objets répliqués

Si la stratégie de gestion du cycle de vie des informations (ILM) de votre déploiement inclut une règle qui crée des copies répliquées d'objets, vous devez déterminer la quantité de stockage à ajouter et l'emplacement où ajouter les nouveaux volumes de stockage ou nœuds de stockage.

Pour obtenir des conseils sur l'endroit où ajouter du stockage supplémentaire, examinez les règles ILM qui créent des copies répliquées. Si les règles ILM créent deux copies d'objet ou plus, prévoyez d'ajouter du stockage à chaque emplacement où des copies d'objet sont effectuées. À titre d'exemple simple, si vous avez une grille à deux sites et une règle ILM qui crée une copie d'objet sur chaque site, vous devez ["ajouter du stockage"](#) à chaque site pour augmenter la capacité globale des objets de la grille. Pour plus d'informations sur la réplication d'objets, voir ["Qu'est-ce que la réplication"](#).

Pour des raisons de performances, vous devez essayer de maintenir l'équilibre entre la capacité de stockage et la puissance de calcul entre les sites. Ainsi, 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 stratégie ILM plus complexe qui inclut des règles qui placent des objets à différents emplacements en fonction de critères tels que le nom du bucket, ou des règles qui modifient les emplacements des objets au fil du temps, votre analyse de l'emplacement de stockage requis pour l'extension sera similaire, mais plus complexe.

Le graphique de la vitesse à laquelle la capacité de stockage globale est consommée peut vous aider à comprendre la quantité de stockage à ajouter dans l'extension et quand l'espace de stockage supplémentaire sera nécessaire. Vous pouvez utiliser le gestionnaire de grille pour ["capacité de stockage du moniteur et des graphiques"](#).

Lorsque vous planifiez le calendrier d'une extension, n'oubliez pas de prendre en compte le temps nécessaire pour acquérir et installer un stockage supplémentaire.

Ajouter une capacité de stockage pour les objets à code d'effacement

Si votre politique ILM inclut une règle qui crée des copies à code d'effacement, vous devez planifier où ajouter un nouveau stockage et quand ajouter un nouveau stockage. La quantité de stockage que vous ajoutez et le moment de l'ajout peuvent affecter la capacité de stockage utilisable du réseau.

La première étape de la planification d'une extension de stockage consiste à examiner les règles de votre stratégie ILM qui créent des objets à code d'effacement. Étant donné que StorageGRID crée $k+m$ fragments pour chaque objet codé par effacement et stocke chaque fragment sur un nœud de stockage différent, vous devez vous assurer qu'au moins $k+m$ nœuds de stockage disposent d'espace pour les nouvelles données codées par effacement après l'extension. Si le profil de codage d'effacement offre une protection contre la perte de site, vous devez ajouter du stockage à chaque site. Voir ["Que sont les schémas de codage d'effacement"](#) pour plus d'informations sur les profils de codage d'effacement.

Le nombre de nœuds que vous devez ajouter dépend également du degré de remplissage des nœuds existants lorsque vous effectuez l'extension.

Recommandation générale pour l'ajout de capacité de stockage pour les objets à code d'effacement

Si vous souhaitez éviter des calculs détaillés, vous pouvez ajouter deux nœuds de stockage par site lorsque les nœuds de stockage existants atteignent 70 % de leur capacité.

Cette recommandation générale fournit des résultats raisonnables sur une large gamme de schémas de codage d'effacement pour les grilles à site unique et pour les grilles où le codage d'effacement offre une protection contre la perte de site.

Pour mieux comprendre les facteurs qui ont conduit à cette recommandation ou pour élaborer un plan plus précis pour votre site, consultez ["Considérations pour le rééquilibrage des données codées par effacement"](#). Pour une recommandation personnalisée optimisée pour votre situation, contactez votre consultant NetApp Professional Services.

Considérations pour le rééquilibrage des données codées par 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 du codage d'effacement (EC) si vous ne pouvez pas ajouter suffisamment de nœuds de stockage pour le schéma de codage d'effacement que vous utilisez.

Après avoir examiné ces considérations, effectuez l'extension, puis passez à ["Rééquilibrer les données codées par effacement après l'ajout de nœuds de stockage"](#) pour exécuter la procédure.

Qu'est-ce que le rééquilibrage CE ?

Le rééquilibrage EC est une procédure StorageGRID qui peut être requise après une extension de 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 les fragments codés par effacement entre les nœuds de stockage existants et nouvellement ajoutés sur un site.

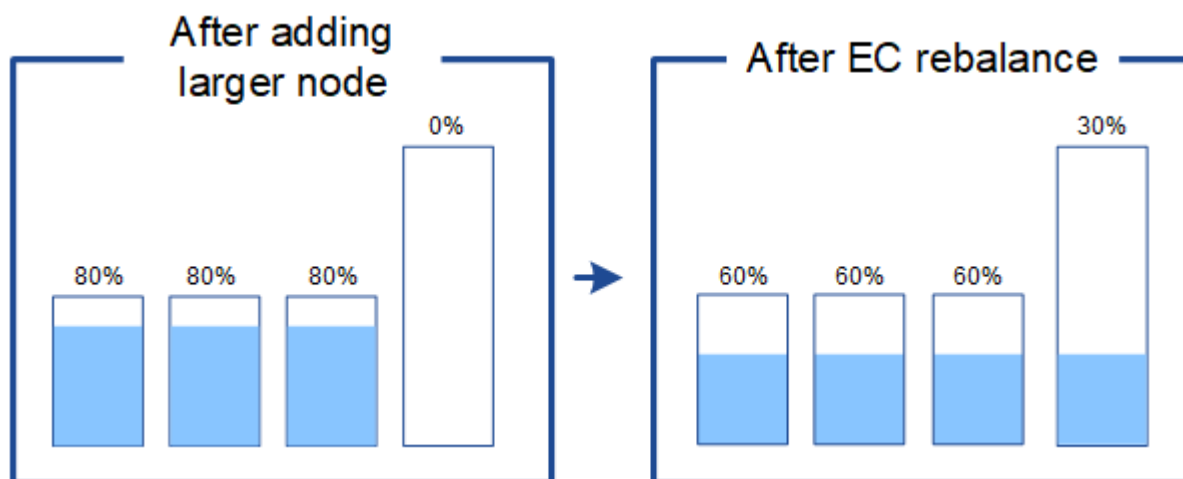
La procédure de rééquilibrage de la CE :

- Déplace uniquement les données d'objet codées par effacement. Il ne déplace pas les données d'objets répliqués.
- Redistribue les données au sein d'un site. Il ne déplace pas de données entre les sites.
- Redistribue les données entre tous les nœuds de stockage d'un site. Il ne redistribue 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 où déplacer les données codées par effacement.
- Redistribue les données codées par effacement de manière uniforme entre les nœuds de stockage sans tenir compte des capacités relatives de chaque nœud.
- Ne distribuera pas de données codées par effacement aux nœuds de stockage qui sont remplis à plus de 80 %.
- Cela pourrait diminuer les performances des opérations ILM et des opérations client S3 lors de son exécution ; des ressources supplémentaires sont nécessaires pour redistribuer les fragments de codage d'effacement.

Une fois la procédure de rééquilibrage de la CE terminée :

- Les données codées par effacement seront déplacées des nœuds de stockage avec moins d'espace disponible vers les nœuds de stockage avec plus d'espace disponible.
- La protection des données des objets codés par effacement restera inchangée.
- Les valeurs utilisées (%) peuvent être différentes entre les nœuds de stockage pour deux raisons :
 - Les copies d'objets répliqués 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 se retrouveront avec approximativement la même quantité de données codées par effacement.

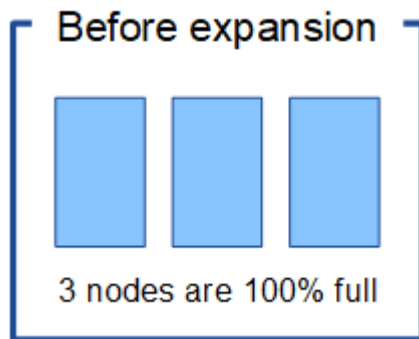
Par exemple, supposons que trois nœuds de 200 To soient chacun remplis à 80 % ($200 \times 0,8 = 160$ To sur chaque nœud, ou 480 To pour le site). Si vous ajoutez un nœud de 400 To et exécutez la procédure de rééquilibrage, tous les nœuds auront désormais approximativement la même quantité de données 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 codées par effacement

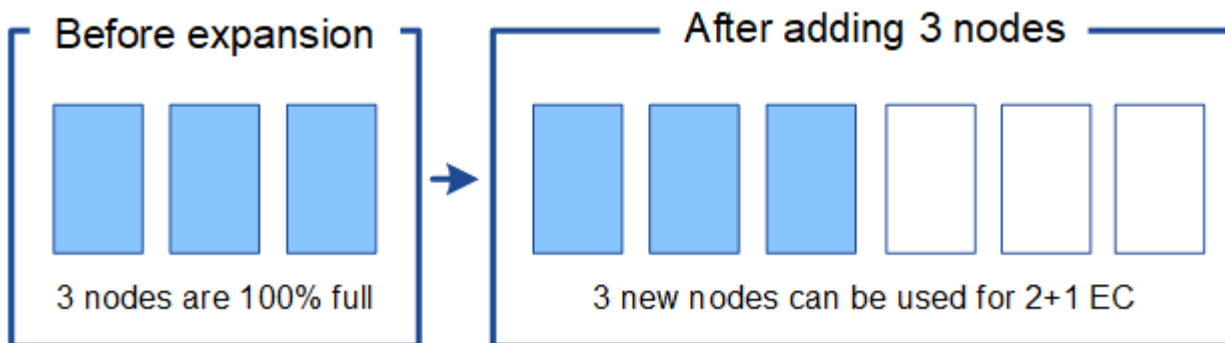
Considérez le scénario suivant :

- StorageGRID s'exécute sur un seul site, qui contient trois nœuds de stockage.
- La politique ILM utilise une règle de codage d'effacement 2+1 pour tous les objets supérieurs à 1,0 Mo et une règle de réplication à 2 copies pour les objets plus petits.
- Tous les nœuds de stockage sont complètement pleins. L'alerte **Low Object Storage** a été déclenchée au niveau de gravité majeur.



Le rééquilibrage n'est pas nécessaire si vous ajoutez suffisamment de nœuds

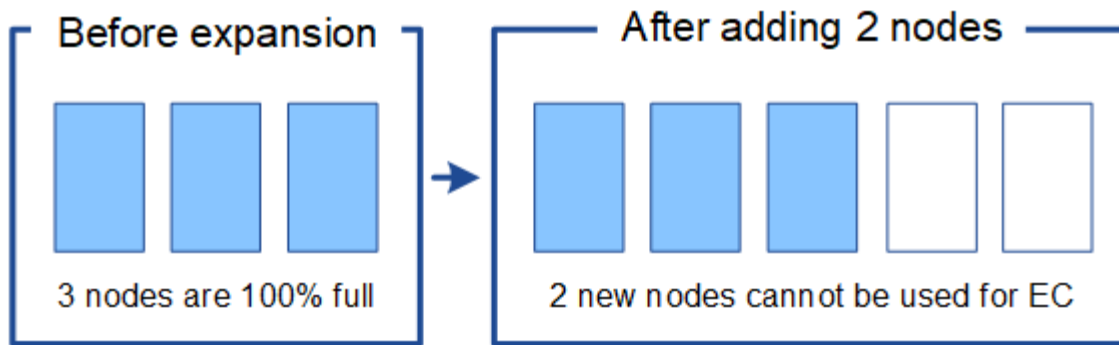
Pour comprendre quand le rééquilibrage EC n'est pas nécessaire, supposons que vous ayez ajouté trois (ou plus) nouveaux nœuds de stockage. Dans ce cas, vous n'avez pas besoin d'effectuer un rééquilibrage EC. Les nœuds de stockage d'origine resteront pleins, mais les nouveaux objets utiliseront désormais les trois nouveaux nœuds pour le codage d'effacement 2+1 : les deux fragments de données et le fragment de parité peuvent chacun être stockés sur un nœud différent.



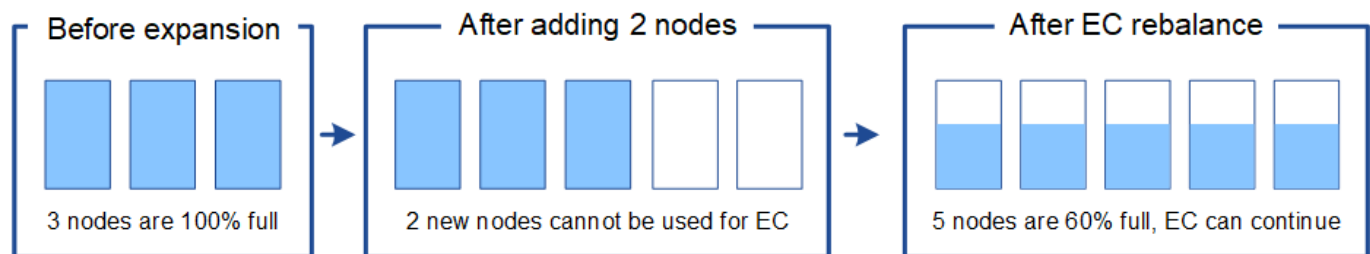
Bien que vous puissiez exécuter la procédure de rééquilibrage EC dans ce cas, le déplacement des données codées par effacement existantes diminuera temporairement les performances de la grille, ce qui pourrait avoir un impact sur les opérations du client.

Un rééquilibrage est nécessaire si vous ne pouvez pas ajouter suffisamment de nœuds

Pour comprendre quand un rééquilibrage EC est nécessaire, supposons que vous ne puissiez ajouter que deux nœuds de stockage, au lieu de trois. Étant donné que le schéma 2+1 nécessite au moins trois nœuds de stockage pour disposer d'espace disponible, les nœuds vides ne peuvent pas être utilisés pour les nouvelles données codées par effacement.



Pour utiliser les nouveaux nœuds de stockage, vous devez exécuter la procédure de rééquilibrage EC. Lorsque cette procédure s'exécute, StorageGRID redistribue les données codées par effacement existantes et les fragments de parité entre tous les nœuds de stockage du site. Dans cet exemple, lorsque la procédure de rééquilibrage EC est terminée, les cinq nœuds ne sont désormais remplis qu'à 60 % et les objets peuvent continuer à être ingérés dans le schéma de codage d'effacement 2+1 sur tous les nœuds de stockage.



Recommandations pour le rééquilibrage de la CE

NetApp nécessite un rééquilibrage EC si *toutes* les affirmations suivantes sont vraies :

- Vous utilisez le codage d'effacement pour vos données d'objet.
- L'alerte **Low Object Storage** a été déclenchée pour un ou plusieurs nœuds de stockage sur un site, indiquant que les nœuds sont remplis à 80 % ou plus.
- Vous ne parvenez pas à ajouter suffisamment de nouveaux nœuds de stockage pour le schéma de codage d'effacement utilisé. Voir ["Ajouter une capacité de stockage pour les objets à code d'effacement"](#) .
- Vos clients S3 peuvent tolérer des performances inférieures pour leurs opérations d'écriture et de lecture pendant que la procédure de rééquilibrage EC est en cours d'exécution.

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 puissent tolérer des performances inférieures pour leurs opérations d'écriture et de lecture pendant l'exécution de la procédure de rééquilibrage EC.

Comment la procédure de rééquilibrage EC interagit avec 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 de la CE ?
Procédures supplémentaires de rééquilibrage de la CE	Non. Vous ne pouvez exécuter qu'une seule procédure de rééquilibrage EC à la fois.
Procédure de déclassement Travaux de réparation de données EC	Non. • Vous ne pouvez pas démarrer une procédure de mise hors service ou une 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 pendant qu'une procédure de mise hors service d'un nœud de stockage ou qu'une réparation de données EC est en cours d'exécution.
Procédure d'extension	Non. Si vous devez ajouter de nouveaux nœuds de stockage dans une extension, exécutez la procédure de rééquilibrage EC après avoir ajouté tous les nouveaux nœuds.
Procédure de mise à niveau	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 de rééquilibrage EC pour effectuer une mise à niveau du logiciel.
Procédure de clonage du nœud de l'appareil	Non. Si vous devez cloner un nœud de stockage d'appliance, exécutez la procédure de rééquilibrage EC après avoir ajouté le nouveau nœud.
Procédure de correctif	Oui. Vous pouvez appliquer un correctif StorageGRID pendant que la procédure de rééquilibrage EC est en cours d'exécution.
Autres procédures de maintenance	Non. Vous devez terminer la procédure de rééquilibrage EC avant d'exécuter d'autres procédures de maintenance.

Comment la procédure de rééquilibrage de la CE interagit avec l'ILM

Pendant que la procédure de rééquilibrage EC est en cours d'exécution, évitez d'effectuer des modifications ILM susceptibles de modifier l'emplacement des objets codés par effacement existants. Par exemple, ne commencez pas à utiliser une règle ILM qui a un profil de codage d'effacement différent. Si vous devez

effectuer de telles modifications ILM, vous devez mettre fin à la procédure de rééquilibrage EC.

Ajouter une capacité de métadonnées

Pour garantir qu'un espace suffisant est disponible pour les métadonnées d'objet, vous devrez peut-être effectuer une procédure d'extension pour 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 uniformément sur tous les nœuds de stockage.

Vous pouvez utiliser Grid Manager pour surveiller la capacité des métadonnées des nœuds de stockage et pour estimer la vitesse à laquelle la capacité des métadonnées est consommée. De plus, l'alerte **Faible stockage de métadonnées** est déclenchée pour un nœud de stockage lorsque l'espace de métadonnées utilisé atteint certains seuils.

Notez que la capacité des métadonnées d'objet d'une grille peut être consommée plus rapidement que sa capacité de stockage d'objet, selon la façon dont vous utilisez la grille. Par exemple, si vous ingérez généralement un grand nombre de petits objets ou ajoutez de grandes quantités de métadonnées utilisateur ou de balises aux objets, vous devrez peut-être ajouter des nœuds de stockage pour augmenter la capacité des métadonnées, même si la capacité de stockage d'objets reste suffisante.

Pour plus d'informations, consultez les éléments suivants :

- ["Gérer le stockage des métadonnées des objets"](#)
- ["Surveiller la capacité des métadonnées des objets pour chaque nœud de stockage"](#)

Lignes directrices pour augmenter la capacité des métadonnées

Avant d'ajouter des nœuds de stockage pour augmenter la capacité des métadonnées, examinez les directives et limitations suivantes :

- En supposant qu'une capacité de stockage d'objets suffisante soit disponible, disposer de plus d'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 aux métadonnées d'objet sur un nœud de stockage donné dépend de l'option de stockage Espace réservé aux métadonnées (paramètre à l'échelle du système), de la quantité de RAM allouée au nœud et de la taille du volume 0 du nœud.
- Vous ne pouvez pas augmenter la capacité des métadonnées en ajoutant des volumes de stockage aux nœuds de stockage existants, car les métadonnées sont stockées uniquement sur le volume 0.
- Vous ne pouvez pas augmenter la capacité des métadonnées en ajoutant un nouveau site.
- StorageGRID conserve trois copies de toutes les métadonnées des objets sur chaque site. Pour cette raison, la capacité des métadonnées de votre système est limitée par la capacité des métadonnées de votre plus petit site.
- Lors de l'ajout de capacité de métadonnées, vous devez ajouter le même nombre de nœuds de stockage à chaque site.

Les nœuds de stockage de métadonnées uniquement ont des exigences matérielles spécifiques :

- Lors de l'utilisation d'appliances StorageGRID , les nœuds de métadonnées uniquement peuvent être configurés uniquement sur les appliances SGF6112 avec douze disques de 1,9 To ou douze disques de 3,8 To.
- Lors de l'utilisation de nœuds basés sur des logiciels, les ressources de nœuds contenant uniquement des métadonnées doivent correspondre aux ressources de nœuds de stockage existantes. Par exemple:
 - Si le site StorageGRID existant utilise des appliances SG6000 ou SG6100, les nœuds de métadonnées uniquement basés sur des logiciels doivent répondre aux exigences minimales suivantes :
 - 128 Go de RAM
 - processeur à 8 cœurs
 - SSD de 8 To ou stockage équivalent pour la base de données Cassandra (rangedb/0)
 - Si le site StorageGRID existant utilise des nœuds de stockage virtuels avec 24 Go de RAM, un processeur à 8 cœurs et 3 To ou 4 To de stockage de métadonnées, les nœuds de métadonnées uniquement basés sur un logiciel doivent utiliser des ressources similaires (24 Go de RAM, un processeur à 8 cœurs et 4 To de stockage de métadonnées (rangedb/0).
- Lors de l'ajout d'un nouveau site StorageGRID , la capacité totale des métadonnées du nouveau site doit, au minimum, correspondre aux sites StorageGRID existants et les nouvelles ressources du site doivent correspondre aux nœuds de stockage des sites StorageGRID existants.

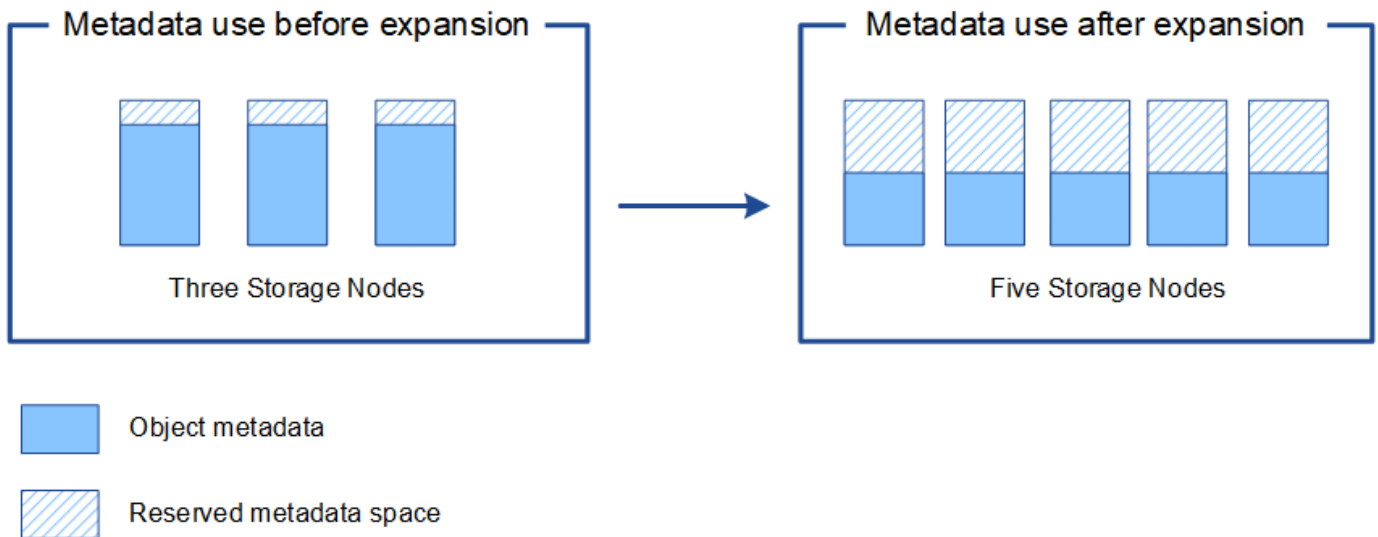
Voir le ["description de ce qu'est l'espace réservé aux métadonnées"](#) .

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 d'objet existantes aux 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. Le côté gauche de la figure représente le volume 0 de trois nœuds de stockage avant une extension. Les métadonnées consomment une partie relativement importante de l'espace de métadonnées disponible de chaque nœud, et l'alerte **Faible stockage de métadonnées** a été déclenchée.

Le côté droit de la figure montre comment les métadonnées existantes sont redistribuées après l'ajout de deux nœuds de stockage au site. La quantité de métadonnées sur chaque nœud a diminué, l'alerte **Faible stockage de métadonnées** n'est plus déclenchée et l'espace disponible pour les métadonnées a augmenté.



Ajoutez des nœuds de grille 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 de grille aux sites existants.

Par exemple, vous pouvez choisir d'ajouter des nœuds de passerelle à utiliser dans un groupe haute disponibilité (HA), ou vous pouvez 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 en une seule opération d'extension :

- Nœuds d'administration non principaux
- Nœuds de stockage
- Nœuds de passerelle

Lorsque vous vous préparez à ajouter des nœuds de grille, tenez compte des limitations 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.
- Lors de l'ajout de nœuds de stockage, vous devez planifier soigneusement le nombre et l'emplacement des nouveaux nœuds. Voir ["Directives pour l'ajout de capacité d'objet"](#) .
- Si l'option **Définir la valeur par défaut du nouveau nœud** est **Non approuvé** dans l'onglet Réseaux clients non approuvés de la page 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 point de terminaison d'équilibrage de charge (**CONFIGURATION > Sécurité > Contrôle du pare-feu**). Consultez les instructions pour ["modifier le paramètre de sécurité du nouveau nœud"](#) et à ["configurer les points de terminaison de l'équilibreur de charge"](#) .

Ajouter un nouveau site

Vous pouvez étendre votre système StorageGRID en ajoutant un nouveau site.

Directives pour l'ajout d'un site

Avant d'ajouter un site, passez en revue les exigences et limitations suivantes :

- Vous ne pouvez ajouter qu'un seul site par opération d'extension.
- Vous ne pouvez pas ajouter de nœuds de grille à un site existant dans le cadre de la 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 des objets d'une grille dépend de la quantité de stockage disponible, de la politique ILM et de la capacité des métadonnées de chaque site.
- Lors du dimensionnement d'un nouveau site, vous devez vous assurer qu'il comprend une capacité de métadonnées suffisante.

StorageGRID conserve une copie de toutes les métadonnées des objets 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 la croissance.

Pour plus d'informations, consultez les éléments suivants :

- ["Gérer le stockage des métadonnées des objets"](#)
- ["Surveiller la capacité des métadonnées des objets pour chaque nœud de stockage"](#)
- Vous devez prendre en compte la bande passante réseau disponible entre les sites et le 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 ingérés.
- Étant donné que votre système StorageGRID reste opérationnel pendant l'extension, vous devez examiner les règles ILM avant de démarrer la procédure d'extension. Vous devez vous assurer que les copies d'objets 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). Si tel est le cas, vous devez créer un nouveau pool de stockage contenant les nœuds de stockage existants et mettre à jour vos 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 deviendra actif.

Pour plus d'informations sur la modification de l'ILM lors de l'ajout d'un nouveau site, consultez le ["exemple de modification d'une politique ILM"](#) .

Rassembler le matériel nécessaire

Avant d'effectuer une opération d'extension, rassemblez le matériel et installez et configurez tout nouveau matériel et réseaux.

Article	Remarques
Archive d'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 exécutée sur la grille. Pour plus de détails, consultez les instructions pour téléchargement et extraction des fichiers d'installation de StorageGRID . Remarque : vous n'avez pas besoin de télécharger de fichiers si vous ajoutez de nouveaux volumes de stockage à des nœuds de stockage existants ou si vous installez un nouveau dispositif StorageGRID .
Ordinateur portable de service	L'ordinateur portable de service dispose des éléments suivants : • Port réseau • Client SSH (par exemple, PuTTY) • "Navigateur Web pris en charge"
`Passwords.txt` déposer	Contient les mots de passe requis pour accéder aux nœuds de la grille sur la ligne de commande. Inclus dans le package de récupération.
Mot de passe d'approvisionnement	La phrase secrète est créée et documentée lors de la première installation du système StorageGRID . La phrase secrète de provisionnement n'est pas dans le <code>Passwords.txt</code> déposer.
Documentation de StorageGRID	• "Administrer StorageGRID" • "Notes de version" • Instructions d'installation pour votre plateforme ◦ "Installer StorageGRID sur Red Hat Enterprise Linux" ◦ "Installer StorageGRID sur Ubuntu ou Debian" ◦ "Installer StorageGRID sur VMware"
Documentation actuelle pour votre plateforme	Pour les versions prises en charge, voir le "Outil de matrice d'interopérabilité (IMT)" .

Téléchargez et extrayez les fichiers d'installation de StorageGRID

[[télécharger-et-extraire-les-fichiers-d'installation]]

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.

À propos de cette tâche

Vous devez effectuer des opérations d'extension à l'aide de la version de StorageGRID actuellement exécutée sur la grille.

Étapes

1. Aller à "[Téléchargements NetApp : StorageGRID](#)".
2. Sélectionnez la version de StorageGRID actuellement en cours d'exécution sur la grille.
3. Sign in avec le nom d'utilisateur et le mot de passe de votre compte NetApp .
4. Lisez le contrat de licence utilisateur final, cochez la case, puis sélectionnez **Accepter et continuer**.
5. Dans la colonne **Installer StorageGRID** de la page de téléchargement, sélectionnez l'option `.tgz` ou `.zip` fichier pour votre plateforme.

La version affichée dans le fichier d'archive d'installation doit correspondre à la version du logiciel actuellement installée.

Utilisez le `.zip` fichier si vous exécutez Windows sur l'ordinateur portable de service.

Plate-forme	Archives d'installation
Red Hat Enterprise Linux	StorageGRID-Webscale- <i>version</i> -RPM- <i>uniqueID</i> .zip StorageGRID-Webscale- <i>version</i> -RPM- <i>uniqueID</i> .tgz
Ubuntu ou Debian ou Appliances	StorageGRID-Webscale- <i>version</i> -DEB- <i>uniqueID</i> .zip StorageGRID-Webscale- <i>version</i> -DEB- <i>uniqueID</i> .tgz
VMware	StorageGRID-Webscale- <i>version</i> -VMware- <i>uniqueID</i> .zip StorageGRID-Webscale- <i>version</i> -VMware- <i>uniqueID</i> .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 l'étape appropriée à votre plateforme pour choisir les fichiers dont vous avez besoin, en fonction de votre plateforme, de la topologie de grille prévue 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, sélectionnez les fichiers appropriés.

Chemin et nom du fichier	Description
	Un fichier texte qui décrit tous les fichiers contenus dans le fichier de téléchargement StorageGRID .
	Une licence gratuite qui ne fournit aucun droit d'assistance pour le produit.
	Package RPM pour l'installation des images de nœuds StorageGRID sur vos hôtes RHEL.

Chemin et nom du fichier	Description
	Package RPM pour l'installation du service hôte StorageGRID sur vos hôtes RHEL.
Outil de script de déploiement	Description
	Un script Python utilisé pour automatiser la configuration d'un système StorageGRID .
	Un script Python utilisé pour automatiser la configuration des appliances StorageGRID .
	Un exemple de fichier de configuration à utiliser avec le <code>configure-storagegrid.py</code> scénario.
	Un 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 l'intégration de Ping Federate.
	Un fichier de configuration vierge à utiliser avec le <code>configure-storagegrid.py</code> scénario.
	Exemple de rôle Ansible et de playbook pour la configuration des hôtes RHEL pour le déploiement du conteneur StorageGRID . Vous pouvez personnaliser le rôle ou le manuel selon vos besoins.
	Un exemple de script Python que vous pouvez utiliser pour vous connecter à l'API Grid Management lorsque l'authentification unique (SSO) est activée à l'aide d'Active Directory ou de Ping Federate.
	Un script d'aide appelé par le compagnon <code>storagegrid-ssoauth-azure.py</code> Script Python pour effectuer des interactions SSO avec Azure.
	Schémas d'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 hors production pour les tests de compatibilité de mise à niveau.

1. Si vous étendez un système Ubuntu ou Debian, sélectionnez les fichiers appropriés.

Chemin et nom du fichier	Description
	Un fichier texte qui décrit tous les fichiers contenus dans le fichier de téléchargement StorageGRID .
	Un fichier de licence NetApp non destiné à la production que vous pouvez utiliser pour les tests et les déploiements de preuve de concept.
	Paquet DEB pour l'installation des images de nœuds StorageGRID sur les 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 les hôtes Ubuntu ou Debian.
Outil de script de déploiement	Description
	Un script Python utilisé pour automatiser la configuration d'un système StorageGRID .
	Un script Python utilisé pour automatiser la configuration des appliances StorageGRID .
	Un 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 l'intégration de Ping Federate.
	Un exemple de fichier de configuration à utiliser avec le <code>configure-storagegrid.py</code> scénario.
	Un fichier de configuration vierge à utiliser avec le <code>configure-storagegrid.py</code> scénario.
	Exemple de rôle Ansible et de playbook pour la configuration des hôtes Ubuntu ou Debian pour le déploiement du conteneur StorageGRID . Vous pouvez personnaliser le rôle ou le manuel selon vos besoins.

Chemin et nom du fichier	Description
	Un exemple de script Python que vous pouvez utiliser pour vous connecter à l'API Grid Management lorsque l'authentification unique (SSO) est activée à l'aide d'Active Directory ou de Ping Federate.
	Un script d'aide appelé par le compagnon <code>storagegrid-ssoauth-azure.py</code> Script Python pour effectuer des interactions SSO avec Azure.
	Schémas d'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 hors production pour les tests de compatibilité de mise à niveau.

1. Si vous étendez un système VMware, sélectionnez les fichiers appropriés.

Chemin et nom du fichier	Description
	Un fichier texte qui décrit tous les fichiers contenus dans le fichier de téléchargement StorageGRID .
	Une licence gratuite qui ne fournit aucun droit d'assistance pour le produit.
	Le fichier de disque de machine virtuelle utilisé comme modèle pour la création de machines virtuelles de nœuds de grille.
	Le fichier modèle Open Virtualization Format(.ovf) et fichier manifeste(.mf) pour déployer le nœud d'administration principal.
	Le fichier modèle(.ovf) et fichier manifeste(.mf) pour déployer des nœuds d'administration non principaux.
	Le fichier modèle(.ovf) et fichier manifeste(.mf) pour le déploiement de nœuds de passerelle.

Chemin et nom du fichier	Description
	Le fichier modèle(.ovf) et fichier manifeste(.mf) pour déployer des nœuds de stockage basés sur des machines virtuelles.
Outil de script de déploiement	Description
	Un script shell Bash utilisé pour automatiser le déploiement de nœuds de grille virtuels.
	Un exemple de fichier de configuration à utiliser avec le <code>deploy-vsphere-ovftool.sh</code> scénario.
	Un script Python utilisé pour automatiser la configuration d'un système StorageGRID .
	Un script Python utilisé pour automatiser la configuration des appliances StorageGRID .
	Un exemple de script Python que vous pouvez utiliser pour vous connecter à l'API Grid Management lorsque l'authentification unique (SSO) est activée. Vous pouvez également utiliser ce script pour l'intégration de Ping Federate.
	Un exemple de fichier de configuration à utiliser avec le <code>configure-storagegrid.py</code> scénario.
	Un fichier de configuration vierge à utiliser avec le <code>configure-storagegrid.py</code> scénario.
	Un exemple de script Python que vous pouvez utiliser pour vous connecter à l'API Grid Management lorsque l'authentification unique (SSO) est activée à l'aide d'Active Directory ou de Ping Federate.
	Un script d'aide appelé par le compagnon <code>storagegrid-ssoauth-azure.py</code> Script Python pour effectuer des interactions SSO avec Azure.

Chemin et nom du fichier	Description
	Schémas d'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 hors production pour les tests de compatibilité de mise à niveau.

1. Si vous étendez un système basé sur une appliance StorageGRID , sélectionnez les fichiers appropriés.

Chemin et nom du fichier	Description
	Package DEB pour l'installation des images de nœuds StorageGRID sur vos appliances.
	Somme de contrôle MD5 pour le fichier <code>/debs/storagegridwebscale-images-version-SHA.deb</code> .



Pour l'installation de l'appareil, ces fichiers ne sont nécessaires que si vous devez éviter le trafic réseau. L'appareil peut télécharger les fichiers requis à partir du nœud d'administration principal.

Vérifier le matériel et le réseau

Avant de commencer l'extension de votre système StorageGRID , assurez-vous des points suivants :

- Le matériel nécessaire pour prendre en charge les nouveaux nœuds de réseau 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 (une exigence pour le réseau Grid). En particulier, vérifiez 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 des nœuds de réseau](#)".

- 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 de grille sur un sous-réseau non utilisé auparavant, vous avez déjà "[ajouté le nouveau sous-réseau](#)" à la liste des sous-réseaux du réseau Grid. 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 Grid 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 grille sur chaque site. L'utilisation de NAT pour relier le réseau Grid à 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 grille et au réseau de grille. Si nécessaire, vous pouvez utiliser NAT entre les clients externes et les nœuds de grille, par exemple pour fournir une adresse IP publique pour un nœud de passerelle.

Ajouter des volumes de stockage

Ajouter des volumes de stockage aux nœuds de stockage

Vous pouvez étendre la capacité de stockage des nœuds de stockage qui sont inférieurs au nombre maximal de volumes pris en charge. Vous devrez peut-être ajouter des volumes de stockage à plusieurs nœuds de stockage pour satisfaire aux exigences ILM pour les copies répliquées ou codées par effacement.

Avant de commencer

Avant d'ajouter des volumes de stockage, consultez les ["directives pour l'ajout de capacité d'objet"](#) pour vous assurer de savoir où ajouter des volumes pour répondre aux exigences de votre politique ILM.



Ces instructions s'appliquent uniquement aux nœuds de stockage basés sur des logiciels. Voir ["Ajouter une étagère d'extension au SG6060 déployé"](#) ou ["Ajouter une étagère d'extension au SG6160 déployé"](#) pour savoir comment ajouter des volumes de stockage au SG6060 ou au SG6160 en installant des étagères d'extension. Les autres nœuds de stockage d'appareils ne peuvent pas être étendus.

À propos de cette 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 qui sont formatés par le système StorageGRID et montés pour stocker des objets. Chaque nœud de stockage peut prendre en charge jusqu'à 48 volumes de stockage, appelés *magasins d'objets* 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 au `/var/local/rangedb/0` point de montage.

Avant d'ajouter de nouveaux volumes de stockage, utilisez le gestionnaire de grille 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 d'appliance, le nom mondial de chaque disque correspond à l'identifiant mondial du volume (WWID) qui apparaît lorsque vous affichez les propriétés de volume standard 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 sur disque liées aux points de montage de volume, la première partie du nom affichée dans la colonne **Nom** du tableau Périphériques de disque (c'est-à-dire *sd*, *sd*, *sd*, etc.) correspond à la valeur affichée dans la colonne **Périphérique** du tableau 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 de votre plateforme pour ajouter de nouveaux volumes de stockage au nœud de stockage.
 - ["VMware : ajouter des volumes de stockage au nœud de stockage"](#)
 - ["Linux : ajouter des volumes à connexion directe ou SAN au nœud de stockage"](#)

VMware : ajouter 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 VMware.
 - ["Installer StorageGRID sur VMware"](#)
- Vous avez le `Passwords.txt` déposer.
- Tu as ["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 récupération ou une autre procédure d'extension est active.

À propos de cette tâche

Le nœud de stockage n'est pas disponible pendant une brève période lorsque vous ajoutez des volumes de stockage. Vous devez effectuer cette procédure sur un nœud de stockage à la fois pour éviter d'impacter les services de grille orientés client.

Étapes

1. Si nécessaire, installez un nouveau matériel de stockage et créez de nouvelles banques de données VMware.
2. Ajoutez un ou plusieurs disques durs à la machine virtuelle pour les 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 comme des disques de machine virtuelle (VMDK). Les VMDK sont plus couramment utilisés et plus faciles à gérer, tandis que les RDM peuvent offrir de meilleures performances pour les charges de travail qui utilisent des tailles d'objet plus grandes (par exemple, supérieures à 100 Mo). Pour plus d'informations sur l'ajout de disques durs aux machines virtuelles, consultez la documentation VMware vSphere.

3. Redémarrez la machine virtuelle en utilisant l'option **Redémarrer le système d'exploitation invité** dans le client VMware vSphere ou en entrant la commande suivante dans une session SSH sur la machine virtuelle :`sudo reboot`



N'utilisez pas **Power Off** ou **Reset** pour redémarrer la machine virtuelle.

4. Configurer le nouveau stockage à utiliser par le nœud de stockage :

a. Connectez-vous au nœud de grille :

- i. Entrez la commande suivante : `ssh admin@grid_node_IP`
- ii. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.
- iii. Entrez la commande suivante pour passer en root : `su -`
- iv. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer. 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 recherche tous les nouveaux volumes de stockage et vous invite à les formater.

c. Entrez **y** pour accepter le formatage.

d. Si l'un des volumes a déjà été formaté, décidez si vous souhaitez le reformater.

- Entrez **y** pour reformater.
- Entrez **n** pour ignorer le reformatage.

Le `setup_rangedbs.sh` le script s'exécute automatiquement.

5. Vérifiez que les services démarrent correctement :

a. Afficher une liste de l'état de tous les services sur le serveur :

```
sudo storagegrid-status
```

Le statut 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. Sign in au Grid Manager à l'aide d'un ["navigateur Web pris en charge"](#).
- b. Sélectionnez **SUPPORT > Outils > Topologie de grille**.
- c. Sélectionnez **site > Nœud de stockage > LDR > Stockage**.
- d. Sélectionnez l'onglet **Configuration** puis l'onglet **Principal**.
- 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 voir les nouveaux magasins d'objets :

- a. Sélectionnez **NODES > site > Storage Node > Storage**.
- b. Consultez les détails dans le tableau **Magasins d'objets**.

Résultat

Vous pouvez utiliser la capacité étendue des nœuds de stockage pour enregistrer les données des objets.

Linux : ajouter des volumes à connexion directe ou SAN au nœud de stockage

Si un nœud de stockage comprend moins de 48 volumes de stockage, vous pouvez augmenter sa capacité en ajoutant de nouveaux périphériques de stockage en blocs, en les rendant visibles pour les hôtes Linux et en ajoutant les nouveaux mappages de périphériques en blocs 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 plateforme Linux.
 - ["Installer StorageGRID sur Red Hat Enterprise Linux"](#)
 - ["Installer StorageGRID sur Ubuntu ou Debian"](#)
- Vous avez le `Passwords.txt` déposer.
- Tu as ["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 récupération ou une autre procédure d'extension est active.

À propos de cette tâche

Le nœud de stockage n'est pas disponible pendant une brève période lorsque vous ajoutez des volumes de stockage. Vous devez effectuer cette procédure sur un nœud de stockage à la fois pour éviter d'impacter les services de grille orientés client.

Étapes

1. Installez le nouveau matériel de stockage.

Pour plus d'informations, consultez la documentation fournie par votre fournisseur de matériel.

2. Créez de nouveaux volumes de stockage de blocs des tailles souhaitées.
 - Connectez les nouveaux disques et mettez à jour la configuration du contrôleur RAID selon les besoins, ou allouez les nouveaux 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, consultez les 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 que root ou avec un compte disposant de l'autorisation sudo.
4. Confirmez que les nouveaux volumes de stockage sont visibles sur l'hôte Linux.

Vous devrez peut-être effectuer une nouvelle analyse des appareils.

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 du nœud de stockage, qui se trouve à l'adresse `/etc/storagegrid/nodes/<node-name>.conf`.
7. Recherchez la section du fichier de configuration du nœud qui contient les mappages de périphériques de stockage en mode bloc d'objets existants.

Dans l'exemple, `BLOCK_DEVICE_RANGEDB_00` à `BLOCK_DEVICE_RANGEDB_03` sont les mappages de périphériques de stockage d'objets 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 stockage en bloc d'objets correspondant aux volumes de stockage en bloc que vous avez ajoutés pour ce nœud de stockage.

Assurez-vous de commencer à la prochaine `BLOCK_DEVICE_RANGEDB_nn`. Ne laissez pas d'espace.

- Sur la base de l'exemple ci-dessus, commencez par `BLOCK_DEVICE_RANGEDB_04`.
- Dans l'exemple ci-dessous, quatre nouveaux volumes de stockage de blocs 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 vos modifications apportées au fichier de configuration du nœud pour le nœud de stockage :

```
sudo storagegrid node validate <node-name>
```

Corrigez les erreurs ou les avertissements avant de passer à l'étape suivante.

Si vous observez une erreur similaire à la suivante, cela signifie que le fichier de configuration du nœud tente de mapper le périphérique de bloc utilisé par <node-name> pour <PURPOSE> au donné <path-name> dans le système de fichiers Linux, mais il n'y a 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 entré 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 répertorié dans le `Passwords.txt` déposer.
12. Vérifiez que les services démarrent correctement :
 - a. Afficher une liste de l'état de tous les services sur le serveur :

```
sudo storagegrid-status
```

Le statut 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. Configurer le nouveau stockage à utiliser par le nœud de stockage :

- a. Configurer les nouveaux volumes de stockage :

```
sudo add_rangedbs.rb
```

Ce script recherche 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 le reformater.
 - Entrez **y** pour reformater.
 - Entrez **n** pour ignorer le reformatage.

Le `setup_rangedbs.sh` le script s'exécute automatiquement.

14. Vérifiez que l'état de stockage du nœud de stockage est en ligne :

- a. Sign in au Grid Manager à l'aide d'un ["navigateur Web pris en charge"](#).
- b. Sélectionnez **SUPPORT > Outils > Topologie de grille**.
- c. Sélectionnez **site > Nœud de stockage > LDR > Stockage**.
- d. Sélectionnez l'onglet **Configuration** puis l'onglet **Principal**.
- 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 voir les nouveaux magasins d'objets :

- a. Sélectionnez **NODES > site > Storage Node > Storage**.
- b. Consultez les détails dans le tableau **Magasins d'objets**.

Résultat

Vous pouvez désormais utiliser la capacité étendue des nœuds de stockage pour enregistrer les données des objets.

Ajouter des nœuds de grille ou un site

Ajouter des nœuds de grille à un site existant ou ajouter un nouveau site

Suivez cette procédure pour ajouter des nœuds de grille à des sites existants ou pour ajouter un nouveau site. Vous ne pouvez effectuer qu'un seul type d'extension à la fois.

Avant de commencer

- Vous avez le ["Accès root ou autorisation de maintenance"](#) .
- Tous les nœuds existants dans la grille sont opérationnels sur tous les sites.
- Toutes les procédures d'extension, de mise à niveau, de mise hors service ou de récupération précédentes sont terminées.



Vous ne pouvez pas démarrer une extension lorsqu'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 suspendre une procédure de mise hors service pour démarrer une extension.

Étapes

1. ["Mettre à jour les sous-réseaux pour Grid Network"](#) .
2. ["Déployer de nouveaux nœuds de grille"](#) .
3. ["Effectuer une expansion"](#) .

Mettre à jour les sous-réseaux pour Grid Network

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 de grille.

StorageGRID conserve une liste des sous-réseaux réseau utilisés pour communiquer entre les nœuds de grille sur le réseau de grille (eth0). Ces entrées incluent les sous-réseaux utilisés pour le réseau Grid par chaque site de votre système StorageGRID ainsi que tous les sous-réseaux utilisés pour NTP, DNS, LDAP ou d'autres serveurs externes accessibles via la passerelle du réseau Grid.

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 de maintenance ou root"](#) .
- Vous disposez de la phrase secrète de provisionnement.
- Vous disposez des adresses réseau, en notation CIDR, des sous-réseaux que vous souhaitez configurer.

À propos de cette tâche

Si l'un des nouveaux nœuds possède une adresse IP de réseau de grille sur un sous-réseau non utilisé auparavant, vous devez ajouter le nouveau sous-réseau à la liste des sous-réseaux du réseau de grille avant de démarrer l'extension. Sinon, vous devrez annuler l'extension, ajouter le nouveau sous-réseau et recommencer la procédure.

N'utilisez pas de sous-réseaux contenant les adresses IPv4 suivantes pour le réseau de grille, le réseau d'administration ou le réseau client d'un nœud :

- 192.168.130.101
- 192.168.131.101
- 192.168.130.102
- 192.168.131.102
- 198.51.100.2
- 198.51.100.4



Par exemple, n'utilisez pas les plages de sous-réseaux suivantes pour le réseau de grille, le réseau d'administration ou le réseau client d'un nœud :

- 192.168.130.0/24 car cette plage de sous-réseaux contient les adresses IP 192.168.130.101 et 192.168.130.102
- 192.168.131.0/24 car cette plage de sous-réseaux contient les adresses IP 192.168.131.101 et 192.168.131.102
- 198.51.100.0/24 car cette plage de sous-réseaux contient les adresses IP 198.51.100.2 et 198.51.100.4

Étapes

1. Sélectionnez **MAINTENANCE > Réseau > Réseau de grille**.
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 la phrase secrète de provisionnement et sélectionnez **Enregistrer**.
4. Attendez que les modifications soient appliquées, puis téléchargez un nouveau package de récupération.
 - a. Sélectionnez **MAINTENANCE > Système > Package de récupération**.
 - b. Saisissez la **phrase secrète de provisionnement**.



Le fichier du package de récupération doit être sécurisé car il contient des clés de chiffrement et des mots de passe qui peuvent être utilisés pour obtenir des données à partir du système StorageGRID. Il est également utilisé pour récupérer le nœud d'administration principal.

Les sous-réseaux que vous avez spécifiés sont configurés automatiquement pour votre système StorageGRID.

Déployer de nouveaux nœuds de grille

Les étapes de déploiement de nouveaux nœuds de grille dans une extension sont les mêmes que celles utilisées lors de la première installation de la grille. Vous devez déployer tous les nouveaux nœuds de grille avant de pouvoir effectuer l'extension.

Lorsque vous développez une grille, les nœuds que vous ajoutez ne doivent pas nécessairement 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 : déployer des nœuds de grille

Vous devez déployer une machine virtuelle dans VMware vSphere pour chaque nœud VMware que vous souhaitez ajouter dans l'extension.

Étapes

1. ["Déployer le nouveau nœud en tant que machine virtuelle"](#) et le connecter à un ou plusieurs réseaux StorageGRID .

Lorsque vous déployez le nœud, vous pouvez éventuellement remapper les ports du nœud ou augmenter les paramètres du processeur ou de la mémoire.

2. Après avoir déployé tous les nouveaux nœuds VMware, ["effectuer la procédure d'expansion"](#) .

Linux : déployer des nœuds de grille

Vous pouvez déployer des nœuds de grille 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 de CPU, de RAM et de stockage des nœuds StorageGRID que vous souhaitez ajouter à votre grille, vous les préparez de la même manière que vous avez préparé les hôtes lors de leur première installation. Ensuite, vous déployez les nœuds d'extension de la même manière que vous avez déployé les nœuds de grille lors de l'installation.

Avant de commencer

- Vous disposez des instructions pour installer StorageGRID pour votre version de Linux et vous avez examiné les exigences matérielles et de stockage.
 - ["Installer StorageGRID sur Red Hat Enterprise Linux"](#)
 - ["Installer StorageGRID sur Ubuntu ou Debian"](#)
- Si vous prévoyez de déployer de nouveaux nœuds de grille sur des hôtes existants, vous avez confirmé que les hôtes existants disposent de suffisamment de CPU, de RAM et de capacité de stockage pour les nœuds supplémentaires.
- Vous avez un plan pour minimiser les domaines de défaillance. Par exemple, vous ne devez pas déployer tous les nœuds de passerelle sur un seul hôte physique.



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 attribué à partir d'un système NetApp ONTAP , vérifiez que le volume n'a pas de stratégie de hiérarchisation FabricPool activée. La désactivation de la hiérarchisation FabricPool pour les volumes utilisés avec les nœuds StorageGRID simplifie le dépannage et les opérations de stockage.

Étapes

1. Si vous ajoutez de nouveaux hôtes, accédez aux instructions d'installation pour déployer les nœuds StorageGRID .
2. Pour déployer les nouveaux hôtes, suivez les instructions de préparation des hôtes.
3. Pour créer des fichiers de configuration de nœud et valider la configuration StorageGRID , suivez les instructions de déploiement des nœuds de grille.

4. Si vous ajoutez des nœuds à un nouvel hôte Linux, démarrez le service 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>]`

Après avoir terminé

Après avoir déployé tous les nouveaux nœuds de grille, vous pouvez ["effectuer l'expansion"](#) .

Appareils : déploiement de stockage, de passerelle ou de nœuds d'administration non principaux

Pour installer le logiciel StorageGRID sur un nœud d'appliance, utilisez le programme d'installation de l'appliance StorageGRID , inclus sur l'appliance. Dans une extension, chaque appliance de stockage fonctionne comme un nœud de stockage unique et chaque appliance de services fonctionne comme un nœud de passerelle unique ou un nœud d'administration non principal. Tout appareil peut se connecter au réseau Grid, au réseau administrateur et au réseau client.

Avant de commencer

- L'appareil a été installé dans un rack ou une armoire, connecté à vos réseaux et sous tension.
- Vous avez terminé le ["Configurer le matériel"](#) mesures.

La configuration du matériel de l'appliance comprend les étapes requises pour la configuration des connexions StorageGRID (liaisons réseau et adresses IP) ainsi que les étapes facultatives pour l'activation du chiffrement des nœuds, la modification du mode RAID et le remappage des ports réseau.

- Tous les sous-réseaux du réseau de grille répertoriés sur la page de configuration IP du programme d'installation de l'appliance StorageGRID ont été définis dans la liste des sous-réseaux du réseau de grille sur le nœud d'administration principal.
- Le micrologiciel 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 réseau. Si les versions ne sont pas compatibles, vous devez mettre à niveau le micrologiciel du programme d'installation de l'appliance StorageGRID .
- Vous disposez d'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'appareil. Vous pouvez utiliser l'adresse IP de n'importe quel réseau StorageGRID connecté.

À propos de cette tâche

Le processus d'installation de StorageGRID sur un nœud d'appliance comporte les phases suivantes :

- Vous spécifiez ou confirmez l'adresse IP du nœud d'administration principal et le nom du nœud de l'appliance.
- Vous démarrez l'installation et attendez que les volumes soient configurés et que le logiciel soit installé.

À mi-chemin des tâches d'installation de l'appareil, l'installation s'interrompt. Pour reprendre l'installation, connectez-vous au Grid Manager, approuvez tous les nœuds de 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 en utilisant le `configure-sga.py` Script d'installation de l'appareil.

Étapes

1. Ouvrez un navigateur et entrez l'une des adresses IP du contrôleur de calcul de l'appareil.

`https://Controller_IP:8443`

La page d'accueil du programme d'installation de l'appliance StorageGRID s'affiche.

2. Dans la section de connexion **Nœud d'administration principal**, déterminez si vous devez spécifier l'adresse IP du nœud 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, est présent sur le même sous-réseau.

3. Si cette adresse IP n'est pas affichée ou si vous devez la modifier, spécifiez l'adresse :

Option	Description
Saisie IP manuelle	a. Décochez la case Activer la découverte du nœud d'administration. b. Saisissez l'adresse IP manuellement. c. Cliquez sur Enregistrer. d. Attendez que l'état de connexion pour que la nouvelle adresse IP soit prête.
Découverte automatique de tous les nœuds d'administration principaux connectés	a. Cochez la case Activer la découverte du nœud d'administration. b. Attendez que la liste des adresses IP découvertes s'affiche. c. Sélectionnez le nœud d'administration principal pour la grille sur laquelle ce nœud de stockage d'appliance sera déployé. d. Cliquez sur Enregistrer. e. Attendez que l'état de connexion pour que la nouvelle adresse IP soit prête.

4. Dans le champ **Nom du nœud**, saisissez le nom que vous souhaitez utiliser pour ce nœud d'appliance et sélectionnez **Enregistrer**.

Le nom du nœud est attribué à ce nœud d'appliance dans le système StorageGRID . Il est affiché sur la page Nœuds (onglet Aperçu) dans le Gestionnaire de grille. Si nécessaire, vous pouvez modifier le nom lorsque vous approuvez le nœud.

5. Dans la section **Installation**, confirmez que l'état actuel est « Prêt à démarrer l'installation de *nom du nœud* dans la grille avec le nœud d'administration principal *admin_ip* » et que le bouton **Démarrer l'installation** est activé.

Si le bouton **Démarrer l'installation** n'est pas activé, vous devrez peut-être modifier la configuration réseau ou les paramètres du port. Pour les instructions, consultez les instructions d'entretien de votre appareil.

6. Depuis la page d'accueil du programme d'installation de l'appliance StorageGRID , sélectionnez **Démarrer**

l'installation.

NetApp® StorageGRID® Appliance Installer

Home

Configure Networking ▾

Configure Hardware ▾

Monitor Installation

Advanced ▾

Home

The installation is ready to be started. Review the settings below, and then click Start Installation.

Primary Admin Node connection

Enable Admin Node discovery

☐

Primary Admin Node IP

172.16.4.210

Connection state

Connection to 172.16.4.210 ready

Cancel

Save

Node name

Node name

NetApp-SGA

Cancel

Save

Installation

Current state

Ready to start installation of NetApp-SGA into grid with Admin Node 172.16.4.210.

Start Installation

L'état actuel passe à « L'installation est en cours » et la page Installation du moniteur s'affiche.

- Si votre extension comprend 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`.

- Si vous devez accéder manuellement à la page d'installation du moniteur, sélectionnez **Installation du moniteur** dans la barre de menus.

La page d'installation du moniteur affiche la progression de l'installation.

Monitor Installation

1. Configure storage			Running
Step	Progress	Status	
Connect to storage controller		Complete	
Clear existing configuration		Complete	
Configure volumes		Creating volume StorageGRID-obj-00	
Configure host settings		Pending	

2. Install OS	Pending
3. Install StorageGRID	Pending
4. Finalize installation	Pending

La barre d'état bleue indique quelle tâche est actuellement en cours. Les barres d'état vertes indiquent les tâches qui ont été effectuées avec succès.



Le programme d'installation garantit que les tâches effectuées lors d'une installation précédente ne sont pas réexécutées. Si vous réexécutez une installation, toutes les tâches qui n'ont pas besoin d'être réexécutées sont affichées avec une barre d'état verte et un statut « Ignoré ».

9. Passez en revue la progression des deux premières étapes de l'installation.

1. Configurer l'appareil

Au cours de cette étape, l'un des processus suivants se produit :

- Pour un dispositif 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 un dispositif de services, le programme d'installation efface toute configuration existante des lecteurs du contrôleur de calcul et configure les paramètres de l'hôte.

2. Installer le système d'exploitation

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 apparaisse dans la fenêtre de la console, vous invitant à utiliser le gestionnaire de grille pour approuver le nœud.



Attendez que tous les nœuds que vous avez ajoutés dans cette extension soient prêts à être approuvés avant d'accéder au gestionnaire de grille pour approuver les nœuds.

Monitor Installation

1. Configure storage	Complete
2. Install OS	Complete
3. Install StorageGRID	Running
4. Finalize installation	Pending

Connected (unencrypted) to: QEMU

```

/platform.type: Device or resource busy
[2017-07-31T22:09:12.362566] INFO -- [INSG] NOTICE: seeding /var/local with c
ontainer data
[2017-07-31T22:09:12.366205] INFO -- [INSG] Fixing permissions
[2017-07-31T22:09:12.369633] INFO -- [INSG] Enabling syslog
[2017-07-31T22:09:12.511533] INFO -- [INSG] Stopping system logging: syslog-n
g.
[2017-07-31T22:09:12.570096] INFO -- [INSG] Starting system logging: syslog-n
g.
[2017-07-31T22:09:12.576360] INFO -- [INSG] Beginning negotiation for downloa
d of node configuration
[2017-07-31T22:09:12.581363] INFO -- [INSG]
[2017-07-31T22:09:12.585066] INFO -- [INSG]
[2017-07-31T22:09:12.588314] INFO -- [INSG]
[2017-07-31T22:09:12.591851] INFO -- [INSG]
[2017-07-31T22:09:12.594886] INFO -- [INSG]
[2017-07-31T22:09:12.598360] INFO -- [INSG]
[2017-07-31T22:09:12.601324] INFO -- [INSG]
[2017-07-31T22:09:12.604759] INFO -- [INSG]
[2017-07-31T22:09:12.607800] INFO -- [INSG]
[2017-07-31T22:09:12.610985] INFO -- [INSG]
[2017-07-31T22:09:12.614597] INFO -- [INSG]
[2017-07-31T22:09:12.618282] INFO -- [INSG] Please approve this node on the A
dmin Node GMI to proceed...

```

Effectuer une expansion

Lorsque vous effectuez l'extension, les nouveaux nœuds de grille 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 disposez de la phrase secrète de provisionnement.
- Vous avez déployé tous les nœuds de grille qui sont ajoutés dans cette extension.
- Vous avez le ["Autorisation d'accès de maintenance ou root"](#).

- Si vous ajoutez des nœuds de stockage, vous avez confirmé que toutes les opérations de réparation de données effectuées dans le cadre d'une récupération sont terminées. Voir "[Vérifier les tâches de réparation de données](#)".
- Si vous ajoutez des nœuds de stockage et que vous souhaitez attribuer un niveau de stockage personnalisé à ces nœuds, vous avez déjà "[créé le niveau de stockage personnalisé](#)". Vous disposez également soit de l'autorisation d'accès root, soit 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'objets ne sont pas stockées sur le nouveau site avant la fin de l'extension. Par exemple, si une règle utilise le pool de stockage par défaut (**Tous les nœuds de stockage**), vous devez "[créer un nouveau pool de stockage](#)" qui contient uniquement les nœuds de stockage existants et "[mettre à jour les règles ILM](#)" et la politique ILM d'utiliser ce nouveau pool de stockage. Sinon, les objets seront copiés sur le nouveau site dès que le premier nœud de ce site deviendra actif.

À propos de cette tâche

L'exécution de l'extension comprend les principales tâches utilisateur suivantes :

1. Configurer l'extension.
2. Démarrer l'extension.
3. Téléchargez un nouveau fichier de package de récupération.
4. Surveillez les étapes et les phases d'extension jusqu'à ce que tous les nouveaux nœuds soient installés et configurés et que tous les services aient démarré.



Certaines étapes et phases d'extension peuvent prendre beaucoup de temps à exécuter sur une grande grille. Par exemple, la diffusion de Cassandra vers un nouveau nœud de stockage peut ne prendre que quelques minutes si la base de données Cassandra est vide. Cependant, si la base de données Cassandra inclut une grande quantité 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 diffusion de données ».

Étapes

1. Sélectionnez **MAINTENANCE > Tâches > Extension**.

La page Extension de la grille apparaît. La section Nœuds en attente répertorie les nœuds prêts à être ajoutés.

Grid Expansion

Approve and configure grid nodes, so that they are added correctly to your StorageGRID system.

Configure Expansion

Pending Nodes

Grid nodes are listed as pending until they are assigned to a site, configured, and approved.

+ Approve

✕ Remove

	Grid Network MAC Address	Name	Type	Platform	Grid Network IPv4 Address
☐	00:50:56:a7:7a:c0	rleo-010-096-106-151	Storage Node	VMware VM	10.96.106.151/22
☐	00:50:56:a7:0f:2e	rleo-010-096-106-156	API Gateway Node	VMware VM	10.96.106.156/22

2. Sélectionnez **Configurer l'extension**.

La boîte de dialogue Sélection du site s'affiche.

3. Sélectionnez le type d'extension que vous démarrez :

- Si vous ajoutez un nouveau site, sélectionnez **Nouveau** et saisissez 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 des **nœuds en attente** et confirmez qu'elle affiche tous les nœuds de grille que vous avez déployés.

Si nécessaire, vous pouvez positionner votre curseur sur l'**Adresse MAC du réseau de grille** d'un nœud pour voir les détails de ce nœud.

Pending Nodes

Grid nodes are listed as

+

 Approve

×

 Remove

Grid Network MAC Address

☐ 00:50:56:a7:7a:c0
 ☐ 00:50:56:a7:0f:2e

Approved Nodes

leo-010-096-106-151

Storage Node

Network

Grid Network	10.96.106.151/22	10.96.104.1
Admin Network	Name	Type
Client Network		

Hardware

VMware VM
 4 CPUs
 8 GB RAM

Disks

55 GB
 55 GB
 55 GB



Si un nœud est manquant, confirmez 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.

- Sélectionnez le bouton radio à côté du premier nœud de grille en attente que vous souhaitez approuver.
- Sélectionnez **Approuver**.

Le formulaire de configuration du nœud de grille apparaît.

- Si nécessaire, modifiez les paramètres généraux :

Champ	Description
Site	Le nom du site auquel le nœud de grille sera associé. Si vous ajoutez plusieurs nœuds, assurez-vous de sélectionner le site approprié pour chaque nœud. Si vous ajoutez un nouveau site, tous les nœuds sont ajoutés au nouveau site.
Nom	Le nom du système pour le nœud. Les noms de système sont requis pour les opérations StorageGRID internes et ne peuvent pas être modifiés.
Type de stockage (nœuds de stockage uniquement)	• Données et métadonnées (« combinées ») : nœud de stockage de données et de métadonnées d'objet • Données uniquement : nœud de stockage contenant uniquement des données d'objet (pas de métadonnées) • Métadonnées uniquement : nœud de stockage contenant uniquement des métadonnées (aucune donnée d'objet)

Champ	Description
Rôle NTP	Le rôle du protocole 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 dotés d'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 Client NTP au nœud.
Service ADC (nœuds de stockage combinés ou de métadonnées uniquement)	Si ce nœud de stockage exécutera le service de contrôleur de domaine administratif (ADC). Le service ADC suit l'emplacement et la disponibilité des services du réseau. Au moins trois nœuds de stockage sur 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. Étant donné que vous ne pouvez pas mettre hors service un nœud de stockage s'il reste trop peu de services ADC, 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. En savoir plus sur le "Quorum du CDA" .
Niveau de stockage (nœuds de stockage combinés ou de données uniquement)	Utilisez le niveau de stockage Par défaut ou sélectionnez le niveau de stockage personnalisé que vous souhaitez attribuer à ce nouveau nœud. Les niveaux de stockage sont utilisés par les pools de stockage ILM, votre sélection peut donc affecter les objets qui seront placés sur le nœud de stockage.

d. Si nécessaire, modifiez les paramètres du réseau de grille, du réseau d'administration et du réseau client.

- **Adresse IPv4 (CIDR)** : l'adresse réseau CIDR pour l'interface réseau. Par exemple : 172.16.10.100/24



Si vous découvrez que des nœuds ont des adresses IP en double sur le réseau Grid pendant que vous approuvez des nœuds, vous devez annuler l'extension, redéployer les machines virtuelles ou les appliances avec une adresse IP non dupliquée et redémarrer l'extension.

- **Passerelle** : la passerelle par défaut du nœud de grille. Par exemple : 172.16.10.1
- **Sous-réseaux (CIDR)** : un ou plusieurs sous-réseaux pour le réseau d'administration.

e. Sélectionnez **Enregistrer**.

Le nœud de grille approuvé est déplacé vers la liste des 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 des nœuds en attente, sélectionnez son bouton radio, puis sélectionnez **Réinitialiser**.
- Pour supprimer définitivement un nœud de réseau 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 que vous souhaitez approuver.



Si possible, vous devez approuver toutes les notes de grille en attente et effectuer une seule extension. Il faudra plus de temps si vous effectuez plusieurs petites extensions.

7. Lorsque vous avez approuvé tous les nœuds de la grille, saisissez la **Phrase secrète de provisionnement** et sélectionnez **Développer**.

Après 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 État du nœud de grille répertorie l'état actuel de chaque nœud de grille.



Au cours de l'étape « Installation des nœuds de grille » pour un nouvel appareil, le programme d'installation de l'appareil StorageGRID montre que l'installation passe de l'étape 3 à l'étape 4, Finaliser l'installation. Une fois l'étape 4 terminée, le contrôleur est redémarré.

Expansion Progress

Lists the status of grid configuration tasks required to change the grid topology. These grid configuration tasks are run automatically by the StorageGRID system.

1. Installing grid nodes

In Progress

Grid Node Status

Lists the installation and configuration status of each grid node included in the expansion.

Search



Name	Site	Grid Network IPv4 Address	Progress	Stage
rleo-010-096-106-151	Data Center 1	10.96.106.151/22		Waiting for Dynamic IP Service peers
rleo-010-096-106-156	Data Center 1	10.96.106.156/22		Waiting for NTP to synchronize

2. Initial configuration

Pending

3. Distributing the new grid node's certificates to the StorageGRID system.

Pending

4. Assigning Storage Nodes to storage grade

Pending

5. Starting services on the new grid nodes

Pending

6. Starting background process to clean up unused Cassandra keys

Pending



Une extension de site inclut une tâche supplémentaire pour configurer Cassandra pour le nouveau site.

- Dès que le lien **Télécharger le package de récupération** apparaît, téléchargez le fichier du package de récupération.

Vous devez télécharger une copie mise à jour du fichier de package de récupération dès que possible après avoir apporté des modifications à la topologie de grille du système StorageGRID . Le fichier Recovery Package vous permet de restaurer le système en cas de panne.

- Sélectionnez le lien de téléchargement.
- Saisissez la phrase secrète d'approvisionnement et sélectionnez **Démarrer le téléchargement**.
- Une fois le téléchargement terminé, ouvrez le .zip fichier et confirmez que vous pouvez accéder au contenu, y compris le `Passwords.txt` déposer.
- Copiez le fichier du package de récupération téléchargé(.zip) vers deux endroits sûrs, sécurisés et séparés.



Le fichier du package de récupération doit être sécurisé car il contient des clés de chiffrement et des mots de passe qui peuvent être utilisés pour obtenir des données à partir du système StorageGRID .

- Si vous ajoutez des nœuds de stockage à un site existant ou 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 diffusion de données ». Ces étapes peuvent prendre plusieurs heures pour chaque nouveau nœud de stockage, en particulier si les nœuds de stockage existants contiennent une grande quantité de métadonnées d'objet.

Ajout de nœuds de stockage

Si vous ajoutez des nœuds de stockage à un site existant, vérifiez le pourcentage affiché dans le message d'état « Démarrage de Cassandra et diffusion des données ».

5. Starting services on the new grid nodes

In Progress

Grid Node Status

Lists the installation and configuration status of each grid node included in the expansion.

⚠ Do not reboot any Storage Nodes during Step 4. The "Starting Cassandra and streaming data" stage might take hours, especially if existing Storage Nodes contain a large amount of object metadata.

Name	Site	Grid Network IPv4 Address	Progress	Stage
rleo-010-096-106-151	Data Center 1	10.96.106.151/22		Starting Cassandra and streaming data (20.4% streamed)
rleo-010-096-106-156	Data Center 1	10.96.106.156/22		Starting services

Ce pourcentage estime le degré d'achèvement de l'opération de streaming Cassandra, en fonction de la quantité totale de données Cassandra disponibles et de la quantité qui a déjà été écrite sur le nouveau nœud.

Ajout d'un site

Si vous ajoutez un nouveau site, utilisez `nodetool status` pour surveiller la progression du streaming Cassandra et voir combien de métadonnées ont été copiées sur le nouveau site pendant l'étape « Extension du cluster Cassandra ». La charge totale de données sur le nouveau site doit être d'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 **Configurer l'extension** réapparaisse.

Après avoir terminé

Selon les types de nœuds de grille que vous avez ajoutés, effectuez des étapes d'intégration et de configuration supplémentaires. Voir "[Étapes de configuration après l'extension](#)".

Configurer le système étendu

Étapes de configuration après l'extension

Une fois l'extension terminée, vous devez effectuer des étapes d'intégration et de configuration supplémentaires.

À propos de cette tâche

Vous devez effectuer les tâches de configuration répertoriées ci-dessous pour les nœuds de grille ou les sites que vous ajoutez dans votre extension. Certaines tâches peuvent être facultatives, en fonction des options sélectionnées lors de l'installation et de l'administration de votre système, et de la manière dont vous souhaitez configurer les nœuds et les sites ajoutés lors 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 sélectionné pour les nouveaux nœuds de stockage.
- Confirmer que la politique ILM répond aux nouvelles exigences. Si des changements de règles sont nécessaires, "[créer de nouvelles règles](#)" et "[mettre à jour la politique ILM](#)". Si les règles sont déjà correctes, "[activer une nouvelle politique](#)" sans aucune modification de règle pour garantir que StorageGRID utilise les nouveaux nœuds.
- Confirmez 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 se produiront si ce nœud tombe en panne. De plus, la désignation de deux nœuds par site comme sources NTP principales garantit une synchronisation précise si un site est isolé du reste du réseau.

2. Si vous avez ajouté un ou plusieurs nœuds de stockage à un site existant :

- "[Afficher les détails du pool de stockage](#)" pour confirmer que chaque nœud que vous avez ajouté est inclus dans les pools de stockage attendus et utilisé dans les règles ILM attendues.
- Confirmer que la politique ILM répond aux nouvelles exigences. Si des changements de règles sont nécessaires, "[créer de nouvelles règles](#)" et "[mettre à jour la politique ILM](#)". Si les règles sont déjà correctes, "[activer une nouvelle politique](#)" sans aucune modification de règle 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 codées par effacement. Voir "[Rééquilibrer les données codées par effacement après l'ajout de nœuds de stockage](#)".

3. Si vous avez ajouté un nœud de passerelle :

- Si des groupes de haute disponibilité (HA) sont utilisés pour les connexions client, ajoutez éventuellement le nœud de passerelle à un groupe HA. Sélectionnez **CONFIGURATION > Réseau > Groupes de haute disponibilité** pour consulter la liste des groupes HA existants et ajouter le nouveau nœud. Voir "[Configurer des groupes de haute disponibilité](#)".

4. Si vous avez ajouté un nœud d'administration :

- a. Si l'authentification unique (SSO) est activée pour votre système StorageGRID, créez une approbation de partie de confiance pour le nouveau nœud d'administration. Vous ne pouvez pas vous connecter au nœud tant que vous n'avez pas créé cette approbation de partie de confiance. 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 HA. Sélectionnez **CONFIGURATION > Réseau > Groupes de haute disponibilité** pour consulter la liste des groupes HA existants et ajouter le nouveau nœud. Voir "[Configurer des groupes de haute disponibilité](#)".

- c. Vous pouvez également copier la base de données du nœud d'administration du nœud d'administration principal vers le nœud d'administration d'extension si vous souhaitez conserver la cohérence des informations d'attribut et d'audit sur chaque nœud d'administration. Voir ["Copier la base de données du nœud d'administration"](#) .
 - d. Vous pouvez également copier la base de données Prometheus du nœud d'administration principal vers le nœud d'administration d'extension si vous souhaitez conserver la cohérence des métriques historiques sur chaque nœud d'administration. Voir ["Copier les métriques Prometheus"](#) .
 - e. Vous pouvez également copier les journaux d'audit existants du nœud d'administration principal vers le nœud d'administration d'extension si vous souhaitez conserver la cohérence des informations du journal historique sur chaque nœud d'administration. Voir ["Copier les journaux d'audit"](#) .
5. Pour vérifier si des nœuds d'extension ont été ajoutés avec un réseau client non approuvé ou pour modifier si le réseau client d'un nœud est approuvé ou non approuvé, accédez à **CONFIGURATION > Sécurité > Contrôle du pare-feu**.

Si le réseau client sur le nœud d'extension n'est pas approuvé, les connexions au nœud sur le réseau client doivent être établies à l'aide d'un point de terminaison d'équilibrage de charge. Voir ["Configurer les points de terminaison de l'équilibreur de charge"](#) et ["Gérer les contrôles du pare-feu"](#) .

6. Configurer le DNS.

Si vous avez spécifié les paramètres DNS séparément pour chaque nœud de grille, vous devez ajouter des paramètres DNS personnalisés par nœud pour les nouveaux nœuds. Voir ["Modifier la configuration DNS pour un nœud de grille unique"](#) .

Pour garantir un bon fonctionnement, spécifiez deux ou trois serveurs DNS. Si vous spécifiez plus de trois, il est possible que seulement trois soient utilisés en raison de limitations connues du système d'exploitation sur certaines plates-formes. Si vous avez des restrictions de routage dans votre environnement, vous pouvez ["personnaliser la liste des serveurs DNS"](#) pour que les nœuds individuels (généralement tous les nœuds d'un site) utilisent un ensemble différent de trois serveurs DNS maximum.

Si possible, utilisez des serveurs DNS auxquels chaque site peut accéder localement pour garantir qu'un site isolé peut résoudre les noms de domaine complets pour les destinations externes.

Vérifiez que le nœud de stockage est actif

Une fois l'opération d'extension qui ajoute de nouveaux nœuds de stockage terminée, le système StorageGRID doit automatiquement commencer à utiliser les nouveaux nœuds de stockage. Vous devez utiliser le système StorageGRID pour vérifier que le nouveau nœud de stockage est actif.

Étapes

1. Sign in 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 correspond à la quantité d'espace total utilisable qui a été utilisée pour les données d'objet.
4. Vérifiez que la valeur de **Utilisé** augmente lorsque vous déplacez votre curseur vers la droite sur le graphique.

Copier la base de données du nœud d'administration

Lors de l'ajout de 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` déposer.
- Vous disposez de la phrase secrète de provisionnement.

À propos de cette 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 sur les serveurs et les services qui font actuellement partie du système ou qui sont ajoutés ultérieurement. Cette base de données de nœud d'administration comprend les informations suivantes :

- Historique des alertes
- Données d'attributs historiques, utilisées dans les graphiques de style hérité sur la page Nœuds

Pour garantir 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 nœud d'administration principal (*thesource Admin Node*) vers un nœud d'administration d'extension peut prendre jusqu'à plusieurs heures. Pendant cette période, le Grid Manager est inaccessible.

Suivez ces étapes 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. Entrez la commande suivante : `ssh admin@grid_node_IP`
 - ii. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.
 - iii. Entrez la commande suivante pour passer en root : `su -`
 - iv. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.
 - b. Exécutez la commande suivante : `recover-access-points`
 - c. Saisissez la phrase secrète d'approvisionnement.
 - d. Arrêter le service MI : `service mi stop`
 - e. Arrêtez le service d'interface de programmation d'application de gestion (mgmt-api) : `service mgmt-api stop`
2. Effectuez les étapes suivantes sur le nœud d'administration d'extension :

- a. Connectez-vous au nœud d'administration de l'extension :
 - i. Entrez la commande suivante : `ssh admin@grid_node_IP`
 - ii. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.
 - iii. Entrez la commande suivante pour passer en root : `su -`
 - iv. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.
 - b. Arrêter le service MI : `service mi stop`
 - c. Arrêtez le service mgmt-api : `service mgmt-api stop`
 - d. Ajoutez la clé privée SSH à l'agent SSH. Entrer: `ssh-add`
 - e. Saisissez le mot de passe d'accès SSH répertorié dans le `Passwords.txt` déposer.
 - 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 écraser la base de données MI sur le nœud d'administration d'extension.
- La base de données et ses données historiques sont copiées sur le nœud d'administration d'extension. Une fois l'opération de copie 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. Entrer: `ssh-add -D`

3. Redémarrez les services sur le nœud d'administration principal : `service servermanager start`

Copier les métriques Prometheus

Après avoir ajouté un nouveau nœud d'administration, vous pouvez éventuellement copier les métriques historiques gérées par Prometheus du nœud d'administration principal vers le nouveau nœud d'administration. La copie des métriques garantit que les métriques historiques sont cohérentes 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` déposer.
- Vous disposez de la phrase secrète de provisionnement.

À propos de cette tâche

Lorsque vous ajoutez un nœud d'administration, le processus d'installation du logiciel crée une nouvelle base de données Prometheus. Vous pouvez conserver la cohérence des mesures historiques entre les nœuds en copiant la base de données Prometheus du nœud d'administration principal (le *nœud d'administration source*) 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. Entrez la commande suivante : `ssh admin@grid_node_IP`
 - b. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.
 - c. Entrez la commande suivante pour passer en root : `su -`
 - d. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.
2. Depuis le nœud d'administration source, arrêtez le service Prometheus : `service prometheus stop`
3. Effectuez les étapes suivantes sur le nouveau nœud d'administration :
 - a. Connectez-vous au nouveau nœud d'administration :
 - i. Entrez la commande suivante : `ssh admin@grid_node_IP`
 - ii. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.
 - iii. Entrez la commande suivante pour passer en root : `su -`
 - iv. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.
 - b. Arrêter le service Prometheus : `service prometheus stop`
 - c. Ajoutez la clé privée SSH à l'agent SSH. Entrer: `ssh-add`
 - d. Saisissez le mot de passe d'accès SSH répertorié dans le `Passwords.txt` déposer.
 - 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 **Entrée** pour confirmer que vous souhaitez détruire la nouvelle base de données Prometheus sur le nouveau nœud 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. Le statut 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. Entrer:

```
ssh-add -D
```

4. Redémarrez le service Prometheus sur le nœud d'administration source.

```
service prometheus start
```

Copier les journaux d'audit

Lorsque vous ajoutez un nouveau nœud d'administration via une procédure d'extension, son service AMS enregistre uniquement les événements et les actions qui se produisent après son adhésion au système. Si nécessaire, vous pouvez copier les journaux d'audit d'un nœud d'administration précédemment 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` déposer.

À propos de cette tâche

Pour rendre les messages d'audit historiques disponibles 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 sur les nœuds d'administration. Vous pouvez ignorer ces étapes si l'une des situations suivantes s'applique :

- Vous avez configuré un serveur Syslog externe et les journaux d'audit sont désormais envoyés au serveur Syslog au lieu des nœuds d'administration.
- Vous avez explicitement spécifié que les messages d'audit doivent être enregistrés uniquement sur les nœuds locaux qui les ont générés.

Voir ["Configurer les messages d'audit et les destinations des journaux"](#) pour plus de détails.

Étapes

1. Connectez-vous au nœud d'administration principal :

- a. Entrez la commande suivante : `ssh admin@_primary_Admin_Node_IP`
- b. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.
- c. Entrez la commande suivante pour passer en root : `su -`
- d. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.

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. Accédez au répertoire d'exportation d'audit :

```
cd /var/local/log
```

4. Renommer la source `audit.log` fichier pour garantir qu'il n'écrase pas le fichier sur le nœud d'administration d'extension sur lequel vous le copiez :

```
ls -l
mv audit.log _new_name_.txt
```

5. Copiez tous les fichiers journaux d'audit vers l'emplacement de destination sur le nœud d'administration d'extension :

```
scp -p * IP_address:/var/local/log
```

6. Si vous êtes invité à saisir la phrase secrète pour `/root/.ssh/id_rsa` , entrez le mot de passe d'accès

SSH pour le nœud d'administration principal répertorié dans le `Passwords.txt` déposer.

7. Restaurer l'original `audit.log` déposer:

```
mv new_name.txt audit.log
```

8. Démarrer le service AMS :

```
service ams start
```

9. Se déconnecter du serveur :

```
exit
```

10. Connectez-vous au nœud d'administration de l'extension :

- Entrez la commande suivante : `ssh admin@expansion_Admin_Node_IP`
- Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.
- Entrez la commande suivante pour passer en root : `su -`
- Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.

Lorsque vous êtes connecté en tant que root, l'invite passe de \$ à # .

11. Mettre à jour les paramètres utilisateur et groupe pour les fichiers journaux d'audit :

```
cd /var/local/log
```

```
chown ams-user:bycast *
```

12. Se déconnecter du serveur :

```
exit
```

Rééquilibrer les données codées par effacement après l'ajout de nœuds de stockage

Après avoir ajouté des nœuds de stockage, vous pouvez utiliser la procédure de rééquilibrage du codage d'effacement (EC) pour redistribuer les fragments codés par 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 examiné le ["considérations pour le rééquilibrage des données codées par effacement"](#) .
- Vous comprenez que les données d'objet répliquées ne seront pas déplacées par cette procédure et que la procédure de rééquilibrage EC ne prend pas en compte l'utilisation des données répliquées sur chaque nœud de stockage lors de la détermination de l'emplacement où déplacer les données codées par effacement.
- Vous avez le `Passwords.txt` déposer.

Que se passe-t-il lorsque cette procédure s'exécute

Avant de commencer la procédure, notez les points suivants :

- La procédure de rééquilibrage EC ne démarrera pas si un ou plusieurs volumes sont hors ligne (démontés) ou s'ils sont en ligne (montés) mais dans un état d'erreur.
- La procédure de rééquilibrage CE réserve temporairement une grande quantité de stockage. Des alertes de stockage peuvent être déclenchées, mais seront résolues une fois le rééquilibrage terminé. S'il n'y a pas suffisamment de stockage pour la réservation, la procédure de rééquilibrage EC échouera. Les réservations de stockage sont libérées lorsque la procédure de rééquilibrage EC est terminée, que la procédure ait échoué ou réussi.
- Si un volume est hors ligne pendant que la procédure de rééquilibrage EC est en cours, la procédure de rééquilibrage prendra fin. Tous les fragments de données déjà déplacés resteront à leur nouvel emplacement et aucune donnée ne sera perdue.

Vous pouvez réexécuter la procédure une fois que tous les volumes sont de nouveau en ligne.

- Lorsque la procédure de rééquilibrage EC est en cours d'exécution, les performances des opérations ILM et des opérations client S3 peuvent être affectées.



Les opérations API S3 pour télécharger des objets (ou des parties d'objet) peuvent échouer pendant la procédure de rééquilibrage EC si elles nécessitent plus de 24 heures pour se terminer. Les opérations PUT de longue durée échoueront si la règle ILM applicable utilise un placement équilibré ou strict lors de l'ingestion. L'erreur suivante sera signalée : 500 Internal Server Error.

- Au cours de cette procédure, tous les nœuds ont une limite de capacité de stockage de 80 %. Les nœuds qui dépassent cette limite, mais stockent toujours en dessous de la partition de données cible, sont exclus de :
 - La valeur du déséquilibre du site
 - Toutes conditions d'achèvement des travaux



La partition des données cibles est calculée en divisant les données totales d'un site par le nombre de nœuds.

- **Conditions d'achèvement des travaux.** La procédure de rééquilibrage de la CE est considérée comme terminée lorsque l'une des conditions suivantes est remplie :
 - Il ne peut plus déplacer de données codées par effacement.
 - Les données de tous les nœuds se situent dans un écart de 5 % par rapport à la partition de données cible.
 - La procédure est en cours depuis 30 jours.

Étapes

1. Vérifiez les détails actuels du stockage d'objets pour le site que vous prévoyez de rééquilibrer.
 - a. Sélectionnez **NODES**.
 - b. Sélectionnez le premier nœud de stockage sur le site.
 - c. Sélectionnez l'onglet **Stockage**.
 - d. Placez votre curseur sur le graphique Stockage utilisé - Données d'objet pour voir la quantité actuelle de données répliquées et de données codées par effacement sur le nœud de stockage.
 - e. Répétez ces étapes pour afficher les autres nœuds de stockage sur le site.

2. Connectez-vous au nœud d'administration principal :

- a. Entrez la commande suivante : `ssh admin@primary_Admin_Node_IP`
- b. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.
- c. Entrez la commande suivante pour passer en root : `su -`
- d. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.

Lorsque vous êtes connecté en tant que root, l'invite passe de \$ à # .

3. Démarrer la procédure :

```
`rebalance-data start --site "nom-du-site"
```

Pour « *site-name* », spécifiez le premier site sur lequel vous avez ajouté un ou plusieurs nouveaux nœuds de stockage. Joindre `site-name` entre guillemets.

La procédure de rééquilibrage EC démarre et un ID de tâche est renvoyé.

4. Copiez l'ID du travail.

5. Surveillez l'état de la procédure de rééquilibrage de la CE.

- Pour afficher l'état d'une seule procédure de rééquilibrage CE :

```
rebalance-data status --job-id job-id
```

Pour `job-id`, spécifiez l'ID qui a été renvoyé lorsque vous avez démarré la procédure.

- Pour afficher l'état de la procédure de rééquilibrage CE en cours et de toutes les procédures précédemment terminées :

```
rebalance-data status
```



Pour obtenir de l'aide sur la commande `rebalance-data` :

```
rebalance-data --help
```

6. Effectuez des étapes supplémentaires, en fonction du statut renvoyé :

- Si `State` est `In progress`, l'opération de rééquilibrage de la CE est toujours en cours. Vous devez surveiller périodiquement la procédure jusqu'à ce qu'elle soit terminée.

Utilisez le `Site Imbalance` valeur permettant d'évaluer le degré de déséquilibre de l'utilisation des données du code d'effacement sur les nœuds de stockage du site. Cette valeur peut varier de 1,0 à 0, 0 indiquant que l'utilisation des données de codage d'effacement est complètement équilibrée sur tous les nœuds de stockage du site.

Le travail de rééquilibrage EC est considéré comme terminé et s'arrêtera lorsque les données de tous les nœuds se situeront dans un écart de 5 % par rapport à la partition de données cible.

- Si `State` est `Success`, en option [examiner le stockage d'objets](#) pour voir les détails mis à jour du site.

Les données codées par effacement devraient désormais être plus équilibrées entre les nœuds de

stockage du site.

° Si State est Failure :

- i. Confirmez que tous les nœuds de stockage du site sont connectés au réseau.
- ii. Recherchez et résolvez toutes les alertes susceptibles d'affecter ces nœuds de stockage.
- iii. Redémarrer la procédure de rééquilibrage de la CE :

```
rebalance-data start --job-id job-id
```

- iv. [Voir le statut](#) de la nouvelle procédure. Si State est toujours Failure , contactez le support technique.

7. Si la procédure de rééquilibrage EC génère trop de charge (par exemple, les opérations d'ingestion sont affectées), mettez la procédure en pause.

```
rebalance-data pause --job-id job-id
```

8. Si vous devez mettre fin à la procédure de rééquilibrage EC (par exemple, pour pouvoir effectuer une mise à niveau du logiciel StorageGRID), saisissez ce qui suit :

```
rebalance-data terminate --job-id job-id
```



Lorsque vous terminez une procédure de rééquilibrage EC, tous les fragments de données qui ont déjà été déplacés restent à leurs nouveaux emplacements. Les données ne sont pas déplacées vers l'emplacement d'origine.

9. Si vous utilisez le codage d'effacement sur plusieurs sites, exécutez cette procédure pour tous les autres sites concernés.

Dépannage de l'extension

Si vous rencontrez des erreurs pendant le processus d'extension de la grille que vous ne parvenez pas à résoudre, ou si une tâche de grille échoue, collectez les fichiers journaux et contactez le support technique.

Avant de contacter le support technique, collectez les fichiers journaux requis pour faciliter le dépannage.

Étapes

1. Connectez-vous au nœud d'extension qui a subi des échecs :

- a. Entrez 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 conteneur exécutant StorageGRID.

- b. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.
- c. Entrez la commande suivante pour passer en root : `su -`
- d. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.

Après vous être connecté en tant que root, l'invite passe de \$ à # .

2. En fonction du stade atteint par l'installation, récupérez l'un des journaux suivants disponibles sur le nœud de grille :

Plate-forme	Journaux
VMware	• /var/log/daemon.log • /var/log/storagegrid/daemon.log • /var/log/storagegrid/nodes/<node-name>.log
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 défaillant ; peut ne pas exister)

Maintenir un système StorageGRID

Maintenance du réseau

Les tâches de maintenance du réseau incluent la mise hors service d'un nœud ou d'un site, le changement de nom d'un réseau, d'un nœud ou d'un site et la maintenance des réseaux. Vous pouvez également exécuter des procédures d'hôte et de middleware ainsi que des procédures de nœud de grille.



Dans ces instructions, « Linux » fait référence à un déploiement Red Hat® Enterprise Linux®, Ubuntu® ou Debian®. Pour une liste des versions prises en charge, consultez le "[Outil de matrice d'interopérabilité NetApp](#)".

Avant de commencer

- Vous avez une compréhension approfondie du système StorageGRID .
- Vous avez examiné la topologie de votre système StorageGRID et vous comprenez la configuration de la grille.
- Vous comprenez que vous devez suivre toutes les instructions à la lettre et tenir compte de tous les avertissements.
- Vous comprenez que les procédures de maintenance non décrites ne sont pas prises en charge ou nécessitent un engagement de services.

Procédures d'entretien des appareils

Pour les procédures matérielles, voir le "[instructions de maintenance pour votre appliance StorageGRID](#)".

Télécharger le package de récupération

Le fichier Recovery Package vous permet de restaurer le système StorageGRID en cas de panne.

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 disposez de la phrase secrète de provisionnement.
- Tu as "[autorisations d'accès spécifiques](#)".

Téléchargez le fichier du package de récupération actuel avant d'apporter des modifications à la topologie de grille du système StorageGRID ou avant de mettre à niveau le logiciel. Ensuite, téléchargez une nouvelle copie du package de récupération après avoir apporté des modifications à la topologie de la grille ou après avoir mis à niveau le logiciel.

Étapes

1. Sélectionnez **MAINTENANCE > Système > Package de récupération**.
2. Saisissez la phrase secrète d'approvisionnement et sélectionnez **Démarrer le téléchargement**.

Le téléchargement démarre immédiatement.

3. Une fois le téléchargement terminé, ouvrez le `.zip` fichier et confirmez que vous pouvez accéder au contenu, y compris le `Passwords.txt` déposer.
4. Copiez le fichier du package de récupération téléchargé(`.zip`) vers deux endroits sûrs, sécurisés et séparés.



Le fichier du package de récupération doit être sécurisé car il contient des clés de chiffrement et des mots de passe qui peuvent être utilisés pour obtenir des données à partir du système StorageGRID .

Décommissionner les nœuds ou le site

Décommissionner un nœud ou un site

Vous pouvez effectuer une procédure de mise hors service pour supprimer définitivement des nœuds de grille 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 :

- Effectuer une "[déclassement des nœuds du réseau](#)" 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 ils peuvent être hors ligne et déconnectés.
- Effectuer une "[déclassement du site](#)" supprimer un site. Vous effectuez une **décommission de site connecté** si tous les nœuds sont connectés à StorageGRID. Vous effectuez une **décommission de site déconnecté** si tous les nœuds sont déconnectés de StorageGRID. Si le site contient un mélange de nœuds connectés et déconnectés, vous devez remettre en ligne tous les nœuds hors ligne.



Avant d'effectuer une mise hors service d'un site déconnecté, contactez votre représentant de compte NetApp . NetApp examinera vos exigences avant d'activer toutes les étapes de l'assistant de mise hors service du site. Vous ne devez pas tenter de décommissionner un site déconnecté si vous pensez qu'il pourrait être possible de récupérer le site ou de récupérer les données d'objet du site.

Décommissionner les nœuds

Déclassement des nœuds de réseau

Vous pouvez utiliser la procédure de mise hors service de nœud pour supprimer un ou plusieurs nœuds de grille sur un ou plusieurs sites. Vous ne pouvez pas désactiver le nœud d'administration principal.

Quand mettre hors service un nœud

Utilisez la procédure de mise hors service du nœud lorsque l'une des situations suivantes est vraie :

- Vous avez ajouté un nœud de stockage plus grand dans une extension et vous souhaitez supprimer un ou plusieurs nœuds de stockage plus petits, tout en préservant les objets.



Si vous souhaitez remplacer un appareil plus ancien par un appareil plus récent, pensez "[clonage du nœud de l'appareil](#)" au lieu d'ajouter un nouvel appareil dans une extension, puis de mettre hors service l'ancien appareil.

- 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 principal.
- Votre réseau comprend un nœud déconnecté que vous ne pouvez pas récupérer ou remettre en ligne.
- Votre grille comprend un nœud d'archive.

Comment décommissionner un nœud

Vous pouvez mettre hors service les nœuds de réseau connectés ou les nœuds de réseau déconnectés.

Mettre hors service les nœuds connectés

En général, vous devez mettre hors service les nœuds de grille uniquement lorsqu'ils sont connectés au système StorageGRID et uniquement lorsque tous les nœuds sont en état normal (ils ont des icônes vertes sur les pages **NODES** et sur la page **Decommission Nodes**).

Pour les instructions, voir "[Décommissionner les nœuds de réseau connectés](#)".

Décommissionner les nœuds déconnectés

Dans certains cas, vous devrez peut-être mettre hors service un nœud de réseau qui n'est pas actuellement connecté au réseau (un nœud dont l'état est inconnu ou administrativement hors service).

Pour les instructions, voir "[Décommissionner les nœuds de réseau déconnectés](#)".

Éléments à prendre en compte avant de mettre hors service un nœud

Avant d'effectuer l'une ou l'autre procédure, examinez les considérations relatives à chaque type de nœud :

- "[Considérations relatives à la mise hors service du nœud d'administration ou de passerelle](#)"
- "[Considérations relatives à la mise hors service du nœud de stockage](#)"

Considérations relatives à la mise hors service des nœuds d'administration ou de passerelle

Passez en revue les considérations relatives à la mise hors service d'un nœud d'administration ou d'un nœud de passerelle.

Considérations pour le nœud d'administration

- Vous ne pouvez pas désactiver le nœud d'administration principal.
- Vous ne pouvez pas désactiver un nœud d'administration si l'une de ses interfaces réseau fait partie d'un groupe de haute disponibilité (HA). Vous devez d'abord supprimer les interfaces réseau du groupe HA. Voir les instructions pour "[gestion des groupes HA](#)".
- Si nécessaire, vous pouvez modifier en toute sécurité les politiques ILM lors de la mise hors service d'un nœud d'administration.
- Si vous désactivez un nœud d'administration et que l'authentification unique (SSO) est activée pour votre système StorageGRID, vous devez penser à supprimer l'approbation de la partie de confiance du nœud des services de fédération Active Directory (AD FS).

- Si vous utilisez ["fédération de réseau"](#) , assurez-vous que l'adresse IP du nœud que vous mettez hors service n'a pas été spécifiée pour une connexion à une fédération de grille.
- Lorsque vous désactivez un nœud d'administration déconnecté, vous perdez les journaux d'audit de ce nœud ; cependant, ces journaux doivent également exister sur le nœud d'administration principal.

Considérations relatives au nœud de passerelle

- Vous ne pouvez pas désactiver un nœud de passerelle si l'une de ses interfaces réseau fait partie d'un groupe de haute disponibilité (HA). Vous devez d'abord supprimer les interfaces réseau du groupe HA. Voir les instructions pour ["gestion des groupes HA"](#) .
- Si nécessaire, vous pouvez modifier en toute sécurité les stratégies ILM lors de la mise hors service d'un nœud de passerelle.
- Si vous utilisez ["fédération de réseau"](#) , assurez-vous que l'adresse IP du nœud que vous mettez hors service n'a pas été spécifiée pour une connexion à une fédération de grille.
- Vous pouvez mettre hors service en toute sécurité un nœud de passerelle lorsqu'il est déconnecté.

Considérations relatives aux nœuds de stockage

Considérations relatives à la mise hors service des nœuds de stockage

Avant de mettre hors service un nœud de stockage, déterminez si vous pouvez cloner le nœud à la place. Ensuite, si vous décidez de mettre hors service le nœud, vérifiez comment StorageGRID gère les objets et les métadonnées pendant la procédure de mise hors service.

Quand cloner un nœud au lieu de le mettre hors service

Si vous souhaitez remplacer un nœud de stockage d'appareil plus ancien par un appareil plus récent ou plus grand, envisagez de cloner le nœud d'appareil au lieu d'ajouter un nouvel appareil dans une extension, puis de mettre hors service l'ancien appareil.

Le clonage de nœud d'appliance vous permet de remplacer facilement un nœud d'appliance existant par une appliance compatible sur le même site StorageGRID . Le processus de clonage transfère toutes les données vers le nouvel appareil, met le nouvel appareil en service et laisse l'ancien appareil dans un état de pré-installation.

Vous pouvez cloner un nœud d'appliance si vous en avez besoin :

- Remplacer un appareil qui arrive en fin de vie.
- Mettez à niveau un nœud existant pour profiter d'une technologie d'appareil améliorée.
- Augmentez la capacité de stockage de la grille sans modifier le nombre de nœuds de stockage dans votre système StorageGRID .
- Améliorez l'efficacité du stockage, par exemple en modifiant le mode RAID.

Voir ["Clonage de nœud d'appareil"](#) pour plus de détails.

Considérations relatives aux nœuds de stockage connectés

Passez en revue les considérations relatives à la mise hors service d'un nœud de stockage connecté.

- Vous ne devez pas mettre hors service plus de 10 nœuds de stockage dans une seule procédure de mise hors service de nœud.
- Le système doit, à tout moment, inclure suffisamment de nœuds de stockage pour satisfaire aux exigences opérationnelles, y compris la "[Quorum du CDA](#)" et l'actif "[Politique ILM](#)". Pour satisfaire à cette restriction, vous devrez peut-être ajouter un nouveau nœud de stockage dans une opération d'extension avant de pouvoir mettre hors service un nœud de stockage existant.

Soyez prudent lorsque vous désaffectez des nœuds de stockage dans une grille contenant uniquement des nœuds de métadonnées basés sur des logiciels. Si vous désactivez tous les nœuds configurés pour stocker à la fois des objets et des métadonnées, la possibilité de stocker des objets est supprimée de la grille. Voir "[Types de nœuds de stockage](#)" pour plus d'informations sur les nœuds de stockage contenant uniquement des métadonnées.

- Lorsque vous supprimez un nœud de stockage, de grands volumes de données d'objets sont transférés sur le réseau. Bien que ces transferts ne devraient pas affecter les opérations normales du système, ils peuvent affecter la quantité totale de bande passante réseau consommée par le système StorageGRID.
- Les tâches associées à la mise hors service du nœud de stockage ont une priorité inférieure à celle des tâches associées aux opérations normales du système. Cela signifie que la mise hors service n'interfère pas avec les opérations normales du système StorageGRID et n'a pas besoin d'être planifiée pour une période d'inactivité du système. Étant donné que le déclassement est effectué en arrière-plan, il est difficile d'estimer combien de temps le processus prendra. En général, la mise hors service se termine plus rapidement lorsque le système est silencieux ou si un seul nœud de stockage est supprimé à la fois.
- La mise hors service d'un nœud de stockage peut prendre des jours ou des semaines. Planifiez cette procédure en conséquence. Bien que le processus de mise hors service soit conçu pour ne pas avoir d'impact sur les opérations du système, il peut limiter d'autres procédures. En général, vous devez effectuer toutes les mises à niveau ou extensions système prévues avant de supprimer les nœuds de grille.
- Si vous devez effectuer une autre procédure de maintenance pendant que les nœuds de stockage sont supprimés, vous pouvez "[suspendre la procédure de déclassement](#)" et reprenez-le une fois l'autre procédure terminée.



Le bouton **Pause** est activé uniquement lorsque les étapes d'évaluation ILM ou de mise hors service des données codées par effacement sont atteintes ; cependant, l'évaluation ILM (migration des données) continuera de s'exécuter en arrière-plan.

- Vous ne pouvez pas exécuter d'opérations de réparation de données sur aucun nœud de grille lorsqu'une tâche de mise hors service est en cours d'exécution.
- Vous ne devez apporter aucune modification à une stratégie ILM pendant la mise hors service d'un nœud de stockage.
- Pour supprimer définitivement et en toute sécurité les données, vous devez effacer les lecteurs du nœud de stockage une fois la procédure de mise hors service terminée.

Considérations relatives aux nœuds de stockage déconnectés

Passez en revue les considérations relatives à la mise hors service d'un nœud de stockage déconnecté.

- Ne mettez jamais hors service un nœud déconnecté à moins d'être sûr qu'il ne peut pas être remis en ligne ou récupéré.



N'exécutez pas cette procédure si vous pensez qu'il est possible de récupérer les données de l'objet à partir du nœud. Contactez plutôt le support technique pour déterminer si la récupération du nœud est possible.

- Lorsque vous mettez hors service un nœud de stockage déconnecté, StorageGRID utilise les données d'autres nœuds de stockage pour reconstruire les données et métadonnées d'objet qui se trouvaient sur le nœud déconnecté.
- Une perte de données peut se produire si vous mettez hors service plusieurs nœuds de stockage déconnectés. Le système peut ne pas être en mesure de reconstruire les données si le nombre de copies d'objets, de fragments codés par effacement ou de métadonnées d'objets disponibles n'est pas suffisant. Lors de la mise hors service des nœuds de stockage dans une grille avec des nœuds basés uniquement sur des métadonnées logicielles, la mise hors service de tous les nœuds configurés pour stocker à la fois des objets et des métadonnées supprime tout le stockage d'objets de la grille. Voir "[Types de nœuds de stockage](#)" pour plus d'informations sur les nœuds de stockage contenant uniquement des métadonnées.



Si vous avez plusieurs nœuds de stockage déconnectés que vous ne pouvez pas récupérer, contactez le support technique pour déterminer la meilleure marche à suivre.

- Lorsque vous mettez hors service un nœud de stockage déconnecté, StorageGRID démarre les tâches de réparation des données à la fin du processus de mise hors service. Ces tâches tentent de reconstruire les données et les métadonnées de l'objet qui ont été stockées sur le nœud déconnecté.
- Lorsque vous mettez hors service 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 à s'exécuter et ne sont pas surveillées par la procédure de mise hors service. Vous devez surveiller manuellement ces tâches et les redémarrer si nécessaire. Voir "[Vérifier les tâches de réparation de données](#)".
- Si vous désactivez un nœud de stockage déconnecté qui contient la seule copie d'un objet, l'objet sera perdu. Les tâches de réparation de données ne peuvent reconstruire et récupérer des objets que si au moins une copie répliquée ou suffisamment de fragments codés par effacement existent sur les nœuds de stockage actuellement connectés.

Quel est le quorum de l'ADC ?

Vous ne pourrez peut-être pas mettre hors service certains nœuds de stockage sur un site si trop peu de services de contrôleur de domaine administratif (ADC) restent après la mise hors service.

Le service ADC, présent sur certains nœuds de stockage, conserve les informations de topologie de grille et fournit des services de configuration à la grille. Le système StorageGRID nécessite qu'un quorum de services ADC soit disponible sur chaque site et à tout moment.

Vous ne pouvez pas mettre hors service un nœud de stockage si la suppression du nœud entraîne le non-respect du quorum ADC. Pour satisfaire le quorum ADC lors d'une mise hors service, un minimum de trois nœuds de stockage sur chaque site doivent disposer du service ADC. Si un site dispose de plus de trois nœuds de stockage avec le service ADC, une simple majorité de ces nœuds doit rester disponible après la mise hors service : $((0.5 * \text{Storage Nodes with ADC}) + 1)$



Soyez prudent lorsque vous désaffectez des nœuds de stockage dans une grille contenant uniquement des nœuds de métadonnées basés sur des logiciels. Si vous désactivez tous les nœuds configurés pour stocker à la fois des objets et des métadonnées, la possibilité de stocker des objets est supprimée de la grille. Voir "[Types de nœuds de stockage](#)" pour plus d'informations sur les nœuds de stockage contenant uniquement des métadonnées.

Par exemple, supposons qu'un site comprend actuellement six nœuds de stockage avec des services ADC et que vous souhaitez mettre hors service trois nœuds de stockage. En raison de l'exigence de quorum de l'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 initialement mettre hors service que deux nœuds de stockage.
- Lors de la deuxième procédure de mise hors service, vous pouvez supprimer le troisième nœud de stockage, car le quorum ADC ne nécessite désormais que trois services ADC pour rester disponibles : $((0.5 * 4) + 1)$.

Si vous devez mettre hors service un nœud de stockage mais que vous ne pouvez pas le faire en raison de l'exigence de quorum ADC, ajoutez un nouveau nœud de stockage dans un "[expansion](#)" et précisez qu'il doit disposer d'un service ADC. Ensuite, mettez hors service le nœud de stockage existant.

Examiner la politique ILM et la configuration du stockage

Si vous prévoyez de mettre hors service un nœud de stockage, vous devez consulter la politique ILM de votre système StorageGRID avant de démarrer le processus de mise hors service.

Lors de la mise hors service, toutes les données d'objet sont migrées du nœud de stockage mis 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 politique répond à vos exigences en matière de données avant de commencer la mise hors service et une fois celle-ci terminée.

Vous devriez revoir les règles de chaque "[politique ILM active](#)" pour garantir que le système StorageGRID continuera à disposer d'une capacité suffisante du type correct et aux emplacements corrects pour permettre la mise hors service d'un nœud de stockage.

Considérez ce qui suit :

- Sera-t-il possible pour les services d'évaluation ILM de copier les données d'objet de manière à ce que les règles ILM soient satisfaites ?
- Que se passe-t-il si un site devient temporairement indisponible pendant le démantèlement ? Des copies supplémentaires peuvent-elles être réalisées dans un autre endroit ?
- Comment le processus de déclassement affectera-t-il la distribution finale du contenu ? Comme décrit dans "[Consolider les nœuds de stockage](#)" , tu devrais "[ajouter de nouveaux nœuds de stockage](#)" avant de mettre hors service les anciens. Si vous ajoutez un nœud de stockage de remplacement plus grand après la mise hors service d'un nœud de stockage plus petit, les anciens nœuds de stockage pourraient être proches de leur capacité et le nouveau nœud de stockage pourrait n'avoir presque aucun contenu. La plupart des opérations d'écriture pour les nouvelles données d'objet seraient alors dirigées vers le nouveau nœud de stockage, réduisant ainsi l'efficacité globale des opérations du système.

- Le système comprendra-t-il à tout moment suffisamment de nœuds de stockage pour satisfaire les politiques ILM actives ?



Une politique ILM qui ne peut pas être satisfaite entraînera des retards et des alertes, et pourrait interrompre le fonctionnement du système StorageGRID .

Vérifiez que la topologie proposée qui résultera du processus de déclassement satisfait la politique ILM en évaluant les zones répertoriées dans le tableau.

Zone à évaluer	Ce qu'il faut prendre en compte
Capacité disponible	Y aura-t-il suffisamment de capacité de stockage pour accueillir toutes les données d'objet stockées dans le système StorageGRID , y compris les copies permanentes des données d'objet actuellement stockées sur le nœud de stockage à mettre hors service ? Y aura-t-il suffisamment de capacité pour gérer la croissance prévue des données d'objets stockées pendant un intervalle de temps raisonnable après la fin du déclassement ?
Lieu de stockage	S'il reste suffisamment de capacité dans le système StorageGRID dans son ensemble, la capacité est-elle aux bons endroits pour satisfaire les règles métier du système StorageGRID ?
Type de stockage	Y aura-t-il suffisamment de stockage du type approprié une fois le déclassement terminé ? Par exemple, les règles ILM peuvent déplacer du contenu d'un type de stockage vers un autre à mesure que le contenu vieillit. Dans ce cas, vous devez vous assurer qu'un espace de stockage suffisant du type approprié est disponible dans la configuration finale du système StorageGRID .

Consolider les nœuds de stockage

Vous pouvez consolider les nœuds de stockage pour réduire le nombre de nœuds de stockage pour un site ou un déploiement tout en augmentant la capacité de stockage.

Lorsque vous consolidez les nœuds de stockage, vous "[étendre le système StorageGRID](#)" en ajoutant de nouveaux nœuds de stockage de plus grande capacité, puis en mettant hors service les anciens nœuds de stockage de plus petite capacité. Au cours de la procédure de mise hors service, les objets sont migrés des anciens nœuds de stockage vers les nouveaux nœuds de stockage.



Si vous regroupez des appareils plus anciens et plus petits avec de nouveaux modèles ou des appareils de plus grande capacité, pensez à "[clonage du nœud de l'appareil](#)" (ou utilisez le clonage de nœud d'appareil et la procédure de mise hors service si vous n'effectuez pas de remplacement 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 plus grands, puis utiliser la procédure de mise hors service

pour supprimer les trois anciens nœuds de stockage de plus petite capacité.

En ajoutant une nouvelle capacité avant de supprimer les nœuds de stockage existants, vous garantissez une distribution plus équilibrée des données sur le système StorageGRID . Vous réduisez également la possibilité qu'un nœud de stockage existant soit poussé au-delà du niveau de filigrane de stockage.

Mettre hors service plusieurs nœuds de stockage

Si vous devez supprimer plusieurs nœuds de stockage, vous pouvez les mettre hors service de manière séquentielle ou en parallèle.



Soyez prudent lorsque vous désaffectez des nœuds de stockage dans une grille contenant uniquement des nœuds de métadonnées basés sur des logiciels. Si vous désactivez tous les nœuds configurés pour stocker à la fois des objets et des métadonnées, la possibilité de stocker des objets est supprimée de la grille. Voir "[Types de nœuds de stockage](#)" pour plus d'informations sur les nœuds de stockage contenant uniquement des métadonnées.

- Si vous désactivez les nœuds de stockage de manière séquentielle, vous devez attendre que le premier nœud de stockage termine sa désactivation avant de commencer à désactiver le nœud de stockage suivant.
- Si vous mettez hors service des nœuds de stockage en parallèle, les nœuds de stockage traitent simultanément les tâches de mise hors service pour tous les nœuds de stockage en cours de mise hors service. Cela peut entraîner une situation dans laquelle toutes les copies permanentes d'un fichier sont marquées comme « en lecture seule », désactivant temporairement la suppression dans les grilles où cette fonctionnalité est activée.

Vérifier les tâches de réparation de données

Avant de mettre hors service un nœud de grille, vous devez confirmer qu'aucune tâche de réparation de données n'est active. Si des réparations ont échoué, vous devez les redémarrer et les laisser se terminer avant d'effectuer la procédure de mise hors service.

À propos de cette tâche

Si vous devez mettre hors service un nœud de stockage déconnecté, vous devrez également effectuer ces étapes une fois la procédure de mise hors service terminée pour garantir que la tâche de réparation des données s'est terminée avec succès. Vous devez vous assurer que tous les fragments codés par effacement qui se trouvaient sur le nœud supprimé ont été restaurés avec succès.

Ces étapes s'appliquent uniquement aux systèmes dotés d'objets codés par effacement.

Étapes

1. Connectez-vous au nœud d'administration principal :
 - a. Entrez la commande suivante : `ssh admin@grid_node_IP`
 - b. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.
 - c. Entrez la commande suivante pour passer en root : `su -`
 - d. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.

Lorsque vous êtes connecté en tant que root, l'invite passe de \$ à # .

2. Vérifiez les réparations en cours : `repair-data show-ec-repair-status`

- Si vous n'avez jamais exécuté de tâche de réparation de données, le résultat est `No job found`. Vous n'avez pas besoin de redémarrer les tâches de réparation.
- Si la tâche de réparation des données a été exécutée précédemment ou est en cours d'exécution, la sortie répertorie les informations relatives à la réparation. Chaque réparation possède un identifiant de réparation unique.

```
root@ADM1-0:~# repair-data show-ec-repair-status
```

Repair ID	Affected Nodes / Volumes	Start Time	End Time	State	Estimated Bytes Affected	Bytes Repaired	Percentage
4216507958013005550	DC1-S1-0-182 (Volumes: 2)	2022-08-17T21:37:30.051543	2022-08-17T21:37:37.328998	Completed	1015788876	0	0
18214680851049518682	DC1-S1-0-182 (Volumes: 1)	2022-08-17T20:37:58.869362	2022-08-17T20:38:45.299688	Completed	0	0	100
7962734388032289010	DC1-S1-0-182 (Volumes: 0)	2022-08-17T20:42:29.578740		Stopped			Unknown



En option, vous pouvez utiliser le gestionnaire de grille pour surveiller les processus de restauration en cours et afficher un historique de restauration. Voir "[Restaurer les données d'objet à l'aide de Grid Manager](#)".

3. Si l'État prend en charge toutes les réparations `Completed`, vous n'avez pas besoin de redémarrer les tâches de réparation.
4. Si l'État pour toute réparation est `Stopped`, vous devez recommencer cette réparation.
 - a. Obtenez l'ID de réparation pour la réparation ayant échoué à partir de la sortie.
 - b. Exécutez le `repair-data start-ec-node-repair` commande.

Utilisez le `--repair-id` option pour spécifier l'ID de réparation. Par exemple, si vous souhaitez réessayer une réparation avec l'ID de réparation 949292, exécutez cette commande : `repair-data start-ec-node-repair --repair-id 949292`

- c. Continuez à suivre l'état des réparations des données CE jusqu'à ce que l'état de toutes les réparations soit `Completed`.

Rassembler le matériel nécessaire

Avant d'effectuer la mise hors service d'un nœud de grille, vous devez obtenir les informations suivantes.

Article	Remarques
Paquet de relance .zip déposer	Vous devez " télécharger le package de récupération le plus récent " .zip déposer(<code>sgws-recovery-package-id-revision.zip</code>). Vous pouvez utiliser le fichier Recovery Package pour restaurer le système en cas de panne.
`Passwords.txt` déposer	Ce fichier contient les mots de passe requis pour accéder aux nœuds de grille sur la ligne de commande et est inclus dans le package de récupération.
Mot de passe d'approvisionnement	La phrase secrète est créée et documentée lors de la première installation du système StorageGRID . La phrase secrète de provisionnement n'est pas dans le <code>Passwords.txt</code> déposer.

Article	Remarques
Description de la topologie du système StorageGRID avant la mise hors service	Si disponible, obtenez toute documentation décrivant la topologie actuelle du système.

Informations connexes

["Configuration requise pour le navigateur Web"](#)

Accéder à la page des nœuds de déclassement

Lorsque vous accédez à la page Décommissionner les nœuds dans le gestionnaire de grille, vous pouvez voir en un coup d'œil quels nœuds peuvent être mis hors service.

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 de maintenance ou root"](#) .



Soyez prudent lorsque vous désaffectez des nœuds de stockage dans une grille contenant uniquement des nœuds de métadonnées basés sur des logiciels. Si vous désactivez tous les nœuds configurés pour stocker à la fois des objets et des métadonnées, la possibilité de stocker des objets est supprimée de la grille. Voir ["Types de nœuds de stockage"](#) pour plus d'informations sur les nœuds de stockage contenant uniquement des métadonnées.

Étapes

1. Sélectionnez **MAINTENANCE > Tâches > Mise hors service**.
2. Sélectionnez **Désactiver les nœuds**.

La page Décommissionner les nœuds s'affiche. À partir de cette page, vous pouvez :

- Déterminer quels nœuds du réseau peuvent être mis hors service actuellement.
- Voir la santé de tous les nœuds de la grille
- Trier la liste par ordre croissant ou décroissant par **Nom**, **Site**, **Type** ou **A un ADC**.
- Saisissez des termes de recherche pour trouver rapidement des nœuds particuliers.

Dans cet exemple, la colonne Décommission possible indique que vous pouvez mettre hors service le nœud de passerelle et l'un des quatre nœuds de stockage.

Name	Site	Type	Has ADC	Health	Decommission Possible
DC1-ADM1	Data Center 1	Admin Node	-		No, member of HA group(s): HAGroup. Before you can decommission this node, you must remove it from all HA groups.
DC1-ARC1	Data Center 1	Archive Node	-		No, you can't decommission an Archive Node unless the node is disconnected.
☐ DC1-G1	Data Center 1	API Gateway Node	-		
DC1-S1	Data Center 1	Storage Node	Yes		No, site Data Center 1 requires a minimum of 3 Storage Nodes with ADC services.
DC1-S2	Data Center 1	Storage Node	Yes		No, site Data Center 1 requires a minimum of 3 Storage Nodes with ADC services.
DC1-S3	Data Center 1	Storage Node	Yes		No, site Data Center 1 requires a minimum of 3 Storage Nodes with ADC services.
☐ DC1-S4	Data Center 1	Storage Node	No		

3. Consultez la colonne **Déclassement possible** pour chaque nœud que vous souhaitez mettre hors service.

Si un nœud de grille peut être mis hors service, cette colonne comprend une coche verte et la colonne de gauche comprend une case à cocher. Si un nœud ne peut pas être mis hors service, cette colonne décrit le problème. S'il existe plusieurs raisons pour lesquelles un nœud ne peut pas être mis hors service, la raison la plus critique est indiquée.

Déclassement Raison possible	Description	Étapes à suivre pour résoudre le problème
Non, la mise hors service du <i>type de nœud</i> n'est pas prise en charge.	Vous ne pouvez pas désactiver le nœud d'administration principal.	Aucun.
Non, au moins un nœud du réseau est déconnecté. Remarque : ce message s'affiche uniquement pour les nœuds de réseau connectés.	Vous ne pouvez pas mettre hors service un nœud de réseau connecté si un nœud de réseau est déconnecté. La colonne Santé inclut l'une de ces icônes pour les nœuds de grille déconnectés : (gris) : Administrativement en panne (bleu) : Inconnu	Vous devez remettre en ligne tous les nœuds déconnectés ou "mettre hors service tous les nœuds déconnectés" avant de pouvoir supprimer un nœud connecté. Remarque : si votre réseau contient plusieurs nœuds déconnectés, le logiciel vous demande de les mettre hors service tous en même temps, ce qui augmente le risque de résultats inattendus.

Déclassement Raison possible	Description	Étapes à suivre pour résoudre le problème
Non, un ou plusieurs nœuds requis sont actuellement déconnectés et doivent être récupérés. Remarque : ce message s'affiche uniquement pour les nœuds de grille déconnectés.	Vous ne pouvez pas mettre hors service 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).	- Consultez les messages de mise hors service possible pour tous les nœuds déconnectés. - Déterminez quels nœuds ne peuvent pas être mis hors service car ils sont nécessaires. - Si l'état d'un nœud requis est administrativement en panne, remettez le nœud en ligne. - Si l'état d'un nœud requis est inconnu, effectuez une procédure de récupération de nœud pour récupérer le nœud requis.
Non, membre du(des) groupe(s) HA : <i>nom du groupe</i>. Avant de pouvoir mettre hors service ce nœud, vous devez le supprimer de tous les groupes HA.	Vous ne pouvez pas désactiver un nœud d'administration ou un nœud de passerelle si une interface de nœud appartient à un groupe de haute disponibilité (HA).	Modifiez le groupe HA pour supprimer l'interface du nœud ou supprimer l'intégralité du groupe HA. Voir "Configurer des groupes de haute disponibilité".
Non, le site x nécessite un minimum de n nœuds de stockage avec des services ADC.	Nœuds de stockage uniquement. Vous ne pouvez pas mettre hors service un nœud de stockage si le nombre de nœuds restant sur le site est insuffisant pour prendre en charge les exigences de quorum ADC.	Effectuer une expansion. Ajoutez un nouveau nœud de stockage au site et spécifiez qu'il doit disposer d'un service ADC. Voir les informations sur le "Quorum du CDA".

Déclassement Raison possible	Description	Étapes à suivre pour résoudre le problème
Non, un ou plusieurs profils de codage 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 mettre hors service un nœud de stockage à moins qu'il ne reste suffisamment de nœuds pour les profils de codage d'effacement existants. Par exemple, si un profil de codage d'effacement existe pour le codage d'effacement 4+2, au moins 6 nœuds de stockage doivent rester.	Pour chaque profil de codage d'effacement concerné, effectuez l'une des étapes suivantes, en fonction de la manière dont le profil est utilisé : • Utilisé dans les politiques ILM actives : effectuer une extension. Ajoutez suffisamment de nouveaux nœuds de stockage pour permettre au codage d'effacement de continuer. Voir les instructions pour "étendre votre réseau" . • Utilisé dans une règle ILM mais pas dans les politiques ILM actives : Modifiez ou supprimez la règle, puis désactivez le profil de codage d'effacement. • Non utilisé dans aucune règle ILM : Désactivez le profil de codage d'effacement. Remarque : un message d'erreur s'affiche si vous tentez de désactiver un profil de codage d'effacement et que les données d'objet sont toujours associées au profil. Vous devrez peut-être attendre plusieurs semaines avant de réessayer le processus de désactivation. En savoir plus sur "désactiver un profil de codage d'effacement" .
Non, vous ne pouvez pas mettre hors service un nœud d'archive à moins que le nœud ne soit déconnecté.	Si un nœud d'archive est toujours connecté, vous ne pouvez pas le supprimer.	Remarque : la prise en charge des nœuds d'archive a été supprimée. Si vous devez mettre hors service un nœud d'archive, consultez "Mise hors service des nœuds de grille (site de documentation StorageGRID 11.8)"

Décommissionner les nœuds de réseau déconnectés

Vous devrez peut-être mettre hors service un nœud qui n'est pas actuellement connecté au réseau (un nœud dont l'état est inconnu ou administrativement hors service).

Avant de commencer

- Vous comprenez les considérations relatives au déclassement "[Nœuds d'administration et de passerelle](#)" et les considérations relatives au déclassement "[Nœuds de stockage](#)".
- Vous avez obtenu tous les éléments prérequis.
- Vous avez vérifié qu'aucune tâche de réparation de données n'est active. Voir "[Vérifier les tâches de réparation de données](#)".
- Vous avez confirmé que la récupération du nœud de stockage n'est en cours nulle part dans la grille. Si tel est le cas, vous devez attendre que toute reconstruction de Cassandra effectuée dans le cadre de la récupération soit terminée. Vous pouvez ensuite procéder au démantèlement.
- Vous avez assuré qu'aucune autre procédure de maintenance ne sera exécutée pendant l'exécution de la procédure de mise hors service du nœud, sauf si la procédure de mise hors service du nœud est suspendue.
- La colonne **Désactivation possible** pour le ou les nœuds déconnectés que vous souhaitez mettre hors service inclut une coche verte.
- Vous disposez de la phrase secrète de provisionnement.

À propos de cette tâche

Vous pouvez identifier les nœuds déconnectés en recherchant l'icône bleue Inconnu  ou l'icône grise Administrativement vers le bas  dans la colonne **Santé**.

Avant de mettre hors service un nœud déconnecté, notez les points suivants :

- Cette procédure est principalement destinée à supprimer un seul nœud déconnecté. Si votre réseau contient plusieurs nœuds déconnectés, le logiciel vous demande de les mettre hors service tous en même temps, ce qui augmente le risque de résultats inattendus.



Une perte de données peut se produire si vous mettez hors service plusieurs nœuds de stockage déconnectés à la fois. Voir "[Considérations relatives aux nœuds de stockage déconnectés](#)".



Soyez prudent lorsque vous désaffectez des nœuds de stockage dans une grille contenant uniquement des nœuds de métadonnées basés sur des logiciels. Si vous désactivez tous les nœuds configurés pour stocker à la fois des objets et des métadonnées, la possibilité de stocker des objets est supprimée de la grille. Voir "[Types de nœuds de stockage](#)" pour plus d'informations sur les nœuds de stockage contenant uniquement des métadonnées.

- 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.

Étapes

1. À moins que vous ne mettiez hors service un nœud d'archive (qui doit être déconnecté), essayez de remettre en ligne ou de récupérer les nœuds de grille déconnectés.

Voir "[Procédures de récupération des nœuds de grille](#)" pour les instructions.

2. Si vous ne parvenez pas à récupérer un nœud de réseau déconnecté et que vous souhaitez le mettre hors service pendant qu'il est déconnecté, cochez la case correspondant à ce nœud.



Si votre réseau contient plusieurs nœuds déconnectés, le logiciel vous demande de les mettre hors service tous en même temps, ce qui augmente le risque de résultats inattendus.



Soyez prudent lorsque vous choisissez de mettre hors service plusieurs nœuds de réseau déconnectés à la fois, en particulier si vous sélectionnez plusieurs nœuds de stockage déconnectés. Si vous avez plusieurs nœuds de stockage déconnectés que vous ne pouvez pas récupérer, contactez le support technique pour déterminer la meilleure marche à suivre.

3. Saisissez la phrase secrète d'approvisionnement.

Le bouton **Démarrer la mise hors service** est activé.

4. Cliquez sur **Démarrer la mise hors service**.

Un avertissement s'affiche, indiquant que vous avez sélectionné un nœud déconnecté et que les données de l'objet seront perdues si le nœud possède la seule copie d'un objet.

5. Passez en revue 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 package de récupération est généré contenant la modification de la configuration de la grille.

6. Dès que le nouveau package de récupération est disponible, cliquez sur le lien ou sélectionnez **MAINTENANCE > Système > Pack de récupération** pour accéder à la page du package de récupération. Ensuite, téléchargez le .zip déposer.

Voir les instructions pour "[téléchargement du package de récupération](#)".



Téléchargez le package de récupération dès que possible pour vous assurer de pouvoir récupérer votre réseau en cas de problème lors de la procédure de mise hors service.



Le fichier du package de récupération doit être sécurisé car il contient des clés de chiffrement et des mots de passe qui peuvent être utilisés pour obtenir des données à partir du système StorageGRID.

7. Surveillez régulièrement la page de mise hors service pour vous assurer que tous les nœuds sélectionnés sont mis hors service avec succès.

La mise hors service des nœuds de stockage peut prendre des jours ou des semaines. Lorsque toutes les tâches sont terminées, la liste de sélection des nœuds s'affiche à nouveau avec un message de réussite. Si vous avez mis hors service un nœud de stockage déconnecté, un message d'information indique que les tâches de réparation ont été démarrées.

8. Une fois les nœuds arrêtés automatiquement dans le cadre de la procédure de mise hors service, supprimez toutes les machines virtuelles restantes ou autres ressources associées au nœud mis hors service.



N'effectuez pas cette étape tant que les nœuds ne se sont pas arrêtés automatiquement.

9. Si vous mettez hors service un nœud de stockage, surveillez l'état des tâches de réparation des **données répliquées** et des **données à code d'effacement (EC)** qui sont automatiquement démarrées pendant le processus de mise hors service.

Données répliquées

- Pour obtenir une estimation du pourcentage d'achèvement de la réparation répliquée, ajoutez le `show-replicated-repair-status` option à la commande `repair-data`.

```
repair-data show-replicated-repair-status
```

- Pour déterminer si les réparations sont terminées :
 - a. Sélectionnez **NODES > Nœud de stockage en cours de réparation > ILM**.
 - b. Passez en revue les attributs dans la section Évaluation. Lorsque les réparations sont terminées, l'attribut **En attente - Tout** indique 0 objet.
- Pour suivre la réparation plus en détail :
 - a. Sélectionnez **SUPPORT > Outils > Topologie de grille**.
 - b. Sélectionnez **grid > Nœud de stockage en cours de réparation > LDR > Data Store**.
 - c. Utilisez une combinaison des attributs suivants pour déterminer, aussi bien que possible, si les réparations répliquées sont complètes.



Des incohérences de Cassandra peuvent être présentes et les réparations ayant échoué 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 supérieure à la période d'analyse actuelle (fournie par l'attribut **Période d'analyse — Estimée**), cela signifie que l'analyse ILM n'a trouvé aucun objet à haut risque devant être réparé sur aucun nœud.



Les objets à haut risque sont des objets qui risquent d'être complètement perdus. Cela n'inclut pas les objets qui ne satisfont pas à leur configuration ILM.

- **Période d'analyse — Estimée (XSCM)** : utilisez cet attribut pour estimer quand un changement de politique sera appliqué aux objets précédemment ingérés. Si l'attribut **Réparations tentées** n'augmente pas pendant une période supérieure à la période d'analyse actuelle, il est probable que des réparations répliquées sont effectuées. Notez que la période d'analyse peut changer. L'attribut **Période d'analyse — Estimée (XSCM)** s'applique à l'ensemble de la grille et correspond au maximum de toutes les périodes d'analyse des nœuds. Vous pouvez interroger l'historique de l'attribut **Période d'analyse — Estimée** pour la grille afin de déterminer une période appropriée.

Données codées par effacement (EC)

Pour surveiller la réparation des données codées par effacement et réessayer toutes les demandes qui auraient échoué :

1. Déterminer l'état des réparations des données codées par effacement :
 - Sélectionnez **SUPPORT > Outils > Métriques** pour afficher le temps estimé jusqu'à l'achèvement et le pourcentage d'achèvement de la tâche en cours. Ensuite, sélectionnez **EC Overview** dans la section Grafana. Consultez les tableaux de bord **Temps estimé d'achèvement du travail EC de la grille** et **Pourcentage d'achèvement du travail EC de la grille**.
 - Utilisez cette commande pour voir l'état d'un élément spécifique `repair-data` opération:

```
repair-data show-ec-repair-status --repair-id repair ID
```

- Utilisez cette commande pour lister toutes les réparations :

```
repair-data show-ec-repair-status
```

La sortie répertorie les informations, y compris `repair ID` , pour toutes les réparations effectuées et en cours.

2. Si la sortie indique que l'opération de réparation a échoué, utilisez le `--repair-id` possibilité de réessayer la réparation.

Cette commande réessaie une réparation de nœud ayant échoué, en utilisant l'ID de réparation 6949309319275667690 :

```
repair-data start-ec-node-repair --repair-id 6949309319275667690
```

Cette commande réessaie une réparation de volume ayant échoué, en utilisant l'ID de réparation 6949309319275667690 :

```
repair-data start-ec-volume-repair --repair-id 6949309319275667690
```

Après avoir terminé

Dès que les nœuds déconnectés ont été mis hors service et que toutes les tâches de réparation des données ont été terminées, vous pouvez mettre hors service tous les nœuds de réseau connectés selon vos besoins.

Ensuite, effectuez ces étapes après avoir terminé la procédure de mise hors service :

- Assurez-vous que les disques du nœud de réseau mis hors service sont nettoyés. Utilisez un outil ou un service d'effacement de données disponible dans le commerce pour supprimer définitivement et en toute sécurité les données des lecteurs.
- Si vous avez mis hors service un nœud d'appliance et que les données sur l'appliance étaient protégées à l'aide du chiffrement de nœud, utilisez le programme d'installation de l'appliance StorageGRID pour effacer la configuration du serveur de gestion des clés (Clear KMS). Vous devez effacer la configuration KMS si vous souhaitez ajouter l'appareil à une autre grille. Pour les instructions, voir ["Surveiller le chiffrement des nœuds en mode maintenance"](#) .

Décommissionner les nœuds de réseau connectés

Vous pouvez mettre hors service et supprimer définitivement les nœuds connectés au réseau.

Avant de commencer

- Vous comprenez les considérations relatives au déclassement ["Nœuds d'administration et de passerelle"](#) et les considérations relatives au déclassement ["Nœuds de stockage"](#) .
- Vous avez rassemblé tout le matériel nécessaire.
- Vous avez vérifié qu'aucune tâche de réparation de données n'est active.
- Vous avez confirmé que la récupération du nœud de stockage n'est en cours nulle part dans la grille. Si tel est le cas, attendez que toute reconstruction de Cassandra effectuée dans le cadre de la récupération soit terminée. Vous pouvez ensuite procéder au démantèlement.

- Vous avez assuré qu'aucune autre procédure de maintenance ne sera exécutée pendant l'exécution de la procédure de mise hors service du nœud, sauf si la procédure de mise hors service du nœud est suspendue.
- Vous disposez de la phrase secrète de provisionnement.
- Les nœuds de la grille sont connectés.
- La colonne **Désactivation possible** du ou des nœuds que vous souhaitez désactiver inclut une coche verte.



La mise hors service ne démarrera pas si un ou plusieurs volumes sont hors ligne (démontés) ou s'ils sont en ligne (montés) mais dans un état d'erreur.



Si un ou plusieurs volumes sont mis hors ligne pendant qu'une mise hors service est en cours, le processus de mise hors service se termine une fois que ces volumes sont remis en ligne.

- Tous les nœuds de la grille ont une santé normale (verte) . Si vous voyez l'une de ces icônes dans la colonne **Santé**, vous devez essayer de résoudre le problème :

Icône	Couleur	Gravité
	Jaune	Avis
	Orange clair	Mineure
	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 tâches de réparation de données"](#).



Ne supprimez pas la machine virtuelle ou d'autres ressources d'un nœud de grille avant d'y être invité dans cette procédure.



Soyez prudent lorsque vous désaffectez des nœuds de stockage dans une grille contenant uniquement des nœuds de métadonnées basés sur des logiciels. Si vous désactivez tous les nœuds configurés pour stocker à la fois des objets et des métadonnées, la possibilité de stocker des objets est supprimée de la grille. Voir ["Types de nœuds de stockage"](#) pour plus d'informations sur les nœuds de stockage contenant uniquement des métadonnées.

À propos de cette tâche

Lorsqu'un nœud est mis hors service, ses services sont désactivés et le nœud s'arrête automatiquement.

Étapes

1. À partir de la page Décommissionner les nœuds, cochez la case correspondant à chaque nœud de grille

que vous souhaitez décommissionner.

2. Saisissez la phrase secrète d'approvisionnement.

Le bouton **Démarrer la mise hors service** est activé.

3. Sélectionnez **Démarrer la mise hors service**.
4. Consultez la liste des nœuds dans la boîte de dialogue de confirmation et sélectionnez **OK**.

La procédure de mise hors service du nœud démarre et la progression est affichée pour chaque nœud.



Ne mettez pas un nœud de stockage hors ligne une fois la procédure de mise hors service commencée. La modification de l'état peut entraîner la non-copie de certains contenus vers d'autres emplacements.

5. Dès que le nouveau Recovery Package est disponible, sélectionnez le lien Recovery Package dans la bannière ou sélectionnez **MAINTENANCE > Système > Recovery package** pour accéder à la page Recovery Package. Ensuite, téléchargez le .zip déposer.

Voir "[téléchargement du package de récupération](#)".



Téléchargez le package de récupération dès que possible pour vous assurer de pouvoir récupérer votre réseau en cas de problème lors de la procédure de mise hors service.

6. Surveillez régulièrement la page Décommissionner les nœuds pour vous assurer que tous les nœuds sélectionnés sont correctement mis hors service.



La mise hors service des nœuds de stockage peut prendre des jours ou des semaines.

Lorsque toutes les tâches sont terminées, la liste de sélection des nœuds s'affiche à nouveau avec un message de réussite.

Après avoir terminé

Effectuez ces étapes après avoir terminé la procédure de mise hors service du nœud :

1. Suivez l'étape appropriée à votre plateforme. Par exemple:
 - **Linux** : vous souhaitez peut-être détacher les volumes et supprimer les fichiers de configuration de nœud que vous avez créés lors de l'installation. Voir "[Installer StorageGRID sur Red Hat Enterprise Linux](#)" et "[Installer StorageGRID sur Ubuntu ou Debian](#)".
 - **VMware** : Vous souhaitez peut-être utiliser l'option « Supprimer du disque » de vCenter pour supprimer la machine virtuelle. Vous devrez peut-être également supprimer tous les disques de données indépendants de la machine virtuelle.
 - *** Appareil StorageGRID *** : le nœud de l'appareil revient automatiquement à un état non déployé où vous pouvez accéder au programme d'installation de l'appareil StorageGRID . Vous pouvez mettre l'appareil hors tension ou l'ajouter à un autre système StorageGRID .
2. Assurez-vous que les disques du nœud de réseau mis hors service sont nettoyés. Utilisez un outil ou un service d'effacement de données disponible dans le commerce pour supprimer définitivement et en toute sécurité les données des lecteurs.
3. Si vous avez mis hors service un nœud d'appliance et que les données sur l'appliance étaient protégées à l'aide du chiffrement de nœud, utilisez le programme d'installation de l'appliance StorageGRID pour effacer

la configuration du serveur de gestion des clés (Clear KMS). Vous devez effacer la configuration KMS si vous souhaitez ajouter l'appareil à une autre grille. Pour les instructions, voir "[Surveiller le chiffrement des nœuds en mode maintenance](#)".

Suspendre et reprendre le processus de mise hors service des nœuds de stockage

Si vous devez effectuer une deuxième procédure de maintenance, vous pouvez suspendre 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** est activé uniquement lorsque les étapes d'évaluation ILM ou de mise hors service des données codées par effacement sont atteintes ; cependant, l'évaluation ILM (migration des données) continuera de 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 avez le "[Autorisation d'accès de maintenance ou root](#)".

Étapes

1. Sélectionnez **MAINTENANCE > Tâches > Mise hors service**.

La page de mise hors service apparaît.

2. Sélectionnez **Désactiver les nœuds**.

La page Décommissionner les nœuds s'affiche. Lorsque la procédure de mise hors service atteint l'une des étapes suivantes, le bouton **Pause** est activé.

- Évaluation de l'ILM
- Mise hors service des données codées par effacement

3. Sélectionnez **Pause** pour suspendre la procédure.

L'étape en cours est en pause et le bouton **Reprendre** est activé.

Decommission Nodes

A new Recovery Package has been generated as a result of the configuration change. Go to the [Recovery Package](#) page to download it.

Decommissioning procedure has been paused. Click 'Resume' to resume the procedure.

The progress for each node is displayed while the decommission procedure is running. When all tasks are complete, the node selection list is redisplayed.

Search

Name	Type	Progress	Stage
DC1-S5	Storage Node		Evaluating ILM

Pause

Resume

4. Une fois l'autre procédure de maintenance terminée, sélectionnez **Reprendre** pour procéder à la mise hors service.

Site de déclassement

Considérations relatives à la suppression d'un site

Avant d'utiliser la procédure de déclassement de site pour supprimer un site, vous devez examiner les considérations.

Que se passe-t-il lorsque vous décommissionnez un site

Lorsque vous mettez hors service un site, StorageGRID supprime définitivement tous les nœuds du site et le site lui-même du système StorageGRID .

Une fois la procédure de démantèlement du site 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 ni de profils de codage d'effacement faisant référence au site. Lorsque StorageGRID met hors service un site, il supprime automatiquement ces pools de stockage et désactive ces profils de codage d'effacement.

Différences entre les procédures de déclassement d'un site connecté et d'un site déconnecté

Vous pouvez utiliser la procédure de déclassement de site pour supprimer un site dans lequel tous les nœuds sont connectés à StorageGRID (appelé déclassement de site connecté) ou pour supprimer un site dans lequel tous les nœuds sont déconnectés de StorageGRID (appelé déclassement de site déconnecté). Avant de commencer, vous devez comprendre les différences entre ces procédures.



Si un site contient un mélange de sites connectés () et les nœuds déconnectés ( ou ), vous devez remettre tous les nœuds hors ligne en ligne.

- La mise hors service d'un site connecté vous permet de supprimer un site opérationnel du système StorageGRID . Par exemple, vous pouvez effectuer une mise hors service d'un site connecté pour supprimer un site fonctionnel mais qui n'est plus nécessaire.
- Lorsque StorageGRID supprime un site connecté, il utilise ILM pour gérer les données d'objet sur le site. Avant de pouvoir démarrer la mise hors service d'un site connecté, vous devez supprimer le site de toutes les règles ILM et activer une nouvelle stratégie ILM. Les processus ILM de migration des données d'objet et les processus internes de suppression d'un site peuvent se produire en même temps, mais la meilleure pratique consiste à laisser les étapes ILM se terminer avant de démarrer la procédure de mise hors service proprement dite.
- Une mise hors service de site déconnecté vous permet de supprimer un site défaillant du système StorageGRID . Par exemple, vous pouvez effectuer une mise hors service d'un site déconnecté pour supprimer 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 fait aucune tentative pour préserver les données. Cependant, avant de pouvoir démarrer la mise hors service d'un site déconnecté, vous devez supprimer le site de toutes les règles ILM et activer une nouvelle stratégie ILM.



Avant d'effectuer une procédure de déclassement de site déconnecté, vous devez contacter votre représentant de compte NetApp . NetApp examinera vos exigences avant d'activer toutes les étapes de l'assistant de mise hors service du site. Vous ne devez pas tenter de décommissionner un site déconnecté si vous pensez qu'il pourrait être possible de récupérer le site ou de récupérer les données d'objet du site.

Exigences générales pour la suppression d'un site connecté ou déconnecté

Avant de supprimer un site connecté ou déconnecté, vous devez prendre connaissance des exigences suivantes :

- Vous ne pouvez pas désactiver un site qui inclut le nœud d'administration principal.
- Vous ne pouvez pas désactiver un site si l'un des nœuds possède une interface appartenant à un groupe de haute disponibilité (HA). Vous devez soit modifier le groupe HA pour supprimer l'interface du nœud, soit supprimer l'intégralité du groupe HA.
- Vous ne pouvez pas désactiver un site s'il contient un mélange de sites connectés () et déconnecté ( ou ) nœuds.
- Vous ne pouvez pas mettre hors service un site si un nœud d'un autre site est déconnecté ( ou ).
- Vous ne pouvez pas démarrer la procédure de déclassement du site si une opération ec-node-repair est en cours. Voir "[Vérifier les tâches de réparation de données](#)" pour suivre les réparations des données codées par effacement.
- Pendant que la procédure de déclassement du site est en cours :
 - Vous ne pouvez pas créer de règles ILM qui font référence au site en cours de mise hors service. 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 "[suspendre la procédure pendant la suppression des nœuds de stockage](#)". Le bouton **Pause** est activé uniquement lorsque les étapes d'évaluation ILM ou de mise hors service des données codées par effacement sont atteintes ; cependant, l'évaluation ILM (migration des données) continuera de s'exécuter en arrière-plan. Une fois la deuxième procédure de maintenance terminée, vous pouvez reprendre la mise hors service.

- Si vous devez récupérer un nœud après avoir démarré la procédure de mise hors service du site, vous devez contacter le support.
- Vous ne pouvez pas désactiver plus d'un site 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 de parties de confiance pour le site des services de fédération Active Directory (AD FS).

Exigences relatives à la gestion du cycle de vie de l'information (ILM)

Dans le cadre de la suppression d'un site, vous devez mettre à jour votre configuration ILM. L'assistant de déclassement du site vous guide à travers un certain nombre d'étapes préalables pour garantir les éléments suivants :

- Le site n'est référencé par aucune politique ILM. Si tel est le cas, vous devez modifier les politiques ou créer et activer des politiques avec de nouvelles règles ILM.
- Aucune règle ILM ne fait référence au site, même si ces règles ne sont utilisées dans aucune politique. Vous devez supprimer ou modifier toutes les règles qui font référence au site.

Lorsque StorageGRID met hors service le site, il désactive automatiquement tous les profils de codage d'effacement inutilisés qui font référence au site et supprime automatiquement tous les pools de stockage inutilisés qui font référence au site. Si le pool de stockage Tous les nœuds de stockage 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 avez une bonne compréhension du fonctionnement d'ILM et que vous êtes familiarisé avec la création de pools de stockage, de profils de codage d'effacement, de règles ILM et de la simulation et de l'activation d'une stratégie ILM. Voir ["Gérer les 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 quoi faire des données d'objet existantes sur le site lorsque vous créez de nouvelles règles ILM et une nouvelle stratégie ILM. Vous pouvez effectuer l'une ou les deux actions suivantes :

- 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 mettre hors service un site à Raleigh parce que vous avez ajouté un nouveau site à Sunnyvale. Dans cet exemple, vous souhaitez déplacer toutes les données d'objet de l'ancien site vers le nouveau site. Avant de mettre à jour vos règles et politiques ILM, vous devez vérifier la capacité des deux sites. Vous devez vous assurer que le site de Sunnyvale dispose d'une capacité suffisante pour accueillir les données d'objet du site de Raleigh et qu'une capacité adéquate restera à Sunnyvale pour la croissance future.



Pour garantir qu'une capacité adéquate est disponible, vous devrez peut-être ["étendre une 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'objets du site sélectionné.

Exemple de suppression de données : Supposons que vous utilisiez actuellement une règle ILM à 3 copies pour répliquer les données d'objet sur trois sites. Avant de mettre hors service un site, vous pouvez créer une règle ILM équivalente à 2 copies pour stocker des données sur seulement deux sites. Lorsque vous activez une nouvelle stratégie ILM qui utilise la règle à 2 copies, StorageGRID supprime les copies du troisième site car elles ne répondent plus aux exigences ILM. Toutefois, les données de l'objet seront toujours protégées et la capacité des deux sites restants restera la même.



Ne créez jamais une règle ILM à copie unique pour prendre en charge la suppression d'un site. Une règle ILM qui crée une seule copie répliquée pour une période donnée expose les données à un risque de perte permanente. Si une seule copie répliquée d'un objet existe, cet objet est perdu si un nœud de stockage échoue ou présente une erreur importante. Vous perdez également temporairement l'accès à l'objet pendant les procédures de maintenance telles que les mises à niveau.

Exigences supplémentaires pour le déclassement d'un site connecté

Avant que StorageGRID puisse supprimer un site connecté, vous devez vous assurer des points suivants :

- Tous les nœuds de votre système StorageGRID doivent avoir un état de connexion **Connecté** (); cependant, les nœuds peuvent avoir des alertes actives.



Vous pouvez effectuer les étapes 1 à 4 de l'assistant de déclassement du site si un ou plusieurs nœuds sont déconnectés. Cependant, vous ne pouvez pas terminer l'étape 5 de l'assistant, qui démarre le processus de mise hors service, à moins que tous les nœuds ne soient connectés.

- Si le site que vous prévoyez de supprimer contient un nœud de passerelle ou un nœud d'administration utilisé pour l'équilibrage de charge, vous devrez peut-être "[étendre une grille](#)" pour ajouter un nouveau nœud équivalent sur un autre site. Assurez-vous que les clients peuvent se connecter au nœud de remplacement avant de démarrer la procédure de mise hors service du site.
- Si le site que vous prévoyez de supprimer contient des nœuds de passerelle ou des nœuds d'administration qui se trouvent dans un groupe haute disponibilité (HA), vous pouvez suivre les étapes 1 à 4 de l'assistant de mise hors service du site. Cependant, vous ne pouvez pas terminer 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 HA. Si les clients existants se connectent à un groupe HA qui inclut des nœuds du site, vous devez vous assurer qu'ils peuvent continuer à se connecter à StorageGRID après la suppression du site.
- Si les clients se connectent directement aux nœuds de stockage sur le site que vous prévoyez de supprimer, vous devez vous assurer qu'ils peuvent se connecter aux nœuds de stockage sur d'autres sites avant de démarrer la procédure de mise hors service du site.
- Vous devez fournir suffisamment d'espace sur les sites restants pour accueillir toutes les données d'objet qui seront déplacées en raison de modifications apportées à une politique ILM active. Dans certains cas, vous devrez peut-être "[étendre une grille](#)" en ajoutant des nœuds de stockage, des volumes de stockage ou de nouveaux sites avant de pouvoir terminer la mise hors service d'un site connecté.
- Vous devez prévoir suffisamment de temps pour que la procédure de mise hors service soit terminée. Les processus StorageGRID ILM peuvent prendre des jours, des semaines, voire des mois, pour déplacer ou supprimer les données d'objet du site avant que le site puisse être mis hors service.



Le déplacement ou la suppression des données d'objet d'un site peut prendre des jours, des semaines, voire des mois, en fonction de la quantité de données sur le site, de la charge sur votre système, des latences du réseau et de la nature des modifications ILM requises.

- Dans la mesure du possible, vous devez effectuer les étapes 1 à 4 de l'assistant de déclassement du site le plus tôt possible. La procédure de déclassement s'effectuera plus rapidement et avec moins d'interruptions et d'impacts sur les performances si vous autorisez le déplacement des données du site avant de démarrer la procédure de déclassement proprement dite (en sélectionnant **Démarrer la déclassement** à l'étape 5 de l'assistant).

Exigences supplémentaires pour le déclassement d'un site déconnecté

Avant que StorageGRID puisse supprimer un site déconnecté, vous devez vous assurer des points suivants :

- Vous avez contacté votre représentant de compte NetApp . NetApp examinera vos exigences avant d'activer toutes les étapes de l'assistant de mise hors service du site.



Vous ne devez pas tenter de décommissionner un site déconnecté si vous pensez qu'il pourrait être possible de récupérer le site ou de récupérer des données d'objet à partir du site. Voir "[Comment le support technique récupère un site](#)".

- Tous les nœuds du site doivent avoir un état de connexion parmi les suivants :
 - **Inconnu** (🌀): Pour une raison inconnue, un nœud est déconnecté ou les services sur le nœud sont indisponibles de manière inattendue. Par exemple, un service sur le nœud peut être arrêté ou le nœud peut avoir perdu sa connexion réseau en raison d'une panne de courant ou d'une panne inattendue.
 - **Administrativement en panne** (🌑): Le nœud n'est pas connecté au réseau pour une raison attendue. Par exemple, le nœud ou les services sur le nœud ont été arrêtés correctement.
- 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 afficher ou récupérer les données d'objet stockées sur le site. Lorsque StorageGRID exécute cette procédure, il ne tente pas de préserver les données du site déconnecté.



Si vos règles et votre politique 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 à la cohérence lors de la suppression d'un site

La cohérence d'un bucket S3 détermine si StorageGRID réplique entièrement les métadonnées d'objet sur tous les nœuds et sites avant d'indiquer à un client que l'ingestion d'objet a réussi. La cohérence fournit un équilibre entre la disponibilité des objets et la cohérence de ces objets sur différents nœuds de stockage et sites.

Lorsque StorageGRID supprime un site, il doit s'assurer qu'aucune donnée n'est écrite sur le site en cours de suppression. Par conséquent, il remplace temporairement la cohérence de chaque bucket ou conteneur. Une fois le processus de déclassement du site démarré, StorageGRID utilise temporairement la cohérence de site forte pour empêcher l'écriture des métadonnées d'objet sur le site en cours de suppression.

En raison de ce remplacement temporaire, sachez que toutes les opérations d'écriture, de mise à jour et de suppression de client qui se produisent pendant la mise hors service d'un site peuvent échouer si plusieurs nœuds deviennent indisponibles sur les sites restants.

Rassembler le matériel nécessaire

Avant de déclasser un site, vous devez vous procurer les matériaux suivants.

Article	Remarques
Paquet de relance .zip déposer	Vous devez télécharger le package de récupération le plus récent .zip déposer(<code>sgws-recovery-package-id-revision.zip</code>). Vous pouvez utiliser le fichier Recovery Package pour restaurer le système en cas de panne. "Téléchargez le package de récupération"
`Passwords.txt` déposer	Ce fichier contient les mots de passe requis pour accéder aux nœuds de grille sur la ligne de commande et est inclus dans le package de récupération.
Mot de passe d'approvisionnement	La phrase secrète est créée et documentée lors de la première installation du système StorageGRID . La phrase secrète de provisionnement n'est pas dans le <code>Passwords.txt</code> déposer.
Description de la topologie du système StorageGRID avant la mise hors service	Si disponible, obtenez toute documentation décrivant la topologie actuelle du système.

Informations connexes

["Configuration requise pour le navigateur Web"](#)

Étape 1 : Sélectionner le site

Pour déterminer si un site peut être mis hors service, commencez par accéder à l'assistant de mise hors service du 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 avez le ["Autorisation d'accès root ou autorisations de maintenance et ILM"](#) .

Étapes

1. Sélectionnez **MAINTENANCE > Tâches > Mise hors service**.
2. Sélectionnez **Site de déclassement**.

L'étape 1 (Sélectionner un site) de l'assistant de déclassement du site s'affiche. Cette étape comprend une liste alphabétique des sites de votre système StorageGRID .

Decommission Site

1

2

3

4

5

6

Select Site

View Details

Revise ILM Policy

Remove ILM References

Resolve Node Conflicts

Monitor Decommission

When you decommission a site, all nodes at the site and the site itself are permanently removed from the StorageGRID system.

Review the table for the site you want to remove. If Decommission Possible is Yes, select the site. Then, select **Next** to ensure that the site is not referred to by ILM and that all StorageGRID nodes are in the correct state.

You might not be able to remove certain sites. For example, you cannot decommission the site that contains the primary Admin Node or a site that contains an Archive Node.

Sites

	Site Name	Used Storage Capacity ?	Decommission Possible
☐	Raleigh	3.93 MB	✓
☐	Sunnyvale	3.97 MB	✓
	Vancouver	3.90 MB	No. This site contains the primary Admin Node.

Next

- Affichez les valeurs dans la colonne **Capacité de stockage utilisée** pour déterminer la quantité de stockage actuellement utilisée pour les données d'objet sur 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.

- Pour la mise hors service d'un site connecté, cette valeur représente la quantité de données d'objet qui devront être déplacées vers d'autres sites ou supprimées par ILM avant que vous puissiez mettre hors service ce site en toute sécurité.
- Pour une mise hors service d'un site déconnecté, cette valeur représente la quantité de stockage de données de votre système qui deviendra inaccessible lorsque vous mettrez hors service ce site.



Si votre politique ILM a été conçue pour protéger contre la perte d'un seul site, des copies de vos données d'objet doivent toujours exister sur les sites restants.

- Consultez les raisons dans la colonne **Déclassement possible** pour déterminer quels sites peuvent être déclassés actuellement.



S'il existe plusieurs raisons pour lesquelles un site ne peut pas être mis hors service, la raison la plus critique est indiquée.

Déclassement	Raison possible	Description	Prochaine étape
Coche verte (✓)		Vous pouvez désactiver ce site.	Aller à la prochaine étape .

Déclassement Raison possible	Description	Prochaine étape
Non. Ce site contient le nœud d'administration principal.	Vous ne pouvez pas désactiver un site contenant le nœud d'administration principal.	Aucun. Vous ne pouvez pas effectuer cette procédure.
Non. Ce site contient un ou plusieurs nœuds d'archives.	Vous ne pouvez pas désactiver un site contenant un nœud d'archive.	Aucun. Vous ne pouvez pas effectuer cette procédure.
Non. Tous les nœuds de ce site sont déconnectés. Contactez votre représentant de compte NetApp .	Vous ne pouvez pas effectuer la mise hors service d'un site connecté à moins que chaque nœud du site ne soit connecté ().	Si vous souhaitez effectuer une décommission d'un site déconnecté, vous devez contacter votre représentant de compte NetApp , qui examinera vos besoins et activera le reste de l'assistant de décommission du site. IMPORTANT : Ne mettez jamais les nœuds en ligne hors ligne afin de pouvoir supprimer un site. Vous perdrez des données.

L'exemple montre un système StorageGRID avec trois sites. La coche verte () pour les sites de Raleigh et de Sunnyvale indique que vous pouvez mettre hors service ces sites. Cependant, vous ne pouvez pas désactiver le site de Vancouver car il contient le nœud d'administration principal.

1. Si la mise hors service est possible, sélectionnez le bouton radio correspondant au site.

Le bouton **Suivant** est activé.

2. Sélectionnez **Suivant**.

L'étape 2 (Afficher les détails) apparaît.

Étape 2 : Afficher les détails

À partir de l'étape 2 (Afficher les détails) de l'assistant de mise hors service du site, vous pouvez vérifier les nœuds inclus sur le site, voir la quantité d'espace utilisée sur chaque nœud de stockage et évaluer la quantité d'espace libre disponible sur les autres sites de votre grille.

Avant de commencer

Avant de mettre hors service un site, vous devez vérifier la quantité de données d'objets existantes sur le site.

- Si vous effectuez une mise hors service d'un site connecté, vous devez comprendre la quantité de données d'objets actuellement présentes sur le site avant de mettre à jour ILM. En fonction des capacités du site et de vos besoins en matière de protection des données, vous pouvez créer de nouvelles règles ILM pour déplacer des données vers d'autres sites ou pour supprimer des données d'objet du site.

- Effectuez toutes les extensions de nœud de stockage requises avant de démarrer la procédure de mise hors service, si possible.
- Si vous effectuez une mise hors service d'un site déconnecté, vous devez comprendre la quantité de données d'objet qui deviendront définitivement inaccessibles lorsque vous supprimerez le site.

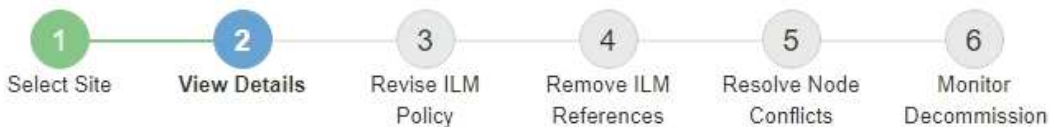


Si vous effectuez une mise hors service d'un site déconnecté, ILM ne peut pas déplacer ou supprimer les données d'objet. Toutes les données restantes sur le site seront perdues. Cependant, si votre politique ILM a été conçue pour protéger contre la perte d'un seul site, des copies de vos données d'objet 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), examinez tous les avertissements liés au site que vous avez choisi de supprimer.

Decommission Site



Data Center 2 Details

This site includes a Gateway Node. If clients are currently connecting to this node, you must configure an equivalent node at another site. Be sure clients can connect to the replacement node before starting the decommission procedure.

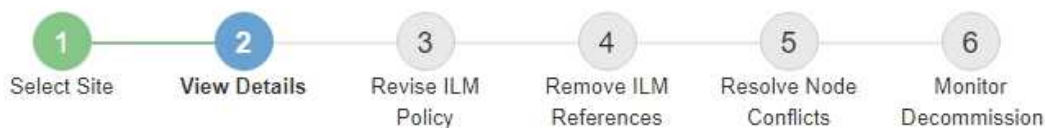
This site contains a mixture of connected and disconnected nodes. Before you can remove this site, you must bring all offline (blue or gray) nodes back online. Contact technical support if you need assistance.

Un avertissement apparaît dans ces cas :

- Le site comprend un nœud de passerelle. Si des clients S3 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 sites connectés () et les nœuds déconnectés (ou). Avant de pouvoir supprimer ce site, vous devez remettre tous les nœuds hors ligne en ligne.

2. Consultez les détails du site que vous avez choisi de supprimer.

Decommission Site



Raleigh Details

Number of Nodes: 3 Free Space: 475.38 GB
Used Space: 3.93 MB Site Capacity: 475.38 GB

Node Name	Node Type	Connection State	Details
RAL-S1-101-196	Storage Node	✓	1.30 MB used space
RAL-S2-101-197	Storage Node	✓	1.30 MB used space
RAL-S3-101-198	Storage Node	✓	1.34 MB used space

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

[Previous](#)[Next](#)

Les informations suivantes sont incluses pour le site sélectionné :

- Nombre de nœuds
- L'espace total utilisé, l'espace libre et la capacité de tous les nœuds de stockage du site.
 - Pour la mise hors service d'un site connecté, la valeur **Espace utilisé** représente la quantité de données d'objet qui doivent être déplacées vers d'autres sites ou supprimées avec ILM.
 - Pour une mise hors service d'un site déconnecté, la valeur **Espace utilisé** indique la quantité de données d'objet qui deviendront inaccessibles lorsque vous supprimerez le site.
- Noms de nœuds, types et états de connexion :
 -  (Connecté)
 -  (Administrativement en panne)
 -  (Inconnu)
- Détails sur chaque nœud :
 - Pour chaque nœud de stockage, la quantité d'espace qui a été utilisée pour les données d'objet.

- Pour les nœuds d'administration et les nœuds de passerelle, indiquez si le nœud est actuellement utilisé dans un groupe haute disponibilité (HA). Vous ne pouvez pas désactiver un nœud d'administration ou un nœud de passerelle utilisé dans un groupe HA. Avant de commencer la mise hors service, modifiez les groupes HA pour supprimer tous les nœuds du site ou supprimez le groupe HA s'il inclut uniquement des nœuds de ce site. Pour les instructions, voir "[Gérer les groupes de haute disponibilité \(HA\)](#)".

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 effectuez la mise hors service d'un site connecté et que vous prévoyez d'utiliser ILM pour déplacer les données d'objet du site sélectionné (au lieu de simplement les supprimer), vous devez vous assurer que les autres sites disposent d'une capacité suffisante pour accueillir les données déplacées et qu'une capacité adéquate reste disponible pour 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 qu'une capacité de stockage adéquate est disponible après la suppression du site, vous devrez peut-être effectuer une extension avant d'exécuter cette procédure.

4. Sélectionnez **Suivant**.

L'étape 3 (Réviser la politique ILM) apparaît.

Étape 3 : Réviser les politiques ILM

À partir de l'étape 3 (Réviser les politiques ILM) de l'assistant de mise hors service du site, vous pouvez déterminer si le site est référencé par une politique ILM.

Avant de commencer

Vous avez une bonne compréhension de la façon de "[gérer les objets avec ILM](#)". Vous êtes familiarisé avec la création de pools de stockage et de règles ILM, ainsi qu'avec la simulation et l'activation d'une politique ILM.

À propos de cette tâche

StorageGRID ne peut pas désactiver un site si une règle ILM dans une politique (active ou inactive) fait référence à ce site.

Si une politique ILM fait référence au site que vous souhaitez mettre hors service, vous devez supprimer ces politiques ou les modifier afin qu'elles répondent aux exigences suivantes :

- Protégez entièrement toutes les données de l'objet.

- Ne faites pas référence au site que vous décommissionnez.
- N'utilisez pas de pools de stockage qui font référence au site ou n'utilisez pas l'option Tous les sites.
- N'utilisez pas de profils de codage d'effacement qui font référence au site.
- N'utilisez pas la règle « Créer 2 copies » des installations StorageGRID 11.6 ou antérieures.



Ne créez jamais une règle ILM à copie unique pour prendre en charge la suppression d'un site. Une règle ILM qui crée une seule copie répliquée pour une période donnée expose les données à un risque de perte permanente. Si une seule copie répliquée d'un objet existe, cet objet est perdu si un nœud de stockage échoue ou présente une erreur importante. Vous perdez également temporairement l'accès à l'objet pendant les procédures de maintenance telles que les mises à niveau.



Si vous effectuez une *décommission d'un site connecté*, vous devez prendre en compte la manière dont StorageGRID doit gérer les données d'objet actuellement présentes sur le site que vous souhaitez supprimer. En fonction de vos exigences en matière de protection des données, de nouvelles règles peuvent déplacer les données d'objet existantes vers différents sites ou supprimer toutes les copies d'objet supplémentaires qui ne sont plus nécessaires.

Contactez le support technique si vous avez besoin d'aide pour concevoir une nouvelle politique.

Étapes

1. À partir de l'étape 3 (Réviser les politiques ILM), déterminez si des politiques ILM font référence au site que vous avez sélectionné pour la mise hors service.
2. Si aucune politique n'est répertoriée, sélectionnez **Suivant** pour accéder à "[Étape 4 : Supprimer les références ILM](#)".
3. Si une ou plusieurs stratégies ILM *actives* sont répertoriées, clonez chaque stratégie existante ou créez de nouvelles stratégies qui ne font pas référence au site en cours de mise hors service :
 - a. Sélectionnez le lien de la politique dans la colonne Nom de la politique.

La page des détails de la politique ILM pour la politique apparaît dans un nouvel onglet du navigateur. La page Site de déclassement restera ouverte sur l'autre onglet.

- b. Suivez ces directives et instructions selon vos besoins :

- Travailler avec les règles ILM :
 - "[Créer un ou plusieurs pools de stockage](#)" qui ne font pas référence au site.
 - "[Modifier ou remplacer les règles](#)" qui font référence au site.



Ne sélectionnez pas la règle **Créer 2 copies** car cette règle utilise le pool de stockage **Tous les nœuds de stockage**, ce qui n'est pas autorisé.

- Travailler avec les politiques ILM :
 - "[Cloner une politique ILM existante](#)" ou "[créer une nouvelle politique ILM](#)".
 - Assurez-vous que la règle par défaut et les autres règles ne font pas référence au site.



Vous devez confirmer que les règles ILM sont dans le bon ordre. Lorsque la politique est activée, les objets nouveaux et existants sont évalués par les règles dans l'ordre répertorié, en commençant par le haut.

c. Ingérez des objets de test et simulez la politique pour garantir que les règles correctes sont appliquées.



Des erreurs dans une politique ILM peuvent entraîner une perte de données irrécupérable. Examinez et simulez attentivement la politique avant de l'activer pour confirmer qu'elle fonctionnera comme prévu.



Lorsque vous activez une nouvelle stratégie ILM, StorageGRID l'utilise pour gérer tous les objets, y compris les objets existants et les objets nouvellement ingérés. Avant d'activer une nouvelle stratégie ILM, vérifiez toutes les modifications apportées au placement des objets répliqués et codés par effacement existants. La modification de l'emplacement d'un objet existant peut entraîner des problèmes de ressources temporaires lorsque les nouveaux emplacements sont évalués et mis en œuvre.

d. Activez les nouvelles politiques et assurez-vous que les anciennes politiques sont désormais inactives.

Si vous souhaitez activer plusieurs politiques, "[suivez les étapes pour créer des balises de politique ILM](#)".

Si vous effectuez une mise hors service d'un site connecté, StorageGRID commence à supprimer les données d'objet du site sélectionné dès que vous activez la nouvelle stratégie ILM. Le déplacement ou la suppression de toutes les copies d'objets peut prendre des semaines. Bien que vous puissiez démarrer en toute sécurité la mise hors service d'un site alors que les données d'objet existent toujours sur le site, la procédure de mise hors service s'exécutera plus rapidement et avec moins d'interruptions et d'impacts sur les performances si vous autorisez le déplacement des données du site avant de démarrer la procédure de mise hors service proprement dite (en sélectionnant **Démarrer la mise hors service** à l'étape 5 de l'assistant).

4. Pour chaque politique *inactive*, modifiez-la ou supprimez-la en sélectionnant d'abord le lien de chaque politique comme décrit dans les étapes précédentes.
 - "[Modifier la politique](#)" il ne s'agit donc pas du site à démanteler.
 - "[Supprimer une politique](#)".
5. Une fois que vous avez terminé d'apporter des modifications aux règles et politiques ILM, aucune autre politique ne devrait être répertoriée à l'étape 3 (Réviser les politiques ILM). Sélectionnez **Suivant**.

L'étape 4 (Supprimer les références ILM) apparaît.

Étape 4 : Supprimer les références ILM

À partir de l'étape 4 (Supprimer les références ILM) de l'assistant de mise hors service du site, vous devez supprimer ou modifier toutes les règles ILM inutilisées qui font référence au site, même si les règles ne sont utilisées dans aucune stratégie ILM.

Étapes

1. Déterminez si des règles ILM inutilisées font référence au site.

Si des règles ILM sont répertoriées, ces règles font toujours référence au site mais ne sont utilisées dans aucune politique.



Lorsque StorageGRID met hors service le site, il désactive automatiquement tous les profils de codage d'effacement inutilisés qui font référence au site et supprime automatiquement tous 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.

2. Modifier ou supprimer chaque règle inutilisée :

- Pour modifier une règle, accédez à la page des règles ILM et mettez à jour tous les emplacements qui utilisent un profil de codage d'effacement ou un pool de stockage faisant référence au site. Ensuite, revenez à l'**Étape 4 (Supprimer les références ILM)**.
- Pour supprimer une règle, sélectionnez l'icône de la corbeille  et sélectionnez **OK**.



Vous devez supprimer la règle **Créer 2 copies** avant de pouvoir mettre hors service un site.

3. Confirmez qu'aucune règle ILM inutilisée ne fait référence au site et que le bouton **Suivant** est activé.

4. Sélectionnez **Suivant**.



Tous les pools de stockage et profils de codage d'effacement restants qui font référence au site deviendront invalides lorsque le site sera supprimé. Lorsque StorageGRID met hors service le site, il désactive automatiquement tous les profils de codage d'effacement inutilisés qui font référence au site et supprime automatiquement tous 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) apparaît.

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 de mise hors service du site, vous pouvez déterminer si des nœuds de votre système StorageGRID sont déconnectés ou si des nœuds du site sélectionné appartiennent à un groupe de haute disponibilité (HA). Une fois les conflits de nœuds résolus, 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 correct, comme suit :

- Tous les nœuds de votre système StorageGRID doivent être connectés ().



Si vous effectuez une mise hors service d'un 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 démarrera pas si un ou plusieurs volumes sont hors ligne (démontés) ou s'ils sont en ligne (montés) mais dans un état d'erreur.



Si un ou plusieurs volumes sont mis hors ligne pendant qu'une mise hors service est en cours, le processus de mise hors service se termine une fois que ces volumes sont remis en ligne.

- Aucun nœud du site que vous supprimez ne peut avoir une interface appartenant à un groupe de haute disponibilité (HA).

À propos de cette tâche

Si un nœud est répertorié pour l'étape 5 (Résoudre les conflits de nœuds), vous devez corriger le problème avant de pouvoir démarrer la mise hors service.

Avant de commencer la procédure de déclassement du site à partir de cette page, passez en revue les considérations suivantes :

- Vous devez prévoir suffisamment de temps pour que la procédure de mise hors service soit terminée.



Le déplacement ou la suppression des données d'objet d'un site peut prendre des jours, des semaines, voire des mois, en fonction de la quantité de données sur le site, de la charge sur votre système, des latences du réseau et de la nature des modifications ILM requises.

- Pendant que la procédure de déclassement du site est en cours :
 - Vous ne pouvez pas créer de règles ILM qui font référence au site en cours de mise hors service. 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 suspendre la procédure pendant la suppression des nœuds de stockage. Le bouton **Pause** est activé pendant l'étape « Décommissionnement des données répliquées et codées par effacement ».

- Si vous devez récupérer un nœud après avoir démarré la procédure de mise hors service du site, vous devez contacter le support.

Étapes

1. Consultez la section des nœuds déconnectés de l'étape 5 (Résoudre les conflits de nœuds) pour déterminer si des nœuds de votre système StorageGRID ont un état de connexion inconnu () ou administrativement vers le bas ().

Decommission Site



Before you can decommission the site, you must ensure the following:

- All nodes in your StorageGRID system are connected.
Note: If you are performing a disconnected site decommission, all nodes at the site you are removing must be disconnected.
- No node at the selected site belongs to a high availability (HA) group.

If a node is listed in either table, you must correct the issue before you can continue.

1 disconnected node in the grid

The following nodes have a Connection State of Unknown (blue) or Administratively Down (gray). You must bring these disconnected nodes back online.

For help bringing nodes back online, see the instructions for [monitoring and troubleshooting StorageGRID](#) and the [recovery and maintenance](#) instructions.

Node Name	Connection State	Site	Type
DC1-S3-99-193	Administratively Down	Data Center 1	Storage Node

1 node in the selected site belongs to an HA group

Passphrase

Provisioning Passphrase

Previous

Start Decommission

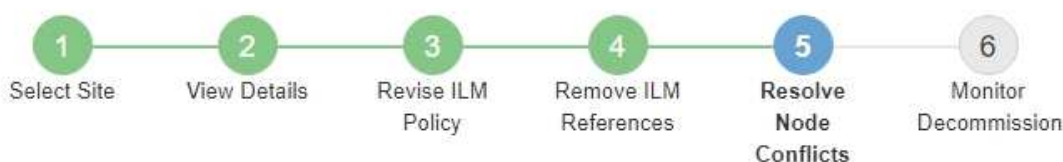
2. Si des nœuds sont déconnectés, remettez-les en ligne.

Voir le "[Procédures de nœud](#)". Contactez le support technique si vous avez besoin d'aide.

3. Une fois tous les nœuds déconnectés remis en ligne, consultez la section Groupes HA de l'étape 5 (Résoudre les conflits de nœuds).

Ce tableau répertorie tous les nœuds du site sélectionné qui appartiennent à un groupe de haute disponibilité (HA).

Decommission Site



Before you can decommission the site, you must ensure the following:

- All nodes in your StorageGRID system are connected.
Note: If you are performing a disconnected site decommission, all nodes at the site you are removing must be disconnected.
- No node at the selected site belongs to a high availability (HA) group.

If a node is listed in either table, you must correct the issue before you can continue:

All grid nodes are connected

1 node in the selected site belongs to an HA group

The following nodes in the selected site belong to a high availability (HA) group. You must either edit the HA group to remove the node's interface or remove the entire HA group.

[Go to HA Groups page.](#)

For information about HA groups, see the instructions for [administering StorageGRID](#)

HA Group Name	Node Name	Node Type
HA group	DC1-GW1-99-190	API Gateway Node

Passphrase

Provisioning Passphrase ?

Previous

Start Decommission

4. Si des nœuds sont répertoriés, effectuez l'une des opérations suivantes :

- Modifiez chaque groupe HA affecté pour supprimer l'interface de nœud.
- Supprimez un groupe HA qui inclut uniquement les nœuds de ce site. Consultez 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 de provisionnement** est activé.

5. Saisissez la phrase secrète d'approvisionnement.

Le bouton **Démarrer la mise hors service** devient activé.

Decommission Site



Before you can decommission the site, you must ensure the following:

- All nodes in your StorageGRID system are connected.
Note: If you are performing a disconnected site decommission, all nodes at the site you are removing must be offline.
- No node at the selected site belongs to a high availability (HA) group.

If a node is listed in either table, you must correct the issue before you can continue.

All grid nodes are connected

No nodes in the selected site belong to an HA group

Passphrase

Provisioning Passphrase ?

.....|

Previous

Start Decommission

6. Si vous êtes prêt à démarrer la procédure de déclassement du site, sélectionnez **Démarrer la déclassement**.

Un avertissement répertorie le site et les nœuds qui seront supprimés. Nous vous rappelons qu'il faudra peut-être des jours, des semaines, voire des mois pour supprimer complètement le site.

Warning

The following site and its nodes have been selected for decommissioning and will be permanently removed from the StorageGRID system:

Data Center 3

- DC3-S1
- DC3-S2
- DC3-S3

When StorageGRID removes a site, it temporarily uses strong-site consistency to prevent object metadata from being written to the site being removed. Client write and delete operations can fail if multiple nodes become unavailable at the remaining sites.

This procedure might take days, weeks, or even months to complete. Select **Maintenance > Decommission** to monitor the decommission progress.

Do you want to continue?

Cancel

OK

7. Relisez l'avertissement. Si vous êtes prêt à commencer, sélectionnez **OK**.

Un message apparaît lorsque la nouvelle configuration de grille est générée. Ce processus peut prendre un certain temps, en fonction du type et du nombre de nœuds de réseau mis hors service.

Passphrase

Provisioning Passphrase 

 Generating grid configuration. This may take some time depending on the type and the number of decommissioned grid nodes.

Previous

Start Decommission 

Une fois la nouvelle configuration de grille générée, l'étape 6 (Décommission du moniteur) s'affiche.



Le bouton **Précédent** 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 (Surveillance de la mise hors service) de l'assistant de la page Mise hors service du site, vous pouvez surveiller la progression à mesure que le site est supprimé.

À propos de cette tâche

Lorsque StorageGRID supprime un site connecté, il supprime les nœuds dans cet ordre :

1. Nœuds de passerelle
2. Nœuds d'administration
3. Nœuds de stockage

Lorsque StorageGRID supprime un site déconnecté, il supprime les nœuds dans cet ordre :

1. Nœuds de passerelle
2. Nœuds de stockage
3. Nœuds d'administration

Chaque nœud de passerelle ou nœud d'administration peut ne nécessiter que quelques minutes ou une heure pour être supprimé ; cependant, les nœuds de stockage peuvent prendre des jours ou des semaines.

Étapes

1. Dès qu'un nouveau package de récupération a été généré, téléchargez le fichier.

Decommission Site



 A new Recovery Package has been generated as a result of the configuration change. Go to the [Recovery Package](#) page to download it.



Téléchargez le package de récupération dès que possible pour vous assurer de pouvoir récupérer votre réseau en cas de problème lors de la procédure de mise hors service.

- a. Sélectionnez le lien dans le message ou sélectionnez **MAINTENANCE > Système > Pack de récupération**.
- b. Téléchargez le .zip déposer.

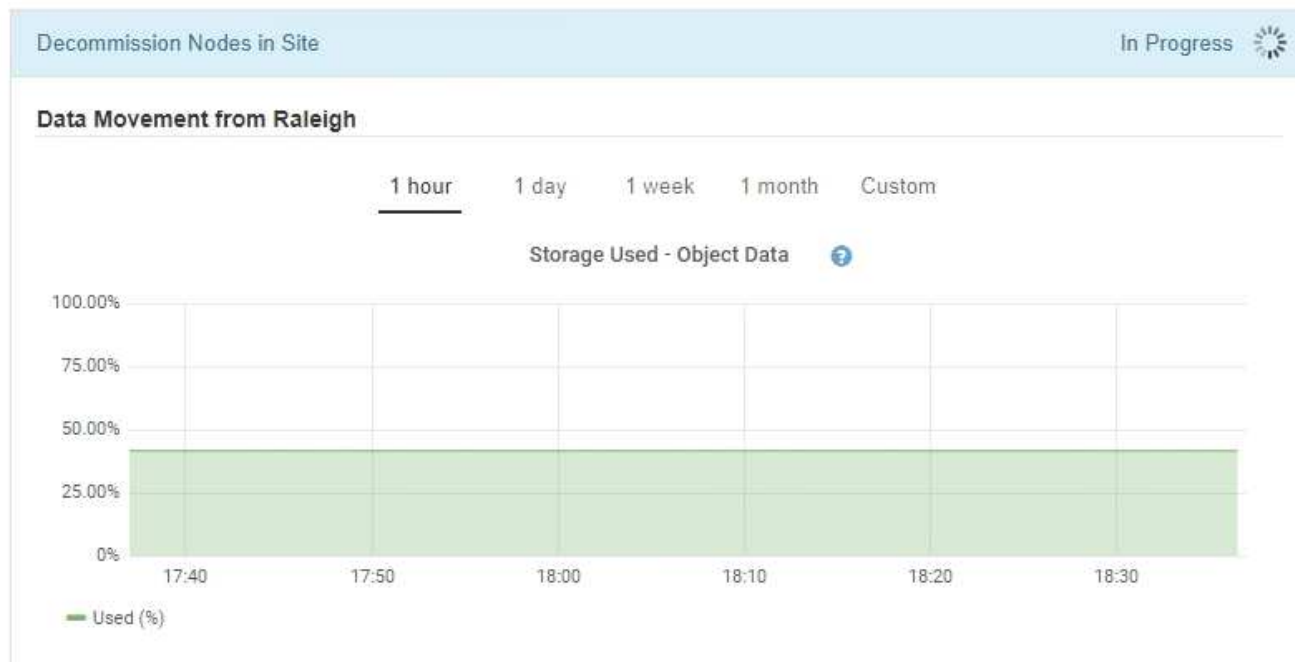
Voir les instructions pour "[téléchargement du package de récupération](#)".



Le fichier du package de récupération doit être sécurisé car il contient des clés de chiffrement et des mots de passe qui peuvent être utilisés pour obtenir des données à partir du système StorageGRID .

2. À l'aide du graphique de mouvement des données, surveillez le mouvement des données d'objet de ce site vers d'autres sites.

Le déplacement des données a commencé lorsque vous avez activé la nouvelle politique ILM à l'étape 3 (Réviser la politique ILM). Le déplacement des données se produira 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 à mesure que les nœuds sont supprimés.

Lorsqu'un nœud de stockage est supprimé, chaque nœud passe par une série d'étapes. Bien que la plupart de ces étapes se produisent rapidement, voire imperceptiblement, vous devrez peut-être attendre des jours, voire des semaines, pour que d'autres étapes se terminent, en fonction de la quantité de données à déplacer. Un délai supplémentaire est nécessaire pour gérer les données codées par effacement et réévaluer l'ILM.

Node Progress

 Depending on the number of objects stored, Storage Nodes might take significantly longer to decommission. Extra time is needed to manage erasure coded data and re-evaluate ILM.

The progress for each node is displayed while the decommission procedure is running. If you need to perform another maintenance procedure, select **Pause** to suspend the decommission (only allowed during certain stages).

Pause **Resume**



Name	Type	Progress	Stage
RAL-S1-101-196	Storage Node		Decommissioning Replicated and Erasure Coded Data
RAL-S2-101-197	Storage Node		Decommissioning Replicated and Erasure Coded Data
RAL-S3-101-198	Storage Node		Decommissioning Replicated and Erasure Coded Data

Si vous surveillez la progression de la mise hors service d'un site connecté, reportez-vous à ce tableau pour comprendre les étapes de mise hors service d'un nœud de stockage :

Scène	Durée estimée
En attente	Minute ou moins
Attendre les écluses	Minutes
Préparer la tâche	Minute ou moins
Marquage LDR déclassé	Minutes
Mise hors service des données répliquées et codées par effacement	Heures, jours ou semaines en fonction de la quantité de données Remarque : si vous devez effectuer d'autres activités de maintenance, vous pouvez suspendre la mise hors service du site pendant cette étape.
État de l'ensemble LDR	Minutes
Vider les files d'attente d'audit	De quelques minutes à quelques heures, en fonction du nombre de messages et de la latence du réseau.
Complet	Minutes

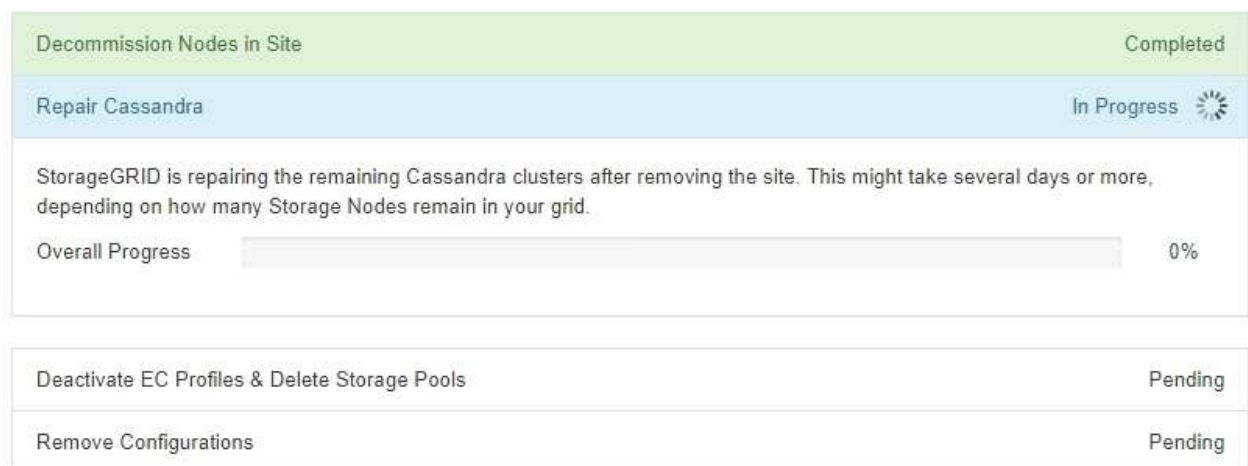
Si vous surveillez la progression de la mise hors service d'un site déconnecté, reportez-vous à ce tableau pour comprendre les étapes de mise hors service d'un nœud de stockage :

Scène	Durée estimée
En attente	Minute ou moins
Attendre les écluses	Minutes
Préparer la tâche	Minute ou moins
Désactiver les services externes	Minutes
Révocation du certificat	Minutes
Désinscription du nœud	Minutes
Désenregistrement du niveau de stockage	Minutes
Suppression du groupe de stockage	Minutes

Scène	Durée estimée
Suppression d'entité	Minutes
Complet	Minutes

4. Une fois que tous les nœuds ont atteint l'étape Terminé, attendez que les opérations de mise hors service du site restantes soient terminées.
 - Au cours de l'étape **Réparer Cassandra**, StorageGRID effectue les réparations nécessaires sur les clusters Cassandra qui restent dans votre grille. Ces réparations peuvent prendre plusieurs jours, voire plus, selon le nombre de nœuds de stockage restants dans votre réseau.

Decommission Site Progress



- 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 codage d'effacement faisant référence au site sont désactivés.
 - Tous les pools de stockage faisant référence au site sont supprimés.



Le pool de stockage Tous les nœuds de stockage (StorageGRID 11.6 et versions antérieures) est également supprimé car il utilise le site Tous les sites.

- Enfin, lors de l'étape **Supprimer la configuration**, toutes les références restantes au site et à ses nœuds sont supprimées du reste de la grille.

Decommission Site Progress

Decommission Nodes in Site	Completed
Repair Cassandra	Completed
Deactivate EC Profiles & Delete Storage Pools	Completed
Remove Configurations	In Progress 
StorageGRID is removing the site and node configurations from the rest of the grid.	

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.

Decommission Site



The previous decommission procedure completed successfully at 2021-01-12 14:28:32 MST.

When you decommission a site, all nodes at the site and the site itself are permanently removed from the StorageGRID system.

Review the table for the site you want to remove. If Decommission Possible is Yes, select the site. Then, select **Next** to ensure that the site is not referred to by ILM and that all StorageGRID nodes are in the correct state.

You might not be able to remove certain sites. For example, you cannot decommission the site that contains the primary Admin Node or a site that contains an Archive Node.

Sites

	Site Name	Used Storage Capacity 	Decommission Possible
☒	Sunnyvale	4.79 MB	
☐	Vancouver	4.90 MB	No. This site contains the primary Admin Node.

Next

Après avoir terminé

Effectuez ces tâches après avoir terminé la procédure de déclassement du site :

- Assurez-vous que les lecteurs 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 en toute sécurité les données des lecteurs.
- Si le site comprend un ou plusieurs nœuds d'administration et que l'authentification unique (SSO) est activée pour votre système StorageGRID, supprimez toutes les approbations de parties de confiance pour le site des services de fédération Active Directory (AD FS).
- Une fois les nœuds mis hors tension automatiquement dans le cadre de la procédure de mise hors service

du site connecté, supprimez les machines virtuelles associées.

Renommer la grille, le site ou le nœud

Utiliser la procédure de renommage

Selon vos besoins, 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 quand vous en avez besoin.

Quelle est la procédure de renommage ?

Lorsque vous installez StorageGRID initialement, vous spécifiez un nom pour la grille, chaque site et chaque nœud. Ces noms initiaux sont connus sous le nom de *noms de système* et ce sont les noms initialement affichés dans StorageGRID.

Les noms de système sont requis pour les opérations StorageGRID internes et ne peuvent pas être modifiés. Cependant, vous pouvez utiliser la procédure de renommage pour définir de nouveaux *noms d'affichage* pour la grille, chaque site et chaque nœud. Ces noms d'affichage apparaissent dans divers emplacements StorageGRID à la place (ou dans certains cas, en plus) des noms de système sous-jacents.

Utilisez la procédure de renommage pour corriger les fautes de frappe, pour implémenter une convention de dénomination différente ou pour indiquer qu'un site et tous ses nœuds ont été déplacés. Contrairement aux noms système, les noms d'affichage peuvent être mis à jour à tout moment et sans impact sur les opérations StorageGRID .

Où apparaissent les noms du système et d'affichage ?

Le tableau suivant résume l'emplacement où les noms de système et les noms d'affichage sont affichés dans l'interface utilisateur StorageGRID et dans les fichiers StorageGRID .

Pays	Nom du système	Nom d'affichage
Pages du gestionnaire de grille	Affiché sauf si l'élément est renommé	Si un élément est renommé, il est affiché à la place du nom du système dans ces emplacements : • Tableau de bord • Page des nœuds • Pages de configuration pour les groupes de haute disponibilité, les points de terminaison d'équilibrage de charge, les interfaces VLAN, les serveurs de gestion de clés, les mots de passe de grille et le contrôle du pare-feu • Alertes • Définitions des pools 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, l'extension, la récupération et la vérification de l'existence des objets • Pages d'assistance (journaux et diagnostics) • Page d'authentification unique, à côté du nom d'hôte du nœud d'administration dans le tableau des détails du nœud d'administration
NODES > onglet Aperçu pour un nœud	Toujours affiché	Affiché uniquement si l'élément est renommé
Pages héritées dans le gestionnaire de grille (par exemple, SUPPORT > Topologie de la grille)	Montré	Non affiché
API node-health	Toujours revenu	Renvoyé uniquement si l'élément est renommé

Pays	Nom du système	Nom d’affichage
Invite lors de l’utilisation de SSH pour accéder à un nœud	Affiché comme nom principal, sauf si l’élément a été renommé : <pre>admin@SYSTEM-NAME: ~ \$</pre> Inclus entre parenthèses lorsque l’élément est renommé : <pre>admin@DISPLAY-NAME (SYSTEM-NAME) :~ \$</pre>	Affiché comme nom principal lorsque l’élément est renommé : <pre>admin@DISPLAY-NAME (SYSTEM-NAME) :~ \$</pre>
`Passwords.txt` fichier dans le package de récupération	Montré comme Server Name	Montré comme Display Name
`/etc/hosts` fichier sur tous les nœuds Par exemple: <pre>10.96.99.128 SYSTEM-NAME 28989c59-a2c3-4d30-bb09-6879adf2437f DISPLAY-NAME localhost-grid # storagegrid-gen-host</pre>	Toujours affiché dans la deuxième colonne	Lorsque l’élément est renommé, affiché 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 à leurs noms d’affichage.

Exigences relatives au nom d’affichage

Avant d’utiliser cette procédure, vérifiez les exigences relatives aux noms d’affichage.

Noms d’affichage des nœuds

Les noms d’affichage des nœuds doivent suivre ces règles :

- Doit être unique sur 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 pas plus de 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 trait d’union.
- Ça ne peut pas être que des chiffres.

- 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 qui était précédemment utilisé par un autre nœud, à condition que le changement de nom n’entraîne pas un nom d’affichage ou un nom système en double.

Noms d’affichage pour la grille et les sites

Les noms d’affichage de la grille et des sites suivent les mêmes règles, à l’exception de ces exceptions :

- Peut inclure des espaces.
- Peut inclure ces caractères spéciaux : = - _ : , . @ !
- Peut commencer et se terminer par des caractères spéciaux, y compris des tirets.
- Peut être composé uniquement de chiffres ou de caractères spéciaux.

Meilleures pratiques en matière de nom d’affichage

Si vous prévoyez de renommer plusieurs éléments, documentez votre schéma de dénomination général avant d’utiliser cette procédure. Élaborez un système garantissant que les noms sont uniques, cohérents et faciles à comprendre en un coup d’œil.

Vous pouvez utiliser n’importe quelle convention de dénomination adaptée aux besoins de votre organisation. Tenez compte de ces suggestions de base sur ce qu’il faut inclure :

- **Indicateur de site** : Si vous avez plusieurs sites, ajoutez un code de site à chaque nom de nœud.
- **Type de nœud** : les noms de nœuds indiquent généralement le type de nœud. Vous pouvez utiliser des abréviations telles que `s` , `adm` , et `gw` (Nœud de stockage, nœud d’administration et nœud de passerelle).
- **Numéro de nœud** : si un site contient plusieurs nœuds d’un type particulier, ajoutez un numéro unique au nom de chaque nœud.

Réfléchissez à deux fois avant d’ajouter des détails spécifiques aux noms qui sont 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, les emplacements des racks ou les numéros de modèle des appareils peuvent changer si vous déplacez l’équipement ou mettez à niveau le matériel.

Exemples de noms d’affichage

Supposons que votre système StorageGRID dispose de trois centres de données et de nœuds de types différents dans chaque centre de données. 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 avez le ["Autorisation d’accès de maintenance ou root"](#) .
- Vous disposez de la phrase secrète de provisionnement.
- Vous comprenez les exigences et les meilleures pratiques relatives aux noms d’affichage. Voir ["Renommer la grille, les sites et les nœuds"](#) .

Comment renommer une grille, des sites ou des nœuds

Vous pouvez renommer votre système StorageGRID , un ou plusieurs sites ou un ou plusieurs nœuds.

Vous pouvez utiliser un nom d’affichage qui a déjà été utilisé par un autre nœud, à condition que le changement de nom n’entraîne pas un nom d’affichage ou un nom système en double.

Sélectionnez les éléments à renommer

Pour commencer, sélectionnez les éléments que vous souhaitez 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	Instruction
Noms de tout (ou presque tout) dans votre système	a. Sélectionnez Sélectionner tout . b. Vous pouvez également effacer tous les éléments que vous ne souhaitez pas renommer.
Nom de la grille	Cochez la case correspondant à 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. Vous pouvez également effacer tous les nœuds que vous ne souhaitez pas renommer.
Nom d'un site	Cochez la case correspondant au site.
Nom d'un nœud	Cochez la case correspondant au nœud.

3. Sélectionnez **Continuer**.

4. Consultez le tableau, qui comprend 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 lors 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 être son nom d'hôte.
- La colonne **Type** indique le type de l'élément : Grille, Site ou le type spécifique de nœud.

Proposer de nouveaux noms

Pour l'étape **Proposer de nouveaux noms**, vous pouvez saisir un nom d'affichage pour chaque élément individuellement ou renommer les éléments en bloc.

Renommer les éléments individuellement

Suivez ces étapes pour saisir un nom d’affichage pour chaque élément que vous souhaitez renommer.

Étapes

1. Dans le champ **Nom d’affichage**, saisissez un nom d’affichage proposé pour chaque élément de la liste.

Voir ["Renommer la grille, les sites et les nœuds"](#) pour apprendre les exigences de dénomination.

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 du tableau.

3. Lorsque vous avez proposé de nouveaux noms pour tous les éléments du tableau, sélectionnez **Renommer**.

Un message de réussite apparaît. Les nouveaux noms d’affichage sont désormais utilisés dans tout Grid Manager.

Renommer des éléments en masse

Utilisez l’outil de renommage en masse si les noms d’éléments partagent une chaîne commune que vous souhaitez remplacer par une chaîne différente.

Étapes

1. Pour l’étape **Proposer de nouveaux noms**, sélectionnez **Utiliser l’outil de renommage en masse**.

L’**Aperçu de renommage** inclut tous les éléments qui ont été affichés pour l’étape **Proposer de nouveaux noms**. Vous pouvez utiliser l’aperçu pour voir à quoi ressembleront les noms d’affichage après avoir remplacé une chaîne partagée.

2. Dans le champ **Chaîne existante**, saisissez 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 partout où il se trouve dans les noms sur la gauche.

3. Sélectionner  pour supprimer tous 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. Sélectionner  pour supprimer le site de l’aperçu de renommage.

Bulk rename tool

Rename preview ?

Data-Center-1

X

Data-Center-1-ADM1

X

Data-Center-1-ARC1

X

Data-Center-1-G1

X

Data-Center-1-S1

X

Data-Center-1-S2

X

Data-Center-1-S3

X

Data-Center-1-S4

▼

Cancel

Add names

Enter the shared string you want to replace. Then, enter a new string to use instead. Optionally, remove any items that you do not want to rename with this tool.

Existing string

Data-Center-1

The string you want to replace. Represented by *italicized text* in the preview section.

New string

The string you want to use instead. Represented by **bolded text** in the preview section.

4. Dans le champ **Nouvelle chaîne**, saisissez la chaîne de remplacement que vous souhaitez utiliser à la place. Par exemple, entrez **DC1**.

Voir "[Renommer la grille, les sites et les nœuds](#)" pour apprendre les exigences de dénomination.

Au fur et à mesure que vous entrez la chaîne de remplacement, les noms sur la gauche sont mis à jour, vous pouvez donc vérifier que les nouveaux noms seront corrects.

1469

Bulk rename tool

×

Rename preview ?

DC1-ADM1 ✕

DC1-ARC1 ✕

DC1-G1 ✕

DC1-S1 ✕

DC1-S2 ✕

DC1-S3 ✕

DC1-S4 ✕

Cancel

Add names

Enter the shared string you want to replace. Then, enter a new string to use instead. Optionally, remove any items that you do not want to rename with this tool.

Existing string

Data-Center-1

The string you want to replace. Represented by *italicized text* in the preview section.

New string

DC1

The string you want to use instead. Represented by **bolded text** in the preview section.

- Lorsque vous êtes satisfait des noms affichés dans l'aperçu, sélectionnez **Ajouter des noms** pour ajouter les noms au tableau pour l'étape **Proposer de nouveaux noms**.
- Apportez les modifications supplémentaires requises ou sélectionnez ✕ pour supprimer tous les éléments que vous ne souhaitez pas renommer.
- Lorsque vous êtes prêt à renommer tous les éléments du tableau, sélectionnez **Renommer**.

Un message de réussite s'affiche. Les nouveaux noms d'affichage sont désormais utilisés dans tout Grid Manager.

Télécharger le package de récupération

Une fois que vous avez terminé de renommer les 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` déposer.

Étapes

- Saisissez la phrase secrète d'approvisionnement.
- Sélectionnez **Télécharger le package de récupération**.

Le téléchargement démarre immédiatement.

- Une fois le téléchargement terminé, ouvrez le `Passwords.txt` fichier pour voir le nom du serveur pour tous les nœuds et les noms d'affichage pour tous les nœuds renommés.
- Copiez le `sgws-recovery-package-id-revision.zip` fichier dans deux emplacements sûrs, sécurisés et séparés.



Le fichier du package de récupération doit être sécurisé car il contient des clés de chiffrement et des mots de passe qui peuvent être utilisés pour obtenir des données à partir du système StorageGRID .

5. Sélectionnez **Terminer** pour revenir à la première étape.

Rétablir les noms d’affichage aux noms système

Vous pouvez rétablir le nom système d’origine d’une grille, d’un site ou d’un nœud renommé. Lorsque vous rétablissez le nom système d’un élément, les pages Grid Manager et les autres emplacements StorageGRID n’affichent plus de **Nom d’affichage** pour cet élément. Seul le nom du 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 pour lesquels vous souhaitez rétablir les noms système.
3. Sélectionnez **Continuer**.
4. Pour l’étape **Proposer de nouveaux noms**, rétablissez les noms d’affichage aux noms système 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 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.

- b. Sélectionnez **Renommer**.

Un message de réussite apparaît. Les noms d'affichage de ces éléments ne sont plus utilisés.

Revenir aux noms de système en masse

- a. Pour l'étape **Proposer de nouveaux noms**, sélectionnez **Utiliser l'outil de renommage en masse**.
- b. Dans le champ **Chaîne existante**, saisissez la chaîne de nom d'affichage que vous souhaitez remplacer.
- c. Dans le champ **Nouvelle chaîne**, saisissez la chaîne de nom du système que vous souhaitez utiliser à la place.
- d. Sélectionnez **Ajouter des noms** pour ajouter les noms au tableau pour l'étape **Proposer de nouveaux noms**.
- e. Confirmez que chaque entrée dans le champ **Nom d'affichage** correspond au nom dans le champ **Nom du système**. Apportez des 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 rétablis ne sont plus inclus dans le `Passwords.txt` déposer.

Procédures de nœud

Procédures de maintenance des nœuds

Vous devrez peut-être effectuer des procédures de maintenance liées à des nœuds de grille ou à des services de nœuds spécifiques.

Procédures du gestionnaire de serveur

Le gestionnaire de serveur s'exécute sur chaque nœud de grille pour superviser le démarrage et l'arrêt des services et pour garantir que les services rejoignent et quittent correctement le système StorageGRID . Le gestionnaire de serveur surveille également les services sur chaque nœud de grille et tente automatiquement de redémarrer tous les services qui signalent des pannes.

Pour exécuter les procédures du Gestionnaire de serveur, vous devez généralement accéder à la ligne de commande du nœud.



Vous ne devez accéder au Gestionnaire de serveur que si le support technique vous a demandé de le faire.



Vous devez fermer la session de l'interpréteur de commandes en cours et vous déconnecter une fois que vous avez terminé avec le Gestionnaire de serveur. Entrer: `exit`

Procédures de redémarrage, d'arrêt et d'alimentation du nœud

Vous utilisez ces procédures pour redémarrer un ou plusieurs nœuds, pour arrêter et redémarrer des nœuds ou pour éteindre et rallumer des nœuds.

Procédures de remappage des ports

Vous pouvez utiliser les procédures de remappage de port pour supprimer les remappages de port d'un nœud, par exemple, si vous souhaitez configurer un point de terminaison d'équilibrage de charge à l'aide d'un port précédemment remappé.

Procédures du gestionnaire de serveur

Afficher l'état et la version du gestionnaire de serveur

Pour chaque nœud de grille, vous pouvez afficher l'état actuel et la version du Gestionnaire de serveur 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` déposer.

Étapes

1. Connectez-vous au nœud de grille :
 - a. Entrez la commande suivante : `ssh admin@grid_node_IP`
 - b. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.
 - c. Entrez la commande suivante pour passer en root : `su -`
 - d. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.

Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

2. Afficher l'état actuel du Gestionnaire de serveur en cours d'exécution sur le nœud de grille : **`service servermanager status`**

L'état actuel du Gestionnaire de serveur en cours d'exécution sur le nœud de grille est signalé (en cours d'exécution ou non). Si l'état du Gestionnaire de serveur est `running`, le temps d'exécution depuis le dernier démarrage est indiqué. Par exemple:

```
servermanager running for 1d, 13h, 0m, 30s
```

3. Afficher la version actuelle du Gestionnaire de serveur 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 de l'interpréteur de commandes : **exit**

Afficher l'état actuel de tous les services

Vous pouvez afficher l'état actuel de tous les services exécutés sur un nœud de grille à tout moment.

Avant de commencer

Vous avez le `Passwords.txt` déposer.

Étapes

1. Connectez-vous au nœud de grille :
 - a. Entrez la commande suivante : `ssh admin@grid_node_IP`
 - b. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.
 - c. Entrez la commande suivante pour passer en root : `su -`
 - d. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.

Lorsque vous êtes connecté en tant que root, l'invite passe de \$ à # .

2. Afficher l'état de tous les services exécutés sur le nœud de grille : `storagegrid-status`

Par exemple, la sortie du nœud d'administration principal indique que l'état actuel des services AMS, CMN et NMS est En cours d'exécution. Cette sortie est mise à jour immédiatement si l'état d'un service change.

```

Host Name          190-ADM1
IP Address
Operating System Kernel 4.9.0      Verified
Operating System Environment Debian 9.4    Verified
StorageGRID Webscale Release 11.1.0    Verified
Networking          Verified
Storage Subsystem    Verified
Database Engine      5.5.9999+default Running
Network Monitoring   11.1.0     Running
Time Synchronization 1:4.2.8p10+dfsg Running
ams                  11.1.0     Running
cmn                  11.1.0     Running
nms                  11.1.0     Running
ssm                  11.1.0     Running
mi                   11.1.0     Running
dynip                11.1.0     Running
nginx                1.10.3     Running
tomcat               8.5.14     Running
grafana              4.2.0      Running
mgmt api             11.1.0     Running
prometheus           1.5.2+ds   Running
persistence          11.1.0     Running
ade exporter         11.1.0     Running
attrDownPurge        11.1.0     Running
attrDownSampl        11.1.0     Running
attrDownSamp2        11.1.0     Running
node exporter        0.13.0+ds  Running

```

3. Revenez à la ligne de commande, appuyez sur **Ctrl+C**.
4. Vous pouvez également afficher un rapport statique pour tous les services exécutés sur le nœud de grille :
`/usr/local/servermanager/reader.rb`

Ce rapport inclut 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 de l'interpréteur de commandes : `exit`

Démarrer le Gestionnaire de serveur et tous les services

Vous devrez peut-être démarrer le Gestionnaire de serveur, qui démarre également tous les services sur le nœud de grille.

Avant de commencer

Vous avez le `Passwords.txt` déposer.

À propos de cette tâche

Le démarrage du Gestionnaire de serveur sur un nœud de grille où il est déjà en cours d'exécution entraîne un redémarrage du Gestionnaire de serveur et de tous les services sur le nœud de grille.

Étapes

1. Connectez-vous au nœud de grille :
 - a. Entrez la commande suivante : `ssh admin@grid_node_IP`
 - b. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.
 - c. Entrez la commande suivante pour passer en root : `su -`

d. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.

Lorsque vous êtes connecté en tant que root, l'invite passe de \$ à # .

2. Démarrer le gestionnaire de serveur : `service servermanager start`

3. Déconnectez-vous de l'interpréteur de commandes : `exit`

Redémarrez le Gestionnaire de serveur et tous les services

Vous devrez peut-être redémarrer le gestionnaire de serveur et tous les services exécutés sur un nœud de grille.

Avant de commencer

Vous avez le `Passwords.txt` déposer.

Étapes

1. Connectez-vous au nœud de grille :

a. Entrez la commande suivante : `ssh admin@grid_node_IP`

b. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.

c. Entrez la commande suivante pour passer en root : `su -`

d. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.

Lorsque vous êtes connecté en tant que root, l'invite passe de \$ à # .

2. Redémarrez le Gestionnaire de serveur et tous les services sur le nœud de grille : `service servermanager restart`

Le gestionnaire de serveur et tous les services sur le nœud de grille sont arrêtés puis redémarrés.



En utilisant le `restart` commande est la même que l'utilisation de la `stop` commande suivie de la `start` commande.

3. Déconnectez-vous de l'interpréteur de commandes : `exit`

Arrêtez le gestionnaire de serveur et tous les services

Le Gestionnaire de serveur est conçu pour s'exécuter à tout moment, mais vous devrez peut-être arrêter le Gestionnaire de serveur et tous les services exécutés sur un nœud de grille.

Avant de commencer

Vous avez le `Passwords.txt` déposer.

Étapes

1. Connectez-vous au nœud de grille :

a. Entrez la commande suivante : `ssh admin@grid_node_IP`

- b. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.
- c. Entrez la commande suivante pour passer en root : `su -`
- d. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.

Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#` .

2. Arrêtez le gestionnaire de serveur et tous les services exécutés sur le nœud de grille : `service servermanager stop`

Le gestionnaire de serveur et tous les services exécutés sur le nœud de grille sont correctement arrêtés. L'arrêt des services peut prendre jusqu'à 15 minutes.

3. Déconnectez-vous de l'interpréteur de commandes : `exit`

Afficher l'état actuel du service

Vous pouvez afficher l'état actuel d'un service exécuté sur un nœud de grille à tout moment.

Avant de commencer

Vous avez le `Passwords.txt` déposer.

Étapes

1. Connectez-vous au nœud de grille :

- a. Entrez la commande suivante : `ssh admin@grid_node_IP`
- b. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.
- c. Entrez la commande suivante pour passer en root : `su -`
- d. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.

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 servicename status` L'état actuel du service demandé exécuté 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 de l'interpréteur de commandes : `exit`

Arrêter le service

Certaines procédures de maintenance nécessitent l'arrêt d'un seul service tout en maintenant les autres services du nœud de grille en cours d'exécution. Arrêtez les services individuels uniquement lorsque cela vous est demandé par une procédure de maintenance.

Avant de commencer

Vous avez le `Passwords.txt` déposer.

À propos de cette tâche

Lorsque vous utilisez ces étapes pour « arrêter administrativement » un service, le Gestionnaire de serveur ne redémarre pas automatiquement le service. Vous devez démarrer le service unique manuellement ou redémarrer le Gestionnaire de serveur.

Si vous devez arrêter le service LDR sur un nœud de stockage, sachez que l'arrêt du service peut prendre un certain temps s'il existe des connexions actives.

Étapes

1. Connectez-vous au nœud de grille :
 - a. Entrez la commande suivante : `ssh admin@grid_node_IP`
 - b. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.
 - c. Entrez la commande suivante pour passer en root : `su -`
 - d. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.

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
```



Les services peuvent prendre jusqu'à 11 minutes pour s'arrêter.

3. Déconnectez-vous de l'interpréteur de commandes : `exit`

Informations connexes

["Forcer la fin du service"](#)

Forcer la fin du service

Si vous devez arrêter un service immédiatement, vous pouvez utiliser le `force-stop` commande.

Avant de commencer

Vous avez le `Passwords.txt` déposer.

Étapes

1. Connectez-vous au nœud de grille :
 - a. Entrez la commande suivante : `ssh admin@grid_node_IP`
 - b. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.
 - c. Entrez la commande suivante pour passer en root : `su -`

d. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.

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 terminer le service.

3. Déconnectez-vous de l'interpréteur de commandes : `exit`

Démarrer ou redémarrer 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` déposer.

Étapes

1. Connectez-vous au nœud de grille :

- a. Entrez la commande suivante : `ssh admin@grid_node_IP`
- b. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.
- c. Entrez la commande suivante pour passer en root : `su -`
- d. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.

Lorsque vous êtes connecté en tant que root, l'invite passe de \$ à # .

2. Décidez quelle commande émettre, selon que le service est 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 actuellement en cours d'exécution, utilisez le `restart` commande pour arrêter le service puis le redémarrer : `service servicename restart`

Par exemple:

```
service ldr restart
```

+



En utilisant le `restart` commande est la même que l'utilisation de la `stop` commande suivie de la `start` commande. Vous pouvez émettre `restart` même si le service est actuellement arrêté.

3. Déconnectez-vous de l'interpréteur de commandes : `exit`

Utiliser un fichier DoNotStart

Si vous effectuez diverses procédures de maintenance ou de configuration sous la direction du support technique, il peut vous être demandé d'utiliser un fichier DoNotStart pour empêcher le démarrage des services lorsque le Gestionnaire de serveur 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 dont vous souhaitez empêcher le démarrage. Au démarrage, le Gestionnaire de serveur recherche le fichier DoNotStart. Si le fichier est présent, le service (et tous les services qui en dépendent) ne peuvent pas démarrer. Lorsque le fichier DoNotStart est supprimé, le service précédemment arrêté démarrera au prochain démarrage ou redémarrage du Gestionnaire de serveur. Les services ne démarrent pas automatiquement 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 un 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` déposer.

Étapes

1. Connectez-vous au nœud de grille :

- a. Entrez la commande suivante : `ssh admin@grid_node_IP`
- b. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.
- c. Entrez la commande suivante pour passer en root : `su -`
- d. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.

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 dont le démarrage doit être empêché. Par exemple,

```
touch /etc/sv/ldr/DoNotStart
```

Un fichier DoNotStart est créé. Aucun contenu de fichier n'est nécessaire.

Lorsque le Gestionnaire de serveur ou le nœud de grille est redémarré, le Gestionnaire de serveur redémarre, mais pas le service.

3. Déconnectez-vous de l'interpréteur de commandes : `exit`

Supprimer 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` déposer.

Étapes

1. Connectez-vous au nœud de grille :

- a. Entrez la commande suivante : `ssh admin@grid_node_IP`
- b. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.
- c. Entrez la commande suivante pour passer en root : `su -`
- d. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.

Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

2. Supprimez le fichier DoNotStart du répertoire de service : `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 de l'interpréteur de commandes : `exit`

Dépannage du gestionnaire de serveur

Si un problème survient lors de l'utilisation du Gestionnaire de serveur, vérifiez son fichier journal.

Les messages d'erreur liés au Gestionnaire de serveur sont capturés dans le fichier journal du Gestionnaire de serveur, qui se trouve à l'adresse : `/var/local/log/servermanager.log`

Consultez ce fichier pour les messages d'erreur concernant les échecs. Transmettez le problème au support technique si nécessaire. Il se peut que l'on vous demande de transmettre les fichiers journaux au support technique.

Service avec un état d'erreur

Si vous détectez qu'un service est entré dans un état d'erreur, essayez de redémarrer le service.

Avant de commencer

Vous avez le `Passwords.txt` déposer.

À propos de cette tâche

Le Gestionnaire de serveur surveille les services et redémarre ceux qui se sont arrêtés de manière inattendue. Si un service échoue, le Gestionnaire de serveur tente de le redémarrer. Si trois tentatives de démarrage d'un service échouent dans un délai de cinq minutes, le service entre dans un état d'erreur. Le Gestionnaire de serveur ne tente pas d'effectuer un autre redémarrage.

Étapes

1. Connectez-vous au nœud de grille :
 - a. Entrez la commande suivante : `ssh admin@grid_node_IP`
 - b. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.
 - c. Entrez la commande suivante pour passer en root : `su -`
 - d. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.
2. Confirmer l'état d'erreur du service : `service servicename status`

Par exemple:

```
service ldr status
```

Si le service est dans un état d'erreur, le message suivant est renvoyé : `servicename in error state`. Par exemple:

```
ldr in error state
```



Si l'état du service est `disabled`, voir les instructions pour ["suppression d'un fichier DoNotStart pour un service"](#).

3. Tentez 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 de l'interpréteur de commandes : `exit`

Procédures de redémarrage, d'arrêt et d'alimentation

Effectuer un redémarrage progressif

Vous pouvez effectuer un redémarrage progressif pour redémarrer plusieurs nœuds de grille sans provoquer d'interruption de service.

Avant de commencer

- Vous êtes connecté au gestionnaire de grille sur le nœud d'administration principal et vous utilisez un ["navigateur Web pris en charge"](#).



Vous devez être connecté au nœud d'administration principal pour effectuer cette procédure.

- Vous avez le ["Autorisation d'accès de maintenance ou root"](#).

À propos de cette tâche

Utilisez cette procédure si vous devez redémarrer plusieurs nœuds en même temps. Par exemple, vous pouvez utiliser cette procédure après avoir modifié le mode FIPS de la grille. ["Politique de sécurité TLS et SSH"](#). Lorsque le mode FIPS change, vous devez redémarrer tous les nœuds pour que la modification prenne effet.



Si vous n'avez besoin de redémarrer qu'un seul nœud, vous pouvez ["redémarrer le nœud à partir de l'onglet Tâches"](#).

Lorsque StorageGRID redémarre les nœuds de la grille, il émet le `reboot` commande sur chaque nœud, ce qui provoque l'arrêt et le redémarrage du nœud. Tous les services sont redémarrés automatiquement.

- Le redémarrage d'un nœud VMware redémarre la machine virtuelle.
- Le redémarrage d'un nœud Linux redémarre le conteneur.
- Le redémarrage d'un nœud d'appliance StorageGRID redémarre le contrôleur de calcul.

La procédure de redémarrage progressif peut redémarrer plusieurs nœuds en même temps, à ces exceptions près :

- Deux nœuds du même type ne seront pas redémarrés en même temps.
- Les nœuds de passerelle et les nœuds d'administration ne seront pas redémarrés en même temps.

Au lieu de cela, ces nœuds sont redémarrés séquentiellement pour garantir que les groupes HA, les données d'objet et les services de nœuds critiques restent toujours disponibles.

Lorsque vous redémarrez le nœud d'administration principal, votre navigateur perd temporairement l'accès au gestionnaire de grille, vous ne pouvez donc plus surveiller la procédure. Pour cette raison, le nœud d'administration principal est redémarré en dernier.

Effectuer un redémarrage progressif

Vous sélectionnez les nœuds que vous souhaitez redémarrer, vérifiez vos sélections, démarrez la procédure de redémarrage et surveillez la progression.

Sélectionner les nœuds

Dans un premier temps, accédez à la page de redémarrage progressif et sélectionnez les nœuds que vous souhaitez redémarrer.

Étapes

1. Sélectionnez **MAINTENANCE > Tâches > Redémarrage progressif**.
2. Vérifiez l'état de la connexion et les icônes d'alerte dans la colonne **Nom du nœud**.



Vous ne pouvez pas redémarrer un nœud s'il est déconnecté du réseau. Les cases à cocher sont désactivées pour les nœuds avec ces icônes :  ou .

3. Si des nœuds ont des alertes actives, consultez la liste des alertes dans la colonne **Résumé des alertes**.



Pour voir toutes les alertes actuelles pour un nœud, vous pouvez également sélectionner l'option **Nœuds > Onglet Aperçu**.

4. Vous pouvez également effectuer les actions recommandées pour résoudre les alertes actuelles.
5. En option, si tous les nœuds sont connectés et que vous souhaitez tous les redémarrer, cochez la case dans l'en-tête du tableau et sélectionnez **Sélectionner tout**. Sinon, sélectionnez chaque nœud que vous souhaitez redémarrer.

Vous pouvez utiliser les options de filtre du tableau pour afficher des sous-ensembles de nœuds. Par exemple, vous pouvez afficher et sélectionner uniquement les nœuds de stockage ou tous les nœuds d'un certain site.

6. Sélectionnez **Réviser la sélection**.

Sélection d'avis

À cette étape, vous pouvez déterminer la durée totale de la procédure de redémarrage et confirmer que vous avez sélectionné les nœuds appropriés.

1. Sur la page de sélection de révision, examinez le résumé, qui indique le nombre de nœuds qui seront redémarrés et le temps total estimé pour que tous les nœuds redémarrent.
2. En option, pour supprimer un nœud spécifique de la liste de redémarrage, sélectionnez **Supprimer**.
3. En option, pour ajouter d'autres nœuds, sélectionnez **Étape précédente**, sélectionnez les nœuds supplémentaires et sélectionnez **Vérifier la sélection**.
4. Lorsque vous êtes prêt à démarrer la procédure de redémarrage progressif pour tous les nœuds sélectionnés, sélectionnez **Redémarrer les nœuds**.
5. Si vous avez choisi de redémarrer le nœud d'administration principal, lisez le message d'information et sélectionnez **Oui**.



Le nœud d'administration principal sera le dernier nœud à redémarrer. Pendant le redémarrage de ce nœud, la connexion de votre navigateur sera perdue. Lorsque le nœud d'administration principal est à nouveau disponible, vous devez recharger la page de redémarrage progressif.

Surveiller un redémarrage progressif

Pendant que la procédure de redémarrage progressif est en cours d'exécution, vous pouvez la surveiller à partir du nœud d'administration principal.

Étapes

1. Passez en revue l'avancement général de l'opération, qui comprend les informations suivantes :
 - Nombre de nœuds redémarrés
 - Nombre de nœuds en cours de redémarrage
 - Nombre de nœuds restant à redémarrer
2. Consultez le tableau pour chaque type de nœud.

Les tableaux fournissent une barre de progression de l'opération sur chaque nœud et indiquent l'étape de redémarrage de ce nœud, qui peut être l'une des suivantes :

- En attente de redémarrage
- Arrêt des services
- Redémarrage du système
- Démarrage des services
- Redémarrage terminé

Arrêter la procédure de redémarrage progressif

Vous pouvez arrêter la procédure de redémarrage progressif à partir du nœud d'administration principal. Lorsque vous arrêtez la procédure, tous les nœuds dont le statut est « Arrêt des services », « Redémarrage du système » ou « Démarrage des services » termineront l'opération de redémarrage. Cependant, ces nœuds ne seront plus suivis dans le cadre de la procédure.

Étapes

1. Sélectionnez **MAINTENANCE > Tâches > Redémarrage progressif**.
2. À partir de l'étape **Redémarrage du moniteur**, sélectionnez **Arrêter la procédure de redémarrage**.

Redémarrer le nœud de grille à partir de l'onglet Tâches

Vous pouvez redémarrer un nœud de grille individuel à partir de l'onglet Tâches sur la page Nœuds.

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 de maintenance ou root"](#) .
- Vous disposez de la phrase secrète de provisionnement.
- Si vous redémarrez le nœud d'administration principal ou un nœud de stockage, vous avez examiné les considérations suivantes :
 - Lorsque vous redémarrez le nœud d'administration principal, votre navigateur perd temporairement l'accès au gestionnaire de grille.
 - Si vous redémarrez deux nœuds de stockage ou plus sur un site donné, vous risquez de ne pas pouvoir accéder à certains objets pendant la durée du redémarrage. Ce problème peut se produire si

une règle ILM utilise l'option d'ingestion **Double validation** (ou si une règle spécifie **Équilibré** et qu'il n'est pas possible de créer immédiatement toutes les copies requises). Dans ce cas, StorageGRID validera les objets nouvellement ingérés sur deux nœuds de stockage sur le même site et évaluera ILM ultérieurement.

- Pour vous assurer de pouvoir accéder à tous les objets pendant le redémarrage d'un nœud de stockage, arrêtez d'ingérer des objets sur un site pendant environ une heure avant de redémarrer le nœud.

À propos de cette tâche

Lorsque StorageGRID redémarre un nœud de grille, il émet le `reboot` commande sur le nœud, qui provoque l'arrêt et le redémarrage du nœud. Tous les services sont redémarrés automatiquement.

- Le redémarrage d'un nœud VMware redémarre la machine virtuelle.
- Le redémarrage d'un nœud Linux redémarre le conteneur.
- Le redémarrage d'un nœud d'appliance StorageGRID redémarre le contrôleur de calcul.



Si vous devez redémarrer plusieurs nœuds, vous pouvez utiliser le "[procédure de redémarrage progressif](#)".

Étapes

1. Sélectionnez **NODES**.
2. Sélectionnez le nœud de grille que vous souhaitez redémarrer.
3. Sélectionnez l'onglet **Tâches**.
4. Sélectionnez **Redémarrer**.

Une boîte de dialogue de confirmation apparaît. Si vous redémarrez le nœud d'administration principal, la boîte de dialogue de confirmation vous rappelle que la connexion de votre navigateur au gestionnaire de grille sera temporairement perdue lorsque les services seront arrêtés.

5. Saisissez la phrase secrète d'approvisionnement et sélectionnez **OK**.
6. Attendez que le nœud redémarre.

La fermeture des services peut prendre un certain temps.

Lorsque le nœud redémarre, l'icône grise (Administrativement arrêté) apparaît pour le nœud sur la page Nœuds. Lorsque tous les services ont redémarré et que le nœud est correctement connecté au réseau, la page Nœuds 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 au réseau.

Redémarrer le nœud de grille à partir de l'interpréteur de commandes

Si vous devez surveiller l'opération de redémarrage de plus près ou si vous ne parvenez pas à accéder au gestionnaire de grille, vous pouvez vous connecter au nœud de grille et exécuter la commande de redémarrage du gestionnaire de serveur à partir de l'interpréteur de commandes.

Avant de commencer

Vous avez le `Passwords.txt` déposer.

Étapes

1. Connectez-vous au nœud de grille :
 - a. Entrez la commande suivante : `ssh admin@grid_node_IP`
 - b. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.
 - c. Entrez la commande suivante pour passer en root : `su -`
 - d. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.

Lorsque vous êtes connecté en tant que root, l'invite passe de \$ à # .

2. En option, arrêtez les services : `service servermanager stop`

L'arrêt des services est une étape facultative, mais recommandée. L'arrêt des services peut prendre jusqu'à 15 minutes et vous souhaiterez peut-être vous connecter au système à distance pour surveiller le processus d'arrêt avant de redémarrer le nœud à l'étape suivante.

3. Redémarrer le nœud de grille : `reboot`
4. Déconnectez-vous de l'interpréteur de commandes : `exit`

Arrêter le nœud du réseau

Vous pouvez arrêter un nœud de grille à partir de l'interpréteur de commandes du nœud.

Avant de commencer

- Vous avez le `Passwords.txt` déposer.

À propos de cette tâche

Avant d'effectuer cette procédure, passez en revue ces considérations :

- En général, vous ne devez pas arrêter plus d'un nœud à la fois pour éviter les interruptions.
- N'arrêtez pas un nœud pendant une procédure de maintenance, sauf si la documentation ou le support technique vous le demande explicitement.
- Le processus d'arrêt est basé sur 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 sur un site, arrêtez d'ingérer des objets sur ce site pendant environ une heure avant d'arrêter les nœuds.

Si une règle ILM utilise l'option d'ingestion **Double validation** (ou si une règle utilise l'option **Équilibrée** 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 arrêtés, vous risquez de ne pas pouvoir accéder aux objets nouvellement ingérés pendant la durée de l'arrêt. Les opérations d'écriture peuvent également échouer si trop peu de nœuds de stockage restent disponibles sur le site. Voir "[Gérer les objets avec ILM](#)".

Étapes

1. Connectez-vous au nœud de grille :

- a. Entrez la commande suivante : `ssh admin@grid_node_IP`
- b. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.
- c. Entrez la commande suivante pour passer en root : `su -`
- d. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.

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 vous souhaitez peut-être vous connecter au système à distance pour 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, émettez la commande d'arrêt : `shutdown -h now`

Effectuez cette étape quel que soit le résultat de l' `service servermanager stop` commande.



Après avoir émis le `shutdown -h now` commande sur un nœud d'appareil, vous devez redémarrer l'appareil pour redémarrer le nœud.

Pour l'appareil, cette commande arrête le contrôleur, mais l'appareil est toujours sous tension. Vous devez compléter l'étape suivante.

4. Si vous mettez hors tension un nœud d'appareil, suivez les étapes correspondant à votre appareil.

SG6160

- a. Coupez l'alimentation du contrôleur de stockage SG6100-CN.
- b. Attendez que le voyant d'alimentation bleu du contrôleur de stockage SG6100-CN s'éteigne.

SGF6112

- a. Coupez l'alimentation de l'appareil.
- b. Attendez que le voyant d'alimentation bleu s'éteigne.

SG6000

- a. Attendez que le voyant vert Cache Active à l'arrière des contrôleurs de stockage s'éteigne.

Cette LED s'allume lorsque les données mises en cache doivent être écrites sur les lecteurs. Vous devez attendre que cette LED s'éteigne avant de couper l'alimentation.

- b. Coupez l'alimentation de l'appareil et attendez que le voyant d'alimentation bleu s'éteigne.

SG5800

- a. Attendez que le voyant vert Cache Active à l'arrière du contrôleur de stockage s'éteigne.

Cette LED s'allume lorsque les données mises en cache doivent être écrites sur les lecteurs. Vous devez attendre que cette LED s'éteigne avant de couper l'alimentation.

- b. Depuis la page d'accueil de SANtricity System Manager, sélectionnez **Afficher les opérations en cours**.
- c. Confirmez que toutes les opérations sont terminées avant de passer à l'étape suivante.
- d. Éteignez les deux interrupteurs d'alimentation sur l'étagère du contrôleur et attendez que tous les voyants de l'étagère du contrôleur s'éteignent.

SG5700

- a. Attendez que le voyant vert Cache Active à l'arrière du contrôleur de stockage s'éteigne.

Cette LED s'allume lorsque les données mises en cache doivent être écrites sur les lecteurs. Vous devez attendre que cette LED s'éteigne avant de couper l'alimentation.

- b. Coupez l'alimentation de l'appareil et attendez que toutes les activités des voyants LED et de l'affichage à sept segments s'arrêtent.

SG100 ou SG1000

- a. Coupez l'alimentation de l'appareil.
- b. Attendez que le voyant d'alimentation bleu s'éteigne.

Mettre l'hôte hors tension

Avant de mettre un hôte hors tension, vous devez arrêter les services sur tous les nœuds de grille de cet hôte.

Étapes

1. Connectez-vous au nœud de grille :

- a. Entrez la commande suivante : `ssh admin@grid_node_IP`
- b. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.
- c. Entrez la commande suivante pour passer en root : `su -`
- d. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.

Lorsque vous êtes connecté en tant que root, l'invite passe de \$ à # .

2. Arrêtez tous les services en cours d'exécution sur le nœud : `service servermanager stop`

L'arrêt des services peut prendre jusqu'à 15 minutes et vous souhaitez peut-être vous connecter au système à distance pour surveiller le processus d'arrêt.

3. Répétez les étapes 1 et 2 pour chaque nœud sur l'hôte.
4. Si vous avez 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, émettez la commande d'arrêt : `shutdown -h now`

Effectuez cette étape quel que soit le résultat de l' `service servermanager stop` commande.



Après avoir émis le `shutdown -h now` commande sur un nœud d'appareil, vous devez redémarrer l'appareil pour redémarrer le nœud.

Pour l'appareil, cette commande arrête le contrôleur, mais l'appareil est toujours sous tension. Vous devez compléter l'étape suivante.

6. Si vous mettez hors tension un nœud d'appareil, suivez les étapes correspondant à votre appareil.

SG6160

- a. Coupez l'alimentation du contrôleur de stockage SG6100-CN.
- b. Attendez que le voyant d'alimentation bleu du contrôleur de stockage SG6100-CN s'éteigne.

SGF6112

- a. Coupez l'alimentation de l'appareil.
- b. Attendez que le voyant d'alimentation bleu s'éteigne.

SG6000

- a. Attendez que le voyant vert Cache Active à l'arrière des contrôleurs de stockage s'éteigne.

Cette LED s'allume lorsque les données mises en cache doivent être écrites sur les lecteurs. Vous devez attendre que cette LED s'éteigne avant de couper l'alimentation.

- b. Coupez l'alimentation de l'appareil et attendez que le voyant d'alimentation bleu s'éteigne.

SG5800

- a. Attendez que le voyant vert Cache Active à l'arrière du contrôleur de stockage s'éteigne.

Cette LED s'allume lorsque les données mises en cache doivent être écrites sur les lecteurs. Vous devez attendre que cette LED s'éteigne avant de couper l'alimentation.

- b. Depuis la page d'accueil de SANtricity System Manager, sélectionnez **Afficher les opérations en cours**.
- c. Confirmez que toutes les opérations sont terminées avant de passer à l'étape suivante.
- d. Éteignez les deux interrupteurs d'alimentation sur l'étagère du contrôleur et attendez que tous les voyants de l'étagère du contrôleur s'éteignent.

SG5700

- a. Attendez que le voyant vert Cache Active à l'arrière du contrôleur de stockage s'éteigne.

Cette LED s'allume lorsque les données mises en cache doivent être écrites sur les lecteurs. Vous devez attendre que cette LED s'éteigne avant de couper l'alimentation.

- b. Coupez l'alimentation de l'appareil et attendez que toutes les activités des voyants LED et de l'affichage à sept segments s'arrêtent.

SG110 ou SG1100

- a. Coupez l'alimentation de l'appareil.
- b. Attendez que le voyant d'alimentation bleu s'éteigne.

SG100 ou SG1000

- a. Coupez l'alimentation de l'appareil.
- b. Attendez que le voyant d'alimentation bleu s'éteigne.

7. Déconnectez-vous de l'interpréteur de commandes : `exit`

Informations connexes

- ["Appareils de stockage SGF6112 et SG6160"](#)
- ["Appareils de stockage SG6000"](#)
- ["Appareils de stockage SG5700"](#)
- ["Appareils de stockage SG5800"](#)
- ["Appareils de service SG110 et SG1100"](#)
- ["Appareils de service SG100 et SG1000"](#)

Éteindre et rallumer tous les nœuds du réseau

Vous devrez peut-être arrêter l'intégralité de votre système StorageGRID , par exemple, si vous déplacez un centre de données. Ces étapes fournissent un aperçu de haut niveau de la séquence recommandée pour effectuer un arrêt et un démarrage contrôlés.

Lorsque vous mettez hors tension tous les nœuds d'un site ou d'une grille, vous ne pourrez pas accéder aux objets ingérés tant que les nœuds de stockage sont hors ligne.

Arrêter les services et fermer les nœuds du réseau

Avant de pouvoir mettre hors tension un système StorageGRID , vous devez arrêter tous les services exécutés sur chaque nœud de grille, puis arrêter toutes les machines virtuelles VMware, les moteurs de conteneur et les appliances StorageGRID .

À propos de cette 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 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 cet 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 impacter la fonctionnalité ou la disponibilité de votre réseau.

Étapes

1. Empêchez toutes les applications clientes d'accéder à la grille.
2. Connectez-vous à chaque nœud de passerelle :
 - a. Entrez la commande suivante : `ssh admin@grid_node_IP`
 - b. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.
 - c. Entrez la commande suivante pour passer en root : `su -`
 - d. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.

Lorsque vous êtes connecté en tant que root, l'invite passe de \$ à # .

3. Arrêtez tous les services en cours d'exécution sur le nœud : `service servermanager stop`

L'arrêt des services peut prendre jusqu'à 15 minutes et vous souhaiterez peut-être vous connecter au système à distance pour surveiller le processus d'arrêt.

4. Répétez les deux étapes précédentes pour arrêter les services sur tous les nœuds de stockage et les nœuds d'administration non principaux.

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 sur un nœud de stockage d'appliance, vous devez redémarrer l'appliance pour redémarrer le nœud.

5. Pour le nœud d'administration principal, répétez les étapes pour [connexion au nœud](#) et [arrêter tous les services sur le nœud](#).
6. Pour les nœuds exécutés 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 exécutés sur des machines virtuelles VMware et pour les nœuds de stockage d'appliance, émettez la commande d'arrêt : `shutdown -h now`

Effectuez cette étape quel que soit le résultat de l' `service servermanager stop` commande.

Pour l'appareil, cette commande arrête le contrôleur de calcul, mais l'appareil est toujours sous tension. Vous devez compléter l'étape suivante.

8. Si vous disposez de nœuds d'appareil, suivez les étapes correspondant à votre appareil.

SG110 ou SG1100

- a. Coupez l'alimentation de l'appareil.
- b. Attendez que le voyant d'alimentation bleu s'éteigne.

SG100 ou SG1000

- a. Coupez l'alimentation de l'appareil.
- b. Attendez que le voyant d'alimentation bleu s'éteigne.

SG6160

- a. Coupez l'alimentation du contrôleur de stockage SG6100-CN.
- b. Attendez que le voyant d'alimentation bleu du contrôleur de stockage SG6100-CN s'éteigne.

SGF6112

- a. Coupez l'alimentation de l'appareil.
- b. Attendez que le voyant d'alimentation bleu s'éteigne.

SG6000

- a. Attendez que le voyant vert Cache Active à l'arrière des contrôleurs de stockage s'éteigne.

Cette LED s'allume lorsque les données mises en cache doivent être écrites sur les lecteurs. Vous devez attendre que cette LED s'éteigne avant de couper l'alimentation.

- b. Coupez l'alimentation de l'appareil et attendez que le voyant d'alimentation bleu s'éteigne.

SG5800

- a. Attendez que le voyant vert Cache Active à l'arrière du contrôleur de stockage s'éteigne.

Cette LED s'allume lorsque les données mises en cache doivent être écrites sur les lecteurs. Vous devez attendre que cette LED s'éteigne avant de couper l'alimentation.

- b. Depuis la page d'accueil de SANtricity System Manager, sélectionnez **Afficher les opérations en cours**.
- c. Confirmez que toutes les opérations sont terminées avant de passer à l'étape suivante.
- d. Éteignez les deux interrupteurs d'alimentation sur l'étagère du contrôleur et attendez que tous les voyants de l'étagère du contrôleur s'éteignent.

SG5700

- a. Attendez que le voyant vert Cache Active à l'arrière du contrôleur de stockage s'éteigne.

Cette LED s'allume lorsque les données mises en cache doivent être écrites sur les lecteurs. Vous devez attendre que cette LED s'éteigne avant de couper l'alimentation.

- b. Coupez l'alimentation de l'appareil et attendez que toutes les activités des voyants LED et de l'affichage à sept segments s'arrêtent.

9. Si nécessaire, déconnectez-vous de l'interpréteur de commandes : `exit`

La grille StorageGRID a maintenant été arrêtée.

Démarrer les nœuds de grille



Si l'ensemble du réseau est arrêté depuis plus de 15 jours, vous devez contacter le support technique avant de redémarrer un nœud du réseau. N'essayez pas les procédures de récupération qui reconstruisent les données Cassandra. Cela pourrait entraîner une perte de données.

Si possible, mettez sous tension les nœuds du réseau dans cet ordre :

- Appliquez d'abord l'alimentation aux nœuds d'administration.
- Appliquez l'alimentation aux nœuds de passerelle en dernier.



Si un hôte comprend plusieurs nœuds de grille, les nœuds reviendront automatiquement en ligne lorsque vous mettrez l'hôte sous tension.

Étapes

1. Mettez sous tension les hôtes du nœud d'administration principal et de tous les nœuds d'administration non principaux.



Vous ne pourrez pas vous connecter aux nœuds d'administration tant que les nœuds de stockage n'auront pas été redémarrés.

2. Mettez sous tension les hôtes de tous les nœuds de stockage.

Vous pouvez mettre sous tension ces nœuds dans n'importe quel ordre.

3. Mettez sous tension les hôtes de tous les nœuds de passerelle.
4. Sign in au gestionnaire de grille.
5. Sélectionnez **NODES** et surveillez l'état des nœuds de la grille. Vérifiez qu'il n'y a pas d'icônes d'alerte à côté des noms de nœuds.

Informations connexes

- ["Appareils de stockage SGF6112 et SG6160"](#)
- ["Appareils de service SG110 et SG1100"](#)
- ["Appareils de service SG100 et SG1000"](#)
- ["Appareils de stockage SG6000"](#)
- ["Appareils de stockage SG5800"](#)
- ["Appareils de stockage SG5700"](#)

Procédures de remappage des ports

Supprimer les remappages de ports

Si vous souhaitez configurer un point de terminaison pour le service Load Balancer et que vous souhaitez utiliser un port qui a déjà été configuré comme port mappé d'un remappage de port, vous devez d'abord supprimer le remappage de port existant, sinon le point de terminaison ne sera pas efficace. Vous devez exécuter un script sur chaque nœud d'administration et nœud de passerelle comportant des ports remappés en conflit

pour supprimer tous les remappages de ports du nœud.

À propos de cette tâche

Cette procédure supprime tous les remappages de ports. Si vous devez conserver certains remappages, contactez le support technique.

Pour plus d'informations sur la configuration des points de terminaison de l'équilibreur de charge, consultez "[Configuration des points de terminaison de l'équilibreur de charge](#)".



Si le remappage du port fournit un accès client, reconfigurez le client pour utiliser un port différent comme point de terminaison d'équilibrage de charge afin d'éviter la perte de service. Dans le cas contraire, la suppression du mappage de port entraînera la perte de l'accès client et devra être planifiée de manière appropriée.



Cette procédure ne fonctionne pas pour un système StorageGRID déployé en tant que conteneur sur des hôtes bare metal. Voir les instructions pour "[suppression des remappages de ports sur les hôtes bare metal](#)".

Étapes

1. Connectez-vous au nœud.

a. Entrez 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 conteneur exécutant StorageGRID.

b. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.

c. Entrez la commande suivante pour passer en root : `su -`

d. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.

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 : `reboot`

4. Déconnectez-vous de l'interpréteur de commandes : `exit`

5. Répétez ces étapes sur chaque nœud d'administration et nœud de passerelle comportant des ports remappés en conflit.

Supprimer les remappages de ports sur les hôtes bare metal

Si vous souhaitez configurer un point de terminaison pour le service Load Balancer et que vous souhaitez utiliser un port qui a déjà été configuré comme port mappé d'un remappage de port, vous devez d'abord supprimer le remappage de port existant, sinon le point de terminaison ne sera pas efficace.

À propos de cette tâche

Si vous exécutez StorageGRID sur des hôtes bare metal, suivez cette procédure au lieu de la procédure générale de suppression des remappages de ports. Vous devez modifier le fichier de configuration de nœud pour chaque nœud d'administration et nœud de passerelle qui possède des ports remappés en conflit pour

supprimer tous les remappages de ports du nœud et redémarrer le nœud.



Cette procédure supprime tous les remappages de ports. Si vous devez conserver certains remappages, contactez le support technique.

Pour plus d'informations sur la configuration des points de terminaison de l'équilibreur de charge, consultez les instructions d'administration de StorageGRID.



Cette procédure peut entraîner une perte temporaire de service lors du redémarrage des nœuds.

Étapes

1. Connectez-vous à l'hôte prenant en charge 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 du nœud.

Le fichier de configuration du nœud se trouve à l'adresse `/etc/storagegrid/nodes/node-name.conf`.

4. Localisez la section du fichier de configuration du nœud qui contient les remappages de port.

Voir les deux dernières lignes de 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_REMAP_INBOUND` pour supprimer les remappages de port.

```

PORT_REMAP =
PORT_REMAP_INBOUND =

```

6. Exécutez la commande suivante pour valider vos modifications apportées au fichier de configuration du nœud : `sudo storagegrid node validate node-name`

Corrigez les erreurs ou les avertissements avant de passer à l'étape suivante.
7. Exécutez la commande suivante pour redémarrer le nœud sans remappage de port : `sudo storagegrid node start node-name`
8. Connectez-vous au nœud en tant qu'administrateur en utilisant le mot de passe répertorié dans le `Passwords.txt` déposer.
9. Vérifiez que les services démarrent correctement.
 - a. Afficher une liste des statuts de tous les services sur le serveur : `sudo storagegrid-status`

Le statut est mis à jour automatiquement.

b. Attendez que tous les services aient le statut « 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 comportant des ports remappés en conflit.

Procédures réseau

Mettre à jour les sous-réseaux pour Grid Network

StorageGRID maintient une liste des sous-réseaux réseau utilisés pour communiquer entre les nœuds de grille sur le réseau de grille (eth0). Ces entrées incluent les sous-réseaux utilisés pour le réseau Grid par chaque site de votre système StorageGRID ainsi que tous les sous-réseaux utilisés pour NTP, DNS, LDAP ou d'autres serveurs externes accessibles via la passerelle du 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 de grille.

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 de maintenance ou root"](#) .
- Vous disposez de la phrase secrète de provisionnement.
- Vous disposez des adresses réseau, en notation CIDR, des sous-réseaux que vous souhaitez configurer.

À propos de cette tâche

Si vous effectuez une activité d'extension qui inclut l'ajout d'un nouveau sous-réseau, vous devez ajouter un nouveau sous-réseau à la liste des sous-réseaux du réseau de grille avant de démarrer la procédure d'extension. Sinon, vous devrez annuler l'extension, ajouter le nouveau sous-réseau et redémarrer l'extension.

N'utilisez pas de sous-réseaux contenant les adresses IPv4 suivantes pour le réseau de grille, le réseau d'administration ou le réseau client d'un nœud :

- 192.168.130.101
- 192.168.131.101
- 192.168.130.102
- 192.168.131.102
- 198.51.100.2
- 198.51.100.4



Par exemple, n'utilisez pas les plages de sous-réseaux suivantes pour le réseau de grille, le réseau d'administration ou le réseau client d'un nœud :

- 192.168.130.0/24 car cette plage de sous-réseaux contient les adresses IP 192.168.130.101 et 192.168.130.102
- 192.168.131.0/24 car cette plage de sous-réseaux contient les adresses IP 192.168.131.101 et 192.168.131.102
- 198.51.100.0/24 car cette plage de sous-réseaux contient les adresses IP 198.51.100.2 et 198.51.100.4

Ajouter un sous-réseau

Étapes

1. Sélectionnez **MAINTENANCE > Réseau > Réseau de grille**.
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 la phrase secrète de provisionnement et sélectionnez **Enregistrer**.
4. Attendez que les modifications soient appliquées, puis téléchargez un nouveau package de récupération.
 - a. Sélectionnez **MAINTENANCE > Système > Package de récupération**.
 - b. Saisissez la **phrase secrète de provisionnement**.



Le fichier du package de récupération doit être sécurisé car il contient des clés de chiffrement et des mots de passe qui peuvent être utilisés pour obtenir des données à partir du système StorageGRID . Il est également utilisé pour récupérer le nœud d'administration principal.

Les sous-réseaux que vous avez spécifiés sont configurés automatiquement pour votre système StorageGRID .

Modifier un sous-réseau

Étapes

1. Sélectionnez **MAINTENANCE > Réseau > Réseau de grille**.
2. Sélectionnez le sous-réseau que vous souhaitez modifier et effectuez les modifications nécessaires.

3. Saisissez la phrase secrète 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 package de récupération.
 - a. Sélectionnez **MAINTENANCE > Système > Package de récupération**.
 - b. Saisissez la **phrase secrète de provisionnement**.

Supprimer un sous-réseau

Étapes

1. Sélectionnez **MAINTENANCE > Réseau > Réseau de grille**.
2. Sélectionnez l'icône de suppression  à côté du sous-réseau.
3. Saisissez la phrase secrète 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 package de récupération.
 - a. Sélectionnez **MAINTENANCE > Système > Package de récupération**.
 - b. Saisissez la **phrase secrète de provisionnement**.

Configurer les adresses IP

Directives relatives aux adresses IP

Vous pouvez effectuer la configuration du réseau en configurant les adresses IP des nœuds de grille à l'aide de l'outil Modifier l'IP.

Vous devez utiliser l'outil Modifier l'IP pour apporter la plupart des modifications à la configuration réseau initialement définie lors du déploiement de la grille. Les modifications manuelles utilisant des commandes et des fichiers réseau Linux standard peuvent ne pas se propager à tous les services StorageGRID et peuvent ne pas persister lors des mises à niveau, des redémarrages ou des procédures de récupération de nœud.



La procédure de changement d'IP peut être une procédure perturbatrice. Certaines parties de la grille peuvent être indisponibles jusqu'à ce que la nouvelle configuration soit appliquée.



Si vous apportez des modifications à la liste des sous-réseaux du réseau de grille uniquement, utilisez le gestionnaire de grille pour ajouter ou modifier la configuration du réseau. Sinon, utilisez l'outil Modifier l'IP si le gestionnaire de grille est inaccessible en raison d'un problème de configuration réseau ou si vous effectuez à la fois une modification de routage du réseau de grille et d'autres modifications de réseau en même temps.



Si vous souhaitez modifier l'adresse IP du réseau de grille pour tous les nœuds de la grille, utilisez le [procédure spéciale pour les modifications à l'échelle du réseau](#) .

Interfaces Ethernet

L'adresse IP attribuée à eth0 est toujours l'adresse IP du réseau de grille du nœud de grille. L'adresse IP attribuée à eth1 est toujours l'adresse IP du réseau d'administration du nœud de grille. L'adresse IP attribuée à eth2 est toujours l'adresse IP du réseau client du nœud de grille.

Notez que sur certaines plates-formes, telles que 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 plateformes, l'onglet **SSM > Ressources** peut afficher l'adresse IP du réseau Grid, Admin et 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 changement d'adresse IP si vous souhaitez modifier les adresses IP, les masques de sous-réseau et les passerelles par défaut d'un nœud de grille. L'utilisation de l'outil Modifier IP entraînera la statique des adresses DHCP.

Groupes de haute disponibilité (HA)

- Si une interface réseau client est contenue dans un groupe HA, vous ne pouvez pas modifier l'adresse IP du réseau client pour cette interface en une adresse située en dehors du sous-réseau configuré pour le groupe HA.
- Vous ne pouvez pas modifier l'adresse IP du réseau client avec la valeur d'une adresse IP virtuelle existante attribuée à un groupe HA configuré sur l'interface réseau client.
- Si une interface réseau Grid est contenue dans un groupe HA, vous ne pouvez pas modifier l'adresse IP du réseau Grid pour cette interface en une adresse située en dehors du sous-réseau configuré pour le groupe HA.
- Vous ne pouvez pas modifier l'adresse IP du réseau Grid avec la valeur d'une adresse IP virtuelle existante attribuée à un groupe HA configuré sur l'interface du réseau Grid.

Modifier la configuration du réseau de nœuds

Vous pouvez modifier la configuration réseau d'un ou plusieurs nœuds à l'aide de l'outil Modifier l'IP. Vous pouvez modifier la configuration du réseau Grid ou ajouter, modifier ou supprimer les réseaux administrateur ou client.

Avant de commencer

Vous avez le `Passwords.txt` déposer.

À propos de cette tâche

Linux : si vous ajoutez un nœud de grille au réseau d'administration ou au réseau client pour la première fois et que vous n'avez pas configuré auparavant `ADMIN_NETWORK_TARGET` ou `CLIENT_NETWORK_TARGET` dans le fichier de configuration du nœud, vous devez le faire maintenant.

Consultez les instructions d'installation de StorageGRID pour votre système d'exploitation Linux :

- ["Installer StorageGRID sur Red Hat Enterprise Linux"](#)
- ["Installer StorageGRID sur 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'appareil StorageGRID lors de l'installation initiale, le réseau ne peut pas être ajouté à l'aide de l'outil Modifier l'adresse IP uniquement. Tout d'abord, vous devez ["mettre l'appareil en mode maintenance"](#) , configurez les liens, remettez l'appareil en mode de fonctionnement normal, puis utilisez l'outil Modifier l'IP pour modifier la configuration du réseau. Voir le ["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 administrateur :

- Vous pouvez ajouter un nœud à un réseau client ou à un réseau administrateur 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 administrateur en supprimant l'adresse IP/le masque de sous-réseau du nœud sur ce réseau.

Les nœuds ne peuvent pas être supprimés du réseau Grid.



Les échanges d'adresses IP ne sont pas autorisés. Si vous devez échanger des adresses IP entre les nœuds 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 approbation de partie de confiance configurée à l'aide de l'adresse IP du nœud d'administration (au lieu de son nom de domaine complet, comme recommandé) deviendra invalide. Vous ne pourrez plus vous connecter au nœud. Immédiatement après avoir modifié l'adresse IP, vous devez mettre à jour ou reconfigurer la partie de confiance du nœud dans Active Directory Federation Services (AD FS) avec la nouvelle adresse IP. Voir les instructions pour "[configuration de SSO](#)".



Toutes les modifications que vous apportez au réseau à l'aide de l'outil Modifier l'adresse IP sont propagées au micrologiciel d'installation des appliances StorageGRID. De cette façon, si le logiciel StorageGRID est réinstallé sur un appareil, ou si un appareil est placé en mode maintenance, la configuration réseau sera correcte.

Étapes

1. Connectez-vous au nœud d'administration principal :

- a. Entrez la commande suivante : `ssh admin@primary_Admin_Node_IP`
- b. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.
- c. Entrez la commande suivante pour passer en root : `su -`
- d. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.

Lorsque vous êtes connecté en tant que root, l'invite passe de \$ à # .

2. Démarrez l'outil Change IP en entrant la commande suivante : `change-ip`
3. Saisissez la phrase secrète de provisionnement à l'invite.

Le menu principal apparaît.

```

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. Sélectionnez éventuellement **1** pour choisir les nœuds à mettre à jour. Sélectionnez ensuite 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 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 » sélectionné.

Une fois votre sélection effectuée, le menu principal apparaît, avec le champ **Nœuds sélectionnés** mis à jour pour refléter votre choix. Toutes les actions ultérieures sont effectuées uniquement 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

Une fois votre sélection effectuée, 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 la valeur actuelle.

La modification de l'adresse IP, de la longueur du préfixe, de la passerelle ou du MTU d'une interface configurée par DHCP modifiera l'interface en statique. Lorsque vous choisissez de modifier une interface configurée par DHCP, un avertissement s'affiche pour vous informer que l'interface deviendra statique.

Interfaces configurées comme *fixed* ne peut pas être modifié.

- b. Pour définir une nouvelle valeur, saisissez-la au 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 administrateur ou client du nœud en saisissant **d** ou **0.0.0.0/0**.
- e. Après avoir modifié tous les nœuds que vous souhaitez modifier, entrez **q** pour revenir au menu principal.

Vos modifications sont conservées jusqu'à ce qu'elles soient effacées ou appliquées.

6. Vérifiez vos modifications en sélectionnant l'une des options suivantes :

- **5:** Affiche les modifications dans la sortie qui sont isolées pour afficher uniquement l'élément modifié. Les modifications sont surlignées 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 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 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 dans la sortie qui affiche la configuration complète. Les modifications sont surlignées en vert (ajouts) ou en rouge (suppressions).



Certaines interfaces de ligne de commande peuvent afficher des ajouts et des suppressions à l'aide d'un formatage barré. L'affichage correct dépend de la prise en charge par votre client terminal des séquences d'échappement VT100 nécessaires.

7. Sélectionnez l'option **7** pour valider toutes les modifications.

Cette validation garantit que les règles des réseaux Grid, Admin et Client, telles que la non-utilisation de sous-réseaux qui se chevauchent, ne sont pas violées.

Dans cet exemple, la validation a renvoyé des erreurs.

```

Validating new networking configuration... FAILED.

DK-10-224-5-20-G1: The admin subnet 172.18.0.0/16 overlaps the 172.18.0.0/21 grid network.
DK-10-224-5-22-S1: Duplicate Grid IP 172.16.5.18 (also in use by DK-10-224-5-21-ADM1)

You must correct these errors before you can apply any changes.
Checking for Grid Network IP address swaps... PASSED.

Press Enter to continue

```

Dans cet exemple, la validation a réussi.

```

Validating new networking configuration... PASSED.
Checking for Grid Network IP address swaps... PASSED.

Press Enter to continue

```

8. Une fois la validation effectuée, choisissez l'une des options suivantes :

- **8**: Enregistrer les modifications non appliquées.

Cette option vous permet de quitter l'outil Change IP et de le redémarrer plus tard, 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** : appliquer les modifications immédiatement et redémarrer automatiquement chaque nœud si nécessaire.

Si la nouvelle configuration réseau ne nécessite aucune modification du réseau physique, vous pouvez sélectionner **appliquer** pour appliquer les modifications immédiatement. Les nœuds seront redémarrés automatiquement, si nécessaire. Les nœuds qui doivent être redémarrés seront affichés.

- **étape** : appliquer les modifications la prochaine fois que les nœuds sont redémarrés manuellement.

Si vous devez apporter des modifications à la configuration du réseau physique ou virtuel pour que la nouvelle configuration réseau fonctionne, vous devez utiliser l'option **stage**, arrêter les nœuds concernés, apporter les modifications nécessaires au réseau physique et redémarrer les nœuds concernés. Si vous sélectionnez **Appliquer** sans avoir d'abord effectué ces modifications réseau, les modifications échoueront généralement.



Si vous utilisez l'option **stage**, vous devez redémarrer le nœud dès que possible après la préparation afin de minimiser les interruptions.

- **annuler** : N'effectuez aucune modification de réseau pour le moment.

Si vous ne saviez pas que les modifications proposées nécessitent le redémarrage des nœuds, vous pouvez différer les modifications pour minimiser l'impact sur l'utilisateur. En sélectionnant **Annuler**, vous revenez au menu principal et conservez vos modifications afin que vous puissiez les appliquer ultérieurement.

Lorsque vous sélectionnez **appliquer** ou **étape**, 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.

Lors de l'approvisionnement, la sortie affiche l'état au fur et à mesure que les mises à jour sont appliquées.

```
Generating new grid networking description file...
```

```
Running provisioning...
```

```
Updating grid network configuration on Name
```

Une fois les modifications appliquées ou mises en scène, un nouveau package de récupération est généré suite à la modification de la configuration de la grille.

10. Si vous avez sélectionné **étape**, suivez ces étapes une fois le provisionnement terminé :

a. Effectuez les modifications de réseau physiques ou virtuelles requises.

Modifications du réseau physique : effectuez les modifications nécessaires au réseau physique, en arrêtant le nœud en toute sécurité si nécessaire.

Linux : Si vous ajoutez le nœud à un réseau d'administration ou à un réseau client pour la première fois, assurez-vous d'avoir ajouté l'interface comme décrit dans "[Linux : ajouter des interfaces à un nœud existant](#)".

a. Redémarrez les nœuds affectés.

11. Sélectionnez **0** pour quitter l'outil Modifier l'IP une fois vos modifications terminées.

12. Téléchargez un nouveau package de récupération à partir du gestionnaire de grille.

a. Sélectionnez **MAINTENANCE > Système > Package de récupération**.

b. Saisissez la phrase secrète d'approvisionnement.

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 des sous-réseaux du réseau d'administration d'un ou de plusieurs nœuds.

Avant de commencer

- Vous avez le `Passwords.txt` déposer.

Vous pouvez ajouter, supprimer ou modifier des sous-réseaux pour tous les nœuds de la liste des sous-réseaux du réseau d'administration.

N'utilisez pas de sous-réseaux contenant les adresses IPv4 suivantes pour le réseau de grille, le réseau d'administration ou le réseau client d'un nœud :

- 192 168 130 101
- 192 168 131 101
- 192 168 130 102
- 192 168 131 102
- 198.51.100.2
- 198.51.100.4



Par exemple, n'utilisez pas les plages de sous-réseaux suivantes pour le réseau de grille, le réseau d'administration ou le réseau client d'un nœud :

- 192.168.130.0/24 car cette plage de sous-réseaux contient les adresses IP 192.168.130.101 et 192.168.130.102
- 192.168.131.0/24 car cette plage de sous-réseaux contient les adresses IP 192.168.131.101 et 192.168.131.102
- 198.51.100.0/24 car cette plage de sous-réseaux contient les adresses IP 198.51.100.2 et 198.51.100.4

Étapes

1. Connectez-vous au nœud d'administration principal :

- Entrez la commande suivante : `ssh admin@primary_Admin_Node_IP`
- Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.
- Entrez la commande suivante pour passer en root : `su -`
- Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.

Lorsque vous êtes connecté en tant que root, l'invite passe de \$ à # .

2. Démarrez l'outil Change IP en entrant la commande suivante : `change-ip`

3. Saisissez la phrase secrète de provisionnement à l'invite.

Le menu principal apparaît.

```
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. Vous pouvez également limiter les réseaux/nœuds sur lesquels les opérations sont effectuées. Choisissez l'une des options suivantes :

- 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 (sélection par site, puis par nom)
 - **3** : Nœud unique (sélection par IP actuelle)
 - **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 apparaît. Le champ Nœuds sélectionnés reflète votre nouvelle sélection et désormais 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 d'administration (option **3**).

6. Choisissez l'une des options suivantes :

- Ajoutez un sous-réseau en entrant cette commande : `add CIDR`
- Supprimez un sous-réseau en entrant cette commande : `del CIDR`
- Définissez la liste des sous-réseaux en entrant cette commande : `set CIDR`



Pour toutes les commandes, vous pouvez saisir plusieurs adresses en utilisant 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 en utilisant la « flèche vers le haut » pour rappeler les valeurs précédemment saisies dans l'invite de saisie actuelle, puis les modifier si nécessaire.

L'exemple d'entrée ci-dessous montre l'ajout de sous-réseaux à la liste des sous-réseaux du réseau d'administration :

7. Lorsque vous êtes prêt, entrez **q** pour revenir à l'écran du menu principal. Vos modifications sont conservées jusqu'à ce qu'elles soient effacées ou appliquées.



Si vous avez sélectionné l'un des modes de sélection de nœuds « tous » à l'étape 2, appuyez sur **Entrée** (sans **q**) pour accéder au nœud suivant dans la liste.

8. Choisissez l'une des options suivantes :

- Sélectionnez l'option **5** pour afficher les modifications dans la sortie qui est isolée pour afficher uniquement l'élément modifié. Les modifications sont surlignées en vert (ajouts) ou en rouge (suppressions), comme indiqué dans l'exemple de sortie ci-dessous :


```
=====
Site: Data Center 1
=====
DC1-ADM1-105-154 Admin Subnets                                add 172.17.0.0/16
                                                                del 172.16.0.0/16
                                                                [ 172.14.0.0/16 ]
                                                                [ 172.15.0.0/16 ]
                                                                [ 172.17.0.0/16 ]
                                                                [ 172.19.0.0/16 ]
                                                                [ 172.20.0.0/16 ]
                                                                [ 172.21.0.0/16 ]
Press Enter to continue
```

- Sélectionnez l'option **6** pour afficher les modifications dans la sortie qui affiche la configuration complète. Les modifications sont surlignées en vert (ajouts) ou en rouge (suppressions). **Remarque :** certains émulateurs de terminal peuvent afficher les ajouts et les suppressions à l'aide d'un formatage barré.

Lorsque vous essayez 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 attribué les sous-réseaux de serveur 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 vers 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 avoir appliqué les modifications à la liste des sous-réseaux.



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

9. Sélectionnez l'option **7** pour valider toutes les modifications mises en place.

Cette validation garantit que les règles des réseaux Grid, Admin et Client sont respectées, comme l'utilisation de sous-réseaux qui se chevauchent.

10. Vous pouvez également sélectionner l'option **8** pour enregistrer toutes les modifications effectuées et revenir ultérieurement pour continuer à apporter des modifications.

Cette option vous permet de quitter l'outil Change IP et de le redémarrer plus tard, 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 les modifications et à provisionner la nouvelle configuration réseau. Pendant l'approvisionnement, la sortie affiche l'état au fur et à mesure que les mises à jour sont appliquées, 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 à partir du gestionnaire de grille.

- a. Sélectionnez **MAINTENANCE > Système > Package de récupération**.
- b. Saisissez la phrase secrète d'approvisionnement.

Ajouter ou modifier des listes de sous-réseaux sur Grid Network

Vous pouvez utiliser l'outil Modifier IP pour ajouter ou modifier des sous-réseaux sur le réseau Grid.

Avant de commencer

- Vous avez le `Passwords.txt` déposer.

Vous pouvez ajouter, supprimer ou modifier des sous-réseaux dans la liste des sous-réseaux du réseau Grid. Les modifications affecteront le routage sur tous les nœuds de la grille.



Si vous apportez des modifications à la liste des sous-réseaux du réseau de grille uniquement, utilisez le gestionnaire de grille pour ajouter ou modifier la configuration du réseau. Sinon, utilisez l'outil Modifier l'IP si le gestionnaire de grille est inaccessible en raison d'un problème de configuration réseau ou si vous effectuez à la fois une modification de routage du réseau de grille et d'autres modifications de réseau en même temps.

N'utilisez pas de sous-réseaux contenant les adresses IPv4 suivantes pour le réseau de grille, le réseau d'administration ou le réseau client d'un nœud :

- 192.168.130.101
- 192.168.131.101
- 192.168.130.102
- 192.168.131.102
- 198.51.100.2
- 198.51.100.4



Par exemple, n'utilisez pas les plages de sous-réseaux suivantes pour le réseau de grille, le réseau d'administration ou le réseau client d'un nœud :

- 192.168.130.0/24 car cette plage de sous-réseaux contient les adresses IP 192.168.130.101 et 192.168.130.102
- 192.168.131.0/24 car cette plage de sous-réseaux contient les adresses IP 192.168.131.101 et 192.168.131.102
- 198.51.100.0/24 car cette plage de sous-réseaux contient les adresses IP 198.51.100.2 et 198.51.100.4

Étapes

1. Connectez-vous au nœud d'administration principal :

- Entrez la commande suivante : `ssh admin@primary_Admin_Node_IP`
- Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.
- Entrez la commande suivante pour passer en root : `su -`
- Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.

Lorsque vous êtes connecté en tant que root, l'invite passe de \$ à # .

2. Démarrez l'outil Change IP en entrant la commande suivante : `change-ip`

3. Saisissez la phrase secrète de provisionnement à l'invite.

Le menu principal apparaît.

```
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 grille s'appliquent à l'ensemble du réseau.

5. Choisissez l'une des options suivantes :

- Ajoutez un sous-réseau en entrant cette commande : `add CIDR`
- Supprimez un sous-réseau en entrant cette commande : `del CIDR`
- Définissez la liste des sous-réseaux en entrant cette commande : `set CIDR`



Pour toutes les commandes, vous pouvez saisir plusieurs adresses en utilisant 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 en utilisant la « flèche vers le haut » pour rappeler les valeurs précédemment saisies dans l'invite de saisie actuelle, puis les modifier si nécessaire.

L'exemple d'entrée ci-dessous montre la configuration des sous-réseaux pour la liste des 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, entrez **q** pour revenir à l'écran du menu principal. Vos modifications sont conservées jusqu'à ce qu'elles soient effacées ou appliquées.
7. Choisissez l'une des options suivantes :
- Sélectionnez l'option **5** pour afficher les modifications dans la sortie qui est isolée pour afficher uniquement l'élément modifié. Les modifications sont surlignées en vert (ajouts) ou en rouge (suppressions), comme indiqué dans l'exemple de sortie ci-dessous :

```
Grid Network Subnet List (GNSL)
-----
add 172.30.0.0/21
add 172.31.0.0/21
del 172.16.0.0/21
del 172.17.0.0/21
del 172.18.0.0/21
[ 172.30.0.0/21 ]
[ 172.31.0.0/21 ]
[ 192.168.0.0/21 ]
Press Enter to continue
```

- Sélectionnez l'option **6** pour afficher les modifications dans la sortie qui affiche la configuration complète. Les modifications sont surlignées en vert (ajouts) ou en rouge (suppressions).



Certaines interfaces de ligne de commande peuvent afficher des ajouts et des suppressions à l'aide d'un formatage barré.

8. Sélectionnez l'option **7** pour valider toutes les modifications mises en place.

Cette validation garantit que les règles des réseaux Grid, Admin et Client sont respectées, comme l'utilisation de sous-réseaux qui se chevauchent.

9. Vous pouvez également sélectionner l'option **8** pour enregistrer toutes les modifications effectuées et revenir ultérieurement pour continuer à apporter des modifications.

Cette option vous permet de quitter l'outil Change IP et de le redémarrer plus tard, 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 les modifications et à provisionner la nouvelle configuration réseau. Pendant l'approvisionnement, la sortie affiche l'état au fur et à mesure que les mises à jour sont appliquées, 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 des modifications apportées au réseau de grille, sélectionnez l'une des options suivantes :

- **appliquer** : appliquer les modifications immédiatement et redémarrer automatiquement chaque nœud si nécessaire.

Si la nouvelle configuration réseau doit fonctionner simultanément avec l'ancienne configuration réseau sans aucune modification externe, vous pouvez utiliser l'option **appliquer** pour une modification de configuration entièrement automatisée.

- **étape** : appliquer les modifications au prochain redémarrage des nœuds.

Si vous devez apporter des modifications à la configuration du réseau physique ou virtuel pour que la nouvelle configuration réseau fonctionne, vous devez utiliser l'option **stage**, arrêter les nœuds concernés, apporter les modifications nécessaires au réseau physique et redémarrer les nœuds concernés.



Si vous utilisez l'option **stage**, redémarrez le nœud dès que possible après la mise en scène pour minimiser les interruptions.

- **annuler** : N'effectuez aucune modification de réseau pour le moment.

Si vous ne saviez pas que les modifications proposées nécessitent le redémarrage des nœuds, vous pouvez différer les modifications pour minimiser l'impact sur l'utilisateur. En sélectionnant **Annuler**, vous revenez au menu principal et conservez vos modifications afin que vous puissiez les appliquer ultérieurement.

Une fois les modifications appliquées ou mises en scène, un nouveau package de récupération est généré suite à la modification de la configuration de la grille.

12. Si la configuration est interrompue en raison d'erreurs, les options suivantes sont disponibles :

- Pour terminer la procédure de changement d'IP et revenir au menu principal, entrez **a**.
- Pour réessayer l'opération qui a échoué, entrez **r**.
- Pour passer à l'opération suivante, entrez **c**.

L'opération ayant échoué peut être retentée ultérieurement en sélectionnant l'option **10** (Appliquer les modifications) dans le menu principal. La procédure de changement d'IP ne sera pas terminée tant que toutes les opérations ne seront pas terminées avec succès.

- Si vous avez dû intervenir manuellement (pour redémarrer un nœud, par exemple) et que vous êtes sûr que l'action que l'outil pense avoir échoué a été effectivement effectuée avec succès, saisissez **f** pour la marquer comme réussie et passer à l'opération suivante.

13. Téléchargez un nouveau package de récupération à partir du gestionnaire de grille.

a. Sélectionnez **MAINTENANCE > Système > Package de récupération**.

b. Saisissez la phrase secrète d'approvisionnement.



Le fichier du package de récupération doit être sécurisé car il contient des clés de chiffrement et des mots de passe qui peuvent être utilisés pour obtenir des données à partir du système StorageGRID .

Modifier les adresses IP de tous les nœuds de la grille

Si vous devez modifier l'adresse IP du réseau de grille pour tous les nœuds de la grille, vous devez suivre cette procédure spéciale. Vous ne pouvez pas effectuer de modification d'adresse IP du réseau à l'échelle de la grille en utilisant la procédure de modification des nœuds individuels.

Avant de commencer

- Vous avez le `Passwords.txt` déposer.

Pour garantir 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 administrateur ou client.

Si vous souhaitez modifier les adresses IP et le MTU des nœuds d'un seul site, suivez les instructions "[Modifier la configuration du réseau de nœuds](#)" instructions.

Étapes

1. Planifiez à l'avance les modifications que vous devez apporter en dehors de l'outil Modifier l'adresse IP, telles que les modifications apportées au DNS ou au NTP, ainsi que les modifications apportées à la configuration de l'authentification unique (SSO), si elle est 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 d'adresse IP.



Si les serveurs DNS existants ne sont pas accessibles au réseau sur les nouvelles adresses IP, ajoutez les nouveaux serveurs DNS avant d'effectuer la procédure de modification d'adresse IP.



Si SSO est activé pour votre système StorageGRID et que toutes les approbations de parties de confiance ont été configurées à l'aide d'adresses IP de nœud d'administration (au lieu de noms de domaine complets, comme recommandé), soyez prêt à mettre à jour ou à reconfigurer ces approbations de parties de confiance dans Active Directory Federation Services (AD FS) immédiatement après avoir modifié les 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. Entrez la commande suivante : `ssh admin@primary_Admin_Node_IP`
- b. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.
- c. Entrez la commande suivante pour passer en root : `su -`
- d. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.

Lorsque vous êtes connecté en tant que root, l'invite passe de \$ à # .

3. Démarrez l'outil Change IP en entrant la commande suivante : `change-ip`
4. Saisissez la phrase secrète de provisionnement à l'invite.

Le menu principal apparaît. Par défaut, le `Selected nodes` le champ est défini sur `all` .

```

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: █

```

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 apporter des modifications au réseau.

Une fois votre sélection effectuée, l'invite affiche les noms des nœuds, le nom du réseau de grille, le type de données (IP/masque, passerelle ou MTU) et les valeurs actuelles.

La modification de l'adresse IP, de la longueur du préfixe, de la passerelle ou du MTU d'une interface configurée par DHCP modifiera l'interface en statique. Un avertissement s'affiche avant chaque interface configurée par DHCP.

Interfaces configurées comme *fixed* ne peut pas être modifié.

- a. Pour définir une nouvelle valeur, saisissez-la au format indiqué pour la valeur actuelle.
 - b. Après avoir modifié tous les nœuds que vous souhaitez modifier, entrez **q** pour revenir au menu principal.

Vos modifications sont conservées jusqu'à ce qu'elles soient effacées ou appliquées.

6. Vérifiez vos modifications en sélectionnant l'une des options suivantes :
 - **5**: Affiche les modifications dans la sortie qui sont isolées pour afficher uniquement l'élément modifié. Les modifications sont surlignées 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 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 dans la sortie qui affiche la configuration complète. Les modifications sont surlignées en vert (ajouts) ou en rouge (suppressions).



Certaines interfaces de ligne de commande peuvent afficher des ajouts et des suppressions à l'aide d'un formatage barré. L'affichage correct dépend de la prise en charge par votre client terminal des 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 la non-utilisation de sous-réseaux qui se chevauchent, ne sont pas violées.

Dans cet exemple, la validation a renvoyé des erreurs.

```

Validating new networking configuration... FAILED.

DK-10-224-S-20-G1: The admin subnet 172.18.0.0/16 overlaps the 172.18.0.0/21 grid network.
DK-10-224-S-22-S1: Duplicate Grid IP 172.16.5.18 (also in use by DK-10-224-S-21-ADM1)

You must correct these errors before you can apply any changes.
Checking for Grid Network IP address swaps... PASSED.

Press Enter to continue

```

Dans cet exemple, la validation a réussi.

```

Validating new networking configuration... PASSED.
Checking for Grid Network IP address swaps... PASSED.

Press Enter to continue

```

8. Une fois la validation effectuée, sélectionnez **10** pour appliquer la nouvelle configuration réseau.
9. Sélectionnez **étape** pour appliquer les modifications au prochain redémarrage des nœuds.



Vous devez sélectionner **étape**. N'effectuez pas de redémarrage progressif, que ce soit manuellement ou en sélectionnant **appliquer** au lieu de **étape** ; la grille ne démarrera pas correctement.

10. Une fois vos modifications terminées, sélectionnez **0** pour quitter l'outil Modifier l'IP.
11. Arrêtez tous les nœuds simultanément.



L'ensemble du réseau doit être arrêté, de sorte que tous les nœuds soient hors service en même temps.

12. Effectuez les modifications de réseau physiques ou virtuelles requises.
13. Vérifiez que tous les nœuds de la grille sont hors service.
14. Allumez tous les nœuds.
15. Une fois le réseau démarré avec succès :
 - a. Si vous avez ajouté de nouveaux serveurs NTP, supprimez les anciennes valeurs du serveur NTP.
 - b. Si vous avez ajouté de nouveaux serveurs DNS, supprimez les anciennes valeurs de serveur DNS.
16. Téléchargez le nouveau package de récupération à partir du gestionnaire de grille.
 - a. Sélectionnez **MAINTENANCE > Système > Package de récupération**.
 - b. Saisissez la phrase secrète d'approvisionnement.

Informations connexes

- ["Ajouter ou modifier des listes de sous-réseaux sur Grid Network"](#)
- ["Arrêter le nœud du réseau"](#)

Ajouter des interfaces au nœud existant

Linux : ajouter des interfaces d'administration ou de client à un nœud existant

Suivez ces étapes pour ajouter une interface sur le réseau d'administration ou le réseau client à un nœud Linux après son installation.

Si vous n'avez pas configuré `ADMIN_NETWORK_TARGET` ou `CLIENT_NETWORK_TARGET` dans le fichier de configuration du nœud sur l'hôte Linux lors de l'installation, utilisez cette procédure pour ajouter l'interface. Pour plus d'informations sur le fichier de configuration du nœud, consultez les instructions relatives à votre système d'exploitation Linux :

- ["Installer StorageGRID sur Red Hat Enterprise Linux"](#)
- ["Installer StorageGRID sur Ubuntu ou Debian"](#)

Vous effectuez cette procédure sur le serveur Linux hébergeant le nœud qui a besoin de la nouvelle attribution 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 l'IP. Voir ["Modifier la configuration"](#)

du réseau de nœuds" .

Étapes

1. Connectez-vous au serveur Linux hébergeant le nœud.
2. Modifier le fichier de configuration du nœud : `/etc/storagegrid/nodes/node-name.conf` .



Ne spécifiez aucun autre paramètre réseau, sinon une erreur de validation se produira.

- a. Ajoutez 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. Exécutez la commande de validation du nœud :

```
sudo storagegrid node validate node-name
```

4. Résoudre toutes les erreurs de validation.
5. Exécutez la commande de rechargement du nœud :

```
sudo storagegrid node reload node-name
```

Linux : ajouter des interfaces trunk ou d'accès à un nœud

Vous pouvez ajouter des interfaces de jonction ou d'accès supplémentaires à un nœud Linux après son installation. Les interfaces que vous ajoutez sont affichées sur la page Interfaces VLAN et sur la page Groupes HA.

Avant de commencer

- Vous avez accès aux instructions d'installation de StorageGRID sur votre plateforme Linux.
 - ["Installer StorageGRID sur Red Hat Enterprise Linux"](#)
 - ["Installer StorageGRID sur Ubuntu ou Debian"](#)
- Vous avez le `Passwords.txt` déposer.
- Tu as ["autorisations d'accès spécifiques"](#) .



N'essayez pas d'ajouter des interfaces à un nœud pendant qu'une mise à niveau logicielle, une procédure de récupération ou une procédure d'extension est active.

À propos de cette tâche

Suivez ces étapes pour ajouter une ou plusieurs interfaces supplémentaires à un nœud Linux après l'installation du nœud. Par exemple, vous souhaitez peut-être ajouter une interface de jonction à un nœud d'administration ou de passerelle, afin de pouvoir utiliser des interfaces VLAN pour séparer le trafic appartenant à différentes applications ou locataires. Ou, vous souhaitez peut-être ajouter une interface d'accès à utiliser dans 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 ajouter l'interface directement à un groupe HA ; vous n'avez pas besoin de configurer une interface VLAN.

Le nœud n'est pas disponible pendant une brève période lorsque vous ajoutez des 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_#####=value
```

Pour *#####*, 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 Interfaces VLAN et sur la page Groupes HA.

Par exemple:

```
INTERFACE_TARGET_0001=ens256, Trunk
```



Ne spécifiez aucun autre paramètre réseau, sinon une erreur de validation se produira.

4. Exécutez la commande suivante pour valider vos modifications dans le fichier de configuration du nœud :

```
sudo storagegrid node validate node-name
```

Corrigez 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
```

Après avoir terminé

- Si vous avez ajouté une ou plusieurs interfaces trunk, accédez à ["configurer 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, accédez à ["configurer des groupes de haute disponibilité"](#) pour ajouter les nouvelles interfaces directement aux groupes HA.

VMware : ajouter des interfaces de jonction ou d'accès à un nœud

Vous pouvez ajouter une jonction ou une interface d'accès à un nœud de machine virtuelle une fois le nœud installé. Les interfaces que vous ajoutez sont affichées sur la page Interfaces VLAN et sur la page Groupes HA.

Avant de commencer

- Vous avez accès aux instructions pour "[installer StorageGRID sur votre plateforme VMware](#)".
- Vous disposez de machines virtuelles VMware Admin Node et Gateway Node.
- Vous disposez d'un sous-réseau réseau qui n'est pas utilisé comme réseau de grille, d'administration ou de client.
- Vous avez le `Passwords.txt` déposer.
- Tu as "[autorisations d'accès spécifiques](#)".



N'essayez pas d'ajouter des interfaces à un nœud pendant qu'une mise à niveau logicielle, une procédure de récupération ou une procédure d'extension est active.

À propos de cette tâche

Suivez ces étapes pour ajouter une ou plusieurs interfaces supplémentaires à un nœud VMware une fois le nœud installé. Par exemple, vous souhaitez peut-être ajouter une interface de jonction à un nœud d'administration ou de passerelle, afin de pouvoir utiliser des interfaces VLAN pour séparer le trafic appartenant à différentes applications ou locataires. Ou vous souhaitez peut-être ajouter une interface d'accès à utiliser dans 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 ajouter l'interface directement à un groupe HA ; vous n'avez pas besoin de configurer une interface VLAN.

Le nœud peut être indisponible pendant une brève période lorsque vous ajoutez des interfaces.

Étapes

1. Dans vCenter, ajoutez une nouvelle carte réseau (type VMXNET3) à un nœud d'administration et à une machine virtuelle de nœud de passerelle. Cochez les cases **Connecté** et **Connecter à la mise sous tension**.

Network adapter 4 *		CLIENT683_old_vlan	☒ Connected
Status	☒ Connect At Power On		
Adapter Type	VMXNET 3		
DirectPath I/O	☒ Enable		

2. Utilisez SSH pour vous connecter au nœud d'administration ou au nœud de passerelle.
3. Utiliser `ip link show` pour confirmer que la nouvelle interface réseau ens256 est détectée.

```

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

```

Après avoir terminé

- Si vous avez ajouté une ou plusieurs interfaces trunk, accédez à ["configurer 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, accédez à ["configurer des groupes de haute disponibilité"](#) pour ajouter les nouvelles interfaces directement aux groupes HA.

Configurer les serveurs DNS

Vous pouvez ajouter, mettre à jour et supprimer des serveurs DNS afin de pouvoir utiliser des noms d'hôtes de noms de domaine complets (FQDN) plutôt que des adresses IP.

Pour utiliser des noms de domaine complets (FQDN) au lieu d'adresses IP lors de la spécification de 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 points de terminaison des services de plateforme, les pools de stockage Cloud, etc.

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 de maintenance ou root"](#).
- Vous disposez des adresses IP des serveurs DNS à configurer.

À propos de cette tâche

Pour garantir un bon fonctionnement, spécifiez deux ou trois serveurs DNS. Si vous spécifiez plus de trois, il est possible que seulement trois soient utilisés en raison de limitations connues du système d'exploitation sur certaines plates-formes. Si vous avez des restrictions de routage dans votre environnement, vous pouvez ["personnaliser la liste des serveurs DNS"](#) pour que les nœuds individuels (généralement tous les nœuds d'un site) utilisent un ensemble différent de trois serveurs DNS maximum.

Si possible, utilisez des serveurs DNS auxquels chaque site peut accéder localement pour garantir qu'un site isolé peut résoudre les noms de domaine complets pour les destinations externes.

Ajouter un serveur DNS

Suivez ces étapes 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

Suivez ces étapes 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 effectuez les modifications nécessaires.
3. Sélectionnez **Enregistrer**.

Supprimer un serveur DNS

Suivez ces étapes pour supprimer une adresse IP d'un serveur DNS.

Étapes

1. Sélectionnez **MAINTENANCE > Réseau > Serveurs DNS**.
2. Sélectionnez l'icône de suppression  à côté de l'adresse IP.
3. Sélectionnez **Enregistrer**.

Modifier la configuration DNS pour un nœud de grille 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** sur le Gestionnaire de grille pour configurer les serveurs DNS. Utilisez le script suivant uniquement si vous devez utiliser différents serveurs DNS pour différents nœuds de grille.

Étapes

1. Connectez-vous au nœud d'administration principal :
 - a. Entrez la commande suivante : `ssh admin@primary_Admin_Node_IP`
 - b. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.
 - c. Entrez la commande suivante pour passer en root : `su -`
 - d. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.

Lorsque vous êtes connecté en tant que root, l'invite passe de \$ à # .

- e. Ajoutez la clé privée SSH à l'agent SSH. Entrer: `ssh-add`
- f. Saisissez le mot de passe d'accès SSH répertorié dans le `Passwords.txt` déposer.
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 pour ajouter des serveurs de noms.
6. Suivez les instructions demandées pour les autres commandes.
7. Enregistrez vos modifications et quittez l'application : `save`
8. Fermez l'interpréteur de commandes sur le serveur : `exit`
9. Pour chaque nœud de la grille, répétez les étapes à partir de [connexion au nœud](#) à travers [fermeture de l'interpréteur de commandes](#) .
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. Entrer: `ssh-add -D`

Gérer les serveurs NTP

Vous pouvez ajouter, mettre à jour ou supprimer des serveurs NTP (Network Time Protocol) pour garantir que les données sont synchronisées avec précision entre les nœuds de grille 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 ["Autorisation d'accès de maintenance ou root"](#) .
- Vous disposez de la phrase secrète de provisionnement.
- Vous disposez des adresses IPv4 des serveurs NTP à configurer.

Comment StorageGRID utilise NTP

Le système StorageGRID utilise le protocole NTP (Network Time Protocol) pour synchroniser l'heure entre tous les nœuds de la grille.

Sur chaque site, au moins deux nœuds du système StorageGRID se voient attribuer le rôle NTP principal. Ils se synchronisent avec un minimum suggéré de quatre et un maximum de six sources de temps externes et entre eux. 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 principaux.

Les serveurs NTP externes se connectent aux nœuds auxquels vous avez précédemment attribué des rôles NTP principaux. Pour cette raison, il est recommandé de spécifier au moins deux nœuds avec des rôles NTP principaux.

Directives du 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. Pour cette raison, il est recommandé de spécifier au moins deux nœuds avec des rôles NTP principaux.
- 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 se produiront si ce nœud tombe en panne. De plus, la désignation de deux nœuds par site comme sources NTP principales garantit une synchronisation précise si un site est isolé du reste du réseau.
- Les serveurs NTP externes spécifiés doivent utiliser le protocole NTP. Vous devez spécifier des références de serveur NTP de Stratum 3 ou supérieur pour éviter les problèmes de dérive temporelle.



Lorsque vous spécifiez 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 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 les environnements de haute précision](#)".

Configurer les serveurs NTP

Suivez ces étapes 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, selon les besoins.

Vous devez inclure au moins quatre serveurs NTP et vous pouvez spécifier jusqu'à six serveurs.

3. Saisissez la phrase secrète de provisionnement de votre système StorageGRID, puis sélectionnez **Enregistrer**.

La page est désactivée jusqu'à ce que les mises à jour de configuration soient terminées.



Si tous vos serveurs NTP échouent au test de connexion après avoir enregistré les nouveaux serveurs NTP, ne continuez pas. Contactez le support technique.

Résoudre les problèmes de serveur NTP

Si vous rencontrez des problèmes avec la stabilité ou la disponibilité des serveurs NTP initialement spécifiés lors de l'installation, vous pouvez mettre à jour la liste des sources NTP externes utilisées par le système StorageGRID en ajoutant des serveurs supplémentaires ou en mettant à jour ou en supprimant des serveurs existants.

Restaurer la connectivité réseau pour les nœuds isolés

Dans certaines circonstances, un ou plusieurs groupes de nœuds peuvent ne pas être en mesure de contacter le reste du réseau. Par exemple, les modifications d'adresse IP à l'échelle d'un site ou d'un réseau peuvent entraîner l'isolement de nœuds.

À propos de cette tâche

L'isolement des nœuds est indiqué par :

- Alertes, telles que **Impossible de communiquer avec le nœud (Alertes > Actuel)**
- Diagnostics liés à la connectivité (**SUPPORT > Outils > Diagnostics**)

Certaines des conséquences de l'isolement des nœuds sont les suivantes :

- Si plusieurs nœuds sont isolés, vous ne pourrez peut-être pas vous connecter ni accéder au gestionnaire de grille.

- Si plusieurs nœuds sont isolés, les valeurs d'utilisation du stockage et de quota affichées sur le tableau de bord du gestionnaire de locataires peuvent être obsolètes. Les totaux seront mis à jour lorsque la connectivité réseau sera rétablie.

Pour résoudre le problème d'isolement, 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 qui ne contient pas le nœud 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 isolé ou au groupe de nœuds de contacter à nouveau l'ensemble de la grille.



Si le système de noms de domaine multidiffusion (mDNS) est désactivé dans les réseaux, vous devrez peut-être exécuter l'utilitaire de ligne de commande sur chaque nœud isolé.

Étapes

Cette procédure ne s'applique pas lorsque seuls certains services sont hors ligne ou signalent des erreurs de communication.

1. Accéder au nœud et vérifier `/var/local/log/dynip.log` pour les messages d'isolement.

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, elle contiendra un message indiquant que le nœud est peut-être isolé.

Sur les déploiements Linux, les messages d'isolation apparaîtraient 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 au réseau.

```
# /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.
- L'état du service IP dynamique est « En cours d'exécution » après avoir exécuté le `storagegrid-status` commande.
- Sur la page Nœuds, 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, il peut y avoir d'autres problèmes de réseau qui doivent être résolus.

Procédures d'hôte et de middleware

Linux : migrer le nœud de grille vers un 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 la fonctionnalité ou la disponibilité de votre grille.

Par exemple, vous souhaitez peut-être migrer un nœud pour effectuer une mise à jour corrective du système d'exploitation et redémarrer.

Avant de commencer

- Vous avez planifié votre déploiement StorageGRID pour inclure la prise en charge de la migration.
 - ["Exigences de migration des conteneurs de nœuds pour Red Hat Enterprise Linux"](#)
 - ["Exigences de migration de conteneurs Node pour Ubuntu ou Debian"](#)
- L'hôte cible est déjà préparé pour l'utilisation de StorageGRID .
- Le stockage partagé est utilisé pour tous les volumes de stockage par nœud
- Les interfaces réseau ont des noms cohérents entre 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. Cependant, si vous disposez de plusieurs nœuds du même type (deux nœuds de passerelle, par exemple), n'installez pas toutes les instances sur le même hôte.

Exporter le nœud depuis l'hôte source

Dans un premier temps, arrêtez le nœud de grille et exportez-le depuis l'hôte Linux source.

Exécutez les commandes suivantes sur l'hôte *source*.

Étapes

1. Obtenir l'état de tous les nœuds actuellement en cours d'exécution sur l'hôte source.

```
sudo storagegrid node status all
```

Exemple de sortie :

```
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 sortie :

```
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 sortie :

```
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. Prenez note de la import commande suggérée dans la sortie.

Vous exécuterez cette commande sur l'hôte cible à l'étape suivante.

Importer un nœud sur l'hôte cible

Après avoir exporté le nœud depuis l'hôte source, vous importez et validez le nœud sur l'hôte cible. La validation confirme que le nœud a accès aux mêmes périphériques de stockage de blocs et d'interface réseau que ceux dont il disposait 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 sortie :

```
Finished importing node DC1-S3 from /dev/mapper/sgws-dc1-s3-var-local.  
You should run 'storagegrid node validate DC1-S3'
```

2. Validez la configuration du nœud sur le nouvel hôte.

```
sudo storagegrid node validate DC1-S3
```

Exemple de sortie :

```
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, corrigez-les avant de démarrer le nœud migré.

Pour obtenir des informations de dépannage, consultez les instructions d'installation de StorageGRID pour votre système d'exploitation Linux.

- ["Installer StorageGRID sur Red Hat Enterprise Linux"](#)
- ["Installer StorageGRID sur 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. Sign in au gestionnaire de grille et vérifiez que l'état du nœud est vert sans alerte.



Vérifier que l'état du nœud est vert garantit que le nœud migré a complètement redémarré et rejoint la grille. Si le statut n'est pas vert, ne migrez aucun nœud supplémentaire afin de ne pas avoir 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
```

Confirmez que le nœud migré a un état d'exécution en cours d'exécution.

VMware : configurer la machine virtuelle pour un redémarrage automatique

Si la machine virtuelle ne redémarre pas après le redémarrage de VMware vSphere Hypervisor, vous devrez peut-être configurer la machine virtuelle pour un redémarrage

automatique.

Vous devez exécuter cette procédure si vous remarquez qu'une machine virtuelle ne redémarre pas pendant que vous récupérez un nœud de grille ou effectuez une autre procédure de maintenance.

Étapes

1. Dans l'arborescence VMware vSphere Client, sélectionnez la machine virtuelle qui n'est pas démarrée.
2. Cliquez avec le bouton droit sur la machine virtuelle et sélectionnez **Mettre sous tension**.
3. Configurez VMware vSphere Hypervisor pour redémarrer automatiquement la machine virtuelle à l'avenir.

Récupérer ou remplacer les nœuds

Avertissements et considérations pour la récupération des nœuds de grille

Si un nœud de grille tombe en panne, vous devez le récupérer dès que possible. Vous devez examiner tous les avertissements et considérations relatifs à la récupération des nœuds avant de commencer.



StorageGRID est un système distribué composé de plusieurs nœuds fonctionnant les uns avec les autres. N'utilisez pas d'instantanés de disque pour restaurer les nœuds de grille. Reportez-vous plutôt aux procédures de récupération et de maintenance pour chaque type de nœud.



Si un site StorageGRID entier est en panne, contactez le support technique. Le support technique travaillera avec vous pour développer et exécuter un plan de récupération de site qui maximise la quantité de données récupérées et répond à vos objectifs commerciaux. Voir ["Comment le support technique récupère un site"](#).

Voici quelques-unes des raisons pour lesquelles il est nécessaire de récupérer un nœud de réseau défaillant dès que possible :

- Un nœud de grille défaillant peut réduire la redondance des données système et objet, vous laissant vulnérable au risque de perte de données permanente si un autre nœud tombe en panne.
- Un nœud de réseau défaillant peut avoir un impact sur l'efficacité des opérations quotidiennes.
- Un nœud de réseau défaillant peut réduire votre capacité à surveiller les opérations du système.
- Un nœud de grille défaillant peut provoquer une erreur de serveur interne 500 si des règles ILM strictes sont en place.
- Si un nœud de grille n'est pas récupéré rapidement, les délais de récupération peuvent augmenter. Par exemple, des files d'attente peuvent se développer et doivent être effacées avant que la récupération ne soit terminée.

Suivez toujours la procédure de récupération pour le type spécifique de nœud de grille que vous récupérez. Les procédures de récupération varient pour les nœuds d'administration principaux ou non principaux, les nœuds de passerelle, les nœuds d'appliance et les nœuds de stockage.

Conditions préalables à la récupération des nœuds de grille

Toutes les conditions suivantes sont supposées lors de la récupération des nœuds de grille :

- Le matériel physique ou virtuel défaillant a été remplacé et configuré.
- La version du programme d'installation de l'appliance StorageGRID sur l'appliance de remplacement correspond à la version du logiciel de votre système StorageGRID, comme décrit dans ["Vérifier et mettre 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 récupération et le nœud d'administration principal.
- Si vous récupérez un nœud de stockage d'appliance, vous devez spécifier le même type de stockage que l'appliance d'origine (combiné, métadonnées uniquement ou données uniquement) lors de l'installation de

l'appliance. Si vous spécifiez un type de stockage différent, la récupération échouera et nécessitera la réinstallation de l'appliance avec le type de stockage correct spécifié.

Ordre de récupération des nœuds en cas de défaillance d'un serveur hébergeant plusieurs nœuds de grille

Si un serveur hébergeant plusieurs nœuds de grille tombe en panne, vous pouvez récupérer les nœuds dans n'importe quel ordre. Cependant, si le serveur défaillant héberge le nœud d'administration principal, vous devez d'abord récupérer ce nœud. La récupération du nœud d'administration principal en premier empêche les autres récupérations de nœuds de s'arrêter pendant qu'elles attendent de contacter le nœud d'administration principal.

Adresses IP des nœuds récupérés

N'essayez pas de récupérer 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 inutilisée.

Si vous utilisez une nouvelle adresse IP pour déployer le nouveau nœud, puis récupérez le nœud, la nouvelle adresse IP continuera d'être utilisée pour le nœud récupéré. Si vous souhaitez revenir à l'adresse IP d'origine, utilisez l'outil Modifier l'IP une fois la récupération terminée.

Rassembler les matériaux nécessaires à la récupération des nœuds du réseau

Avant d'effectuer les procédures de maintenance, vous devez vous assurer que vous disposez du matériel nécessaire pour récupérer un nœud de réseau défaillant.

Article	Remarques
Archive d'installation de StorageGRID	Si vous devez récupérer un nœud de grille, vous deveztélécharger les fichiers d'installation de StorageGRID pour votre plateforme. Remarque : vous n'avez pas besoin de télécharger de fichiers si vous récupérez des volumes de stockage défaillants sur un nœud de stockage.
Ordinateur portable de service	L'ordinateur portable de service doit avoir les éléments suivants : • Port réseau • Client SSH (par exemple, PuTTY) • "Navigateur Web pris en charge"

Article	Remarques
Paquet de relance .zip déposer	Obtenir une copie du package de récupération le plus récent .zip déposer: <code>sgws-recovery-package-id-revision.zip</code> Le contenu de la .zip les fichiers sont mis à jour à chaque modification du système. Il vous est demandé de stocker la version la plus récente du package de récupération dans un endroit sûr après avoir effectué ces modifications. Utilisez la copie la plus récente pour récupérer après une panne de réseau. Si le nœud d'administration principal fonctionne normalement, vous pouvez télécharger le package de récupération à partir du gestionnaire de grille. Sélectionnez MAINTENANCE > Système > Package de récupération. Si vous ne pouvez pas accéder au Grid Manager, vous pouvez trouver des copies chiffrées du package de récupération sur certains nœuds de stockage contenant le service ADC. Sur chaque nœud de stockage, examinez cet emplacement pour le package de récupération : <code>/var/local/install/sgws-recovery-package-grid-id-revision.zip.gpg</code> Utilisez le package de récupération avec le numéro de révision le plus élevé.
`Passwords.txt` déposer	Contient les mots de passe requis pour accéder aux nœuds de la grille sur la ligne de commande. Inclus dans le package de récupération.
Mot de passe d'approvisionnement	La phrase secrète est créée et documentée lors de la première installation du système StorageGRID . La phrase secrète de provisionnement n'est pas dans le <code>Passwords.txt</code> déposer.
Documentation actuelle pour votre plateforme	Accédez au site Web du fournisseur de la plateforme pour obtenir de la documentation. Pour connaître les versions actuellement prises en charge par votre plateforme, consultez le "Outil de matrice d'interopérabilité NetApp".

Téléchargez et extrayez les fichiers d'installation de StorageGRID

Téléchargez le logiciel et extrayez les fichiers, sauf si vous êtes "[récupération de volumes de stockage défaillants sur un nœud de stockage](#)".

Vous devez utiliser la version de StorageGRID actuellement exécutée sur la grille.

Étapes

1. Déterminez quelle version du logiciel est actuellement installée. En haut du gestionnaire de grille, sélectionnez l'icône d'aide et sélectionnez **À propos**.
2. Aller à la "[Page de téléchargement NetApp pour StorageGRID](#)".

- Sélectionnez la version de StorageGRID actuellement en cours d'exécution sur la grille.

Les versions du logiciel StorageGRID ont ce format : 11.x.y .

- Sign in avec le nom d'utilisateur et le mot de passe de votre compte NetApp .
- Lisez le contrat de licence utilisateur final, cochez la case, puis sélectionnez **Accepter et continuer**.
- Dans la colonne **Installer StorageGRID** de la page de téléchargement, sélectionnez l'option .tgz ou .zip fichier pour votre plateforme.

La version affichée dans le fichier d'archive d'installation doit correspondre à la version du logiciel actuellement installée.

Utilisez le .zip fichier si vous utilisez Windows.

Plate-forme	Archives d'installation
Red Hat Enterprise Linux	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

- Téléchargez et extrayez le fichier d'archive.
- Suivez l'étape appropriée à votre plateforme pour choisir les fichiers dont vous avez besoin, en fonction de votre plateforme 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.

- Si vous récupérez un "[Système Red Hat Enterprise Linux](#)" , sélectionnez les fichiers appropriés.

Chemin et nom du fichier	Description
	Un fichier texte qui décrit tous les fichiers contenus dans le fichier de téléchargement StorageGRID .
	Une licence gratuite qui ne fournit aucun droit d'assistance pour le produit.
	Package RPM pour l'installation des images de nœuds StorageGRID sur vos hôtes RHEL.
	Package RPM pour l'installation du service hôte StorageGRID sur vos hôtes RHEL.

Chemin et nom du fichier	Description
Outil de script de déploiement	Description
	Un script Python utilisé pour automatiser la configuration d'un système StorageGRID .
	Un script Python utilisé pour automatiser la configuration des appliances StorageGRID .
	Un exemple de fichier de configuration à utiliser avec le <code>configure-storagegrid.py</code> scénario.
	Un 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 l'intégration de Ping Federate.
	Un fichier de configuration vierge à utiliser avec le <code>configure-storagegrid.py</code> scénario.
	Exemple de rôle Ansible et de playbook pour la configuration des hôtes RHEL pour le déploiement du conteneur StorageGRID . Vous pouvez personnaliser le rôle ou le manuel selon vos besoins.
	Un exemple de script Python que vous pouvez utiliser pour vous connecter à l'API Grid Management lorsque l'authentification unique (SSO) est activée à l'aide d'Active Directory ou de Ping Federate.
	Un script d'aide appelé par le compagnon <code>storagegrid-ssoauth-azure.py</code> Script Python pour effectuer des interactions SSO avec Azure.
	Schémas d'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 hors production pour les tests de compatibilité de mise à niveau.

1. Si vous récupérez un "Système Ubuntu ou Debian" , sélectionnez les fichiers appropriés.

Chemin et nom du fichier	Description
	Un fichier texte qui décrit tous les fichiers contenus dans le fichier de téléchargement StorageGRID .
	Un fichier de licence NetApp non destiné à la production que vous pouvez utiliser pour les tests et les déploiements de preuve de concept.
	Paquet DEB pour l'installation des images de nœuds StorageGRID sur les hôtes Ubuntu ou Debian.
	Somme de contrôle MD5 pour le fichier <code>/debs/storagegrid-webscale-images-version-SHA.deb</code> .
	Paquet DEB pour l'installation du service hôte StorageGRID sur les hôtes Ubuntu ou Debian.
Outil de script de déploiement	Description
	Un script Python utilisé pour automatiser la configuration d'un système StorageGRID .
	Un script Python utilisé pour automatiser la configuration des appliances StorageGRID .
	Un 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 l'intégration de Ping Federate.
	Un exemple de fichier de configuration à utiliser avec le <code>configure-storagegrid.py</code> scénario.
	Un fichier de configuration vierge à utiliser avec le <code>configure-storagegrid.py</code> scénario.
	Exemple de rôle Ansible et de playbook pour la configuration des hôtes Ubuntu ou Debian pour le déploiement du conteneur StorageGRID . Vous pouvez personnaliser le rôle ou le manuel selon vos besoins.

Chemin et nom du fichier	Description
	Un exemple de script Python que vous pouvez utiliser pour vous connecter à l'API Grid Management lorsque l'authentification unique (SSO) est activée à l'aide d'Active Directory ou de Ping Federate.
	Un script d'aide appelé par le compagnon <code>storagegrid-ssoauth-azure.py</code> Script Python pour effectuer des interactions SSO avec Azure.
	Schémas d'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 hors production pour les tests de compatibilité de mise à niveau.

1. Si vous récupérez un "Système VMware" , sélectionnez les fichiers appropriés.

Chemin et nom du fichier	Description
	Un fichier texte qui décrit tous les fichiers contenus dans le fichier de téléchargement StorageGRID .
	Une licence gratuite qui ne fournit aucun droit d'assistance pour le produit.
	Le fichier de disque de machine virtuelle utilisé comme modèle pour la création de machines virtuelles de nœuds de grille.
	Le fichier modèle Open Virtualization Format(.ovf) et fichier manifeste(.mf) pour déployer le nœud d'administration principal.
	Le fichier modèle(.ovf) et fichier manifeste(.mf) pour déployer des nœuds d'administration non principaux.
	Le fichier modèle(.ovf) et fichier manifeste(.mf) pour le déploiement de nœuds de passerelle.

Chemin et nom du fichier	Description
	Le fichier modèle(<code>.ovf</code>) et fichier manifeste(<code>.mf</code>) pour déployer des nœuds de stockage basés sur des machines virtuelles.
Outil de script de déploiement	Description
	Un script shell Bash utilisé pour automatiser le déploiement de nœuds de grille virtuels.
	Un exemple de fichier de configuration à utiliser avec le <code>deploy-vsphere-ovftool.sh</code> scénario.
	Un script Python utilisé pour automatiser la configuration d'un système StorageGRID .
	Un script Python utilisé pour automatiser la configuration des appliances StorageGRID .
	Un exemple de script Python que vous pouvez utiliser pour vous connecter à l'API Grid Management lorsque l'authentification unique (SSO) est activée. Vous pouvez également utiliser ce script pour l'intégration de Ping Federate.
	Un exemple de fichier de configuration à utiliser avec le <code>configure-storagegrid.py</code> scénario.
	Un fichier de configuration vierge à utiliser avec le <code>configure-storagegrid.py</code> scénario.
	Un exemple de script Python que vous pouvez utiliser pour vous connecter à l'API Grid Management lorsque l'authentification unique (SSO) est activée à l'aide d'Active Directory ou de Ping Federate.
	Un script d'aide appelé par le compagnon <code>storagegrid-ssoauth-azure.py</code> Script Python pour effectuer des interactions SSO avec Azure.

Chemin et nom du fichier	Description
	Schémas d'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 hors production pour les tests de compatibilité de mise à niveau.

1. Si vous récupérez un système basé sur une appliance StorageGRID , sélectionnez les fichiers appropriés.

Chemin et nom du fichier	Description
	Package DEB pour l'installation des images de nœuds StorageGRID sur vos appliances.
	Somme de contrôle MD5 pour le fichier <code>/debs/storagegridwebscale-images-version-SHA.deb</code> .



Pour l'installation de l'appareil, ces fichiers ne sont nécessaires que si vous devez éviter le trafic réseau. L'appareil peut télécharger les fichiers requis à partir du nœud d'administration principal.

Sélectionnez la procédure de récupération du nœud

Vous devez sélectionner la procédure de récupération appropriée pour le type de nœud défaillant.

Nœud de grille	Procédure de récupération
Plus d'un nœud de stockage	Contactez le support technique. Si plusieurs nœuds de stockage sont défaillants, le support technique doit aider à la récupération pour éviter les incohérences de la base de données qui pourraient entraîner une perte de données. Une procédure de récupération du site peut être nécessaire. "Comment le support technique récupère un site"
Un seul nœud de stockage	La procédure de récupération du nœud de stockage dépend du type et de la durée de la panne. "Récupérer après une panne de nœud de stockage"

Nœud de grille	Procédure de récupération
Nœud d'administration	La procédure du nœud d'administration varie selon que vous devez récupérer le nœud d'administration principal ou un nœud d'administration non principal. "Récupérer après une panne du nœud d'administration"
Nœud de passerelle	"Récupérer après une panne du nœud de passerelle"
Nœud d'archive	"Récupération après une panne de nœud d'archivage (site de documentation StorageGRID 11.8)"



Si un serveur hébergeant plusieurs nœuds de grille tombe en panne, vous pouvez récupérer les nœuds dans n'importe quel ordre. Cependant, si le serveur défaillant héberge le nœud d'administration principal, vous devez d'abord récupérer ce nœud. La récupération du nœud d'administration principal en premier empêche les autres récupérations de nœuds de s'arrêter pendant qu'elles attendent de contacter le nœud d'administration principal.

Récupérer après une panne de nœud de stockage

Récupérer après une panne de nœud de stockage

La procédure de récupération d'un nœud de stockage défaillant dépend du type de défaillance et du type de nœud de stockage défaillant.

Utilisez ce tableau pour sélectionner la procédure de récupération pour un nœud de stockage défaillant.

Problème	Action	Remarques
- Plusieurs nœuds de stockage sont tombés en panne. - Un deuxième nœud de stockage est tombé en panne moins de 15 jours après une panne ou une récupération d'un nœud de stockage. Cela inclut le cas où un nœud de stockage échoue alors que la récupération d'un autre nœud de stockage est toujours en cours.	Contactez le support 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 une perte de données. Le support technique peut déterminer quand il est possible de commencer la récupération d'un deuxième nœud de stockage en toute sécurité. Remarque : si plusieurs nœuds de stockage contenant le service ADC échouent sur un site, vous perdez toutes les demandes de service de plateforme en attente pour ce site.

Problème	Action	Remarques
Plusieurs nœuds de stockage sur un site sont tombés en panne ou un site entier est tombé en panne.	Contactez le support technique. Il peut être nécessaire d'effectuer une procédure de récupération de site.	Le support technique évaluera votre situation et élaborera un plan de récupération. Voir "Comment le support technique récupère un site" .
Un nœud de stockage d'appareil est en panne.	"Récupérer le nœud de stockage de l'appareil"	La procédure de récupération des nœuds de stockage de l'apppliance est la même pour toutes les pannes.
Un ou plusieurs volumes de stockage sont tombés en panne, mais le lecteur système est intact	"Récupérer après une panne de volume de stockage lorsque le lecteur système est intact"	Cette procédure est utilisée pour les nœuds de stockage basés sur des logiciels.
Le lecteur système est en panne.	"Récupérer après une panne du lecteur système"	La procédure de remplacement du nœud dépend de la plate-forme de déploiement et de la défaillance éventuelle de volumes de stockage.



Certaines procédures de récupération StorageGRID utilisent Reaper pour gérer les réparations Cassandra. Les réparations se produisent automatiquement dès que les services concernés ou requis ont commencé. Vous remarquerez peut-être une sortie de script qui mentionne « reaper » ou « réparation Cassandra ». Si vous voyez un message d'erreur indiquant que la réparation a échoué, exécutez la commande indiquée dans le message d'erreur.

Récupérer le nœud de stockage de l'appareil

Avertissements concernant la récupération des nœuds de stockage de l'apppliance

La procédure de récupération d'un nœud de stockage d'apppliance StorageGRID défaillant est la même, que vous récupériez après la perte du lecteur système ou après la perte de volumes de stockage uniquement.



Si plusieurs nœuds de stockage sont en panne (ou sont hors ligne), contactez le support technique. N'effectuez pas la procédure de récupération suivante. Une perte de données pourrait survenir.



S'il s'agit de la deuxième panne d'un nœud de stockage en moins de 15 jours après une panne ou une récupération d'un nœud de stockage, contactez le support technique. La reconstruction de Cassandra sur deux nœuds de stockage ou plus dans un délai de 15 jours peut entraîner une perte de données.



Si plusieurs nœuds de stockage d'un site sont défaillants, une procédure de récupération de site peut être nécessaire. Voir ["Comment le support technique récupère un site"](#).



Si les règles ILM sont configurées pour stocker une seule copie répliquée et que la copie existe sur un volume de stockage défaillant, vous ne pourrez pas récupérer l'objet.



Pour les procédures de maintenance matérielle, telles que les instructions de remplacement d'un contrôleur ou de réinstallation de SANtricity OS, consultez le ["instructions d'entretien de votre appareil de stockage"](#) .

Préparer le nœud de stockage de l'appareil pour la réinstallation

Lors de la récupération 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 nœud de stockage défaillant :

- a. Entrez la commande suivante : `ssh admin@grid_node_IP`
- b. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.
- c. Entrez la commande suivante pour passer en root : `su -`
- d. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.

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'appareil redémarre et votre session SSH se termine. Il faut généralement environ 5 minutes pour que le programme d'installation de l'appliance StorageGRID soit disponible, bien que dans certains cas, vous devrez peut-être attendre jusqu'à 30 minutes.



N'essayez pas d'accélérer le redémarrage en coupant puis en éteignant l'appareil ou en le réinitialisant. Vous risquez d'interrompre les mises à niveau automatiques du BIOS, du BMC ou d'autres micrologiciels.

Le nœud de stockage de l'appliance StorageGRID est réinitialisé et les données sur le nœud de stockage ne sont plus accessibles. Les adresses IP configurées lors du processus d'installation d'origine doivent rester intactes ; cependant, il est recommandé de confirmer cela une fois la procédure terminée.

Après avoir exécuté le `sgareinstall` commande, tous les comptes, mots de passe et clés SSH provisionnés par StorageGRID sont supprimés et de nouvelles clés d'hôte sont générées.

Démarrer l'installation de l'appliance StorageGRID

Pour installer StorageGRID sur un nœud de stockage d'appliance, utilisez le programme d'installation de l'appliance StorageGRID , inclus sur l'appliance.

Avant de commencer

- L'appareil a été installé dans un rack, connecté 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 StorageGRID .
- Tous les sous-réseaux du réseau de grille répertoriés sur la page de configuration IP du programme d'installation de l'appliance StorageGRID ont été définis dans la liste des sous-réseaux du réseau de grille sur le nœud d'administration principal.
- Vous avez effectué ces tâches préalables en suivant les instructions d'installation de votre dispositif 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 de l'appliance. Vous pouvez utiliser l'adresse IP du réseau d'administration (port de gestion 1 sur le contrôleur), du réseau de grille ou du réseau client.

À propos de cette 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.



Lors de la récupération d'un nœud de stockage d'appliance, réinstallez-le avec le même type de stockage que l'appliance d'origine (combiné, métadonnées uniquement ou données uniquement). Si vous spécifiez un type de stockage différent, la récupération échouera et nécessitera la réinstallation de l'appliance avec le type de stockage correct spécifié.

- À mi-chemin du processus, l'installation s'arrête. Pour reprendre l'installation, vous devez vous connecter au 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 se termine et l'appliance est redémarrée.

Étapes

1. Ouvrez un navigateur et saisissez 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 du nœud d'administration principal, déterminez si vous devez spécifier l'adresse IP du nœud d'administration principal.

Le programme d'installation de l'appliance StorageGRID peut découvrir cette adresse IP automatiquement, en supposant que le nœud d'administration principal, ou au moins un autre nœud de grille avec ADMIN_IP configuré, est présent sur le même sous-réseau.

3. Si cette adresse IP n'est pas affichée ou si vous devez la modifier, spécifiez l'adresse :

Option	Étapes
Saisie IP manuelle	- Décochez la case Activer la découverte du nœud d'administration. - Saisissez l'adresse IP manuellement. - Cliquez sur Enregistrer. - Attendez que l'état de connexion de la nouvelle adresse IP devienne « prêt ».
Découverte automatique de tous les nœuds d'administration principaux connectés	- Cochez la case Activer la découverte du nœud d'administration. - Dans la liste des adresses IP découvertes, sélectionnez le nœud d'administration principal de la grille sur laquelle ce nœud de stockage d'appliance sera déployé. - Cliquez sur Enregistrer. - Attendez que l'état de connexion de la nouvelle adresse IP devienne « prêt ».

- Dans le champ **Nom du nœud**, entrez le même nom d'hôte (nom du système) que celui utilisé pour le nœud que vous récupérez, puis cliquez sur **Enregistrer**.
- Dans la section Installation, confirmez que l'état actuel est « Prêt à démarrer l'installation de *node name* dans la grille avec le nœud d'administration principal ``admin_ip`` et que le bouton **Démarrer l'installation** est activé.

Si le bouton **Démarrer l'installation** n'est pas activé, vous devrez peut-être modifier la configuration réseau ou les paramètres du port. Pour les instructions, consultez les instructions d'entretien de votre appareil.

- Depuis la page d'accueil du programme d'installation de l'appliance StorageGRID , cliquez sur **Démarrer l'installation**.

NetApp® StorageGRID® Appliance Installer

[Home](#)[Configure Networking ▾](#)[Configure Hardware ▾](#)[Monitor Installation](#)[Advanced ▾](#)

Home

 The installation is ready to be started. Review the settings below, and then click Start Installation.

Primary Admin Node connection

Enable Admin Node
discovery ☐

Primary Admin Node IP

Connection state

Connection to 172.16.4.210 ready

Node name

Node name

Installation

Current state

Ready to start installation of NetApp-SGA into grid with Admin Node 172.16.4.210.

L'état actuel passe à « L'installation est en cours » et la page Installation du moniteur s'affiche.



Si vous devez accéder manuellement à la page d'installation du moniteur, cliquez sur **Installation du moniteur** dans la barre de menus. Voir "[Surveiller l'installation de l'appareil](#)".

Surveiller l'installation de l'appliance StorageGRID

Le programme d'installation de l'appliance StorageGRID fournit un état jusqu'à ce que l'installation soit terminée. Une fois l'installation du logiciel terminée, l'appareil est redémarré.

Étapes

1. Pour suivre la progression de l'installation, cliquez sur **Surveiller l'installation** dans la barre de menus.

La page d'installation du moniteur affiche la progression de l'installation.

Monitor Installation

1. Configure storage			Running
Step	Progress	Status	
Connect to storage controller		Complete	
Clear existing configuration		Complete	
Configure volumes		Creating volume StorageGRID-obj-00	
Configure host settings		Pending	
2. Install OS			Pending
3. Install StorageGRID			Pending
4. Finalize installation			Pending

La barre d'état bleue indique quelle tâche est actuellement en cours. Les barres d'état vertes indiquent les tâches qui ont été effectuées avec succès.



Le programme d'installation garantit que les tâches effectuées lors d'une installation précédente ne sont pas réexécutées. Si vous réexécutez une installation, toutes les tâches qui n'ont pas besoin d'être réexécutées sont affichées avec une barre d'état verte et un statut « Ignoré ».

2. Passez en revue la progression des deux premières étapes de l'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 les volumes et configure les paramètres de l'hôte.

- **2. Installer le système d'exploitation**

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 **Install StorageGRID** s'interrompe 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.

Monitor Installation

1. Configure storage	Complete
2. Install OS	Complete
3. Install StorageGRID	Running
4. Finalize installation	Pending

Connected (unencrypted) to: QEMU

```

/platform.type: Device or resource busy
[2017-07-31T22:09:12.362566] INFO -- [INSG] NOTICE: seeding /var/local with c
ontainer data
[2017-07-31T22:09:12.366205] INFO -- [INSG] Fixing permissions
[2017-07-31T22:09:12.369633] INFO -- [INSG] Enabling syslog
[2017-07-31T22:09:12.511533] INFO -- [INSG] Stopping system logging: syslog-n
g.
[2017-07-31T22:09:12.570096] INFO -- [INSG] Starting system logging: syslog-n
g.
[2017-07-31T22:09:12.576360] INFO -- [INSG] Beginning negotiation for downloa
d of node configuration
[2017-07-31T22:09:12.581363] INFO -- [INSG]
[2017-07-31T22:09:12.585066] INFO -- [INSG]
[2017-07-31T22:09:12.588314] INFO -- [INSG]
[2017-07-31T22:09:12.591851] INFO -- [INSG]
[2017-07-31T22:09:12.594886] INFO -- [INSG]
[2017-07-31T22:09:12.598360] INFO -- [INSG]
[2017-07-31T22:09:12.601324] INFO -- [INSG]
[2017-07-31T22:09:12.604759] INFO -- [INSG]
[2017-07-31T22:09:12.607800] INFO -- [INSG]
[2017-07-31T22:09:12.610985] INFO -- [INSG]
[2017-07-31T22:09:12.614597] INFO -- [INSG]
[2017-07-31T22:09:12.618282] INFO -- [INSG] Please approve this node on the A
dmin Node GMI to proceed...

```

4. Aller à ["Sélectionnez Démarrer la récupération pour configurer le nœud de stockage de l'appliance"](#) .

Sélectionnez Démarrer la récupération pour configurer le nœud de stockage de l'appliance

Vous devez sélectionner Démarrer la récupération dans le gestionnaire de grille pour configurer un nœud de stockage d'appliance en remplacement du nœud défaillant.

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 de maintenance ou root"](#) .
- Vous disposez de la phrase secrète de provisionnement.

- Vous avez déployé un nœud de stockage d'appliance de récupération.
- Vous disposez de la date de début de toutes les tâches de réparation pour les données codées par effacement.
- Vous avez vérifié que le nœud de stockage n'a pas été reconstruit au cours des 15 derniers jours.

Étapes

1. Depuis le Gestionnaire de grille, sélectionnez **MAINTENANCE > Tâches > Récupération**.
2. Sélectionnez le nœud de grille que vous souhaitez récupérer dans la liste des 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 n'est pas prêt pour la récupération.

3. Saisissez la **phrase secrète de provisionnement**.
4. Cliquez sur **Démarrer la récupération**.

Recovery

Select the failed grid node to recover, enter your provisioning passphrase, and then click Start Recovery to begin the recovery procedure.

Pending Nodes

Search				
	Name	IPv4 Address	State	Recoverable
☒	104-217-S1	10.96.104.217	Unknown	

Passphrase

Provisioning Passphrase

Start Recovery

5. Surveillez la progression de la récupération dans le tableau des nœuds de grille de récupération.

Lorsque le nœud de grille atteint l'étape « En attente des étapes manuelles », passez à la rubrique suivante et effectuez les étapes manuelles pour remonter et reformatier les volumes de stockage de l'appliance.

Recovery

Select the failed grid node to recover, enter your provisioning passphrase, and then click Start Recovery to begin the recovery procedure.

Recovering Grid Node

Name	Start Time	Progress	Stage
dc2-s3	2016-09-12 16:12:40 PDT		Waiting For Manual Steps

Reset



À tout moment pendant la récupération, vous pouvez cliquer sur **Réinitialiser** pour démarrer une nouvelle récupération. Une boîte de dialogue apparaît, indiquant que le nœud sera laissé dans un état indéterminé si vous réinitialisez la procédure.

Info

Reset Recovery

Resetting the recovery procedure leaves the deployed grid node in an indeterminate state. To retry a recovery after resetting the procedure, you must restore the node to a pre-installed state:

- For VMware nodes, delete the deployed VM and then redeploy it.
- For StorageGRID appliance nodes, run "sgareinstall" on the node.
- For Linux nodes, run "storagegrid node force-recovery *node-name*" on the Linux host.

Do you want to reset recovery?

Cancel

OK

Si vous souhaitez réessayer la récupération après avoir réinitialisé la procédure, vous devez restaurer le nœud de l'appliance à un état préinstallé en exécutant `sgareinstall` sur le nœud.

Remonter et reformater les volumes de stockage de l'appareil (étapes manuelles)

Vous devez exécuter manuellement deux scripts pour remonter les volumes de stockage préservés et reformater tous les volumes de stockage défaillants. Le premier script remonte les volumes correctement formatés en tant que volumes de stockage StorageGRID. Le deuxième script reformate tous les volumes non montés, 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 défaillants dont vous savez qu'ils doivent être remplacés.

Exécution du `sn-remount-volumes` Le script peut vous aider à identifier des volumes de stockage supplémentaires défaillants.

- Vous avez vérifié qu'une mise hors service du nœud de stockage n'est pas en cours ou vous avez suspendu la procédure de mise hors service du nœud. (Dans le gestionnaire de grille, sélectionnez **MAINTENANCE > Tâches > Désactivation.**)
- Vous avez vérifié qu'une extension n'est pas en cours. (Dans le gestionnaire de grille, sélectionnez **MAINTENANCE > Tâches > Extension.**)



Contactez le support technique si plusieurs nœuds de stockage sont hors ligne ou si un nœud de stockage de cette grille a été reconstruit au cours des 15 derniers jours. Ne courez pas le `sn-recovery-postinstall.sh` scénario. La reconstruction de Cassandra sur deux ou plusieurs nœuds de stockage à 15 jours d'intervalle peut entraîner une perte de données.

À propos de cette tâche

Pour réaliser cette procédure, vous effectuez ces tâches de haut niveau :

- Connectez-vous au nœud de stockage récupéré.

- Exécutez le `sn-remount-volumes` script pour remonter des 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 du 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, remonte le volume de stockage. Toutes les données existantes sur le volume restent intactes.
- Vérifiez la sortie du script et résolvez les problèmes.
- Exécutez le `sn-recovery-postinstall.sh` scénario. Lorsque ce script s'exécute, il effectue les opérations suivantes.



Ne redémarrez pas un nœud de stockage pendant la récupération avant l'exécution `sn-recovery-postinstall.sh` (étape 4) pour reformater les volumes de stockage défectueux et restaurer les métadonnées de l'objet. Redémarrer le nœud de stockage avant `sn-recovery-postinstall.sh` complète provoque des erreurs pour les services qui tentent de démarrer et provoque la sortie des nœuds de l'appliance StorageGRID du mode de maintenance.

- Reformate tous les volumes de stockage que le `sn-remount-volumes` les scripts n'ont pas pu être montés ou ont été trouvés comme étant mal formatés.



Si 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.

- Reconstitue 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 :

- Entrez la commande suivante : `ssh admin@grid_node_IP`
- Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.
- Entrez la commande suivante pour passer en root : `su -`
- Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.

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 sont tombés en panne, vous pouvez ignorer cette étape et exécuter le deuxième script pour reformater tous les volumes de stockage non montés.

- Exécutez le script : `sn-remount-volumes`

Ce script peut prendre des heures à s'exécuter sur des volumes de stockage contenant des données.

b. Pendant que le script s'exécute, examinez la sortie et répondez à toutes les invites.



Selon vos besoins, vous pouvez utiliser le `tail -f` commande pour surveiller 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 will attempt to restore data redundancy by making
additional replicated copies or EC fragments, according to the rules
in the active ILM policies.

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 will attempt to restore data redundancy by making
additional replicated copies or EC fragments, according to the rules
in the active ILM policies.

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 présentaient des erreurs.

- `/dev/sdb` a réussi le contrôle de cohérence du système de fichiers XFS et avait une structure de volume valide, il a donc été remonté avec succès. Les données sur les appareils remontés par le script sont conservées.
- `/dev/sdc` échec de la vérification de cohérence du système de fichiers XFS car le volume de stockage était nouveau ou corrompu.
- `/dev/sdd` n'a pas pu être monté car le disque n'a pas été initialisé ou le superbloc du disque était corrompu. Lorsque le script ne peut pas monter un volume de stockage, il vous demande si vous souhaitez exécuter la vérification de cohérence du système de fichiers.

- Si le volume de stockage est connecté 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 connecté 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 le contrôle 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 nœud de stockage (le configured LDR noid affiché en haut). Ce message indique que ce volume appartient à un autre nœud de stockage.`

3. Vérifiez la sortie du script et résolvez les problèmes.



Si un volume de stockage a échoué à la vérification de cohérence du système de fichiers XFS ou n'a pas pu être monté, examinez attentivement les messages d'erreur dans la sortie. Vous devez comprendre les implications de l'exécution de la `sn-recovery-postinstall.sh` script sur ces volumes.

- Vérifiez que les résultats incluent une entrée pour tous les volumes attendus. Si des volumes ne sont pas répertoriés, réexécutez le script.
- Consultez les messages de tous les périphériques montés. Assurez-vous qu'il n'y a aucune erreur indiquant qu'un volume de stockage n'appartient pas à ce nœud de stockage.

Dans l'exemple, la sortie pour `/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 pourrait entraîner une perte de données.

- Si des périphériques de stockage n'ont pas pu être montés, notez le nom du périphérique et réparez ou remplacez-le.



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 du volume, qui est une entrée requise lorsque vous exécutez le `repair-data` script pour restaurer les données de l'objet sur le volume (la procédure suivante).

- Après avoir réparé ou remplacé tous les périphériques non montables, exécutez le `sn-remount-volumes` script à nouveau pour confirmer que tous les volumes de stockage qui peuvent 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 qu'il contient seront supprimés. Si vous aviez deux copies des données de l'objet, vous n'en aurez qu'une seule jusqu'à ce que vous terminiez la procédure suivante (restauration des données de l'objet).



Ne courez pas le `sn-recovery-postinstall.sh` script si vous pensez que les données restantes sur un volume de stockage défaillant ne peuvent pas être reconstruites ailleurs dans la grille (par exemple, si votre politique ILM utilise une règle qui ne fait qu'une seule copie ou si les volumes ont échoué sur plusieurs nœuds). Contactez plutôt le support technique pour déterminer comment récupérer vos données.

4. Exécutez le `sn-recovery-postinstall.sh` scénario: `sn-recovery-postinstall.sh`

Ce script reformate tous les volumes de stockage qui n'ont pas pu être montés ou qui se sont avérés mal formatés ; reconstruit la base de données Cassandra sur le nœud, si nécessaire ; et démarre les services sur le nœud de stockage.

Soyez attentif aux 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'exécutera en arrière-plan si une interruption du réseau se produit et met fin à la session SSH, mais vous pouvez afficher la progression à partir de la page de récupération.
- Si le nœud de stockage utilise le service RSM, le script peut sembler se bloquer pendant 5 minutes lorsque les services du nœud sont redémarrés. Ce délai de 5 minutes est attendu à chaque démarrage du service RSM pour la première fois.



Le service RSM est présent sur les nœuds de stockage qui incluent le service ADC.



Certaines procédures de récupération StorageGRID utilisent Reaper pour gérer les réparations Cassandra. Les réparations se produisent automatiquement dès que les services concernés ou requis ont commencé. Vous remarquerez peut-être une sortie de script qui mentionne « reaper » ou « réparation Cassandra ». Si vous voyez 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` le script s'exécute, surveillez la page de récupération dans le gestionnaire de grille.

La barre de progression et la colonne Étape de la page de récupération fournissent un état de haut niveau de l'état de récupération. `sn-recovery-postinstall.sh` scénario.

Recovery

Select the failed grid node to recover, enter your provisioning passphrase, and then click Start Recovery to begin the recovery procedure.

Pending Nodes

Search				
Name	IPv4 Address	State	Recoverable	
No results found.				

Recovering Grid Node

Name	Start Time	Progress	Stage
DC1-S3	2016-06-02 14:03:35 PDT		Recovering Cassandra

6. Après le `sn-recovery-postinstall.sh` le script a démarré les services sur le nœud, vous pouvez restaurer les données de l'objet sur n'importe quel volume de stockage formaté par le script.

Le script vous demande si vous souhaitez utiliser le processus de restauration du volume Grid Manager.

- Dans la plupart des cas, vous devriez ["restaurer les données d'objet à l'aide de Grid Manager"](#) . Répondre `y` pour utiliser le gestionnaire de grille.
- Dans de rares cas, par exemple lorsque le support technique vous le demande ou lorsque vous savez que le nœud de remplacement dispose de moins de volumes disponibles pour le stockage d'objets que le nœud d'origine, vous devez ["restaurer les données de l'objet manuellement"](#) en utilisant le `repair-data` scénario. Si l'un de ces cas s'applique, répondez `n` .



Si vous répondez `n` pour utiliser le processus de restauration de volume de Grid Manager (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 tâches de restauration manuelle à l'aide de Grid Manager.

Après avoir effectué votre sélection, le script se termine et les étapes suivantes pour récupérer les données de l'objet s'affichent. Après avoir examiné ces étapes, appuyez sur n'importe quelle touche pour revenir à la ligne de commande.

Restaurer les données d'objet sur le volume de stockage de l'appareil

Après avoir récupéré les volumes de stockage pour le nœud de stockage de l'appliance, vous pouvez restaurer les données d'objet répliquées ou codées par effacement qui ont été perdues lors de l'échec du nœud de stockage.

Quelle procédure dois-je utiliser ?

Dans la mesure du possible, restaurez les données de l'objet à l'aide de la page **Restauration de volume** dans le gestionnaire de grille.

- Si les volumes sont répertoriés dans **MAINTENANCE > Restauration de volume > Nœuds à restaurer**, restaurez les données de l'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 de volume > Nœuds à restaurer**, suivez les étapes ci-dessous pour utiliser le `repair-data` script pour restaurer les données de l'objet.

Si le nœud de stockage récupéré contient moins de volumes que le nœud qu'il remplace, vous devez utiliser le `repair-data` scénario.



Le script de réparation des données est obsolète et sera supprimé dans une prochaine version. Lorsque cela est possible, utilisez le "[Procédure de restauration de volume dans le gestionnaire de grille](#)".

Utilisez le `repair-data` script pour restaurer les données de l'objet

Avant de commencer

- Vous avez confirmé que le nœud de stockage récupéré a un état de connexion **Connecté***  dans l'onglet ***NODES > Aperçu** dans le Gestionnaire de grille.

À propos de cette tâche

Les données d'objet peuvent être restaurées à partir d'autres nœuds de stockage ou d'un pool de stockage cloud, en supposant que les règles ILM de la grille ont été configurées de manière à ce que des 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 récupérer l'objet.
- Si la seule copie restante d'un objet se trouve dans un pool de stockage Cloud, StorageGRID doit émettre plusieurs requêtes au point de terminaison du pool de stockage Cloud pour restaurer les données de l'objet. Avant d'effectuer cette procédure, contactez le support technique pour obtenir de l'aide afin d'estimer le délai de récupération et les coûts associés.

À propos de la `repair-data` scénario

Pour restaurer les données d'un objet, exécutez la commande `repair-data` scénario. Ce script démarre le processus de restauration des données d'objet et fonctionne avec l'analyse ILM pour garantir que les règles ILM sont respectées.

Sélectionnez **Données répliquées** ou **Données codées par effacement (EC)** ci-dessous pour découvrir les différentes options pour `repair-data` script, selon que vous restaurez des données répliquées ou des données codées par 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` à partir de la ligne de commande du nœud d'administration principal.



Le script de réparation des données est obsolète et sera supprimé dans une prochaine version. Lorsque cela est possible, utilisez le "[Procédure de restauration de volume dans le gestionnaire de grille](#)".

Données répliquées

Deux commandes sont disponibles pour restaurer les données répliquées, selon que vous devez réparer l'intégralité du nœud ou uniquement certains volumes du 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 codées par effacement (EC)

Deux commandes sont disponibles pour restaurer les données codées par effacement, selon que vous devez réparer l'intégralité du nœud ou uniquement certains volumes du nœud :

```
repair-data start-ec-node-repair
```

```
repair-data start-ec-volume-repair
```

Vous pouvez suivre les réparations des données codées par effacement avec cette commande :

```
repair-data show-ec-repair-status
```



Les réparations des données codées par effacement peuvent commencer lorsque certains nœuds de stockage sont hors ligne. Cependant, si toutes les données codées par effacement ne peuvent pas être comptabilisées, la réparation ne peut pas être effectuée. La réparation sera terminée une fois que tous les nœuds seront disponibles.



Le travail de réparation EC réserve temporairement une grande quantité de stockage. Des alertes de stockage peuvent être déclenchées, mais seront résolues une fois la réparation terminée. S'il n'y a pas suffisamment 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 réussi.

Rechercher le nom d'hôte pour le nœud de stockage

1. Connectez-vous au nœud d'administration principal :

- Entrez la commande suivante : `ssh admin@primary_Admin_Node_IP`
- Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.
- Entrez la commande suivante pour passer en root : `su -`
- Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.

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 nœud de stockage pour les volumes de stockage restaurés. Pour voir une liste de tous les nœuds de la grille, saisissez ce qui suit : `cat /etc/hosts` .

Réparer les données si tous les volumes sont en panne

Si tous les volumes de stockage sont en panne, réparez l'ensemble du nœud. Suivez les instructions pour les **données répliquées**, les **données codées par effacement (EC)** ou les deux, selon que vous utilisez des données répliquées, des données codées par effacement (EC) ou les deux.

Si seuls certains volumes sont en panne, accédez à [Réparer les données si seuls certains volumes sont défaillants](#).



Tu ne peux pas courir `repair-data` opérations pour plusieurs nœuds en même temps. Pour récupérer plusieurs nœuds, contactez le support technique.

Données répliquées

Si votre grille comprend des données répliquées, utilisez le `repair-data start-replicated-node-repair` commande avec le `--nodes` option, où `--nodes` est le nom d'hôte (nom du système), pour réparer l'ensemble 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 parvient pas à localiser les données d'objet répliquées. Des alertes peuvent être déclenchées sur les nœuds de stockage dans tout le système. Vous devez déterminer la cause de la perte et si une récupération est possible. Voir "[Enquêter sur les objets perdus](#)".

Données codées par effacement (EC)

Si votre grille contient des données codées par effacement, utilisez le `repair-data start-ec-node-repair` commande avec le `--nodes` option, où `--nodes` est le nom d'hôte (nom du système), pour réparer l'ensemble du nœud de stockage.

Cette commande répare les données codées par effacement sur un nœud de stockage nommé SG-DC-SN3 :

```
repair-data start-ec-node-repair --nodes SG-DC-SN3
```

L'opération renvoie un unique `repair ID` qui identifie ceci `repair_data` opération. Utilisez ceci `repair ID` pour suivre les progrès et les résultats de la `repair_data` opération. Aucun autre commentaire n'est renvoyé une fois le processus de récupération terminé.

Les réparations des données codées par effacement peuvent commencer lorsque certains nœuds de stockage sont hors ligne. La réparation sera terminée une fois que tous les nœuds seront disponibles.

Réparer les données si seuls certains volumes sont défaillants

Si seulement certains volumes sont défaillants, réparez les volumes concernés. Suivez les instructions pour les **données répliquées**, les **données codées par effacement (EC)** ou les deux, selon que vous utilisez des données répliquées, des données codées par effacement (EC) ou les deux.

Si tous les volumes sont en panne, accédez à [Réparer les données si tous les volumes sont en panne](#).

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 être sur le même nœud de stockage. Si vous devez restaurer des volumes pour plusieurs nœuds de stockage, contactez le support technique.

Données répliquées

Si votre grille contient des données répliquées, utilisez le `start-replicated-volume-repair` commande avec le `--nodes` option pour identifier le nœud (où `--nodes` est le nom d'hôte du nœud). Ajoutez ensuite soit le `--volumes` ou `--volume-range` option, comme illustré dans les exemples suivants.

Volume unique : Cette commande restaure les données répliquées sur 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 sur 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
```

Plusieurs volumes non séquentiels : Cette commande restaure les données répliquées sur les 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 parvient pas à localiser les données d'objet répliquées. Des alertes peuvent être déclenchées sur les nœuds de stockage dans tout 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 codées par effacement (EC)

Si votre grille contient des données codées par effacement, utilisez le `start-ec-volume-repair` commande avec le `--nodes` option pour identifier le nœud (où `--nodes` est le nom d'hôte du nœud). Ajoutez ensuite soit le `--volumes` ou `--volume-range` option, comme illustré dans les exemples suivants.

Volume unique : Cette commande restaure les données codées par effacement sur le 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 codées par 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 séquentiels : cette commande restaure les données codées par effacement sur les 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 unique `repair ID` qui identifie ceci `repair_data` opération.

Utilisez ceci `repair ID` pour suivre les progrès et les résultats de la `repair_data` opération. Aucun autre commentaire n'est renvoyé une fois le processus de récupération terminé.



Les réparations des données codées par effacement peuvent commencer lorsque certains nœuds de stockage sont hors ligne. La réparation sera terminée une fois que tous les nœuds seront disponibles.

Réparations de moniteurs

Surveillez l'état des tâches de réparation, selon que vous utilisez des **données répliquées**, des **données codées par effacement (EC)** ou les deux.

Vous pouvez également surveiller l'état des tâches de restauration de volume en cours et afficher un historique des tâches de restauration terminées dans "[Gestionnaire de grille](#)".

Données répliquées

- Pour obtenir une estimation du pourcentage d'achèvement de la réparation répliquée, ajoutez le `show-replicated-repair-status` option à la commande `repair-data`.

```
repair-data show-replicated-repair-status
```

- Pour déterminer si les réparations sont terminées :
 - a. Sélectionnez **NODES > Nœud de stockage en cours de réparation > ILM**.
 - b. Passez en revue les attributs dans la section Évaluation. Lorsque les réparations sont terminées, l'attribut **En attente - Tout** indique 0 objet.
- Pour suivre la réparation plus en détail :
 - a. Sélectionnez **SUPPORT > Outils > Topologie de grille**.
 - b. Sélectionnez **grid > Nœud de stockage en cours de réparation > LDR > Data Store**.
 - c. Utilisez une combinaison des attributs suivants pour déterminer, aussi bien que possible, si les réparations répliquées sont complètes.



Des incohérences de Cassandra peuvent être présentes et les réparations ayant échoué 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 supérieure à la période d'analyse actuelle (fournie par l'attribut **Période d'analyse — Estimée**), cela signifie que l'analyse ILM n'a trouvé aucun objet à haut risque devant être réparé sur aucun nœud.



Les objets à haut risque sont des objets qui risquent d'être complètement perdus. Cela n'inclut pas les objets qui ne satisfont pas à leur configuration ILM.

- **Période d'analyse — Estimée (XSCM)** : utilisez cet attribut pour estimer quand un changement de politique sera appliqué aux objets précédemment ingérés. Si l'attribut **Réparations tentées** n'augmente pas pendant une période supérieure à la période d'analyse actuelle, il est probable que des réparations répliquées sont effectuées. Notez que la période d'analyse peut changer. L'attribut **Période d'analyse — Estimée (XSCM)** s'applique à l'ensemble de la grille et correspond au maximum de toutes les périodes d'analyse des nœuds. Vous pouvez interroger l'historique de l'attribut **Période d'analyse — Estimée** pour la grille afin de déterminer une période appropriée.

Données codées par effacement (EC)

Pour surveiller la réparation des données codées par effacement et réessayer toutes les demandes qui auraient échoué :

1. Déterminer l'état des réparations des données codées par effacement :
 - Sélectionnez **SUPPORT > Outils > Métriques** pour afficher le temps estimé jusqu'à l'achèvement et le pourcentage d'achèvement de la tâche en cours. Ensuite, sélectionnez **EC Overview** dans la section Grafana. Consultez les tableaux de bord **Temps estimé d'achèvement du travail EC de la grille** et **Pourcentage d'achèvement du travail EC de la grille**.
 - Utilisez cette commande pour voir l'état d'un élément spécifique `repair-data` opération:

```
repair-data show-ec-repair-status --repair-id repair ID
```

- Utilisez cette commande pour lister toutes les réparations :

```
repair-data show-ec-repair-status
```

La sortie répertorie les informations, y compris `repair ID` , pour toutes les réparations effectuées et en cours.

2. Si la sortie indique que l'opération de réparation a échoué, utilisez le `--repair-id` possibilité de réessayer la réparation.

Cette commande réessaie une réparation de nœud ayant échoué, en utilisant l'ID de réparation 6949309319275667690 :

```
repair-data start-ec-node-repair --repair-id 6949309319275667690
```

Cette commande réessaie une réparation de volume ayant échoué, en utilisant l'ID de réparation 6949309319275667690 :

```
repair-data start-ec-volume-repair --repair-id 6949309319275667690
```

Vérifier l'état du stockage après la récupération du nœud de stockage de l'appliance

Après avoir récupéré un nœud de stockage d'appliance, vous devez vérifier que l'état souhaité du nœud de stockage de l'appliance est défini sur en ligne et vous assurer que l'état sera en ligne par défaut à chaque redémarrage du serveur de nœud 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 récupéré et la récupération des données est terminée.

Étapes

1. Sélectionnez **SUPPORT > Outils > Topologie de grille**.
2. Vérifiez les valeurs de **Nœud de stockage récupéré > LDR > Stockage > État de stockage — Souhaité** et **État de stockage — Actuel**.

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 – Souhaité**, sélectionnez **En ligne**.
 - c. Cliquez sur **Appliquer les modifications**.
 - d. Cliquez sur l'onglet **Aperçu** et confirmez que les valeurs de **État de stockage — Souhaité** et **État de stockage — Actuel** sont mises à jour sur En ligne.

Récupérer après une panne de volume de stockage lorsque le lecteur système est intact

Récupérer après une panne de volume de stockage lorsque le lecteur système est intact

Vous devez effectuer une série de tâches pour récupérer un nœud de stockage logiciel où un ou plusieurs volumes de stockage sur le nœud de stockage sont tombés en panne, mais le lecteur système est intact. Si seuls les volumes de stockage sont en panne, le nœud de stockage est toujours disponible pour le système StorageGRID .



Cette procédure de récupération s'applique uniquement aux nœuds de stockage basés sur des logiciels. Si les volumes de stockage sont en panne sur un nœud de stockage d'apppliance, utilisez plutôt la procédure d'apppliance : ["Récupérer le nœud de stockage de l'appareil"](#) .

Cette procédure de récupération comprend les tâches suivantes :

- ["Examiner les avertissements pour la récupération du volume de stockage"](#)
- ["Identifier et démonter les volumes de stockage défectueux"](#)
- ["Récupérer les volumes et reconstruire la base de données Cassandra"](#)
- ["Restaurer les données de l'objet"](#)
- ["Vérifiez l'état de stockage"](#)

Avertissements concernant la récupération du volume de stockage

Avant de récupérer des volumes de stockage défectueux pour un nœud de stockage, consultez les avertissements suivants.

Les volumes de stockage (ou rangedbs) d'un nœud 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 de base 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 pourrait également être reconstruite dans les circonstances suivantes :

- 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 tombent en panne et sont récupérés.

Lorsque Cassandra est reconstruit, le système utilise les informations provenant d'autres nœuds de stockage. Si trop de nœuds de stockage sont hors ligne, certaines données Cassandra peuvent ne pas être disponibles. Si Cassandra a été reconstruit récemment, les données Cassandra peuvent ne pas encore être cohérentes sur l'ensemble de la grille. Une perte de données peut se produire si Cassandra est reconstruit alors que trop de nœuds de stockage sont hors ligne ou si deux nœuds de stockage ou plus sont reconstruits à 15 jours d'intervalle.



Si plusieurs nœuds de stockage sont en panne (ou sont hors ligne), contactez le support technique. N'effectuez pas la procédure de récupération suivante. Une perte de données pourrait survenir.



S'il s'agit de la deuxième panne d'un nœud de stockage en moins de 15 jours après une panne ou une récupération d'un nœud de stockage, contactez le support technique. La reconstruction de Cassandra sur deux nœuds de stockage ou plus dans un délai de 15 jours peut entraîner une perte de données.



Si plusieurs nœuds de stockage d'un site sont défaillants, une procédure de récupération de site peut être nécessaire. Voir ["Comment le support technique récupère un site"](#).



Si les règles ILM sont configurées pour stocker une seule copie répliquée et que la copie existe sur un volume de stockage défaillant, vous ne pourrez pas récupérer l'objet.

Informations connexes

["Avertissements et considérations pour la récupération des nœuds de grille"](#)

Identifier et démonter les volumes de stockage défaillants

Lors de la récupération d'un nœud de stockage avec des volumes de stockage défaillants, vous devez identifier et démonter les volumes défaillants. Vous devez vérifier que seuls les volumes de stockage défaillants sont reformatés dans le cadre de la procédure de récupération.

Avant de commencer

Vous êtes connecté au Grid Manager à l'aide d'un ["navigateur Web pris en charge"](#).

À propos de cette tâche

Vous devez récupérer les volumes de stockage défaillants dès que possible.

La première étape du processus de récupération 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 connectés mais ont un système de fichiers corrompu de manière aléatoire, le système peut ne détecter aucune corruption dans les parties inutilisées ou non allouées du disque.



Vous devez terminer cette procédure avant d'effectuer des étapes manuelles pour récupérer les volumes, telles que l'ajout ou la réattache 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 pourriez rencontrer une erreur du système de fichiers qui entraînerait le blocage ou l'échec du script.



Réparez le matériel et fixez correctement les disques avant d'exécuter le `reboot` commande.



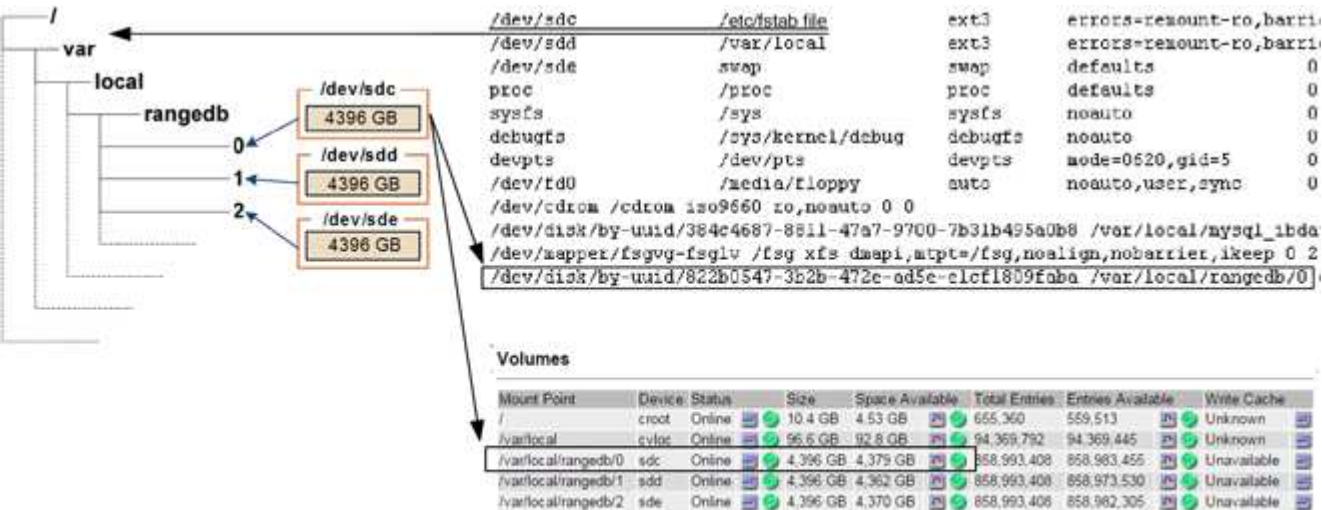
Identifiez soigneusement les volumes de stockage défaillants. Vous utiliserez ces informations pour vérifier quels volumes doivent être reformatés. Une fois qu'un volume a été reformaté, les données sur le volume ne peuvent pas être récupérées.

Pour récupérer correctement les volumes de stockage défaillants, vous devez connaître à la fois les noms des

périphériques des volumes de stockage défaillants et leurs ID de volume.

Lors de l'installation, chaque périphérique de stockage se voit attribuer un identifiant unique universel (UUID) du système de fichiers et est monté sur un répertoire rangedb sur le nœud de stockage à l'aide de cet UUID du système de fichiers attribué. L'UUID du système de fichiers et le répertoire rangedb sont répertoriés dans le /etc/fstab déposer. Le nom du périphérique, le répertoire rangedb et la taille du volume monté sont affichés dans le gestionnaire de grille.

Dans l'exemple suivant, l'appareil /dev/sdc a une taille de volume de 4 To, est monté sur /var/local/rangedb/0 , en utilisant le nom de l'appareil /dev/disk/by-uuid/822b0547-3b2b-472e-ad5e-e1cf1809faba dans le/etc/fstab déposer:



Étapes

1. Suivez les étapes suivantes pour enregistrer les volumes de stockage défaillants et leurs noms de périphériques :
 - a. Sélectionnez **SUPPORT > Outils > Topologie de grille**.
 - b. Sélectionnez **site > nœud de stockage défaillant > LDR > stockage > aperçu > principal** et recherchez les magasins d'objets avec des 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 > nœud de stockage défaillant > SSM > ressources > aperçu > principal**. Déterminez le point de montage et la taille du volume de chaque volume de stockage défaillant 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 nœud de stockage défaillant :

- Entrez la commande suivante : `ssh admin@grid_node_IP`
- Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.
- Entrez la commande suivante pour passer en root : `su -`
- Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.

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, précisez 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.
```

En quelques secondes, le volume est démonté. Des messages apparaissent indiquant chaque étape du processus. Le message final indique que le volume est démonté.

5. Si le démontage échoue parce que le volume est occupé, vous pouvez forcer un démontage en utilisant le `--use-umountof` option:



Forcer un démontage en utilisant le `--use-umountof` Cette option peut entraîner un comportement inattendu ou un blocage des processus ou des 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
```

Récupérer les volumes de stockage défaillants et reconstruire la base de données Cassandra

Vous devez exécuter un script qui reformate et remonte le stockage sur les volumes de stockage défaillants et reconstruit la base de données Cassandra sur le nœud de stockage si le système détermine que cela est nécessaire.

Avant de commencer

- Vous avez le `Passwords.txt` déposer.
- Les lecteurs système du serveur sont intacts.
- La cause de la panne a été identifiée et, si nécessaire, du matériel de stockage de remplacement a déjà été acquis.
- La taille totale du stockage de remplacement est la même que l'original.
- Vous avez vérifié qu'une mise hors service du nœud de stockage n'est pas en cours ou vous avez suspendu la procédure de mise hors service du nœud. (Dans le gestionnaire de grille, sélectionnez **MAINTENANCE > Tâches > Désactivation.**)
- Vous avez vérifié qu'une extension n'est pas en cours. (Dans le gestionnaire de grille, sélectionnez **MAINTENANCE > Tâches > Extension.**)
- Tu as [examiné les avertissements concernant la récupération du volume de stockage](#) .

Étapes

1. Si nécessaire, remplacez le stockage physique ou virtuel défaillant associé aux volumes de stockage défaillants que vous avez identifiés et démontés précédemment.

Ne remontez pas les volumes à 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 Appliance StorageGRID de la page, vérifiez que le mode RAID de stockage est sain.
3. Connectez-vous au nœud de stockage défaillant :
 - a. Entrez la commande suivante : `ssh admin@grid_node_IP`
 - b. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.
 - c. Entrez la commande suivante pour passer en root : `su -`
 - d. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.

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 défaillants du `/etc/fstab` fichier puis enregistrez le fichier.



Commenter un volume défaillant dans le `/etc/fstab` le fichier est insuffisant. Le volume doit être supprimé de `fstab` car le processus de récupération vérifie que toutes les lignes du `fstab` le fichier correspond aux systèmes de fichiers montés.

5. Reformatez tous les volumes de stockage défaillants et reconstruisez la base de données Cassandra si nécessaire. Entrer: `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.
- Vous serez invité à reconstruire la base de données Cassandra si nécessaire.
 - Relisez les avertissements. Si aucune d'entre elles ne s'applique, reconstruisez la base de données Cassandra. Entrez : **y**
 - Si plusieurs nœuds de stockage sont hors ligne ou si un autre nœud de stockage a été reconstruit au cours des 15 derniers jours. Entrez : **n**

Le script se terminera sans reconstruire Cassandra. Contactez le support technique.

- Pour chaque lecteur `rangedb` sur le nœud de stockage, lorsque vous êtes invité à le faire : `Reformat the rangedb drive <name> (device <major number>:<minor number>) ? [y/n] ?`, entrez l'une des réponses suivantes :
 - **y** pour reformater un lecteur qui comportait des erreurs. Cela reformate le volume de stockage et ajoute le volume de stockage reformaté au `/etc/fstab` déposer.
 - **n** si le lecteur ne contient aucune erreur et que vous ne souhaitez pas le reformater.



La sélection de **n** permet de quitter le script. Montez le lecteur (si vous pensez que les données sur le 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 à nouveau.



Certaines procédures de récupération StorageGRID utilisent Reaper pour gérer les réparations Cassandra. Les réparations se produisent automatiquement dès que les services concernés ou requis ont commencé. Vous remarquerez peut-être une sortie de script qui mentionne « reaper » ou « réparation Cassandra ». Si vous voyez 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` doit être reformaté, et Cassandra n'a pas eu besoin d'être reconstruit :


```
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 [restaurer les données d'objet à l'aide de Grid Manager](#) .

Restaurer les données de l'objet sur le volume de stockage où le lecteur système est intact

Après avoir récupéré un volume de stockage sur un nœud de stockage où le lecteur système est intact, vous pouvez restaurer les données d'objet répliquées ou codées par effacement qui ont été perdues lors de la défaillance du volume de stockage.

Quelle procédure dois-je utiliser ?

Dans la mesure du possible, restaurez les données de l'objet à l'aide de la page **Restauration de volume** dans le gestionnaire de grille.

- Si les volumes sont répertoriés dans **MAINTENANCE > Restauration de volume > Nœuds à restaurer**, restaurez les données de l'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 de volume > Nœuds à restaurer**, suivez les étapes ci-dessous pour utiliser le `repair-data` script pour restaurer les données de l'objet.

Si le nœud de stockage récupéré contient moins de volumes que le nœud qu'il remplace, vous devez utiliser le `repair-data` scénario.



Le script de réparation des données est obsolète et sera supprimé dans une prochaine version. Lorsque cela est possible, utilisez le ["Procédure de restauration de volume dans le gestionnaire de grille"](#) .

Utilisez le `repair-data` script pour restaurer les données de l'objet

Avant de commencer

- Vous avez confirmé que le nœud de stockage récupéré a un état de connexion **Connecté***  dans l'onglet ***NODES > Aperçu** dans le Gestionnaire de grille.

À propos de cette tâche

Les données d'objet peuvent être restaurées à partir d'autres nœuds de stockage ou d'un pool de stockage cloud, en supposant que les règles ILM de la grille ont été configurées de manière à ce que des 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 récupérer l'objet.
- Si la seule copie restante d'un objet se trouve dans un pool de stockage Cloud, StorageGRID doit émettre plusieurs requêtes au point de terminaison du pool de stockage Cloud pour restaurer les données de l'objet. Avant d'effectuer cette procédure, contactez le support technique pour obtenir de l'aide afin d'estimer le délai de récupération et les coûts associés.

À propos de la `repair-data` scénario

Pour restaurer les données d'un objet, exécutez la commande `repair-data` scénario. Ce script démarre le processus de restauration des données d'objet et fonctionne avec l'analyse ILM pour garantir que les règles ILM sont respectées.

Sélectionnez **Données répliquées** ou **Données codées par effacement (EC)** ci-dessous pour découvrir les différentes options pour `repair-data` script, selon que vous restaurez des données répliquées ou des données codées par 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` à partir de la ligne de commande du nœud d'administration principal.



Le script de réparation des données est obsolète et sera supprimé dans une prochaine version. Lorsque cela est possible, utilisez le "[Procédure de restauration de volume dans le gestionnaire de grille](#)".

Données répliquées

Deux commandes sont disponibles pour restaurer les données répliquées, selon que vous devez réparer l'intégralité du nœud ou uniquement certains volumes du 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 codées par effacement (EC)

Deux commandes sont disponibles pour restaurer les données codées par effacement, selon que vous devez réparer l'intégralité du nœud ou uniquement certains volumes du nœud :

```
repair-data start-ec-node-repair
```

```
repair-data start-ec-volume-repair
```

Vous pouvez suivre les réparations des données codées par effacement avec cette commande :

```
repair-data show-ec-repair-status
```



Les réparations des données codées par effacement peuvent commencer lorsque certains nœuds de stockage sont hors ligne. Cependant, si toutes les données codées par effacement ne peuvent pas être comptabilisées, la réparation ne peut pas être effectuée. La réparation sera terminée une fois que tous les nœuds seront disponibles.



Le travail de réparation EC réserve temporairement une grande quantité de stockage. Des alertes de stockage peuvent être déclenchées, mais seront résolues une fois la réparation terminée. S'il n'y a pas suffisamment 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 réussi.

Rechercher le nom d'hôte pour le nœud de stockage

1. Connectez-vous au nœud d'administration principal :

- Entrez la commande suivante : `ssh admin@primary_Admin_Node_IP`
- Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.
- Entrez la commande suivante pour passer en root : `su -`
- Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.

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 nœud de stockage pour les volumes de stockage restaurés. Pour voir une liste de tous les nœuds de la grille, saisissez ce qui suit : `cat /etc/hosts` .

Réparer les données si tous les volumes sont en panne

Si tous les volumes de stockage sont en panne, réparez l'ensemble du nœud. Suivez les instructions pour les **données répliquées**, les **données codées par effacement (EC)** ou les deux, selon que vous utilisez des données répliquées, des données codées par effacement (EC) ou les deux.

Si seuls certains volumes sont en panne, accédez à [Réparer les données si seuls certains volumes sont défaillants](#).



Tu ne peux pas courir `repair-data` opérations pour plusieurs nœuds en même temps. Pour récupérer plusieurs nœuds, contactez le support technique.

Données répliquées

Si votre grille comprend des données répliquées, utilisez le `repair-data start-replicated-node-repair` commande avec le `--nodes` option, où `--nodes` est le nom d'hôte (nom du système), pour réparer l'ensemble 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 parvient pas à localiser les données d'objet répliquées. Des alertes peuvent être déclenchées sur les nœuds de stockage dans tout le système. Vous devez déterminer la cause de la perte et si une récupération est possible. Voir "[Enquêteur sur les objets perdus](#)".

Données codées par effacement (EC)

Si votre grille contient des données codées par effacement, utilisez le `repair-data start-ec-node-repair` commande avec le `--nodes` option, où `--nodes` est le nom d'hôte (nom du système), pour réparer l'ensemble du nœud de stockage.

Cette commande répare les données codées par effacement sur un nœud de stockage nommé SG-DC-SN3 :

```
repair-data start-ec-node-repair --nodes SG-DC-SN3
```

L'opération renvoie un unique `repair ID` qui identifie ceci `repair_data` opération. Utilisez ceci `repair ID` pour suivre les progrès et les résultats de la `repair_data` opération. Aucun autre commentaire n'est renvoyé une fois le processus de récupération terminé.

Les réparations des données codées par effacement peuvent commencer lorsque certains nœuds de stockage sont hors ligne. La réparation sera terminée une fois que tous les nœuds seront disponibles.

Réparer les données si seuls certains volumes sont défaillants

Si seulement certains volumes sont défaillants, réparez les volumes concernés. Suivez les instructions pour les **données répliquées**, les **données codées par effacement (EC)** ou les deux, selon que vous utilisez des données répliquées, des données codées par effacement (EC) ou les deux.

Si tous les volumes sont en panne, accédez à [Réparer les données si tous les volumes sont en panne](#).

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 être sur le même nœud de stockage. Si vous devez restaurer des volumes pour plusieurs nœuds de stockage, contactez le support technique.

Données répliquées

Si votre grille contient des données répliquées, utilisez le `start-replicated-volume-repair` commande avec le `--nodes` option pour identifier le nœud (où `--nodes` est le nom d'hôte du nœud). Ajoutez ensuite soit le `--volumes` ou `--volume-range` option, comme illustré dans les exemples suivants.

Volume unique : Cette commande restaure les données répliquées sur 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 sur 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
```

Plusieurs volumes non séquentiels : Cette commande restaure les données répliquées sur les 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 parvient pas à localiser les données d'objet répliquées. Des alertes peuvent être déclenchées sur les nœuds de stockage dans tout 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 codées par effacement (EC)

Si votre grille contient des données codées par effacement, utilisez le `start-ec-volume-repair` commande avec le `--nodes` option pour identifier le nœud (où `--nodes` est le nom d'hôte du nœud). Ajoutez ensuite soit le `--volumes` ou `--volume-range` option, comme illustré dans les exemples suivants.

Volume unique : Cette commande restaure les données codées par effacement sur le 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 codées par 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 séquentiels : cette commande restaure les données codées par effacement sur les 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 unique `repair ID` qui identifie ceci `repair_data` opération.

Utilisez ceci `repair ID` pour suivre les progrès et les résultats de la `repair_data` opération. Aucun autre commentaire n'est renvoyé une fois le processus de récupération terminé.



Les réparations des données codées par effacement peuvent commencer lorsque certains nœuds de stockage sont hors ligne. La réparation sera terminée une fois que tous les nœuds seront disponibles.

Réparations de moniteurs

Surveillez l'état des tâches de réparation, selon que vous utilisez des **données répliquées**, des **données codées par effacement (EC)** ou les deux.

Vous pouvez également surveiller l'état des tâches de restauration de volume en cours et afficher un historique des tâches de restauration terminées dans "[Gestionnaire de grille](#)".

Données répliquées

- Pour obtenir une estimation du pourcentage d'achèvement de la réparation répliquée, ajoutez le `show-replicated-repair-status` option à la commande `repair-data`.

```
repair-data show-replicated-repair-status
```

- Pour déterminer si les réparations sont terminées :
 - a. Sélectionnez **NODES** > **Nœud de stockage en cours de réparation** > **ILM**.
 - b. Passez en revue les attributs dans la section Évaluation. Lorsque les réparations sont terminées, l'attribut **En attente - Tout** indique 0 objet.
- Pour suivre la réparation plus en détail :
 - a. Sélectionnez **SUPPORT** > **Outils** > **Topologie de grille**.
 - b. Sélectionnez **grid** > **Nœud de stockage en cours de réparation** > **LDR** > **Data Store**.
 - c. Utilisez une combinaison des attributs suivants pour déterminer, aussi bien que possible, si les réparations répliquées sont complètes.



Des incohérences de Cassandra peuvent être présentes et les réparations ayant échoué 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 supérieure à la période d'analyse actuelle (fournie par l'attribut **Période d'analyse — Estimée**), cela signifie que l'analyse ILM n'a trouvé aucun objet à haut risque devant être réparé sur aucun nœud.



Les objets à haut risque sont des objets qui risquent d'être complètement perdus. Cela n'inclut pas les objets qui ne satisfont pas à leur configuration ILM.

- **Période d'analyse — Estimée (XSCM)** : utilisez cet attribut pour estimer quand un changement de politique sera appliqué aux objets précédemment ingérés. Si l'attribut **Réparations tentées** n'augmente pas pendant une période supérieure à la période d'analyse actuelle, il est probable que des réparations répliquées sont effectuées. Notez que la période d'analyse peut changer. L'attribut **Période d'analyse — Estimée (XSCM)** s'applique à l'ensemble de la grille et correspond au maximum de toutes les périodes d'analyse des nœuds. Vous pouvez interroger l'historique de l'attribut **Période d'analyse — Estimée** pour la grille afin de déterminer une période appropriée.

Données codées par effacement (EC)

Pour surveiller la réparation des données codées par effacement et réessayer toutes les demandes qui auraient échoué :

1. Déterminer l'état des réparations des données codées par effacement :
 - Sélectionnez **SUPPORT** > **Outils** > **Métriques** pour afficher le temps estimé jusqu'à l'achèvement et le pourcentage d'achèvement de la tâche en cours. Ensuite, sélectionnez **EC Overview** dans la section Grafana. Consultez les tableaux de bord **Temps estimé d'achèvement du travail EC de la grille** et **Pourcentage d'achèvement du travail EC de la grille**.
 - Utilisez cette commande pour voir l'état d'un élément spécifique `repair-data` opération:

```
repair-data show-ec-repair-status --repair-id repair ID
```

- Utilisez cette commande pour lister toutes les réparations :

```
repair-data show-ec-repair-status
```

La sortie répertorie les informations, y compris `repair ID` , pour toutes les réparations effectuées et en cours.

2. Si la sortie indique que l'opération de réparation a échoué, utilisez le `--repair-id` possibilité de réessayer la réparation.

Cette commande réessaie une réparation de nœud ayant échoué, en utilisant l'ID de réparation 6949309319275667690 :

```
repair-data start-ec-node-repair --repair-id 6949309319275667690
```

Cette commande réessaie une réparation de volume ayant échoué, en utilisant 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 avoir récupéré les volumes de stockage, vous devez vérifier que l'état souhaité du nœud de stockage est défini sur en ligne et vous assurer que l'état sera en ligne par défaut à chaque redémarrage du serveur du nœud 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 récupéré et la récupération des données est terminée.

Étapes

1. Sélectionnez **SUPPORT > Outils > Topologie de grille**.
2. Vérifiez les valeurs de **Nœud de stockage récupéré > LDR > Stockage > État de stockage — Souhaité** et **État de stockage — Actuel**.

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 – Souhaité**, sélectionnez **En ligne**.
 - c. Cliquez sur **Appliquer les modifications**.
 - d. Cliquez sur l'onglet **Aperçu** et confirmez que les valeurs de **État de stockage — Souhaité** et **État de stockage — Actuel** sont mises à jour sur En ligne.

Récupérer après une panne du lecteur système

Avertissements pour la récupération du lecteur système du nœud de stockage

Avant de récupérer un lecteur système défaillant d'un nœud de stockage, consultez les instructions générales ["avertissements et considérations pour la récupération des nœuds de grille"](#) et les avertissements spécifiques suivants.

Les nœuds de stockage disposent d'une base de données Cassandra qui inclut des métadonnées d'objet. La base de données Cassandra peut être reconstruite dans les circonstances suivantes :

- Un nœud de stockage est remis en ligne après avoir été hors ligne pendant plus de 15 jours.
- Un volume de stockage est tombé en panne et a été récupéré.
- Le lecteur système et un ou plusieurs volumes de stockage tombent en panne et sont récupérés.

Lorsque Cassandra est reconstruit, le système utilise les informations provenant d'autres nœuds de stockage. Si trop de nœuds de stockage sont hors ligne, certaines données Cassandra peuvent ne pas être disponibles. Si Cassandra a été reconstruit récemment, les données Cassandra peuvent ne pas encore être cohérentes sur l'ensemble de la grille. Une perte de données peut se produire si Cassandra est reconstruit alors que trop de nœuds de stockage sont hors ligne ou si deux nœuds de stockage ou plus sont reconstruits à 15 jours d'intervalle.



Si plusieurs nœuds de stockage sont en panne (ou sont hors ligne), contactez le support technique. N'effectuez pas la procédure de récupération suivante. Une perte de données pourrait survenir.



S'il s'agit de la deuxième panne d'un nœud de stockage en moins de 15 jours après une panne ou une récupération d'un nœud de stockage, contactez le support technique. La reconstruction de Cassandra sur deux nœuds de stockage ou plus dans un délai de 15 jours peut entraîner une perte de données.



Si plusieurs nœuds de stockage d'un site sont défaillants, une procédure de récupération de site peut être nécessaire. Voir ["Comment le support technique récupère un site"](#).



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 sur le nœud de stockage avec des volumes de stockage défaillants avant de récupérer ce nœud de stockage défaillant. Consultez les instructions pour ["récupérer après une panne de volume de stockage lorsque le lecteur système est intact"](#).



Si les règles ILM sont configurées pour stocker une seule copie répliquée et que la copie existe sur un volume de stockage défaillant, vous ne pourrez pas récupérer l'objet.

Remplacer le nœud de stockage

Si le lecteur système est en panne, vous devez d'abord remplacer le nœud de stockage.

Vous devez sélectionner la procédure de remplacement de nœud pour votre plateforme. Les étapes pour remplacer un nœud sont les mêmes pour tous les types de nœuds de grille.



Cette procédure s'applique uniquement aux nœuds de stockage basés sur des logiciels. Vous devez suivre une procédure différente pour ["récupérer 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.

Plate-forme	Procédure
VMware	"Remplacer un nœud VMware"
Linux	"Remplacer un nœud Linux"
OpenStack	Les fichiers de disque et les scripts de machine virtuelle fournis par NetApp pour OpenStack ne sont plus pris en charge pour les opérations de récupération. Si vous devez récupérer un nœud exécuté dans un déploiement OpenStack, téléchargez les fichiers pour votre système d'exploitation Linux. Ensuite, suivez la procédure pour "remplacement d'un nœud Linux" .

Sélectionnez Démarrer la récupération pour configurer le nœud de stockage

Après avoir remplacé un nœud de stockage, vous devez sélectionner Démarrer la récupération dans le gestionnaire de grille pour configurer le nouveau nœud en remplacement du nœud défaillant.

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 de maintenance ou root"](#) .
- Vous disposez de la phrase secrète de provisionnement.
- Vous avez déployé et configuré le nœud de remplacement.
- Vous disposez de la date de début de toutes les tâches de réparation pour les données codées par effacement.
- Vous avez vérifié que le nœud de stockage n'a pas été reconstruit au cours des 15 derniers jours.

À propos de cette tâche

Si le nœud de stockage est installé en tant que conteneur sur un hôte Linux, vous devez effectuer cette étape uniquement si l'une des conditions suivantes est remplie :

- Il fallait utiliser le `--force` drapeau pour importer le nœud, ou vous avez émis `storagegrid node force-recovery node-name`
- Vous avez dû effectuer une réinstallation complète du nœud ou restaurer `/var/local`.

Étapes

1. Depuis le Gestionnaire de grille, sélectionnez **MAINTENANCE > Tâches > Récupération**.
2. Sélectionnez le nœud de grille que vous souhaitez récupérer dans la liste des 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 n'est pas prêt pour la récupération.

3. Saisissez la **phrase secrète de provisionnement**.
4. Cliquez sur **Démarrer la récupération**.

Recovery

Select the failed grid node to recover, enter your provisioning passphrase, and then click Start Recovery to begin the recovery procedure.

Pending Nodes

Search				
Name	IPv4 Address	State	Recoverable	
104-217-S1	10.96.104.217	Unknown	✓	

Passphrase

Provisioning Passphrase

Start Recovery

5. Surveillez la progression de la récupération dans le tableau des nœuds de grille de récupération.



Pendant que la procédure de récupération est en cours, vous pouvez cliquer sur **Réinitialiser** pour démarrer une nouvelle récupération. Une boîte de dialogue apparaît, indiquant que le nœud sera laissé dans un état indéterminé si vous réinitialisez la procédure.

Info

Reset Recovery

Resetting the recovery procedure leaves the deployed grid node in an indeterminate state. To retry a recovery after resetting the procedure, you must restore the node to a pre-installed state:

- For VMware nodes, delete the deployed VM and then redeploy it.
- For StorageGRID appliance nodes, run "sgareinstall" on the node.
- For Linux nodes, run "storagegrid node force-recovery *node-name*" on the Linux host.

Do you want to reset recovery?

Cancel

OK

Si vous souhaitez réessayer la récupération après avoir réinitialisé la procédure, vous devez restaurer le nœud à un état préinstallé, comme suit :

- **VMware** : supprimez le nœud de grille virtuelle déployé. Ensuite, lorsque vous êtes prêt à redémarrer la récupération, 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 des étapes manuelles », accédez à ["Remonter et reformater les volumes de stockage \(étapes manuelles\)"](#) .

Recovery

Select the failed grid node to recover, enter your provisioning passphrase, and then click Start Recovery to begin the recovery procedure.

Recovering Grid Node

Name	Start Time	Progress	Stage
dc2-s3	2016-09-12 16:12:40 PDT		Waiting For Manual Steps

Reset

Remonter et reformater les volumes de stockage (étapes manuelles)

Vous devez exécuter manuellement deux scripts pour remonter les volumes de stockage préservés et reformater les volumes de stockage défaillants. Le premier script remonte les volumes correctement formatés en tant que volumes de stockage StorageGRID . Le deuxième script reformate tous les volumes non montés, reconstruit Cassandra, si nécessaire, et démarre les services.

Avant de commencer

- Vous avez déjà remplacé le matériel de tous les volumes de stockage défaillants dont vous savez qu'ils doivent être remplacés.

Exécution du `sn-remount-volumes` Le script peut vous aider à identifier des volumes de stockage supplémentaires défaillants.

- Vous avez vérifié qu'une mise hors service du nœud de stockage n'est pas en cours ou vous avez suspendu la procédure de mise hors service du nœud. (Dans le gestionnaire de grille, sélectionnez **MAINTENANCE > Tâches > Désactivation.**)
- Vous avez vérifié qu'une extension n'est pas en cours. (Dans le gestionnaire de grille, sélectionnez **MAINTENANCE > Tâches > Extension.**)
- Tu as [examiné les avertissements pour la récupération du lecteur système du nœud de stockage](#) .



Contactez le support technique si plusieurs nœuds de stockage sont hors ligne ou si un nœud de stockage de cette grille a été reconstruit au cours des 15 derniers jours. Ne courez pas le `sn-recovery-postinstall.sh` scénario. La reconstruction de Cassandra sur deux ou plusieurs nœuds de stockage à 15 jours d'intervalle peut entraîner une perte de données.

À propos de cette tâche

Pour réaliser cette procédure, vous effectuez ces tâches de haut niveau :

- Connectez-vous au nœud de stockage récupéré.
- Exécutez le `sn-remount-volumes` script pour remonter des 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 du 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, remonte le volume de stockage. Toutes les données existantes sur le volume restent intactes.
- Vérifiez la sortie du script et résolvez les problèmes.
- Exécutez le `sn-recovery-postinstall.sh` scénario. Lorsque ce script s'exécute, il effectue les opérations suivantes.



Ne redémarrez pas un nœud de stockage pendant la récupération avant l'exécution `sn-recovery-postinstall.sh` pour reformater les volumes de stockage défectueux et restaurer les métadonnées des objets. Redémarrer le nœud de stockage avant `sn-recovery-postinstall.sh` complète provoque des erreurs pour les services qui tentent de démarrer et provoque la sortie des nœuds de l'appliance StorageGRID du mode de maintenance. Voir l'étape pour [script de post-installation](#).

- Reformate tous les volumes de stockage que le `sn-remount-volumes` les scripts n'ont pas pu être montés ou ont été trouvés comme étant mal formatés.



Si 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.

- Reconstitue 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 :

- Entrez la commande suivante : `ssh admin@grid_node_IP`
- Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.
- Entrez la commande suivante pour passer en root : `su -`
- Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.

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 sont tombés en panne, vous pouvez ignorer cette étape et exécuter le deuxième script pour reformater tous les volumes de stockage non montés.

- Exécutez le script : `sn-remount-volumes`

Ce script peut prendre des heures à s'exécuter sur des volumes de stockage contenant des données.

- Pendant que le script s'exécute, examinez la sortie et répondez à toutes les invites.



Selon vos besoins, vous pouvez utiliser le `tail -f` commande pour surveiller 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 will attempt to restore data redundancy by making
additional replicated copies or EC fragments, according to the rules
in
the active ILM policies.

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 will attempt to restore data redundancy by making
additional replicated copies or EC fragments, according to the rules
in
the active ILM policies.

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 présentaient des erreurs.

- `/dev/sdb`` a réussi le contrôle de cohérence du système de fichiers XFS et avait une structure de volume valide, il a donc été remonté avec succès. Les données sur les appareils remontés par le script sont conservées.
- `/dev/sdc`` échec de la vérification de cohérence du système de fichiers XFS car le volume de stockage était nouveau ou corrompu.
- `/dev/sdd`` n'a pas pu être monté car le disque n'a pas été initialisé ou le superbloc du disque était corrompu. Lorsque le script ne peut pas monter un volume de stockage, il vous demande si vous souhaitez exécuter la vérification de cohérence du système de fichiers.
 - Si le volume de stockage est connecté 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 connecté 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 du nœud LDR dans le fichier `volID` ne correspondait pas à l'ID de ce nœud de stockage (le ``configured LDR noid` affiché en haut). Ce message indique que ce volume appartient à un autre nœud de stockage.

3. Vérifiez la sortie du script et résolvez les problèmes.



Si un volume de stockage a échoué à la vérification de cohérence du système de fichiers XFS ou n'a pas pu être monté, examinez attentivement les messages d'erreur dans la sortie. Vous devez comprendre les implications de l'exécution de la `sn-recovery-postinstall.sh` script sur ces volumes.

- Vérifiez que les résultats incluent une entrée pour tous les volumes attendus. Si des volumes ne sont pas répertoriés, réexécutez le script.
- Consultez les messages de tous les périphériques montés. Assurez-vous qu'il n'y a aucune erreur indiquant qu'un volume de stockage n'appartient pas à ce nœud de stockage.

Dans l'exemple, la sortie pour `/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 pourrait entraîner une perte de données.

- Si des périphériques de stockage n'ont pas pu être montés, notez le nom du périphérique et réparez ou remplacez-le.



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 du volume, qui est une entrée requise lorsque vous exécutez le `repair-data` script pour restaurer les données de l'objet sur le volume (la procédure suivante).

- d. Après avoir réparé ou remplacé tous les périphériques non montables, exécutez le `sn-remount-volumes` script à nouveau pour confirmer que tous les volumes de stockage qui peuvent 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 qu'il contient seront supprimés. Si vous aviez deux copies des données de l'objet, vous n'en aurez qu'une seule jusqu'à ce que vous terminiez la procédure suivante (restauration des données de l'objet).



Ne courez pas le `sn-recovery-postinstall.sh` script si vous pensez que les données restantes sur un volume de stockage défaillant ne peuvent pas être reconstruites ailleurs dans la grille (par exemple, si votre politique ILM utilise une règle qui ne fait qu'une seule copie ou si les volumes ont échoué sur plusieurs nœuds). Contactez plutôt le support technique pour déterminer comment récupérer vos données.

4. Exécutez le `sn-recovery-postinstall.sh` scénario: `sn-recovery-postinstall.sh`

Ce script reformate tous les volumes de stockage qui n'ont pas pu être montés ou qui se sont avérés mal formatés ; reconstruit la base de données Cassandra sur le nœud, si nécessaire ; et démarre les services sur le nœud de stockage.

Soyez attentif aux 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'exécutera en arrière-plan si une interruption du réseau se produit et met fin à la session SSH, mais vous pouvez afficher la progression à partir de la page de récupération.
- Si le nœud de stockage utilise le service RSM, le script peut sembler se bloquer pendant 5 minutes lorsque les services du nœud sont redémarrés. Ce délai de 5 minutes est attendu à chaque démarrage du service RSM pour la première fois.



Le service RSM est présent sur les nœuds de stockage qui incluent le service ADC.



Certaines procédures de récupération StorageGRID utilisent Reaper pour gérer les réparations Cassandra. Les réparations se produisent automatiquement dès que les services concernés ou requis ont commencé. Vous remarquerez peut-être une sortie de script qui mentionne « reaper » ou « réparation Cassandra ». Si vous voyez 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` le script s'exécute, surveillez la page de récupération dans le gestionnaire de grille.

La barre de progression et la colonne Étape de la page de récupération fournissent un état de haut niveau

de l'état de récupération. `sn-recovery-postinstall.sh` scénario.

Recovery

Select the failed grid node to recover, enter your provisioning passphrase, and then click Start Recovery to begin the recovery procedure.

Pending Nodes

Search				
Name	IPv4 Address	State	Recoverable	
No results found.				

Recovering Grid Node

Name	Start Time	Progress	Stage
DC1-S3	2016-06-02 14:03:35 PDT		Recovering Cassandra

6. Après le `sn-recovery-postinstall.sh` le script a démarré les services sur le nœud, vous pouvez restaurer les données de l'objet sur n'importe quel volume de stockage formaté par le script.

Le script vous demande si vous souhaitez utiliser le processus de restauration du volume Grid Manager.

- Dans la plupart des cas, vous devriez "[restaurer les données d'objet à l'aide de Grid Manager](#)". Répondre `y` pour utiliser le gestionnaire de grille.
- Dans de rares cas, par exemple lorsque le support technique vous le demande ou lorsque vous savez que le nœud de remplacement dispose de moins de volumes disponibles pour le stockage d'objets que le nœud d'origine, vous devez "[restaurer les données de l'objet manuellement](#)" en utilisant le `repair-data` scénario. Si l'un de ces cas s'applique, répondez `n`.



Si vous répondez `n` pour utiliser le processus de restauration de volume de Grid Manager (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 tâches de restauration manuelle à l'aide de Grid Manager.

Après avoir effectué votre sélection, le script se termine et les étapes suivantes pour récupérer les données de l'objet s'affichent. Après avoir examiné ces étapes, appuyez sur n'importe quelle touche pour revenir à la ligne de commande.

Restaurer les données de l'objet sur le volume de stockage (défaillance du lecteur système)

Après avoir récupéré les volumes de stockage d'un nœud de stockage non-appliance, vous pouvez restaurer les données d'objet répliquées ou codées par effacement qui ont été perdues lors de l'échec du nœud de stockage.

Quelle procédure dois-je utiliser ?

Dans la mesure du possible, restaurez les données de l'objet à l'aide de la page **Restauration de volume** dans le gestionnaire de grille.

- Si les volumes sont répertoriés dans **MAINTENANCE > Restauration de volume > Nœuds à restaurer**, restaurez les données de l'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 de volume > Nœuds à restaurer**, suivez les étapes ci-dessous pour utiliser le `repair-data` script pour restaurer les données de l'objet.

Si le nœud de stockage récupéré contient moins de volumes que le nœud qu'il remplace, vous devez utiliser le `repair-data` scénario.



Le script de réparation des données est obsolète et sera supprimé dans une prochaine version. Lorsque cela est possible, utilisez le "[Procédure de restauration de volume dans le gestionnaire de grille](#)".

Utilisez le `repair-data` script pour restaurer les données de l'objet

Avant de commencer

- Vous avez confirmé que le nœud de stockage récupéré a un état de connexion **Connecté***  dans l'onglet ***NODES > Aperçu** dans le Gestionnaire de grille.

À propos de cette tâche

Les données d'objet peuvent être restaurées à partir d'autres nœuds de stockage ou d'un pool de stockage cloud, en supposant que les règles ILM de la grille ont été configurées de manière à ce que des 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 récupérer l'objet.
- Si la seule copie restante d'un objet se trouve dans un pool de stockage Cloud, StorageGRID doit émettre plusieurs requêtes au point de terminaison du pool de stockage Cloud pour restaurer les données de l'objet. Avant d'effectuer cette procédure, contactez le support technique pour obtenir de l'aide afin d'estimer le délai de récupération et les coûts associés.

À propos de la `repair-data` scénario

Pour restaurer les données d'un objet, exécutez la commande `repair-data` scénario. Ce script démarre le processus de restauration des données d'objet et fonctionne avec l'analyse ILM pour garantir que les règles ILM sont respectées.

Sélectionnez **Données répliquées** ou **Données codées par effacement (EC)** ci-dessous pour découvrir les différentes options pour `repair-data` script, selon que vous restaurez des données répliquées ou des données codées par 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` à partir de la ligne de commande du nœud d'administration principal.



Le script de réparation des données est obsolète et sera supprimé dans une prochaine version. Lorsque cela est possible, utilisez le "[Procédure de restauration de volume dans le gestionnaire de grille](#)".

Données répliquées

Deux commandes sont disponibles pour restaurer les données répliquées, selon que vous devez réparer l'intégralité du nœud ou uniquement certains volumes du 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 codées par effacement (EC)

Deux commandes sont disponibles pour restaurer les données codées par effacement, selon que vous devez réparer l'intégralité du nœud ou uniquement certains volumes du nœud :

```
repair-data start-ec-node-repair
```

```
repair-data start-ec-volume-repair
```

Vous pouvez suivre les réparations des données codées par effacement avec cette commande :

```
repair-data show-ec-repair-status
```



Les réparations des données codées par effacement peuvent commencer lorsque certains nœuds de stockage sont hors ligne. Cependant, si toutes les données codées par effacement ne peuvent pas être comptabilisées, la réparation ne peut pas être effectuée. La réparation sera terminée une fois que tous les nœuds seront disponibles.



Le travail de réparation EC réserve temporairement une grande quantité de stockage. Des alertes de stockage peuvent être déclenchées, mais seront résolues une fois la réparation terminée. S'il n'y a pas suffisamment 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 réussi.

Rechercher le nom d'hôte pour le nœud de stockage

1. Connectez-vous au nœud d'administration principal :

- Entrez la commande suivante : `ssh admin@primary_Admin_Node_IP`
- Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.
- Entrez la commande suivante pour passer en root : `su -`
- Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.

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 nœud de stockage pour les volumes de stockage restaurés. Pour voir une liste de tous les nœuds de la grille, saisissez ce qui suit : `cat /etc/hosts`.

Réparer les données si tous les volumes sont en panne

Si tous les volumes de stockage sont en panne, réparez l'ensemble du nœud. Suivez les instructions pour les **données répliquées**, les **données codées par effacement (EC)** ou les deux, selon que vous utilisez des données répliquées, des données codées par effacement (EC) ou les deux.

Si seuls certains volumes sont en panne, accédez à [Réparer les données si seuls certains volumes sont défaillants](#).



Tu ne peux pas courir `repair-data` opérations pour plusieurs nœuds en même temps. Pour récupérer plusieurs nœuds, contactez le support technique.

Données répliquées

Si votre grille comprend des données répliquées, utilisez le `repair-data start-replicated-node-repair` commande avec le `--nodes` option, où `--nodes` est le nom d'hôte (nom du système), pour réparer l'ensemble 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 parvient pas à localiser les données d'objet répliquées. Des alertes peuvent être déclenchées sur les nœuds de stockage dans tout le système. Vous devez déterminer la cause de la perte et si une récupération est possible. Voir "[Enquêteur sur les objets perdus](#)".

Données codées par effacement (EC)

Si votre grille contient des données codées par effacement, utilisez le `repair-data start-ec-node-repair` commande avec le `--nodes` option, où `--nodes` est le nom d'hôte (nom du système), pour réparer l'ensemble du nœud de stockage.

Cette commande répare les données codées par effacement sur un nœud de stockage nommé SG-DC-SN3 :

```
repair-data start-ec-node-repair --nodes SG-DC-SN3
```

L'opération renvoie un unique `repair ID` qui identifie ceci `repair_data` opération. Utilisez ceci `repair ID` pour suivre les progrès et les résultats de la `repair_data` opération. Aucun autre commentaire n'est renvoyé une fois le processus de récupération terminé.

Les réparations des données codées par effacement peuvent commencer lorsque certains nœuds de stockage sont hors ligne. La réparation sera terminée une fois que tous les nœuds seront disponibles.

Réparer les données si seuls certains volumes sont défaillants

Si seulement certains volumes sont défaillants, réparez les volumes concernés. Suivez les instructions pour les **données répliquées**, les **données codées par effacement (EC)** ou les deux, selon que vous utilisez des données répliquées, des données codées par effacement (EC) ou les deux.

Si tous les volumes sont en panne, accédez à [Réparer les données si tous les volumes sont en panne](#) .

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 être sur le même nœud de stockage. Si vous devez restaurer des volumes pour plusieurs nœuds de stockage, contactez le support technique.

Données répliquées

Si votre grille contient des données répliquées, utilisez le `start-replicated-volume-repair` commande avec le `--nodes` option pour identifier le nœud (où `--nodes` est le nom d'hôte du nœud). Ajoutez ensuite soit le `--volumes` ou `--volume-range` option, comme illustré dans les exemples suivants.

Volume unique : Cette commande restaure les données répliquées sur 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 sur 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
```

Plusieurs volumes non séquentiels : Cette commande restaure les données répliquées sur les 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 parvient pas à localiser les données d'objet répliquées. Des alertes peuvent être déclenchées sur les nœuds de stockage dans tout 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 codées par effacement (EC)

Si votre grille contient des données codées par effacement, utilisez le `start-ec-volume-repair` commande avec le `--nodes` option pour identifier le nœud (où `--nodes` est le nom d'hôte du nœud). Ajoutez ensuite soit le `--volumes` ou `--volume-range` option, comme illustré dans les exemples suivants.

Volume unique : Cette commande restaure les données codées par effacement sur le 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 codées par 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 séquentiels : cette commande restaure les données codées par effacement sur les 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 unique `repair ID` qui identifie ceci `repair_data` opération.

Utilisez ceci `repair ID` pour suivre les progrès et les résultats de la `repair_data` opération. Aucun autre commentaire n'est renvoyé une fois le processus de récupération terminé.



Les réparations des données codées par effacement peuvent commencer lorsque certains nœuds de stockage sont hors ligne. La réparation sera terminée une fois que tous les nœuds seront disponibles.

Réparations de moniteurs

Surveillez l'état des tâches de réparation, selon que vous utilisez des **données répliquées**, des **données codées par effacement (EC)** ou les deux.

Vous pouvez également surveiller l'état des tâches de restauration de volume en cours et afficher un historique des tâches de restauration terminées dans "[Gestionnaire de grille](#)".

Données répliquées

- Pour obtenir une estimation du pourcentage d'achèvement de la réparation répliquée, ajoutez le `show-replicated-repair-status` option à la commande `repair-data`.

```
repair-data show-replicated-repair-status
```

- Pour déterminer si les réparations sont terminées :
 - a. Sélectionnez **NODES** > **Nœud de stockage en cours de réparation** > **ILM**.
 - b. Passez en revue les attributs dans la section Évaluation. Lorsque les réparations sont terminées, l'attribut **En attente - Tout** indique 0 objet.
- Pour suivre la réparation plus en détail :
 - a. Sélectionnez **SUPPORT** > **Outils** > **Topologie de grille**.
 - b. Sélectionnez **grid** > **Nœud de stockage en cours de réparation** > **LDR** > **Data Store**.
 - c. Utilisez une combinaison des attributs suivants pour déterminer, aussi bien que possible, si les réparations répliquées sont complètes.



Des incohérences de Cassandra peuvent être présentes et les réparations ayant échoué 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 supérieure à la période d'analyse actuelle (fournie par l'attribut **Période d'analyse — Estimée**), cela signifie que l'analyse ILM n'a trouvé aucun objet à haut risque devant être réparé sur aucun nœud.



Les objets à haut risque sont des objets qui risquent d'être complètement perdus. Cela n'inclut pas les objets qui ne satisfont pas à leur configuration ILM.

- **Période d'analyse — Estimée (XSCM)** : utilisez cet attribut pour estimer quand un changement de politique sera appliqué aux objets précédemment ingérés. Si l'attribut **Réparations tentées** n'augmente pas pendant une période supérieure à la période d'analyse actuelle, il est probable que des réparations répliquées sont effectuées. Notez que la période d'analyse peut changer. L'attribut **Période d'analyse — Estimée (XSCM)** s'applique à l'ensemble de la grille et correspond au maximum de toutes les périodes d'analyse des nœuds. Vous pouvez interroger l'historique de l'attribut **Période d'analyse — Estimée** pour la grille afin de déterminer une période appropriée.

Données codées par effacement (EC)

Pour surveiller la réparation des données codées par effacement et réessayer toutes les demandes qui auraient échoué :

1. Déterminer l'état des réparations des données codées par effacement :
 - Sélectionnez **SUPPORT** > **Outils** > **Métriques** pour afficher le temps estimé jusqu'à l'achèvement et le pourcentage d'achèvement de la tâche en cours. Ensuite, sélectionnez **EC Overview** dans la section Grafana. Consultez les tableaux de bord **Temps estimé d'achèvement du travail EC de la grille** et **Pourcentage d'achèvement du travail EC de la grille**.
 - Utilisez cette commande pour voir l'état d'un élément spécifique `repair-data` opération:


```
repair-data show-ec-repair-status --repair-id repair ID
```

- Utilisez cette commande pour lister toutes les réparations :

```
repair-data show-ec-repair-status
```

La sortie répertorie les informations, y compris `repair ID` , pour toutes les réparations effectuées et en cours.

2. Si la sortie indique que l'opération de réparation a échoué, utilisez le `--repair-id` possibilité de réessayer la réparation.

Cette commande réessaie une réparation de nœud ayant échoué, en utilisant l'ID de réparation 6949309319275667690 :

```
repair-data start-ec-node-repair --repair-id 6949309319275667690
```

Cette commande réessaie une réparation de volume ayant échoué, en utilisant l'ID de réparation 6949309319275667690 :

```
repair-data start-ec-volume-repair --repair-id 6949309319275667690
```

Vérifier l'état du stockage après la récupération du lecteur système du nœud de stockage

Après avoir récupéré le lecteur système d'un nœud de stockage, vous devez vérifier que l'état souhaité du nœud de stockage est défini sur en ligne et vous assurer que l'état sera en ligne par défaut à chaque redémarrage du serveur de nœud 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 récupéré et la récupération des données est terminée.

Étapes

1. Sélectionnez **SUPPORT > Outils > Topologie de grille**.
2. Vérifiez les valeurs de **Nœud de stockage récupéré > LDR > Stockage > État de stockage — Souhaité** et **État de stockage — Actuel**.

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 – Souhaité**, sélectionnez **En ligne**.
 - c. Cliquez sur **Appliquer les modifications**.
 - d. Cliquez sur l'onglet **Aperçu** et confirmez que les valeurs de **État de stockage — Souhaité** et **État de stockage — Actuel** sont mises à jour sur En ligne.

Restaurer 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 de ces procédures pour formater les volumes défaillants :
 - ["Remonter et reformater les volumes de stockage de l'appareil \(étapes manuelles\)"](#)
 - ["Remonter et reformater les volumes de stockage \(étapes manuelles\)"](#)
- Vous avez confirmé que le nœud de stockage sur lequel vous restaurez les objets a un état de connexion **Connecté***  dans l'onglet ***NODES > Aperçu** dans le Gestionnaire de grille.
- Vous avez confirmé ce qui suit :
 - Une extension de grille pour ajouter un nœud de stockage n'est pas en cours.
 - Une mise hors service du nœud de stockage n'est pas en cours ou a échoué.
 - La récupération d'un volume de stockage défaillant n'est pas en cours.
 - La récupération d'un nœud de stockage avec un lecteur système défaillant n'est pas en cours.
 - Un travail de rééquilibrage de la CE n'est pas en cours.
 - Le clonage du nœud de l'appareil n'est pas en cours.

À propos de cette tâche

Une fois les lecteurs remplacés et les étapes manuelles de formatage des volumes effectuées, Grid Manager affiche les volumes comme candidats à la restauration dans l'onglet **MAINTENANCE > Restauration de volume > Nœuds à restaurer**.

Dans la mesure du possible, restaurez les données de l'objet à l'aide de la page Restauration de volume dans le Gestionnaire de grille. Vous pouvez soit [activer le mode de restauration automatique](#) pour démarrer automatiquement la restauration du volume lorsque les volumes sont prêts à être restaurés ou [effectuer manuellement la restauration du volume](#). Suivez ces directives :

- Si les volumes sont répertoriés dans **MAINTENANCE > Restauration de volume > Nœuds à restaurer**, restaurez les données de l'objet comme décrit dans les étapes ci-dessous. Les volumes seront répertoriés si :
 - Certains volumes de stockage d'un nœud, mais pas tous, sont tombés en panne
 - Tous les volumes de stockage d'un nœud sont en panne et sont remplacés par le même nombre de volumes ou plus

La page Restauration de volume dans le gestionnaire de grille vous permet également de [surveiller le processus de restauration du volume](#) et [voir l'historique de la 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 pour restaurer les données de l'objet :
 - ["Restauration des données d'objet sur le volume de stockage \(défaillance du lecteur système\)"](#)
 - ["Restaurer les données de l'objet sur le volume de stockage où le lecteur système est intact"](#)

- "Restaurer les données d'objet sur le volume de stockage de l'appareil"



Le script de réparation des données est obsolète et sera supprimé dans une prochaine version.

Si le nœud de stockage récupéré contient moins de volumes que le nœud qu'il remplace, vous devez utiliser le `repair-data` scénario.

Vous pouvez restaurer deux types de données d'objet :

- Les objets de données répliqués sont restaurés à partir d'autres emplacements, en supposant que les règles ILM de la grille ont été configurées pour rendre les copies d'objets disponibles.
 - 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 récupérer l'objet.
 - Si la seule copie restante d'un objet se trouve dans un pool de stockage Cloud, StorageGRID doit émettre plusieurs requêtes au point de terminaison du pool de stockage Cloud pour restaurer les données de l'objet.
- Les objets de données codés par effacement (EC) sont restaurés en réassemblant les fragments stockés. Les fragments corrompus ou perdus sont recréés par l'algorithme de codage d'effacement à partir des données restantes et des fragments de parité.

Les réparations des données codées par effacement peuvent commencer lorsque certains nœuds de stockage sont hors ligne. Cependant, si toutes les données codées par effacement ne peuvent pas être prises en compte, la réparation ne peut pas être effectuée. La réparation sera terminée une fois que tous les nœuds seront disponibles.



La restauration du volume dépend de la disponibilité des ressources où les copies d'objets sont stockées. La progression de la restauration du volume n'est pas linéaire et peut prendre des jours ou des semaines.

Activer le mode de restauration automatique

Lorsque vous activez le mode de restauration automatique, la restauration du volume démarre automatiquement lorsque les volumes sont prêts à être restaurés.

Étapes

1. Dans Grid Manager, allez dans **MAINTENANCE > Restauration du volume**.
2. Sélectionnez l'onglet **Nœuds à restaurer**, puis faites glisser le bouton bascule du **Mode de restauration automatique** sur la position activée.
3. Lorsque la boîte de dialogue de confirmation s'affiche, vérifiez les détails.



- Vous ne pourrez pas démarrer manuellement les tâches de restauration de volume sur aucun nœud.
- Les restaurations de volume commenceront automatiquement uniquement lorsqu'aucune autre procédure de maintenance n'est en cours.
- Vous pouvez surveiller l'état du travail à partir de la page de suivi de la progression.
- StorageGRID réessaie automatiquement les restaurations de volume qui ne parviennent pas à démarrer.

4. Lorsque vous comprenez les résultats de l'activation du mode de restauration automatique, sélectionnez **Oui** dans la boîte de dialogue de confirmation.

Vous pouvez désactiver le mode de restauration automatique à tout moment.

Restaurer manuellement un volume ou un nœud défaillant

Suivez ces étapes pour restaurer un volume ou un nœud défaillant.

Étapes

1. Dans Grid Manager, allez dans **MAINTENANCE > Restauration du volume**.
2. Sélectionnez l'onglet **Nœuds à restaurer**, puis faites glisser le bouton bascule du **Mode de restauration automatique** sur la position désactivée.

Le numéro sur l'onglet indique le nombre de nœuds avec des volumes nécessitant une restauration.

3. Développez chaque nœud pour voir les volumes qui nécessitent une restauration et leur état.
4. Corrigez tous les problèmes empêchant la restauration de chaque volume. Les problèmes seront indiqués lorsque vous sélectionnez **En attente des étapes manuelles**, s'il s'affiche comme état du volume.
5. Sélectionnez un nœud à restaurer où tous les volumes indiquent un état Prêt à restaurer.

Vous ne pouvez restaurer les volumes que pour un nœud à la fois.

Chaque volume du nœud doit indiquer qu'il est prêt à être restauré.

6. Sélectionnez **Démarrer la restauration**.
7. Répondez à tous les avertissements qui pourraient apparaître ou sélectionnez **Démarrer quand même** pour ignorer les avertissements et démarrer la restauration.

Les nœuds sont déplacés de l'onglet **Nœuds à restaurer** vers l'onglet **Progression de la restauration** lorsque la restauration démarre.

Si une restauration de volume ne peut pas être démarrée, le nœud revient à l'onglet **Nœuds à restaurer**.

Voir 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 en cours de restauration.

Les taux de réparation des données pour les objets répliqués et codés par effacement dans tous les volumes sont des moyennes résumant toutes les restaurations en cours, y compris celles initiées à l'aide de `repair-data` scénario. Le pourcentage d'objets dans 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 où 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 volumes démarrées à partir de Grid Manager.

- Le numéro dans l'en-tête de la section Tâches de restauration indique le nombre de volumes en cours de

restauration ou en file d'attente pour restauration.

- Le tableau affiche des informations sur chaque volume d'un nœud en cours de restauration et sa progression.
 - La progression de chaque nœud affiche le pourcentage pour chaque tâche.
 - Développez la colonne Détails pour afficher l'heure de début de la restauration et l'ID de la tâche.
- Si une restauration de volume échoue :
 - La colonne Statut indique `failed (attempting retry)`, et sera réessayé automatiquement.
 - Si plusieurs tâches de restauration ont échoué, la tâche la plus récente sera automatiquement relancée en premier.
 - L'alerte **Échec de la réparation EC** est déclenchée si les nouvelles tentatives continuent d'échouer. Suivez les étapes de l'alerte pour résoudre le problème.

Afficher l'historique de restauration

L'onglet **Historique de restauration** affiche des informations sur toutes les restaurations de volumes qui ont été effectuées avec succès.



Les tailles ne s'appliquent pas aux objets répliqués et apparaissent uniquement pour les restaurations contenant des objets de données à code d'effacement (EC).

Surveiller les tâches de réparation des données

Vous pouvez surveiller l'état des travaux de réparation en utilisant le `repair-data` script depuis la ligne de commande.

Il s'agit notamment des tâches que vous avez lancées manuellement ou des tâches que StorageGRID a lancées automatiquement dans le cadre d'une procédure de mise hors service.



Si vous exécutez des tâches de restauration de volume, "[surveiller la progression et afficher un historique de ces tâches dans le gestionnaire de grille](#)" plutôt.

Surveiller l'état de `repair-data` tâches en fonction de l'utilisation de **données répliquées**, de **données codées par effacement (EC)** ou des deux.

Données répliquées

- Pour obtenir une estimation du pourcentage d'achèvement de la réparation répliquée, ajoutez le `show-replicated-repair-status` option à la commande `repair-data`.

```
repair-data show-replicated-repair-status
```

- Pour déterminer si les réparations sont terminées :
 - a. Sélectionnez **NODES** > **Nœud de stockage en cours de réparation** > **ILM**.
 - b. Passez en revue les attributs dans la section Évaluation. Lorsque les réparations sont terminées, l'attribut **En attente - Tout** indique 0 objet.
- Pour suivre la réparation plus en détail :
 - a. Sélectionnez **SUPPORT** > **Outils** > **Topologie de grille**.
 - b. Sélectionnez **grid** > **Nœud de stockage en cours de réparation** > **LDR** > **Data Store**.
 - c. Utilisez une combinaison des attributs suivants pour déterminer, aussi bien que possible, si les réparations répliquées sont complètes.



Des incohérences de Cassandra peuvent être présentes et les réparations ayant échoué 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 supérieure à la période d'analyse actuelle (fournie par l'attribut **Période d'analyse — Estimée**), cela signifie que l'analyse ILM n'a trouvé aucun objet à haut risque devant être réparé sur aucun nœud.



Les objets à haut risque sont des objets qui risquent d'être complètement perdus. Cela n'inclut pas les objets qui ne satisfont pas à leur configuration ILM.

- **Période d'analyse — Estimée (XSCM)** : utilisez cet attribut pour estimer quand un changement de politique sera appliqué aux objets précédemment ingérés. Si l'attribut **Réparations tentées** n'augmente pas pendant une période supérieure à la période d'analyse actuelle, il est probable que des réparations répliquées sont effectuées. Notez que la période d'analyse peut changer. L'attribut **Période d'analyse — Estimée (XSCM)** s'applique à l'ensemble de la grille et correspond au maximum de toutes les périodes d'analyse des nœuds. Vous pouvez interroger l'historique de l'attribut **Période d'analyse — Estimée** pour la grille afin de déterminer une période appropriée.

Données codées par effacement (EC)

Pour surveiller la réparation des données codées par effacement et réessayer toutes les demandes qui auraient échoué :

1. Déterminer l'état des réparations des données codées par effacement :
 - Sélectionnez **SUPPORT** > **Outils** > **Métriques** pour afficher le temps estimé jusqu'à l'achèvement et le pourcentage d'achèvement de la tâche en cours. Ensuite, sélectionnez **EC Overview** dans la section Grafana. Consultez les tableaux de bord **Temps estimé d'achèvement du travail EC de la grille** et **Pourcentage d'achèvement du travail EC de la grille**.
 - Utilisez cette commande pour voir l'état d'un élément spécifique `repair-data` opération:

```
repair-data show-ec-repair-status --repair-id repair ID
```

- Utilisez cette commande pour lister toutes les réparations :

```
repair-data show-ec-repair-status
```

La sortie répertorie les informations, y compris `repair ID` , pour toutes les réparations effectuées et en cours.

2. Si la sortie indique que l'opération de réparation a échoué, utilisez le `--repair-id` possibilité de réessayer la réparation.

Cette commande réessaie une réparation de nœud ayant échoué, en utilisant l'ID de réparation 6949309319275667690 :

```
repair-data start-ec-node-repair --repair-id 6949309319275667690
```

Cette commande réessaie une réparation de volume ayant échoué, en utilisant l'ID de réparation 6949309319275667690 :

```
repair-data start-ec-volume-repair --repair-id 6949309319275667690
```

Récupérer après une panne du nœud d'administration

Récupération du nœud d'administration principal ou non principal

Le processus de récupération d'un nœud d'administration dépend du fait qu'il s'agisse du nœud d'administration principal ou d'un nœud d'administration non principal.

Les étapes de haut niveau pour récupérer un nœud d'administration principal ou non principal sont les mêmes, bien que les détails des étapes diffèrent.

Suivez toujours la procédure de récupération appropriée pour le nœud d'administration que vous récupérez. Les procédures semblent identiques à un niveau élevé, mais différent dans les détails.

Choix

- ["Récupérer après une panne du nœud d'administration principal"](#)
- ["Récupérer après une panne d'un nœud d'administration non principal"](#)

Récupérer après une panne du nœud d'administration principal

Récupérer après une panne du nœud d'administration principal

Vous devez effectuer un ensemble spécifique de tâches pour récupérer après une panne du nœud d'administration principal. Le nœud d'administration principal héberge le service de nœud de gestion de configuration (CMN) pour la grille.



Vous devez réparer ou remplacer rapidement un nœud d'administration principal défaillant, sinon la grille risque de perdre sa capacité à ingérer de nouveaux objets. La période exacte dépend de votre taux d'ingestion d'objets : si vous avez besoin d'une évaluation plus précise du délai de votre grille, contactez le support technique.

Le service de nœud de gestion de configuration (CMN) sur le nœud d'administration principal est responsable de l'émission de blocs d'identifiants d'objets pour la grille. Ces identifiants sont attribués aux objets au fur et à mesure de leur ingestion. Les nouveaux objets ne peuvent pas être ingérés à moins que des identifiants ne soient disponibles. L'ingestion d'objets peut continuer pendant que le CMN n'est pas disponible, car environ un mois d'approvisionnement en identifiants est mis en cache dans la grille. Cependant, une fois les identifiants mis en cache épuisés, aucun nouvel objet ne peut être ajouté.

Suivez ces étapes de haut niveau pour récupérer un nœud d'administration principal :

1. ["Copier les journaux d'audit du nœud d'administration principal défaillant"](#)
2. ["Remplacer le nœud d'administration principal"](#)
3. ["Configurer le nœud d'administration principal de remplacement"](#)
4. ["Déterminer s'il existe une exigence de correctif pour le nœud d'administration principal récupéré"](#)
5. ["Restaurer le journal d'audit sur le nœud d'administration principal récupéré"](#)
6. ["Restaurer la base de données du nœud d'administration lors de la récupération d'un nœud d'administration principal"](#)
7. ["Restaurer les métriques Prometheus lors de la récupération d'un nœud d'administration principal"](#)

Copier les journaux d'audit du nœud d'administration principal défaillant

Si vous êtes en mesure de copier les journaux d'audit du nœud d'administration principal défaillant, vous devez les conserver pour conserver l'enregistrement de l'activité et de l'utilisation du système de la grille. Vous pouvez restaurer les journaux d'audit conservés sur le nœud d'administration principal récupéré une fois qu'il est opérationnel.

À propos de cette 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 d'audit 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 panne, vous ne pourrez peut-être 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 récupéré commence à enregistrer les événements dans le journal d'audit dans 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 récupération de l'hôte.

Étapes

1. Connectez-vous au nœud d'administration défaillant si possible. Sinon, connectez-vous au nœud d'administration principal ou à un autre nœud d'administration, si disponible.

- a. Entrez la commande suivante : `ssh admin@grid_node_IP`
- b. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.
- c. Entrez la commande suivante pour passer en root : `su -`
- d. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.

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. Accédez au répertoire d'exportation d'audit :

```
cd /var/local/log
```

4. Renommer la source `audit.log` fichier vers un nom de fichier numéroté unique. Par exemple, renommez le fichier `audit.log` en `2023-10-25.txt.1` .

```
ls -l  
mv audit.log 2023-10-25.txt.1
```

5. Redémarrez le service AMS : `service ams start`
6. 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, saisissez le mot de passe de l'administrateur.

7. Copiez tous les fichiers journaux d'audit vers l'emplacement temporaire : `scp -p * admin@grid_node_IP:/var/local/tmp/saved-audit-logs`

Lorsque vous y êtes invité, saisissez le mot de passe de l'administrateur.

8. Déconnectez-vous en tant que root : `exit`

Remplacer le nœud d'administration principal

Pour récupérer un nœud d'administration principal, vous devez d'abord remplacer le matériel physique ou virtuel.

Vous pouvez remplacer un nœud d'administration principal défaillant par un nœud d'administration principal exécuté sur la même plate-forme, ou vous pouvez remplacer un nœud d'administration principal exécuté sur VMware ou un hôte Linux par un nœud d'administration principal hébergé sur un dispositif de services.

Utilisez la procédure correspondant à la plate-forme de remplacement que vous sélectionnez pour le nœud. Une fois la procédure de remplacement du nœud terminée (qui convient à tous les types de nœuds), cette procédure vous dirigera vers l'étape suivante pour la récupération du nœud d'administration principal.

Plateforme de remplacement	Procédure
VMware	"Remplacer un nœud VMware"
Linux	"Remplacer un nœud Linux"
Appareils de service	"Remplacer un appareil de service"
OpenStack	Les fichiers de disque et les scripts de machine virtuelle fournis par NetApp pour OpenStack ne sont plus pris en charge pour les opérations de récupération. Si vous devez récupérer un nœud exécuté dans un déploiement OpenStack, téléchargez les fichiers pour votre système d'exploitation Linux. Ensuite, suivez la procédure pour "remplacement d'un nœud Linux" .

Configurer le nœud d'administration principal de remplacement

Le nœud de remplacement doit être configuré comme nœud d'administration principal pour votre système StorageGRID .

Avant de commencer

- Pour les nœuds d'administration principaux hébergés sur des machines virtuelles, la machine virtuelle a été déployée, sous tension et initialisée.
- Pour les nœuds d'administration principaux hébergés sur un dispositif de services, vous avez remplacé le dispositif et installé le logiciel. Voir le ["instructions d'installation de votre appareil"](#).
- Vous disposez de la dernière sauvegarde du fichier du package de récupération(`sgws-recovery-package-id-revision.zip`).
- Vous disposez de la phrase secrète de provisionnement.

Étapes

1. Ouvrez votre navigateur Web et accédez à `https://primary_admin_node_ip`.
2. Gérez un mot de passe d'installation temporaire selon vos besoins :
 - Si un mot de passe a déjà été défini à l'aide de l'une de ces méthodes, saisissez le mot de passe pour continuer.
 - Un utilisateur a défini le mot de passe lors de l'accès au programme d'installation précédemment
 - Pour les systèmes bare metal, le mot de passe a été automatiquement importé à partir du fichier de configuration du nœud à `/etc/storagegrid/nodes/<node_name>.conf`
 - Pour les machines virtuelles, le mot de passe SSH/console a été automatiquement importé à partir des propriétés OVF
 - Si aucun mot de passe n'a été défini, vous pouvez éventuellement définir un mot de passe pour sécuriser le programme d'installation de StorageGRID .
3. Cliquez sur **Récupérer un nœud d'administration principal défaillant**.

Welcome

Use this page to install a new StorageGRID system, or recover a failed primary Admin Node for an existing system.

Note: You must have access to a StorageGRID license, network configuration and grid topology information, and NTP settings to complete the installation. You must have the latest version of the Recovery Package file to complete a primary Admin Node recovery.



Install a StorageGRID system



Recover a failed primary Admin
Node

4. Téléchargez la sauvegarde la plus récente du package de récupération :
 - a. Cliquez sur **Parcourir**.
 - b. Recherchez le fichier de package de récupération le plus récent pour votre système StorageGRID et cliquez sur **Ouvrir**.
5. Saisissez la phrase secrète d'approvisionnement.
6. Cliquez sur **Démarrer la récupération**.

Le processus de récupération commence. Le gestionnaire de grille peut devenir indisponible pendant quelques minutes pendant que les services requis démarrent. Une fois la récupération terminée, la page de connexion s'affiche.

7. Si l'authentification unique (SSO) est activée pour votre système StorageGRID et que l'approbation de la partie de confiance pour le nœud d'administration que vous avez récupéré a été configurée pour utiliser le certificat d'interface de gestion par défaut, mettez à jour (ou supprimez et recréez) l'approbation de la partie de confiance 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 récupération du nœud d'administration.



Pour configurer une approbation de partie de confiance, voir "[Configurer l'authentification unique](#)". Pour accéder au certificat de serveur par défaut, connectez-vous à l'interpréteur de commandes du nœud d'administration. Aller à la `/var/local/mgmt-api` répertoire et sélectionnez le `server.crt` déposer.



Après avoir récupéré un nœud d'administration principal, "[déterminer si vous devez appliquer un correctif](#)".

Déterminer les exigences de correctif pour le nœud d'administration principal

Après avoir récupéré un nœud d'administration principal, déterminez si vous devez appliquer un correctif.

Avant de commencer

La récupération du nœud d'administration principal est terminée.

Étapes

1. Sign in au Grid Manager à l'aide d'un ["navigateur Web pris en charge"](#).
2. Sélectionnez **NODES**.
3. Dans la liste de gauche, sélectionnez le nœud d'administration principal.
4. Dans l'onglet Présentation, notez la version affichée dans le champ **Version du logiciel**.
5. Sélectionnez n'importe quel autre nœud de grille.
6. Dans l'onglet Présentation, notez la version affichée dans le champ **Version du logiciel**.
 - Si les versions affichées dans les champs **Version du logiciel** sont les mêmes, vous n'avez pas besoin d'appliquer un correctif.
 - Si les versions affichées dans les champs **Version du logiciel** sont différentes, vous devez ["appliquer un correctif"](#) pour mettre à jour le nœud d'administration principal récupéré vers la même version.

Restaurer le journal d'audit sur le nœud d'administration principal récupéré

Si vous avez pu conserver le journal d'audit du nœud d'administration principal défaillant, vous pouvez le copier sur le nœud d'administration principal que vous récupérez.

Avant de commencer

- Le nœud d'administration récupéré est installé et en cours d'exécution.
- Vous avez copié les journaux d'audit vers un autre emplacement après l'échec du nœud d'administration d'origine.

À propos de cette tâche

Si un nœud d'administration échoue, les journaux d'audit enregistrés sur ce nœud d'administration sont potentiellement perdus. Il peut être possible de préserver les données contre la perte en copiant les journaux d'audit du nœud d'administration défaillant, puis en restaurant ces journaux d'audit sur le nœud d'administration récupéré. En fonction de l'échec, il peut ne pas être possible 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 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 à partir du 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 récupérer un nœud d'administration dès que possible pour restaurer la fonctionnalité de journalisation.

Par défaut, les informations d'audit sont envoyées au journal d'audit sur les nœuds d'administration. Vous pouvez ignorer ces étapes si l'une des situations suivantes s'applique :



- Vous avez configuré un serveur Syslog externe et les journaux d'audit sont désormais envoyés au serveur Syslog au lieu des nœuds d'administration.
- Vous avez explicitement spécifié que les messages d'audit doivent être enregistrés uniquement sur les nœuds locaux qui les ont générés.

Voir ["Configurer les messages d'audit et les destinations des journaux"](#) pour plus de détails.

Étapes

1. Connectez-vous au nœud d'administration récupéré :

- a. Entrez la commande suivante : `ssh admin@recovery_Admin_Node_IP`
- b. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.
- c. Entrez la commande suivante pour passer en root : `su -`
- d. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.

Une fois connecté en tant que root, l'invite passe de \$ à # .

2. Vérifiez quels fichiers d'audit ont été conservés : `cd /var/local/log`

3. Copiez les fichiers journaux d'audit conservés sur le nœud d'administration récupéré : `scp admin@grid_node_IP:/var/local/tmp/saved-audit-logs/YYYY* .`

Lorsque vous y êtes invité, saisissez le mot de passe de l'administrateur.

4. Pour des raisons de sécurité, supprimez les journaux d'audit du nœud de grille défaillant après avoir vérifié qu'ils ont été copiés avec succès sur le nœud d'administration récupéré.
5. Mettre à jour les paramètres utilisateur et groupe des fichiers journaux d'audit sur le nœud d'administration récupéré : `chown ams-user: bycast *`
6. Déconnectez-vous en tant que root : `exit`

Restaurer 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 et les alertes sur un nœud d'administration principal qui a échoué, vous pouvez restaurer la base de données du nœud d'administration. Vous ne pouvez restaurer cette base de données 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` déposer.
- Vous disposez de la phrase secrète de provisionnement.

À propos de cette tâche

Si un nœud d'administration tombe en panne, les informations historiques stockées dans sa base de données de nœud d'administration sont perdues. Cette base de données comprend les informations suivantes :

- Historique des alertes
- Données d'attributs historiques, utilisées dans les graphiques de style hérité sur la page Nœuds

Lorsque vous récupérez un nœud d'administration, le processus d'installation du logiciel crée une base de données de nœud d'administration vide sur le nœud récupéré. Cependant, la nouvelle base de données ne contient que des informations sur les serveurs et les services qui font actuellement partie du système ou qui seront ajoutés ultérieurement.

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 informations historiques en copiant la base de données du nœud d'administration d'un nœud d'administration non principal (le *nœud d'administration source*) 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 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. Entrez la commande suivante : `ssh admin@grid_node_IP`
 - b. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.
 - c. Entrez la commande suivante pour passer en root : `su -`
 - d. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.
2. À partir du nœud d'administration source, arrêtez le service MI : `service mi stop`
3. À partir du nœud d'administration source, arrêtez le service d'interface de programmation d'application de gestion (mgmt-api) : `service mgmt-api stop`
4. Effectuez les étapes suivantes sur le nœud d'administration récupéré :
 - a. Connectez-vous au nœud d'administration récupéré :
 - i. Entrez la commande suivante : `ssh admin@grid_node_IP`
 - ii. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.
 - iii. Entrez la commande suivante pour passer en root : `su -`
 - iv. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.
 - b. Arrêter le service MI : `service mi stop`
 - c. Arrêtez le service mgmt-api : `service mgmt-api stop`
 - d. Ajoutez la clé privée SSH à l'agent SSH. Entrer : `ssh-add`
 - e. Saisissez le mot de passe d'accès SSH répertorié dans le `Passwords.txt` déposer.
 - f. Copiez la base de données du nœud d'administration source vers le nœud d'administration récupéré :
`/usr/local/mi/bin/mi-clone-db.sh Source_Admin_Node_IP`
 - g. Lorsque vous y êtes invité, confirmez que vous souhaitez écraser la base de données MI sur le nœud

d'administration récupéré.

La base de données et ses données historiques sont copiées sur le nœud d'administration récupéré. Une fois l'opération de copie terminée, le script démarre le nœud d'administration récupéré.

- 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. Entrer: `ssh-add -D`

5. Redémarrez les services sur le nœud d'administration source : `service servermanager start`

Restaurer les métriques Prometheus lors de la récupération du nœud d'administration principal

En option, vous pouvez conserver les mesures historiques gérées par Prometheus sur un nœud d'administration principal qui a échoué. Les métriques Prometheus ne peuvent être restaurées 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` déposer.
- Vous disposez de la phrase secrète de provisionnement.

À propos de cette tâche

Si un nœud d'administration échoue, les métriques conservées dans la base de données Prometheus sur le nœud d'administration sont perdues. Lorsque vous récupérez le nœud d'administration, le processus d'installation du logiciel crée une nouvelle base de données Prometheus. Une fois le nœud d'administration récupéré démarré, il enregistre les métriques comme si vous aviez 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 mesures historiques en copiant la base de données Prometheus d'un nœud d'administration non principal (le *nœud d'administration source*) 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. Entrez la commande suivante : `ssh admin@grid_node_IP`
 - b. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.
 - c. Entrez la commande suivante pour passer en root : `su -`
 - d. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.
2. Depuis le nœud d'administration source, arrêtez le service Prometheus : `service prometheus stop`
3. Effectuez les étapes suivantes sur le nœud d'administration récupéré :

- a. Connectez-vous au nœud d'administration récupéré :
 - i. Entrez la commande suivante : `ssh admin@grid_node_IP`
 - ii. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.
 - iii. Entrez la commande suivante pour passer en root : `su -`
 - iv. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.
- b. Arrêter le service Prometheus : `service prometheus stop`
- c. Ajoutez la clé privée SSH à l'agent SSH. Entrer : `ssh-add`
- d. Saisissez le mot de passe d'accès SSH répertorié dans le `Passwords.txt` déposer.
- e. Copiez la base de données Prometheus du nœud d'administration source vers le nœud d'administration récupéré : `/usr/local/prometheus/bin/prometheus-clone-db.sh Source_Admin_Node_IP`
- f. Lorsque vous y êtes invité, appuyez sur **Entrée** pour confirmer que vous souhaitez détruire la nouvelle base de données Prometheus sur le nœud d'administration récupéré.

La base de données Prometheus d'origine et ses données historiques sont copiées sur le nœud d'administration récupéré. Une fois l'opération de copie terminée, le script démarre le nœud d'administration récupéré. Le statut 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. Entrer : `ssh-add -D`
4. Redémarrez le service Prometheus sur le nœud d'administration source. `service prometheus start`

Récupérer après une panne d'un nœud d'administration non principal

Récupérer après une panne d'un nœud d'administration non principal

Vous devez effectuer les tâches suivantes pour récupérer après une panne d'un nœud d'administration non principal. Un nœud d'administration héberge le service de nœud de gestion de configuration (CMN) et est connu comme le 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 principaux.

Suivez ces étapes de haut niveau pour récupérer un nœud d'administration non principal :

1. ["Copier les journaux d'audit du nœud d'administration non principal défaillant"](#)
2. ["Remplacer le nœud d'administration non principal"](#)
3. ["Sélectionnez Démarrer la récupération pour configurer le nœud d'administration non principal"](#)
4. ["Restaurer le journal d'audit sur un nœud d'administration non principal récupéré"](#)
5. ["Restaurer la base de données du nœud d'administration lors de la récupération d'un nœud d'administration non principal"](#)
6. ["Restaurer les métriques Prometheus lors de la récupération d'un nœud d'administration non principal"](#)

Copier les journaux d'audit à partir d'un nœud d'administration non principal défaillant

Si vous êtes en mesure de copier les journaux d'audit du nœud d'administration défaillant, vous devez les conserver pour conserver l'enregistrement de l'activité et de l'utilisation du système de la grille. Vous pouvez restaurer les journaux d'audit conservés sur le nœud d'administration non principal récupéré une fois qu'il est opérationnel.

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 d'audit 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 panne, vous ne pourrez peut-être 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 récupéré commence à enregistrer les événements dans le journal d'audit dans 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 récupération de l'hôte.

1. Connectez-vous au nœud d'administration défaillant si possible. Sinon, connectez-vous au nœud d'administration principal ou à un autre nœud d'administration, si disponible.

- a. Entrez la commande suivante : `ssh admin@grid_node_IP`
- b. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.
- c. Entrez la commande suivante pour passer en root : `su -`
- d. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.

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. Accédez au répertoire d'exportation d'audit :

```
cd /var/local/log
```

4. Renommez le fichier `audit.log` source avec un nom de fichier numéroté unique. Par exemple, renommez le fichier `audit.log` en `2023-10-25.txt.1`.

```
ls -l
mv audit.log 2023-10-25.txt.1
```

5. Redémarrez le service AMS : `service ams start`
6. 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, saisissez le mot de passe de l'administrateur.

7. Copiez tous les fichiers journaux d'audit vers l'emplacement temporaire : `scp -p * admin@grid_node_IP:/var/local/tmp/saved-audit-logs`

Lorsque vous y êtes invité, saisissez le mot de passe de l'administrateur.

8. Déconnectez-vous en tant que root : `exit`

Remplacer le nœud d'administration non principal

Pour récupérer un nœud d'administration non principal, vous devez d'abord remplacer le matériel physique ou virtuel.

Vous pouvez remplacer un nœud d'administration non principal défaillant par un nœud d'administration non principal exécuté sur la même plate-forme, ou vous pouvez remplacer un nœud d'administration non principal exécuté sur VMware ou un hôte Linux par un nœud d'administration non principal hébergé sur un dispositif de services.

Utilisez la procédure correspondant à la plate-forme de remplacement que vous sélectionnez pour le nœud. Une fois la procédure de remplacement du nœud terminée (qui convient à tous les types de nœuds), cette procédure vous dirigera vers l'étape suivante pour la récupération du nœud d'administration non principal.

Plateforme de remplacement	Procédure
VMware	"Remplacer un nœud VMware"
Linux	"Remplacer un nœud Linux"
Appareils de service	"Remplacer un appareil de service"
OpenStack	Les fichiers de disque et les scripts de machine virtuelle fournis par NetApp pour OpenStack ne sont plus pris en charge pour les opérations de récupération. Si vous devez récupérer un nœud exécuté dans un déploiement OpenStack, téléchargez les fichiers pour votre système d'exploitation Linux. Ensuite, suivez la procédure pour "remplacement d'un nœud Linux" .

Sélectionnez Démarrer la récupération pour configurer le nœud d'administration non principal

Après avoir remplacé un nœud d'administration non principal, vous devez sélectionner Démarrer la récupération dans le gestionnaire de grille pour configurer le nouveau nœud en remplacement du nœud défaillant.

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 de maintenance ou root"](#) .
- Vous disposez de la phrase secrète de provisionnement.
- Vous avez déployé et configuré le nœud de remplacement.

Étapes

1. Depuis le Gestionnaire de grille, sélectionnez **MAINTENANCE > Tâches > Récupération**.
2. Sélectionnez le nœud de grille que vous souhaitez récupérer dans la liste des 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 n'est pas prêt pour la récupération.

3. Saisissez la **phrase secrète de provisionnement**.
4. Cliquez sur **Démarrer la récupération**.

Recovery

Select the failed grid node to recover, enter your provisioning passphrase, and then click Start Recovery to begin the recovery procedure.

Pending Nodes

Search				
Name	IPv4 Address	State	Recoverable	
104-217-S1	10.96.104.217	Unknown	✓	

Passphrase

Provisioning Passphrase

.....

Start Recovery

5. Surveillez la progression de la récupération dans le tableau des nœuds de grille de récupération.



Pendant que la procédure de récupération est en cours, vous pouvez cliquer sur **Réinitialiser** pour démarrer une nouvelle récupération. Une boîte de dialogue apparaît, indiquant que le nœud sera laissé dans un état indéterminé si vous réinitialisez la procédure.

Info

Reset Recovery

Resetting the recovery procedure leaves the deployed grid node in an indeterminate state. To retry a recovery after resetting the procedure, you must restore the node to a pre-installed state:

- For VMware nodes, delete the deployed VM and then redeploy it.
- For StorageGRID appliance nodes, run "sgareinstall" on the node.
- For Linux nodes, run "storagegrid node force-recovery *node-name*" on the Linux host.

Do you want to reset recovery?

Cancel

OK

Si vous souhaitez réessayer la récupération après avoir réinitialisé la procédure, vous devez restaurer le nœud à un état préinstallé, comme suit :

- **VMware** : supprimez le nœud de grille virtuelle déployé. Ensuite, lorsque vous êtes prêt à redémarrer la récupération, redéployez le nœud.
- **Linux** : redémarrez le nœud en exécutant cette commande sur l'hôte Linux : `storagegrid node force-recovery node-name`
- **Appareil** : Si vous souhaitez réessayer la récupération après avoir réinitialisé la procédure, vous devez restaurer le nœud de l'appareil à un état préinstallé en exécutant `sgareinstall` sur le nœud. Voir ["Préparer 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 de la partie de confiance pour le nœud d'administration que vous avez récupéré a été configurée pour utiliser le certificat d'interface de gestion par défaut, mettez à jour (ou supprimez et recréez) l'approbation de la partie de confiance 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 récupération du nœud d'administration.



Pour configurer une approbation de partie de confiance, voir ["Configurer l'authentification unique"](#) . Pour accéder au certificat de serveur par défaut, connectez-vous à l'interpréteur de commandes du nœud d'administration. Aller à la `/var/local/mgmt-api` répertoire et sélectionnez le `server.crt` déposer.

Restaurer le journal d'audit sur le nœud d'administration non principal récupéré

Si vous avez pu conserver le journal d'audit du nœud d'administration non principal défaillant, afin que les informations historiques du journal d'audit soient conservées, vous pouvez le copier sur le nœud d'administration non principal que vous récupérez.

Avant de commencer

- Le nœud d'administration récupéré est installé et en cours d'exécution.
- Vous avez copié les journaux d'audit vers un autre emplacement après l'échec du nœud d'administration d'origine.

À propos de cette tâche

Si un nœud d'administration échoue, les journaux d'audit enregistrés sur ce nœud d'administration sont potentiellement perdus. Il peut être possible de préserver les données contre la perte en copiant les journaux d'audit du nœud d'administration défaillant, puis en restaurant ces journaux d'audit sur le nœud d'administration récupéré. En fonction de l'échec, il peut ne pas être possible 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 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 à partir du 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 récupérer un nœud d'administration dès que possible pour restaurer la fonctionnalité de journalisation.

Par défaut, les informations d'audit sont envoyées au journal d'audit sur les nœuds d'administration. Vous pouvez ignorer ces étapes si l'une des situations suivantes s'applique :



- Vous avez configuré un serveur Syslog externe et les journaux d'audit sont désormais envoyés au serveur Syslog au lieu des nœuds d'administration.
- Vous avez explicitement spécifié que les messages d'audit doivent être enregistrés uniquement sur les nœuds locaux qui les ont générés.

Voir "[Configurer les messages d'audit et les destinations des journaux](#)" pour plus de détails.

Étapes

1. Connectez-vous au nœud d'administration récupéré :

a. Entrez la commande suivante :

```
ssh admin@recovery_Admin_Node_IP
```

b. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.

c. Entrez la commande suivante pour passer en root : `su -`

d. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.

Une fois connecté en tant que root, l'invite passe de `$` à `#`.

2. Vérifiez quels fichiers d'audit ont été conservés :

```
cd /var/local/log
```

3. Copiez les fichiers journaux d'audit conservés sur le nœud d'administration récupéré :

```
scp admin@grid_node_IP:/var/local/tmp/saved-audit-logs/YYYY*
```

Lorsque vous y êtes invité, saisissez le mot de passe de l'administrateur.

4. Pour des raisons de sécurité, supprimez les journaux d'audit du nœud de grille défaillant après avoir vérifié qu'ils ont été copiés avec succès sur le nœud d'administration récupéré.

5. Mettre à jour les paramètres utilisateur et groupe des fichiers journaux d'audit sur le nœud d'administration récupéré :

```
chown ams-user:bycast *
```

6. Déconnectez-vous en tant que root : `exit`

Restaurer la base de données du nœud d'administration lors de la récupération d'un nœud d'administration non principal

Si vous souhaitez conserver les informations historiques sur les attributs et les alertes sur un nœud d'administration non principal 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` déposer.
- Vous disposez de la phrase secrète de provisionnement.

À propos de cette tâche

Si un nœud d'administration tombe en panne, les informations historiques stockées dans sa base de données de nœud d'administration sont perdues. Cette base de données comprend les informations suivantes :

- Historique des alertes
- Données d'attributs historiques, utilisées dans les graphiques de style hérité sur la page Nœuds

Lorsque vous récupérez un nœud d'administration, le processus d'installation du logiciel crée une base de données de nœud d'administration vide sur le nœud récupéré. Cependant, la nouvelle base de données ne contient que des informations sur les serveurs et les services qui font actuellement partie du système ou qui seront ajoutés ultérieurement.

Si vous avez restauré un nœud d'administration non principal, vous pouvez restaurer les informations historiques en copiant la base de données du nœud d'administration du nœud d'administration principal (le *nœud d'administration source*) vers le nœud récupéré.



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 source.

Étapes

1. Connectez-vous au nœud d'administration source :
 - a. Entrez la commande suivante : `ssh admin@grid_node_IP`
 - b. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.
 - c. Entrez la commande suivante pour passer en root : `su -`
 - d. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.
2. Exécutez la commande suivante à partir du nœud d'administration source. Ensuite, entrez la phrase secrète de provisionnement si vous y êtes invité. `recover-access-points`
3. À partir du nœud d'administration source, arrêtez le service MI : `service mi stop`
4. À partir du nœud d'administration source, arrêtez le service d'interface de programmation d'application de gestion (mgmt-api) : `service mgmt-api stop`
5. Effectuez les étapes suivantes sur le nœud d'administration récupéré :
 - a. Connectez-vous au nœud d'administration récupéré :
 - i. Entrez la commande suivante : `ssh admin@grid_node_IP`
 - ii. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.
 - iii. Entrez la commande suivante pour passer en root : `su -`
 - iv. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.
 - b. Arrêter le service MI : `service mi stop`
 - c. Arrêtez le service mgmt-api : `service mgmt-api stop`
 - d. Ajoutez la clé privée SSH à l'agent SSH. Entrer: `ssh-add`

- e. Saisissez le mot de passe d'accès SSH répertorié dans le `Passwords.txt` déposer.
- f. Copiez la base de données du nœud d'administration source vers le nœud d'administration récupéré :
`/usr/local/mi/bin/mi-clone-db.sh Source_Admin_Node_IP`
- g. Lorsque vous y êtes invité, confirmez que vous souhaitez écraser la base de données MI sur le nœud d'administration récupéré.

La base de données et ses données historiques sont copiées sur le nœud d'administration récupéré. Une fois l'opération de copie terminée, le script démarre le nœud d'administration récupéré.

- 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. Entrer: `ssh-add -D`

6. Redémarrez les services sur le nœud d'administration source : `service servermanager start`

Restaurer les métriques Prometheus lors de la récupération d'un nœud d'administration non principal

En option, vous pouvez conserver les mesures historiques gérées par Prometheus sur un nœud d'administration non principal 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` déposer.
- Vous disposez de la phrase secrète de provisionnement.

À propos de cette tâche

Si un nœud d'administration échoue, les métriques conservées dans la base de données Prometheus sur le nœud d'administration sont perdues. Lorsque vous récupérez le nœud d'administration, le processus d'installation du logiciel crée une nouvelle base de données Prometheus. Une fois le nœud d'administration récupéré démarré, il enregistre les métriques comme si vous aviez effectué une nouvelle installation du système StorageGRID .

Si vous avez restauré un nœud d'administration non principal, vous pouvez restaurer les mesures historiques en copiant la base de données Prometheus du nœud d'administration principal (le *nœud d'administration source*) vers le nœud 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. Entrez la commande suivante : `ssh admin@grid_node_IP`
 - b. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.
 - c. Entrez la commande suivante pour passer en root : `su -`
 - d. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.
2. Depuis le nœud d'administration source, arrêtez le service Prometheus : `service prometheus stop`

3. Effectuez les étapes suivantes sur le nœud d'administration récupéré :

a. Connectez-vous au nœud d'administration récupéré :

i. Entrez la commande suivante : `ssh admin@grid_node_IP`

ii. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.

iii. Entrez la commande suivante pour passer en root : `su -`

iv. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.

b. Arrêter le service Prometheus : `service prometheus stop`

c. Ajoutez la clé privée SSH à l'agent SSH. Entrer : `ssh-add`

d. Saisissez le mot de passe d'accès SSH répertorié dans le `Passwords.txt` déposer.

e. Copiez la base de données Prometheus du nœud d'administration source vers le nœud d'administration récupéré : `/usr/local/prometheus/bin/prometheus-clone-db.sh Source_Admin_Node_IP`

f. Lorsque vous y êtes invité, appuyez sur **Entrée** pour confirmer que vous souhaitez détruire la nouvelle base de données Prometheus sur le nœud d'administration récupéré.

La base de données Prometheus d'origine et ses données historiques sont copiées sur le nœud d'administration récupéré. Une fois l'opération de copie terminée, le script démarre le nœud d'administration récupéré. Le statut 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. Entrer : `ssh-add -D`

4. Redémarrez le service Prometheus sur le nœud d'administration source. `service prometheus start`

Récupérer après une panne du nœud 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 vous pouvez remplacer un nœud de passerelle exécuté sur VMware ou un hôte Linux par un nœud de passerelle hébergé sur un dispositif de services.

La procédure de remplacement de nœud que vous devez suivre dépend de la plate-forme qui sera utilisée par le nœud de remplacement. Une fois la procédure de remplacement du nœud terminée (qui convient à tous les types de nœuds), cette procédure vous dirigera vers l'étape suivante pour la récupération du nœud de passerelle.

Plateforme de remplacement	Procédure
VMware	"Remplacer un nœud VMware"
Linux	"Remplacer un nœud Linux"

Plateforme de remplacement	Procédure
Appareils de service	"Remplacer un appareil de service"
OpenStack	Les fichiers de disque et les scripts de machine virtuelle fournis par NetApp pour OpenStack ne sont plus pris en charge pour les opérations de récupération. Si vous devez récupérer un nœud exécuté dans un déploiement OpenStack, téléchargez les fichiers pour votre système d'exploitation Linux. Ensuite, suivez la procédure pour "remplacement d'un nœud Linux" .

Sélectionnez Démarrer la récupération pour configurer le nœud de passerelle

Après avoir remplacé un nœud de passerelle, vous devez sélectionner Démarrer la récupération dans le gestionnaire de grille pour configurer le nouveau nœud en remplacement du nœud défaillant.

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 de maintenance ou root"](#).
- Vous disposez de la phrase secrète de provisionnement.
- Vous avez déployé et configuré le nœud de remplacement.

Étapes

1. Depuis le Gestionnaire de grille, sélectionnez **MAINTENANCE > Tâches > Récupération**.
2. Sélectionnez le nœud de grille que vous souhaitez récupérer dans la liste des 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 n'est pas prêt pour la récupération.

3. Saisissez la **phrase secrète de provisionnement**.
4. Cliquez sur **Démarrer la récupération**.

Recovery

Select the failed grid node to recover, enter your provisioning passphrase, and then click Start Recovery to begin the recovery procedure.

Pending Nodes

Search 				
	Name	IPv4 Address	State	Recoverable
☒	104-217-S1	10.96.104.217	Unknown	

Passphrase

Provisioning Passphrase

Start Recovery

5. Surveillez la progression de la récupération dans le tableau des nœuds de grille de récupération.



Pendant que la procédure de récupération est en cours, vous pouvez cliquer sur **Réinitialiser** pour démarrer une nouvelle récupération. Une boîte de dialogue apparaît, indiquant que le nœud sera laissé dans un état indéterminé si vous réinitialisez la procédure.

Info

Reset Recovery

Resetting the recovery procedure leaves the deployed grid node in an indeterminate state. To retry a recovery after resetting the procedure, you must restore the node to a pre-installed state:

- For VMware nodes, delete the deployed VM and then redeploy it.
- For StorageGRID appliance nodes, run "sgareinstall" on the node.
- For Linux nodes, run "storagegrid node force-recovery *node-name*" on the Linux host.

Do you want to reset recovery?

Cancel

OK

Si vous souhaitez réessayer la récupération après avoir réinitialisé la procédure, vous devez restaurer le nœud à un état préinstallé, comme suit :

- **VMware** : supprimez le nœud de grille virtuelle déployé. Ensuite, lorsque vous êtes prêt à redémarrer la récupération, redéployez le nœud.
- **Linux** : redémarrez le nœud en exécutant cette commande sur l'hôte Linux : `storagegrid node force-recovery node-name`
- **Appareil** : Si vous souhaitez réessayer la récupération après avoir réinitialisé la procédure, vous devez restaurer le nœud de l'appareil à un état préinstallé en exécutant `sgareinstall` sur le nœud. Voir

Récupérer après une panne du nœud d'archivage

Récupérer après une panne du nœud d'archivage

La prise en charge des nœuds d'archive a été supprimée.

Pour plus d'informations sur la récupération des nœuds d'archive, voir ["Récupération après une panne de nœud d'archivage \(site de documentation StorageGRID 11.8\)"](#) .

Remplacer le nœud Linux

Remplacer le nœud Linux

Si une panne nécessite le déploiement d'un ou 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 récupérer le nœud de grille. Cette procédure est une étape du processus de récupération des nœuds de grille pour tous les types de nœuds de grille.

« Linux » fait référence à un déploiement Red Hat® Enterprise Linux®, Ubuntu® ou Debian®. Pour une liste des versions prises en charge, consultez le ["Outil de matrice d'interopérabilité NetApp \(IMT\)"](#) .

Cette procédure n'est effectuée qu'en tant qu'étape du processus de récupération des nœuds de stockage basés sur des logiciels, des nœuds d'administration principaux ou non principaux ou des nœuds de passerelle. 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 grille dans n'importe quel ordre. Cependant, la récupération préalable d'un nœud d'administration principal, s'il est présent, empêche la récupération des autres nœuds de grille de se bloquer lorsqu'ils tentent de contacter le nœud d'administration principal pour s'inscrire à la récupération.

Déployer de nouveaux hôtes Linux

À quelques exceptions près, vous préparez les nouveaux hôtes comme vous l'avez fait lors du processus d'installation initial.

Pour déployer des hôtes Linux physiques ou virtuels nouveaux ou réinstallés, suivez la procédure de préparation des hôtes dans les instructions d'installation de StorageGRID pour votre système d'exploitation Linux :

- ["Installer Linux \(Red Hat Enterprise Linux\)"](#)
- ["Installer Linux \(Ubuntu ou Debian\)"](#)

Cette procédure comprend les étapes permettant d'accomplir les tâches suivantes :

1. Installer Linux.
2. Configurer le réseau hôte.

3. Configurer le stockage hôte.
4. Installer le moteur du conteneur.
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 « Déploiement des nœuds de grille ».

Lorsque vous effectuez ces étapes, notez les directives importantes suivantes :

- Assurez-vous d'utiliser les mêmes noms d'interface d'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 une partie ou la totalité des lecteurs ou SSD des nœuds défectueux vers les nœuds de remplacement, vous devez rétablir les mêmes mappages de stockage qui étaient 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, assurez-vous d'utiliser les mêmes paires alias/WWID dans `/etc/multipath.conf` sur l'hôte de remplacement.
- Si le nœud StorageGRID utilise le stockage attribué à partir d'un système NetApp ONTAP , vérifiez que le volume n'a pas de stratégie de hiérarchisation FabricPool activée. La désactivation de la hiérarchisation FabricPool pour les volumes utilisés avec les nœuds StorageGRID simplifie le dépannage et les opérations de stockage.



N'utilisez jamais FabricPool pour hiérarchiser les données liées à StorageGRID vers StorageGRID lui-même. La hiérarchisation des données StorageGRID vers StorageGRID augmente le dépannage et la complexité opérationnelle.

Restaurer les nœuds de la grille sur l'hôte

Pour restaurer un nœud de grille défectueux sur un nouvel hôte Linux, procédez comme suit pour 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 tous les nœuds de grille défectueux.
2. [Démarrer le service hôte StorageGRID](#) .
3. Au besoin, [récupérer tous les nœuds qui ne parviennent pas à démarrer](#) .

Si des volumes de stockage en blocs ont été conservés à partir de l'hôte précédent, vous devrez peut-être effectuer des procédures de récupération supplémentaires. Les commandes de cette section vous aident à déterminer quelles procédures supplémentaires sont requises.

Restaurer et valider les nœuds de la grille

Vous devez restaurer les fichiers de configuration de grille pour tous les nœuds de grille défectueux, puis valider les fichiers de configuration de grille et résoudre les erreurs.

À propos de cette tâche

Vous pouvez importer n'importe quel nœud de grille qui doit être présent sur l'hôte, à condition que son `/var/local` le volume n'a pas été perdu suite à la défaillance de l'hôte précédent. Par exemple, le

`/var/local` Le volume peut toujours exister si vous avez utilisé un 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 sur l'hôte.

S'il n'est pas possible d'importer les 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 survenir 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 que celui utilisé pour le nœud que vous récupérez.

Consultez les instructions d'installation pour plus d'informations sur l'emplacement du `/var/local` volume pour un nœud.

- ["Installer StorageGRID sur Red Hat Enterprise Linux"](#)
- ["Installer StorageGRID sur Ubuntu ou Debian"](#)

Étapes

1. Sur la ligne de commande de l'hôte récupéré, répertoriez tous les nœuds 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 grille sont configurés, attendez-vous à une sortie 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-arcl	/dev/mapper/sgws-arcl-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 qui ont un `/var/local` volume:

- a. Exécutez la commande suivante pour chaque nœud que vous souhaitez importer :`sudo storagegrid node import node-var-local-volume-path`

Le `storagegrid node import` La commande réussit uniquement si le nœud cible a été arrêté correctement sur l'hôte sur lequel elle a été exécutée en dernier. Si ce n'est pas le cas, vous observerez une erreur similaire à la suivante :

`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 indiquant que le nœud appartient à un autre hôte, exécutez à nouveau la commande avec le `--force` drapeau pour terminer l'importation :`sudo storagegrid --force`

```
node import node-var-local-volume-path
```



Tous les nœuds importés avec le `--force` Le drapeau nécessitera des étapes de récupération supplémentaires avant de pouvoir rejoindre la grille, comme décrit dans ["Étapes suivantes : effectuez des étapes de récupération supplémentaires, si nécessaire."](#) .

3. Pour les nœuds de grille qui n'ont pas de `/var/local` volume, recréez le fichier de configuration du nœud pour le restaurer sur l'hôte. Pour les instructions, voir :

- ["Créer des fichiers de configuration de nœud pour Red Hat Enterprise Linux"](#)
- ["Créer 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 que celui utilisé pour le nœud que vous récupérez. Pour les déploiements Linux, assurez-vous que le nom du fichier de configuration contient le nom du nœud. Vous devez utiliser les mêmes interfaces réseau, les mêmes mappages de périphériques de bloc et les mêmes adresses IP lorsque cela est possible. Cette pratique minimise la quantité de données qui doivent être copiées sur le nœud pendant la récupération, ce qui peut rendre la récupération beaucoup plus rapide (dans certains cas, en quelques minutes plutôt qu'en quelques 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 [Corriger les erreurs de périphérique de bloc manquantes](#) .

4. Exécutez la commande suivante sur l'hôte récupéré pour répertorier tous les nœuds StorageGRID .

```
sudo storagegrid node list
```

5. Validez le fichier de configuration de nœud pour chaque nœud de grille dont le nom était affiché dans la sortie de la liste des nœuds de la grille de stockage :

```
sudo storagegrid node validate node-name
```

Vous devez corriger toutes les erreurs ou avertissements avant de démarrer le service hôte StorageGRID . Les sections suivantes donnent plus de détails sur les erreurs qui pourraient avoir une signification particulière lors de la récupération.

Corriger 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 le `/etc/storagegrid/nodes/node-name.conf` déposer.

Vous pourriez voir une erreur ou un avertissement correspondant à ce modèle :

```
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 administrateur ou le réseau client. Cette erreur signifie que le `/etc/storagegrid/nodes/node-name.conf` le fichier mappe le réseau StorageGRID indiqué à 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 effectué les étapes décrites dans "[Déployer 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 fournit un 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 (ou une autre interface virtuelle) sur le périphérique de liaison sur l'hôte, soit utiliser un pont et une paire Ethernet virtuelle (veth).

Corriger les erreurs de périphérique de bloc manquantes

Le système vérifie que chaque nœud récupéré est mappé 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 `node-name` pour `PURPOSE` vers le chemin d'accès donné dans le système de fichiers Linux, mais il n'existe pas de fichier spécial de périphérique de bloc valide, ni de lien logiciel vers un fichier spécial de périphérique de bloc, à cet emplacement.

Vérifiez que vous avez terminé les étapes de "[Déployer 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 du périphérique de bloc manquant, vous pouvez allouer un nouveau périphérique de bloc de la taille et de la catégorie de stockage appropriées et modifier le fichier de configuration du nœud pour modifier la valeur de `BLOCK_DEVICE_PURPOSE` pour pointer vers le nouveau fichier spécial du 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 performances pour Red Hat Enterprise Linux"](#)
- ["Exigences 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 stockage en mode bloc :

- ["Configurer le stockage hôte pour Red Hat Enterprise Linux"](#)
- ["Configurer le stockage hôte pour Ubuntu ou Debian"](#)



Si vous devez fournir un nouveau périphérique de stockage en bloc pour l'une des variables du fichier de configuration commençant par `BLOCK_DEVICE_` étant donné que 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 ne sera pas formaté si vous utilisez un stockage partagé et avez créé un nouveau volume. Si vous n'êtes pas sûr, exécutez la commande suivante sur tous les nouveaux fichiers spéciaux du périphérique de stockage en bloc.



Exécutez la commande suivante uniquement pour les nouveaux périphériques de stockage en blocs. N'exécutez pas cette commande si vous pensez que le stockage en bloc contient toujours des données valides pour le nœud en cours de récupération, car toutes les données sur le périphérique seront perdues.

```
sudo dd if=/dev/zero of=/dev/mapper/my-block-device-name bs=1G count=1
```

Démarrer le service hôte StorageGRID

Pour démarrer vos nœuds StorageGRID et garantir 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 vous assurer que le déploiement se poursuit :

```
sudo storagegrid node status node-name
```

3. Si un nœud renvoie l'état « Non en cours d'exécution » ou « Arrêté », 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
```

Récupérer les nœuds qui ne démarrent pas normalement

Si un nœud StorageGRID ne rejoint pas la grille normalement et n'apparaît pas comme récupérable, il est peut-être corrompu. Vous pouvez forcer le nœud en mode de récupération.

Étapes

1. Confirmez que la configuration réseau du nœud est correcte.

Il est possible que le nœud n'ait pas réussi à rejoindre la grille en raison de mappages d'interface réseau incorrects ou d'une adresse IP ou d'une passerelle de réseau de grille incorrecte.

2. Si la configuration du réseau est correcte, émettez le `force-recovery` commande:

```
sudo storagegrid node force-recovery node-name
```

3. Exécutez les étapes de récupération supplémentaires pour le nœud. Voir "[Étapes suivantes : effectuez des étapes de récupération supplémentaires, si nécessaire.](#)" .

Étapes suivantes : effectuez des étapes de récupération supplémentaires, si nécessaire.

Selon les actions spécifiques que vous avez effectuées pour exécuter les nœuds StorageGRID sur l'hôte de remplacement, vous devrez peut-être effectuer des étapes de récupération supplémentaires pour chaque nœud.

La récupération du nœud est terminée si vous n'avez pas eu besoin d'effectuer de mesures correctives pendant que vous avez remplacé l'hôte Linux ou restauré le nœud de grille défaillant sur le nouvel hôte.

Mesures correctives et prochaines étapes

Lors du remplacement du nœud, vous avez peut-être dû prendre l'une de ces mesures correctives :

- Vous deviez utiliser le `--force` drapeau pour importer le nœud.
- Pour tout `<PURPOSE>` , la valeur de la `BLOCK_DEVICE_<PURPOSE>` La variable du fichier de configuration fait référence à un périphérique de bloc qui ne contient pas les mêmes données qu'avant la panne 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 effectué l'une de ces actions correctives, vous devez effectuer des étapes de récupération supplémentaires.

Type de récupération	Prochaine étape
Nœud d'administration principal	"Configurer le nœud d'administration principal de remplacement"
Nœud d'administration non principal	"Sélectionnez Démarrer la récupération pour configurer le nœud d'administration non principal"
Nœud de passerelle	"Sélectionnez Démarrer la récupération pour configurer le nœud de passerelle"
Nœud de stockage (basé sur un logiciel) : • Si vous deviez utiliser le <code>--force</code> drapeau pour importer le nœud, ou vous avez émis <code>storagegrid node force-recovery node-name</code> • Si vous deviez effectuer une réinstallation complète du nœud ou si vous deviez restaurer <code>/var/local</code>	"Sélectionnez Démarrer la récupération pour configurer le nœud de stockage"
Nœud de stockage (basé sur un logiciel) : • Si vous avez ajouté un nouveau périphérique de bloc. • Si, pour quelque raison que ce soit <code><PURPOSE></code>, la valeur de la <code>BLOCK_DEVICE_<PURPOSE></code> La variable du fichier de configuration fait référence à un périphérique de bloc qui ne contient pas les mêmes données qu'avant la panne de l'hôte.	"Récupérer après une panne de volume de stockage lorsque le lecteur système est intact"

Remplacer le nœud VMware

Lorsque vous récupérez un nœud StorageGRID défaillant hébergé sur VMware, vous supprimez le nœud défaillant et déployez un nœud de récupération.

Avant de commencer

Vous avez déterminé que la machine virtuelle ne peut pas être restaurée et doit être remplacée.

À propos de cette tâche

Vous utilisez VMware vSphere Web Client pour supprimer d'abord la machine virtuelle associée au nœud de grille défaillant. Ensuite, vous pouvez déployer une nouvelle machine virtuelle.

Cette procédure n'est qu'une étape du processus de récupération du nœud de grille. 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 et les nœuds de passerelle.

Étapes

1. Connectez-vous à VMware vSphere Web Client.

2. Accédez à la machine virtuelle du nœud de grille défaillant.
3. Notez toutes les informations nécessaires au déploiement du nœud de récupération.
 - a. Cliquez avec le bouton droit sur la machine virtuelle, sélectionnez l'onglet **Modifier les paramètres** et notez les paramètres utilisés.
 - b. Sélectionnez l'onglet **Options vApp** 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 le rattacher au nœud de grille récupéré.
5. Mettez la machine virtuelle hors tension.
6. Sélectionnez **Actions > Toutes les actions vCenter > Supprimer du disque** pour supprimer la machine virtuelle.
7. Déployez une nouvelle machine virtuelle pour être le nœud de remplacement et connectez-la à un ou plusieurs réseaux StorageGRID . Pour les instructions, voir ["Déploiement d'un nœud StorageGRID en tant que machine virtuelle"](#) .

Lorsque vous déployez le nœud, vous pouvez éventuellement remapper les ports du nœud ou augmenter les paramètres du processeur ou de la mémoire.



Après avoir déployé le nouveau nœud, vous pouvez ajouter de nouveaux disques virtuels en fonction de vos besoins de stockage, rattacher tous les disques durs virtuels conservés à partir du nœud de grille défaillant précédemment supprimé, ou les deux.

8. Terminez la procédure de récupération de nœud, en fonction du type de nœud que vous récupérez.

Type de nœud	Aller à
Nœud d'administration principal	"Configurer le nœud d'administration principal de remplacement"
Nœud d'administration non principal	"Sélectionnez Démarrer la récupération pour configurer le nœud d'administration non principal"
Nœud de passerelle	"Sélectionnez Démarrer la récupération pour configurer le nœud de passerelle"
Nœud de stockage	"Sélectionnez Démarrer la récupération pour configurer le nœud de stockage"

Remplacer le nœud défaillant par un dispositif de services

Remplacer le nœud défaillant par un dispositif de services

Vous pouvez utiliser un dispositif de services pour récupérer un nœud de passerelle défaillant, un nœud d'administration non principal défaillant ou un nœud d'administration principal défaillant hébergé sur VMware, un hôte Linux ou un dispositif de services. Cette procédure est une étape de la procédure de récupération du nœud de grille.

Avant de commencer

- Vous avez déterminé que l'une des situations suivantes est vraie :
 - La machine virtuelle hébergeant le nœud ne peut pas être restaurée.
 - L'hôte Linux physique ou virtuel du nœud de grille est tombé en panne et doit être remplacé.
 - L'appareil de services hébergeant le nœud de grille doit être remplacé.
- Vous avez confirmé que la version du programme d'installation de l'appliance StorageGRID sur l'appliance de services correspond à la version du logiciel de votre système StorageGRID . Voir ["Vérifier et mettre à niveau la version du programme d'installation de l'appliance StorageGRID"](#) .



Ne déployez pas à la fois un dispositif de services SG110 et SG1100 ou un dispositif de services SG100 et SG1000 sur le même site. Des performances imprévisibles pourraient en résulter.

À propos de cette tâche

Vous pouvez utiliser un dispositif de services pour récupérer un nœud de réseau défaillant dans les cas suivants :

- Le nœud défaillant était hébergé sur VMware ou Linux (["changement de plateforme"](#))
- Le nœud défaillant était hébergé sur un dispositif de services (["remplacement de la plateforme"](#))

Installer l'appareil de services (changement de plateforme uniquement)

Lorsque vous récupérez un nœud de grille défaillant hébergé sur VMware ou un hôte Linux et que vous utilisez un dispositif de services pour le nœud de remplacement, vous devez d'abord installer le nouveau matériel du dispositif en utilisant le même nom de nœud (nom du système) que le nœud défaillant.

Avant de commencer

Vous disposez des informations suivantes sur le nœud défaillant :

- **Nom du nœud** : vous devez installer le dispositif de services en utilisant le même nom de nœud que le nœud défaillant. Le nom du nœud est le nom d'hôte (nom du système).
- **Adresses IP** : vous pouvez attribuer au dispositif de services les mêmes adresses IP que le nœud défaillant, ce qui est l'option préférée, ou vous pouvez sélectionner une nouvelle adresse IP inutilisée sur chaque réseau.

À propos de cette tâche

Exécutez cette procédure uniquement si vous récupérez un nœud défaillant hébergé sur VMware ou Linux et que vous le remplacez par un nœud hébergé sur un dispositif de services.

Étapes

1. Suivez les instructions pour installer un nouveau dispositif de services. Voir ["Démarrage rapide pour l'installation du matériel"](#) .
2. Lorsque vous êtes invité à saisir un nom de nœud, utilisez le nom de nœud du nœud défaillant.

Préparer l'appareil pour la réinstallation (remplacement de la plate-forme uniquement)

Lors de la récupération d'un nœud de grille hébergé sur un dispositif de services, vous devez d'abord préparer le dispositif pour la réinstallation du logiciel StorageGRID .

Effectuez cette procédure uniquement si vous remplacez un nœud défaillant hébergé sur un dispositif de services. Ne suivez pas ces étapes si le nœud défaillant était initialement hébergé sur VMware ou sur un hôte Linux.

Étapes

1. Connectez-vous au nœud de grille défaillant :

- a. Entrez la commande suivante : `ssh admin@grid_node_IP`
- b. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.
- c. Entrez la commande suivante pour passer en root : `su -`
- d. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.

Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#` .

2. Préparez l'appareil pour l'installation du logiciel StorageGRID . Entrer: `sgareinstall`

3. Lorsque vous êtes invité à continuer, entrez : `y`

L'appareil redémarre et votre session SSH se termine. Il faut généralement environ 5 minutes pour que le programme d'installation de l'appliance StorageGRID soit disponible, bien que dans certains cas, vous devrez peut-être attendre jusqu'à 30 minutes.

L'appareil de services est réinitialisé et les données sur le nœud de grille ne sont plus accessibles. Les adresses IP configurées lors du processus d'installation d'origine doivent rester intactes ; cependant, il est recommandé de confirmer cela une fois la procédure terminée.

Après avoir exécuté le `sgareinstall` commande, tous les comptes, mots de passe et clés SSH provisionnés par StorageGRID sont supprimés et de nouvelles clés d'hôte sont générées.

Démarrer l'installation du logiciel sur l'appareil de services

Pour installer un nœud de passerelle ou un nœud d'administration sur un dispositif de services, utilisez le programme d'installation du dispositif StorageGRID , inclus sur le dispositif.

Avant de commencer

- L'appareil est installé dans un rack, connecté à vos réseaux et sous tension.
- Les liens réseau et les adresses IP sont configurés 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 principal, vous connaissez l'adresse IP du nœud d'administration principal pour la grille StorageGRID .
- Tous les sous-réseaux du réseau de grille répertoriés sur la page de configuration IP du programme d'installation de l'appliance StorageGRID sont définis dans la liste des sous-réseaux du réseau de grille sur le nœud d'administration principal.

Voir "[Démarrage rapide pour l'installation du matériel](#)".

- Vous utilisez un "[navigateur Web pris en charge](#)".
- Vous disposez d'une des adresses IP attribuées à l'appareil. Vous pouvez utiliser l'adresse IP pour le réseau d'administration, le réseau de grille ou le 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 lors de 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.

À propos de cette tâche

Pour installer le logiciel StorageGRID sur un dispositif de services :

- Pour un nœud d'administration principal, vous spécifiez le nom du nœud, puis téléchargez les packages logiciels appropriés (si nécessaire).
- Pour un nœud d'administration non principal ou un nœud de passerelle, vous spécifiez ou confirmez l'adresse IP du nœud d'administration principal et le nom du nœud.
- Vous démarrez l'installation et attendez que les volumes soient configurés et que le logiciel soit installé.
- À mi-chemin du processus, l'installation s'arrête. Pour reprendre l'installation, vous devez vous connecter au gestionnaire de grille et configurer le nœud en attente en remplacement du nœud défaillant.
- Une fois le nœud configuré, le processus d'installation de l'appliance se termine et l'appliance est redémarrée.

Étapes

1. Ouvrez un navigateur et entrez l'une des adresses IP du dispositif de services.

`https://Controller_IP:8443`

La page d'accueil du programme d'installation de l'appliance StorageGRID s'affiche.

NetApp® StorageGRID® Appliance Installer Help ▾

Home Configure Networking ▾ Configure Hardware ▾ Monitor Installation Advanced ▾

Home

This Node

Node type Gateway ▾

Node name NetApp-SGA

Cancel Save

Primary Admin Node connection

Enable Admin Node discovery ☒ Uncheck to manually enter the Primary Admin Node IP

Connection state Admin Node discovery is in progress

Cancel Save

Installation

Current state Unable to start installation. The Admin Node connection is not ready.

Start installation

2. Pour installer un nœud d'administration principal :

- Dans la section Ce nœud, pour **Type de nœud**, sélectionnez **Administrateur principal**.
- Dans le champ **Nom du nœud**, entrez le même nom que celui utilisé pour le nœud que vous récupérez, puis cliquez sur **Enregistrer**.
- Dans la section Installation, vérifiez la version du logiciel répertoriée sous État actuel

Si la version du logiciel prêt à être installé est correcte, passez directement à l'étape suivante. [Étape d'installation](#) .

- Si vous devez télécharger une version différente du logiciel, dans le menu **Avancé**, sélectionnez ***Télécharger le logiciel StorageGRID ***.

La page Télécharger le logiciel StorageGRID s'affiche.

Upload StorageGRID Software

If this node is the primary Admin Node of a new deployment, you must use this page to upload the StorageGRID software installation package, unless the version of the software you want to install has already been uploaded. If you are adding this node to an existing deployment, you can avoid network traffic by uploading the installation package that matches the software version running on the existing grid. If you do not upload the correct package, the node obtains the software from the grid's primary Admin Node during installation.

Current StorageGRID Installation Software

Version	None
Package Name	None

Upload StorageGRID Installation Software

Software Package	Browse
Checksum File	Browse

a. Cliquez sur **Parcourir** pour télécharger le **Pack logiciel** et le **Fichier de somme de contrôle** pour le logiciel StorageGRID .

Les fichiers sont automatiquement téléchargés après les avoir sélectionnés.

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 principal :

a. Dans la section Ce nœud, pour **Type de nœud**, sélectionnez **Passerelle** ou **Administrateur non principal**, selon le type de nœud que vous restaurez.

b. Dans le champ **Nom du nœud**, entrez le même nom que celui utilisé pour le nœud que vous récupérez, puis cliquez sur **Enregistrer**.

c. Dans la section Connexion du nœud d'administration principal, déterminez si vous devez spécifier l'adresse IP du nœud d'administration principal.

Le programme d'installation de l'appliance StorageGRID peut découvrir cette adresse IP automatiquement, en supposant que le nœud d'administration principal, ou au moins un autre nœud de grille avec ADMIN_IP configuré, est présent sur le même sous-réseau.

d. Si cette adresse IP n'est pas affichée ou si vous devez la modifier, spécifiez l'adresse :

Option	Description
Saisie IP manuelle	a. Décochez la case Activer la découverte du nœud 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
Découverte automatique de tous les nœuds d'administration principaux connectés	a. Cochez la case Activer la découverte du nœud d'administration. b. Dans la liste des adresses IP découvertes, sélectionnez le nœud d'administration principal de la grille sur laquelle ce dispositif de services sera déployé. c. Cliquez sur Enregistrer. d. Attendez que l'état de connexion de la nouvelle adresse IP devienne « prêt ».

4. Dans la section Installation, confirmez que l'état actuel est Prêt à démarrer l'installation du nom du nœud et que le bouton **Démarrer l'installation** est activé.

Si le bouton **Démarrer l'installation** n'est pas activé, vous devrez peut-être modifier la configuration réseau ou les paramètres du port. Pour les instructions, consultez les instructions d'entretien de votre appareil.

5. Depuis la page d'accueil du programme d'installation de l'appliance StorageGRID , cliquez sur **Démarrer l'installation**.

L'état actuel passe à « L'installation est en cours » et la page Installation du moniteur s'affiche.



Si vous devez accéder manuellement à la page d'installation du moniteur, cliquez sur **Installation du moniteur** dans la barre de menus.

Surveillance de l'installation des appareils de services

Le programme d'installation de l'appliance StorageGRID fournit un état jusqu'à ce que l'installation soit terminée. Une fois l'installation du logiciel terminée, l'appareil est redémarré.

Étapes

1. Pour suivre la progression de l'installation, cliquez sur **Surveiller l'installation** dans la barre de menus.

La page d'installation du moniteur affiche la progression de l'installation.

Monitor Installation

1. Configure storage		Complete
2. Install OS		Running
Step	Progress	Status
Obtain installer binaries		Complete
Configure installer		Complete
Install OS		Installer VM running
3. Install StorageGRID		Pending
4. Finalize installation		Pending

La barre d'état bleue indique quelle tâche est actuellement en cours. Les barres d'état vertes indiquent les tâches qui ont été effectuées avec succès.



Le programme d'installation garantit que les tâches effectuées lors d'une installation précédente ne sont pas réexécutées. Si vous réexécutez une installation, toutes les tâches qui n'ont pas besoin d'être réexécutées sont affichées avec une barre d'état verte et un statut « Ignoré ».

2. Passez en revue la progression des deux premières étapes de l'installation.

◦ 1. Configurer le stockage

Au cours de cette étape, le programme d'installation efface toute configuration existante des lecteurs et configure les paramètres de l'hôte.

◦ 2. Installer le système d'exploitation

Au cours de cette étape, le programme d'installation copie l'image du système d'exploitation de base 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 d'appliance non principaux, l'étape **Install 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.

Monitor Installation

1. Configure storage	Complete
2. Install OS	Complete
3. Install StorageGRID	Running
4. Finalize installation	Pending

Connected (unencrypted) to: QEMU

```

/platform.type: Device or resource busy
[2017-07-31T22:09:12.362566] INFO -- [INSG] NOTICE: seeding /var/local with c
ontainer data
[2017-07-31T22:09:12.366205] INFO -- [INSG] Fixing permissions
[2017-07-31T22:09:12.369633] INFO -- [INSG] Enabling syslog
[2017-07-31T22:09:12.511533] INFO -- [INSG] Stopping system logging: syslog-n
g.
[2017-07-31T22:09:12.570096] INFO -- [INSG] Starting system logging: syslog-n
g.
[2017-07-31T22:09:12.576360] INFO -- [INSG] Beginning negotiation for downloa
d of node configuration
[2017-07-31T22:09:12.581363] INFO -- [INSG]
[2017-07-31T22:09:12.585066] INFO -- [INSG]
[2017-07-31T22:09:12.588314] INFO -- [INSG]
[2017-07-31T22:09:12.591851] INFO -- [INSG]
[2017-07-31T22:09:12.594886] INFO -- [INSG]
[2017-07-31T22:09:12.598360] INFO -- [INSG]
[2017-07-31T22:09:12.601324] INFO -- [INSG]
[2017-07-31T22:09:12.604759] INFO -- [INSG]
[2017-07-31T22:09:12.607800] INFO -- [INSG]
[2017-07-31T22:09:12.610985] INFO -- [INSG]
[2017-07-31T22:09:12.614597] INFO -- [INSG]
[2017-07-31T22:09:12.618282] INFO -- [INSG] Please approve this node on the A
dmin Node GMI to proceed...

```

- Pour les nœuds d'administration principaux de l'appliance, une cinquième phase (charger le programme d'installation de StorageGRID) apparaît. Si la cinquième phase est en cours depuis plus de 10 minutes, actualisez la page manuellement.

NetApp® StorageGRID® Appliance Installer
Help

Home
Configure Networking
Configure Hardware
Monitor Installation
Advanced

Monitor Installation

1. Configure storage	Complete
2. Install OS	Complete
3. Install StorageGRID	Complete
4. Finalize installation	Complete
5. Load StorageGRID Installer	Running

Step	Progress	Status
Starting StorageGRID Installer		Do not refresh. You will be redirected when the installer is ready

4. Passez à l'étape suivante du processus de récupération pour le type de nœud de grille d'appareil que vous récupérez.

Type de récupération	Référence
Nœud de passerelle	"Sélectionnez Démarrer la récupération pour configurer le nœud de passerelle"
Nœud d'administration non principal	"Sélectionnez Démarrer la récupération pour configurer le nœud d'administration non principal"
Nœud d'administration principal	"Configurer le nœud d'administration principal de remplacement"

Comment le support technique récupère un site

Si un site StorageGRID entier tombe en panne ou si plusieurs nœuds de stockage tombent en panne, vous devez contacter le support technique. Le support technique évaluera votre situation, élaborera un plan de récupération, puis récupérera les nœuds ou le site défaillants d'une manière qui répond à vos objectifs commerciaux, optimise le temps de récupération et évite toute perte de données inutile.



La récupération du site ne peut être effectuée que par le support technique.

Les systèmes StorageGRID sont résilients à une grande variété de pannes et vous pouvez effectuer vous-même avec succès de nombreuses procédures de récupération et de maintenance. Cependant, il est difficile de créer une procédure de récupération de site simple et généralisée, car les étapes détaillées dépendent de facteurs spécifiques à votre situation. Par exemple:

- Vos objectifs commerciaux** : Après la perte complète d'un site StorageGRID , vous devez évaluer la meilleure façon d'atteindre vos objectifs commerciaux. Par exemple, souhaitez-vous reconstruire le site perdu sur place ? Voulez-vous remplacer le site StorageGRID perdu dans 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 panne** : 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, une perte de données inutile peut se produire.
- **Stratégies ILM actives** : Le nombre, le type et l'emplacement des copies d'objets dans votre grille sont contrôlés par vos stratégies ILM actives. Les spécificités de vos politiques ILM peuvent affecter la quantité de données récupérables, ainsi que les techniques spécifiques requises pour la récupération.



Si un site contient la seule copie d'un objet et que le site est perdu, l'objet est perdu.

- **Cohérence du bucket (ou du conteneur)** : la cohérence appliquée à un bucket (ou à un conteneur) affecte la capacité de StorageGRID à répliquer entièrement les métadonnées de l'objet sur tous les nœuds et sites avant d'indiquer à un client que l'ingestion de l'objet a réussi. Si la valeur de cohérence permet une cohérence éventuelle, certaines métadonnées d'objet peuvent avoir été perdues lors de la défaillance du site. Cela peut affecter la quantité de données récupérables et potentiellement les détails de la procédure de récupération.
- **Historique des modifications récentes** : Les détails de votre procédure de récupération peuvent être affectés par le fait que des procédures de maintenance étaient en cours au moment de la panne ou que des modifications récentes ont été apportées à vos politiques ILM. Le support technique doit évaluer l'historique récent de votre réseau ainsi que sa situation actuelle avant de commencer une récupération de site.



La récupération du site ne peut être effectuée que par le support technique.

Voici un aperçu général du processus utilisé par le support technique pour récupérer un site défaillant :

1. Support technique :
 - a. Fait une évaluation détaillée de l'échec.
 - b. Travaille avec vous pour revoir vos objectifs commerciaux.
 - c. Élabore un plan de rétablissement adapté à votre situation.
2. Si le nœud d'administration principal est en panne, le support technique le récupère.
3. Le support technique récupère tous les nœuds de stockage, selon ce schéma :
 - a. Remplacez le matériel du nœud de stockage ou les machines virtuelles selon les besoins.
 - b. Restaurer les métadonnées de l'objet sur le site défaillant.
 - c. Restaurer les données d'objet sur les nœuds de stockage récupérés.



Une perte de données se produira si les procédures de récupération pour un seul nœud de stockage défaillant sont utilisées.



Lorsqu'un site entier est en panne, le support technique utilise des commandes spécialisées pour restaurer avec succès les objets et les métadonnées des objets.

4. Le support technique récupère les autres nœuds défaillants.

Une fois les métadonnées et les données de l'objet récupérées, le support technique utilise des procédures standard pour récupérer les nœuds de passerelle défaillants ou les nœuds d'administration non principaux.

Informations connexes

["Démantèlement du site"](#)

Comment activer StorageGRID dans votre environnement

Aller à "[Comment activer StorageGRID](#)" pour apprendre à tester et activer des applications dans votre environnement StorageGRID .

Comment gérer StorageGRID avec BlueXP

Aller à "[Gestion de StorageGRID avec BlueXP](#)" pour apprendre à gérer vos systèmes StorageGRID à partir de BlueXP à l'aide de Grid Manager et à utiliser les services de données de BlueXP pour les sauvegardes, la hiérarchisation des données, etc.

Mentions légales

Les mentions légales donnent accès aux déclarations de droits d’auteur, aux marques déposées, aux brevets et bien plus encore.

Copyright

["https://www.netapp.com/company/legal/copyright/"](https://www.netapp.com/company/legal/copyright/)

Marques de commerce

NETAPP, le logo NETAPP et les marques répertoriées sur la page Marques 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/"](https://www.netapp.com/company/legal/trademarks/)

Brevets

Une liste actuelle des brevets détenus par NetApp est disponible 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/"](https://www.netapp.com/company/legal/privacy-policy/)

Open source

Les fichiers d’avis fournissent des informations sur les droits d’auteur et les licences tiers utilisés dans les logiciels NetApp .

https://library.netapp.com/ecm/ecm_download_file/ECMLP3330669

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 DÉLICTELLE (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.